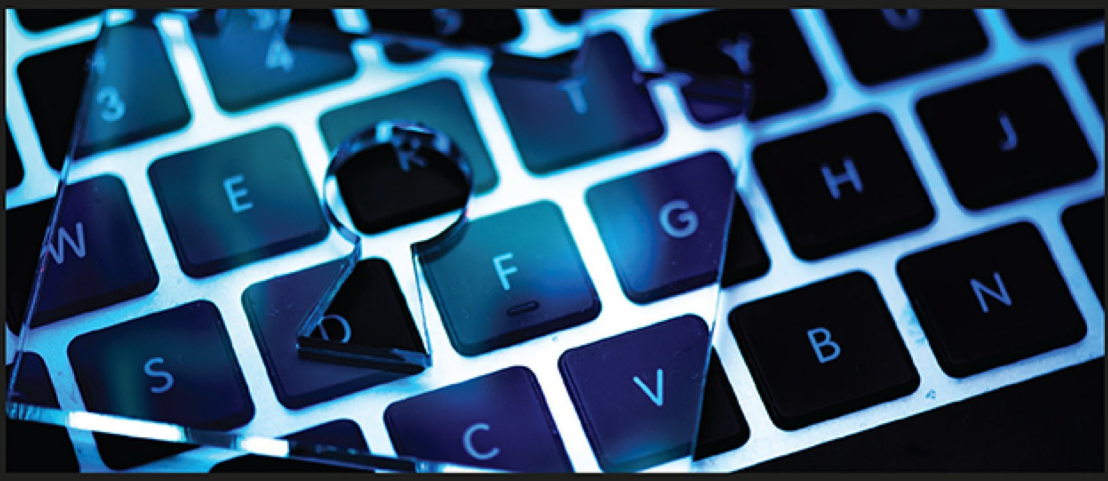
Helion

<packt>



OSINT w praktyce

Jak gromadzić i analizować dane dostępne w sieci

DALE MEREDITH

Tytuł oryginału: The OSINT Handbook: A practical guide to gathering and analyzing online information

Tłumaczenie: Karolina Stangel

ISBN: 978-83-289-2043-9

Copyright © Packt Publishing 2024. First published in the English language under the title 'The OSINT Handbook – (9781837638277)'

Polish edition copyright © 2025 by Helion S.A.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiejkolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/osintw_ebook
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *helion.pl* (księgarnia internetowa, katalog książek)

- Poleć książkę na Facebook.com
- Kup w wersji papierowej
- Oceń książkę

- Księgarnia internetowa
- Lubię to! » Nasza społeczność

Kriście, mojej małej maniaczce komputerowej.

Gdy zajmuję się skomplikowanymi zagadnieniami z dziedziny technologii i cyberbezpieczeństwa, takimi jak hakowanie i ochrona komputerów, wspaniale jest widzieć, że ten świat porwał Cię tak samo jak mnie. Jesteś nie tylko moją córką — jesteś młodszą wersją mnie. Twój entuzjazm dla wszelkich nowości technologicznych sprawia, że nasze rozmowy są wciągające i dają mi dużo radości.

Ta książka opisuje moje przygody w obszarze cyberbezpieczeństwa, ale jest również podziękowaniem dla Ciebie za zainteresowanie tą dziedziną i zapał do uczenia się nowych rzeczy. Mam nadzieję, że Twoje zamiłowanie do technologii będzie palić się jasnym płomieniem i że dalej będziesz zgłębiać nowe pomysły, tak jak to robisz teraz.

Z miłością

Tata

Spis treści

O autorze **11**

O korektorach merytorycznych **12**

Przedmowa **13**

Wprowadzenie **15**

ROZDZIAŁ 1.
Sekrety ukrywania się na widoku — OSINT i jego moc **19**

Wprowadzenie do OSINT 19
Informacje a informacje wywiadowcze 20
Aktywne i pasywne rozpoznanie OSINT 21
Znaczenie OSINT w erze cyfryzacji 21
W czym tkwi urok OSINT? 22
Jak zatem działa OSINT? 22
Framework OSINT 24
Etapy dochodzenia OSINT na konkretnych przykładach 25
Pierwsze kroki i najlepsze praktyki w dziedzinie OSINT 27
Tajniki skutecznego gromadzenia informacji 27
Krótka lista użytecznych zasobów 27
Podsumowanie 28

ROZDZIAŁ 2.
Niewidoczni i nietykalni — znaczenie anonimowości w pracy analityka OSINT **29**

Wprowadzenie do anonimowości i prywatności w OSINT 29
Czynniki prowadzące do utraty anonimowości w OSINT 30
W poszukiwaniu złotego środka — prywatność w dochodzeniach OSINT 35

Ochrona własnego śladu cyfrowego ... 35
Ograniczanie TWOJEGO cyfrowego śladu ... 35
Dlaczego ochrona danych osobowych jest obecnie ważniejsza niż kiedyś? ... 36
Przeglądarki internetowe — pierwszy front walki o dane ... 37
Jak się chronić? ... 38
Skarpetkowe pacynki — tworzenie person internetowych i zarządzanie nimi ... 42
Aktualizowanie wiedzy na temat cyberzagrożeń ... 50
Uzyskiwanie bieżących informacji na temat prywatności i bezpieczeństwa ... 50
Uczenie się na podstawie wcześniejszych naruszeń i incydentów ... 51
Podsumowanie ... 52

ROZDZIAŁ 3.
Narzędzia OSINT — metody i techniki gromadzenia i analizowania informacji ... 53

Wstęp do metod i technik OSINT ... 54
Różnorodność technik OSINT ... 54
Wybór odpowiedniej metody do zadania ... 59
Przeszukiwanie i przeglądanie ogólnodostępnych warstw internetu ... 60
Zaawansowane techniki korzystania z wyszukiwarek internetowych ... 60
Google hacking ... 61
Specjalistyczne wyszukiwarki i katalogi ... 63
Wyszukiwarki naukowe ... 64
Wyszukiwarki kodu ... 65
Wyszukiwarki patentów ... 65
Wyszukiwarki obrazów ... 65
Badanie mediów społecznościowych do celów OSINT ... 67
Pojęcia z zakresu SOCMINT — szczegółowa analiza ... 68
Na świecie istnieją dwa rodzaje danych ... 69
„Rozszerlokuj" to! ... 70
Hasztagi i znaczniki geograficzne ... 71
Nie zapomnijmy o znacznikach geograficznych ... 72
Magiczny świat danych EXIF ... 73
Rozumienie ukrytych źródeł ... 75
Przeszukiwanie i przeglądanie głębszych i mroczniejszych warstw internetu ... 76
Upewnijmy się, że rozumiemy internet ... 76

Zbieranie danych narzędziem theHarvester ... 79
Shodan ... 79
Automatyzacja zbierania i analizy danych OSINT ... 83
Podsumowanie ... 84

ROZDZIAŁ 4.
Wyprawa w nieznane — narzędzia do eksploracji ukrytych danych ... 85
Wprowadzenie do narzędzi do eksploracji ukrytych danych ... 86
Obnażanie sekretów sieci ... 86
Analiza domen i adresów IP ... 87
DNA protokołu WHOIS — definicja i cele ... 87
Zakres zastosowań — nie tylko domeny, lecz również bloki adresów IP ... 89
Cyfrowa lupa — popularne platformy zapytań WHOIS ... 90
Odnajdywanie połączeń ... 92
Ciemna strona mocy — użycie rekordów WHOIS do przeprowadzania ataków ... 93
Analiza rekordów DNS i adresów IP — wiązanie domen z infrastrukturą ... 94
Traceroute i mapowanie sieci — kartografowie cybernetycznych mórz ... 100
Rozpoznanie witryn internetowych — zgłębianie niewidocznych warstw ... 104
Pozyskiwanie danych ze stron internetowych i ich analiza ... 104
Analiza dokumentów i metadanych ... 112
Identyfikacja ukrytych informacji w dokumentach i plikach ... 112
Analiza dokumentów w poszukiwaniu cennych wskazówek ... 113
Wizualizacja danych w OSINT ... 114
Narzędzia i techniki wizualizacji danych w OSINT ... 115
Najlepsze praktyki korzystania z narzędzi do eksploracji ukrytych danych ... 116
Podsumowanie ... 117

ROZDZIAŁ 5.
Od Recon-ng po Trace Labs — wycieczka objazdowa po najlepszych narzędziach OSINT ... 118
Recon-ng — potężny framework narzędzi OSINT ... 119
Uruchamianie modułów Recon-ng i zbieranie informacji ... 119

Maltego — narzędzie do wizualizacji danych i powiązań 123
Początek pracy z Maltego 123
Rozpracowywanie infrastruktury 128
Shodan — wyszukiwarka internetu rzeczy 129
Początek pracy z narzędziem Shodan 130
Korzystanie z interfejsu API wyszukiwarki Shodan 133
Trace Labs — zaawansowany system operacyjny zaprojektowany do działań OSINT 133
Przegląd pakietu narzędzi Aircrack-ng 134
Airmon-ng 136
Airodump-ng 137
Aireplay-ng 138
Aircrack-ng 139
Airbase-ng 140
Airgraph-ng 141
Znajdowanie ukrytych sieci 141
Dodatkowe otwartoźródłowe narzędzia OSINT 143
SpiderFoot 143
Końcowe przemyślenia na temat narzędzi 144
Nadążanie za tempem zmian w dziedzinie OSINT 146
Blogi i witryny internetowe 147
Konferencje i warsztaty 147
Ocena nowych narzędzi 147
Przynależność do społeczności OSINT 148
Podsumowanie 148

ROZDZIAŁ 6.
Oczy i uszy analizy zagrożeń — jak OSINT ogranicza ryzyka cybernetyczne 149

Wprowadzenie do OSINT w analizie zagrożeń 149
Zagrożenia cybernetyczne a OSINT 150
Phishing 151
Socjotechnika 152
Złośliwe oprogramowanie i oprogramowanie wymuszające okup 154
Zaawansowane trwałe zagrożenia 159
Łączenie OSINT z wewnętrznymi systemami bezpieczeństwa 161
Platformy do analizy zagrożeń cybernetycznych i ich integracja z OSINT 163
Niektóre z dostępnych platform 164

Wykorzystanie danych OSINT w procesach analizy zagrożeń 164
Dzielenie się informacjami pochodzącymi z OSINT z innymi platformami i zespołami 166
Tworzenie strategii analizy zagrożeń opartej na OSINT 167
Jakich informacji wywiadowczych potrzebujemy? 167
Rola OSINT 168
Studium przypadku, czyli rola OSINT w prawdziwych incydentach z zakresu cyberbezpieczeństwa 170
Podsumowanie 171

ROZDZIAŁ 7.
Ochrona własnej tożsamości i organizacji przed cyberzagrożeniami 172

Zrozumienie roli OSINT w ochronie tożsamości osób i zasobów organizacji 173
Rola OSINT w zapobieganiu cyberzagrożeniom 173
Osobista higiena cyfrowa a OSINT 174
Identyfikowanie i ograniczanie ryzyka wynikającego z cyfrowego śladu 174
Wyższy poziom prywatności i bezpieczeństwa 177
Ocena i wzmacnianie bezpieczeństwa organizacji dzięki OSINT 178
Wykrywanie ewentualnych podatności 178
Wykrywanie cyberzagrożeń takich jak oprogramowanie wymuszające okup i reagowanie na nie 180
Wykrywanie ataków phishingowych i socjotechnicznych 181
Czas na historię o egzotycznej lilii 182
Grupa Cobalt Dickens i jej sprytne ataki spear phishingowe 183
Prowadzenie dochodzeń w sprawie incydentów i naruszeń cyberbezpieczeństwa 184
Ujawnianie źródeł, zakresów i wpływu cyberincydentów 185
Tworzenie solidnych cyberzabezpieczeń dzięki OSINT 186
Współpraca ze społecznością zajmującą się cyberbezpieczeństwem 187
Adaptacja do zmieniającego się spektrum zagrożeń 187
Aktualizowanie strategii cyberbezpieczeństwa opartej na OSINT 189
Nie zapomnij o narzędziach 189
Podsumowanie 191

O autorze

Dale Meredith to certyfikowany przez EC-Council haker i instruktor oraz certyfikowany trener Microsoftu. Spędził ponad 10 lat na stanowiskach kierowniczych IT wyższego szczebla. Był również dyrektorem ds. technologii w firmie będącej dostawcą usług internetowych. Dzięki doświadczeniu jako instruktor IT jest w stanie wyjaśnić trudne pojęcia i sprawić, że uczestnicy szkoleń są w stanie zrozumieć teorię. Jego styl uczenia łatwo zapada w pamięć i jest zajmujący. Specjalistyczna wiedza pozwoliła Dale'owi sprawdzić się w wielu sytuacjach, w tym jako instruktor firm z rankingu Fortune 500, wykładowca na wielu uczelniach na świecie oraz pracownik Departamentu Bezpieczeństwa Krajowego i innych departamentów wojskowych Stanów Zjednoczonych. Oprócz tworzenia kursów wideo oraz prowadzenia konsultacji i szkoleń stacjonarnych Dale występuje również jako prelegent na konferencjach informatycznych na całym świecie, pomagając zespołom zadbać o bezpieczeństwo ich firm.

Mojej żonie, Alice Meredith. Kumpeli od koncertów, najlepszej przyjaciółce i ostoi. Dziękuję, że wspierasz mnie w mojej miłości do technologii i podtrzymujesz na duchu w trudnych chwilach.

Specjalne podziękowania dla zespołu wydawnictwa Packt Publishing — w którego skład wchodzą Romy, Ashwin, Prachi i zapewne wiele innych osób — za tolerowanie mojego napiętego grafiku i wykazywanie się elastycznością, gdy zaskakiwały mnie życiowe niespodzianki.

Moim wnukom. Dziękuję, że pozwalacie mi być Waszym Batmanem. „Wszystko jest niemożliwe, dopóki ktoś tego nie zrobi" — Bruce Wayne

O korektorach merytorycznych

Deepanshu Khanna jest hakerem, z którego wiedzy korzystają indyjskie siły obronne, rząd, Ministerstwo Spraw Wewnętrznych, policja oraz wiele innych instytucji, takich jak uczelnie wyższe, znane na całym świecie firmy informatyczne, czasopisma i gazety. Zaczął swoją karierę od zaprezentowania popularnego ataku GRUB na konferencji HATCON oraz swoich badań w dziedzinie systemów wykrywania włamań (IDS) i zaawansowanego środowiska wykrywania włamań (AIDE). Pokazywał kolizje haszy MD5 i ataki przepełnienia bufora w praktyce, co było tematem licznych artykułów w czasopismach, takich jak Pentestmag, Hackin9, eForensics, sd-journal i Hack5. Był również prelegentem na publicznych konferencjach, takich jak DEF CON, ToorCon, OWASP, HATCON i H1hackz. Wygłaszał też odczyty na różnych uczelniach i w instytutach.

Kalpa Kalhara Sampath jest wybitnym badaczem i pracownikiem naukowym w dziedzinie bezpieczeństwa informacji, złośliwego oprogramowania i sztucznej inteligencji. Uzyskał tytuł inżyniera w dziedzinie technologii informacyjnej ze specjalizacją w cyberbezpieczeństwie w **Instytucie Technologii Informacyjnej Sri Lanki** (**SLIIT**) oraz tytuł magistra w dziedzinie działań z zakresu cyberbezpieczeństwa na **Uniwersytecie Nowej Południowej Walii** (**UNSW**). Dzięki ponad ośmiu latom doświadczenia znacznie przyczynił się do rozwoju tej dziedziny za pośrednictwem wielu artykułów naukowych. Jest też oddanym wykładowcą i mentorem w dziedzinie etycznego hakowania oraz cyfrowej kryminalistyki. Jego praca wywiera nieustający wpływ na społeczność naukową, ale się do niej nie ogranicza.

Przedmowa

Gromadzenie danych wywiadowczych w rozległym cyfrowym świecie to fundament skutecznej obrony. Najnowsza książka Dale'a Mereditha dotyka samego serca tej skomplikowanej dziedziny. Pozwala na wszechstronną eksplorację zagadnień z zakresu **Open Source Intelligence** (**OSINT**), czyli białego wywiadu. W swoim podręczniku Dale zawarł nieodzowne wskazówki zarówno dla specjalistów i badaczy, jak i dla entuzjastów.

Znam Dale'a od blisko dziesięciu lat: najpierw był moim współpracownikiem, potem kolegą po fachu, a teraz jest przyjacielem. Przez ten czas byłem świadkiem jego niezrównanej pasji do cyberbezpieczeństwa. Dale posiada wyjątkową zdolność przedstawiania zagadnień z tej dziedziny w sposób przystępny i wciągający. Jego praca oświetliła drogę niezliczonym rzeszom specjalistów i ukształtowała sposób, w jaki wchodzimy w interakcje z cyfrowym środowiskiem.

Ta książka to owoc wielu lat eksploracji, praktyki i nauczania w dziedzinie OSINT. To świadectwo zaangażowania Dale'a na rzecz podnoszenia zbiorowego poziomu wiedzy w społeczności cyberbezpieczeństwa. Za pośrednictwem tych stron Dale zaprasza nas do zagłębienia się w dziedzinę OSINT. Oferuje narzędzia, techniki i spostrzeżenia, które odgrywają decydującą rolę w korzystaniu z otaczającego nas ogromu dostępnych publicznie informacji.

Tym, co odróżnia tę pracę od innych, jest umiejętność Dale'a łączenia teorii z praktyką. Wypełnia ona lukę między abstrakcyjnymi pojęciami a praktycznymi zastosowaniami, dzięki czemu czytelnik może zrozumieć nie tylko, jak użyć metod OSINT, lecz również w jakim celu. Ta książka nie jest zwykłym podręcznikiem. To też opowieść, która jest w stanie uchwycić istotę OSINT, powiązanych z tym obszarem wyzwań i jego potencjału, a także odmienić nasze podejście do bezpieczeństwa.

Korzystając z tego niezbędnego dodatku do Twojego arsenału cyberbezpieczeństwa, przygotuj się kolejno na wyzwanie, oświecenie i przypływ mocy. Niezależnie od tego, czy jesteś doświadczonym praktykiem, czy początkującym w tej dziedzinie, dzięki eksploracji OSINT z Dale'em zyskasz nową perspektywę, która poszerzy Twoje zrozumienie i zwiększy możliwości działania w dzisiejszej skomplikowanej rzeczywistości.

— Greg Shields
MVP firmy Microsoft i VMware vExpert

Wprowadzenie

Za chwilę rozpocznie się nasza fascynująca podróż po świecie cyberbezpieczeństwa i **OSINT** (ang. *Open Source Intelligence*, biały wywiad). Zadaniem tej książki jest towarzyszenie Ci podczas eksploracji intrygującego świata cyfrowych informacji oraz sposobów wykorzystania go do różnych celów.

Dzięki temu towarzyszowi poznasz podstawy cyberbezpieczeństwa, zrozumiesz zagrożenia czyhające w internecie i nauczysz się, jak zabezpieczyć swoją cyfrową obecność. Odkryjesz znaczenie czujności w cyfrowym świecie oraz to, że nawet najprostsze działania mogą zwiększyć Twoje szanse w starciu z cyberprzestępcami.

OSINT polega na zbieraniu danych z publicznie dostępnych źródeł, lecz nie ogranicza się do użycia wyszukiwarki Google. Nauczysz się skutecznie wyszukiwać i analizować informacje, które są na wyciągnięcie ręki, ale nie zawsze łatwo je znaleźć!

Dla kogo jest ta książka?

Ta książka jest dla każdego, kto odczuwa głód wiedzy na temat cyfrowego świata, kto pragnie zrozumieć zagrożenia i zabezpieczenia cybernetyczne oraz jest zainteresowany etycznym gromadzeniem i analizowaniem publicznie dostępnych informacji. Niezależnie od tego, czy studiujesz, pracujesz zawodowo w tej dziedzinie czy fascynujesz się cyfrowym światem, dzięki tej książce zdobędziesz ciekawe spojrzenie i umiejętności, które pozwolą Ci poruszać się po złożonym świecie cyberbezpieczeństwa i OSINT.

Co obejmuje ta książka?

Rozdział 1. „Sekrety ukrywania się na widoku — OSINT i jego moc" odpowie na pytanie, czym w ogóle zajmuje się OSINT. Biały wywiad oznacza szperanie w internecie oraz wyszukiwanie ciekawych i ważnych informacji, które teoretycznie są dostępne dla każdego. Przekonamy się też, dlaczego OSINT jest tak użyteczny w dzisiejszych czasach.

Rozdział 2. „Niewidoczni i nietykalni — znaczenie anonimowości w pracy analityka OSINT" jest poświęcony niezbędnym środkom ostrożności. Wyjaśnię, dlaczego powinniśmy trzymać się w cieniu (i zachować anonimowość), gdy wyszukujemy informacje. Chodzi przede wszystkim o bezpieczeństwo i o to, żeby nikt niepotrzebnie nie węszył wokół nas.

Rozdział 3. „Narzędzia OSINT — metody i techniki gromadzenia i analizowania informacji" rzuci nas na głęboką wodę, jeżeli chodzi o narzędzia OSINT. Przyjrzymy się wszelkiego rodzaju sposobom zbierania i analizowania informacji. Nie zaszkodzi nauczyć się paru sztuczek, które ułatwią nam pracę śledczą.

Rozdział 4. „Wyprawa w nieznane — narzędzia do eksploracji ukrytych danych" będzie przypominał poszukiwanie skarbów. Sprawdzimy, jak specjalistyczne narzędzia mogą nam pomóc znaleźć informacje ukryte w internecie. Wszystko będzie się toczyć wokół tego, czego nie da się łatwo znaleźć za pomocą zwykłego zapytania w wyszukiwarce Google.

Rozdział 5. „Od Recon-ng po Trace Labs — wycieczka objazdowa po najlepszych narzędziach OSINT" będzie jak wypełniona po brzegi skrzynka z narzędziami. Wypróbujemy ciekawe programy, witryny, usługi i systemy. Każdy z tych zasobów pomoże Ci być lepszym cyfrowym detektywem, jeżeli tylko będziesz wiedzieć, jak z niego korzystać.

Rozdział 6. „Oczy i uszy analizy zagrożeń — jak OSINT ogranicza ryzyka cybernetyczne" opowiada o tym, jak supermoce OSINT mogą chronić nas przed niebezpieczeństwem w internecie. Ten rozdział pokazuje, w jaki sposób wykorzystać OSINT do wykrywania i eliminowania cyfrowych zagrożeń oraz do ochrony siebie i innych.

Rozdział 7. „Ochrona własnej tożsamości i organizacji przed cyberzagrożeniami" skupia się na ochronie przed „cyberzłolami". Poznasz kilka wspaniałych rozwiązań, które pozwolą lepiej zabezpieczyć przed cyberzagrożeniami zarówno nas samych, jak i nasze organizacje. Wykorzystamy przy tym wszystko, czego wcześniej nauczyliśmy się o OSINT.

Zastosowane konwencje

W książce zastosowano kilka konwencji typograficznych.

`Kod w tekście` wskazuje na fragmenty kodu oraz przypadki użycia poleceń w tekście głównym. Oto przykład: „Funkcja `requests.get()` to prośba o podzielenie się informacjami, a odpowiedź zostaje zachowana w zmiennej `response`".

Z kolei blok kodu będzie oznaczony w taki sposób:

```
from bs4 import BeautifulSoup
import requests
response = requests.get('https://daledumbsitdown.com')
soup = BeautifulSoup(response.text, 'html.parser')
# Drukuje tytuł strony
print(soup.title.string)
```

W celu zwrócenia uwagi na konkretną część bloku kodu użyto pogrubionej czcionki:

```
;; ANSWER SECTION:
host1234.examplehosting.com. 3600 IN A 93.184.216.34
site1.com. 3600 IN CNAME host1234.examplehosting.com.
```

```
site2.net. 3600 IN CNAME host1234.examplehosting.com.
site3.org. 3600 IN CNAME host1234.examplehosting.com.
```

Dane wejściowe i wyjściowe oznaczono podobnie:

```
nslookup
> set type=MX
> daledumbsitdown.com
```

W tekście głównym **pogrubienie** oznacza nowy termin, ważne słowo lub wyrażenie, które pojawia się po raz pierwszy. Oto przykład: „W przypadku **pasywnego rozpoznania** OSINT jesteśmy niczym zjawa, która obserwuje świat, ale nigdy nie wchodzi z nim w interakcje".

Elementy pojawiające się na ekranie, takie jak opcje menu, przyciski czy ikony, będą *wyróżnione* w następujący sposób: „Kliknij prawym klawiszem strumień komunikacji i wybierz opcję *Follow TCP Stream* (obserwuj strumień TCP), aby odtworzyć przepływ i odnaleźć wszelkie możliwe do odczytania pakiety danych, które mogą dostarczać wskazówek na temat ich funkcji i celu". Kursywą oznaczamy również nazwy folderów, plików, rozszerzeń i bibliotek, ścieżki i adresy URL oraz nazwy użytkowników na Twitterze.

Wskazówki lub ważne uwagi

Będą wyglądały w ten sposób.

Sekrety ukrywania się na widoku — OSINT i jego moc

Rozdział 1

Witaj w fascynującym i szalonym świecie **OSINT**! W tym rozdziale zgłębisz ukryte moce OSINT, nauczysz się wielu użytecznych w praktyce technik i zrozumiesz niebanalne znaczenie białego wywiadu w cyfrowej rzeczywistości. Po przeczytaniu tego rozdziału będziesz dysponować niezbędnymi umiejętnościami, aby poruszać się po tym obszarze jak ekspert.

Na początek zajmiemy się następującymi tematami:

- wprowadzenie do OSINT;
- aktywne i pasywne rozpoznanie OSINT;
- znaczenie OSINT w erze cyfryzacji;
- framework OSINT;
- pierwsze kroki i najlepsze praktyki w dziedzinie OSINT.

W tym rozdziale wcielę się w postać godnego zaufania, acz nieco mrocznego rycerza. Podzielę się z Tobą praktycznymi przykładami i udzielę paru rad z pozycji starego wyjadacza. Pomogę Ci odnaleźć się w świecie publicznie dostępnych danych oraz nauczę Cię, jak wyciągać cenne wnioski i wykorzystać OSINT do osiągania założonych celów. Gdy poznasz arkana tej sztuki, będziesz dysponować potężnym zestawem umiejętności, które zapewnią Ci przewagę nad przeciwnikami, większe bezpieczeństwo i pewność siebie przy eksploracji nowych cyfrowych horyzontów.

Nie możesz się doczekać, aby zacząć przygodę z OSINT? Zabierzmy się zatem do pracy i odkryjmy prawdziwy potencjał białego wywiadu.

Wprowadzenie do OSINT

OSINT (ang. *Open Source Intelligence*), często zwany **białym wywiadem**, można zdefiniować jako proces gromadzenia informacji znajdujących się w domenie publicznej, oceniania ich oraz wyciągania na ich podstawie wniosków w celu znalezienia odpowiedzi na określone zagadnienia wywiadowcze.

Informacje a informacje wywiadowcze

Można by powiedzieć, że informacja to zawsze informacja, niezależnie od rodzaju. W tym przypadku różnica jest jednak mniej więcej taka, jak między surowym składnikiem a wytwornym daniem.

1. **Informacje jako punkt wyjścia**

   Zacznijmy od informacji. Myśl o nich jako o nieprzetworzonym surowcu. Otaczają nas ze wszystkich stron w swoich najróżniejszych odsłonach. Tweety i artykuły prasowe, które czytamy, to też informacje — tak samo jak nieprzerwany potok postów w mediach społecznościowych. Informacje są zróżnicowane, również pod kątem jakości. Niektóre są z najwyższej półki, a inne — wręcz niemożliwe do przełknięcia. W świecie OSINT to od nich się wszystko zaczyna.

2. **Informacje wywiadowcze jako produkt końcowy**

   Teraz porozmawiajmy o informacjach wywiadowczych. Jeżeli zwykłe informacje przyrównamy do składników, to informacje wywiadowcze stanowią pełnowartościowy, starannie przygotowany posiłek. Dane wywiadowcze powstają w wyniku zbierania nieprzetworzonych informacji, analizowania ich, zgłębiania kontekstu i przetwarzania w coś sensownego i pożytecznego. Wszystko musi mieć ręce i nogi. Trzeba zidentyfikować wzorce, zwizualizować powiązania i sformułować spostrzeżenia, które są istotne, konkretne i — co najważniejsze — mogą stanowić podstawę do działania.

3. **Przetwarzanie**

   Stworzenie z nieoszlifowanych informacji diamentu, jakim są informacje wywiadowcze, stanowi istotę OSINT. Ten proces wymaga nie lada umiejętności i zaczyna się od zebrania odpowiednich składników, w tym przypadku informacji z różnych ogólnodostępnych źródeł. Potem następuje kluczowy etap, czyli weryfikacja informacji, w ramach której niczym szef kuchni sprawdzamy jakość każdego składnika.

4. **Analiza**

   Po sprawdzeniu informacji zaczyna się analiza. Na tym etapie dzieje się prawdziwa magia. Przeszukujemy informacje pod kątem wzorców lub nieprawidłowości i próbujemy zrozumieć ukrytą w nich historię. Kolejnym etapem jest synteza. Teraz mieszamy składniki, aby przygotować perfekcyjne danie. Łączymy poszczególne elementy w dążeniu do kompleksowego zrozumienia.

5. **Interpretacja**

   Na koniec przychodzi czas na interpretację. Wyciągamy wnioski, staramy się zrozumieć szersze implikacje i oceniamy, w jaki sposób nowo powstałe informacje wywiadowcze mogą pomóc w podejmowaniu decyzji i opracowywaniu strategii.

Aktywne i pasywne rozpoznanie OSINT

Pochylmy się teraz nad różnicą między pasywnymi i aktywnymi działaniami OSINT. To różne oblicza tego samego procesu, które mogą mieć jednak bardzo odmienne konsekwencje.

W przypadku **pasywnego rozpoznania** OSINT jesteśmy niczym zjawa, która obserwuje świat, ale nigdy nie wchodzi z nim w interakcje. Przeszukujemy publiczne zasoby, lecz nikogo nie zaczepiamy. Nie komentujemy postów, nie przesyłamy wiadomości, a już na pewno nie wysyłamy zaproszeń do grona znajomych ani nie klikamy przycisku *Obserwuj*. Niczym siedząca na ścianie mucha zupełnie nie zwracamy na siebie uwagi.

Aktywne rozpoznanie polega na bezpośrednich interakcjach, np. z osobą będącą przedmiotem dochodzenia. Zapraszamy ją do grona znajomych w mediach społecznościowych, komentujemy jej posty, czasami nawet wysyłamy wiadomości. Jesteśmy niczym agent pod przykrywką, a w niektórych firmach nawet tak możemy być traktowani. Nie zapomnijmy jednak uzyskać zgody przełożonego, zanim zaangażujemy się w coś takiego.

Jeżeli planujesz aktywne rozpoznanie, musisz wtopić się w otoczenie jak ninja. „Ale niby jak, Dale?" — zapytasz. No cóż, zacznij od stworzenia kilku kont na różnych platformach. Chcesz wyglądać jak przeciętny Jan Kowalski.

Musimy uwzględnić jeszcze jedną kwestię. Różne organizacje w różny sposób definiują, co zalicza się do rozpoznania pasywnego, a co do aktywnego. Na przykład dołączenie do prywatnej grupy na Facebooku może niektórym z nas wydawać się pasywną obserwacją, ale inni mogą uznać to za interakcję. Dlatego koniecznie musimy znać zasady, jakie w tej kwestii wyznaje nasz pracodawca.

Niektórzy mimo to argumentują, że dołączenie do grupy to działanie pasywne pod warunkiem, iż ograniczamy się do obserwacji i z nikim nie rozmawiamy.

Skomplikowane, prawda?

Znaczenie OSINT w erze cyfryzacji

W tej chwili OSINT jest wykorzystywany przez rządy, firmy, organizacje non profit i inne podmioty. Różnorodność zastosowań białego wywiadu może zaskoczyć, gdyż obejmuje wszystko — od wykrywania zagrożeń bezpieczeństwa, przez badania rynkowe, aż po wywiad konkurencyjny.

Oto niektóre dziedziny, w których OSINT zmienił zasady gry:

- **Badania naukowe**. Naukowcy wykorzystują OSINT, aby zbierać dane na wszelkiego rodzaju tematy, takie jak trendy społeczne, opinia publiczna czy wskaźniki ekonomiczne.
- **Badania biznesowe i rynkowe**. Chcesz dowiedzieć się, co robi konkurencja, śledzić trendy branżowe lub zrozumieć zachowania konsumentów? Z OSINT to żaden problem. Możesz na nim spokojnie oprzeć swoje decyzje biznesowe i strategie rynkowe.

- **Bezpieczeństwo i wywiad**. OSINT może być naszym osobistym Sherlockiem Holmesem, chroniącym nas przed działalnością terrorystyczną i atakami cybernetycznymi. Dobrze jest też wiedzieć, co w trawie piszczy, jeżeli chodzi o zagraniczne rządy, organizacje czy świat przestępczy.
- **Dziennikarstwo śledcze**. Dziennikarze zaprzęgają OSINT do pracy, aby zdobywać sensacyjne informacje na temat polityków, przedsiębiorstw, przestępstw i czego tylko pragną.
- **Postępowania sądowe**. OSINT odgrywa istotną rolę na sali sądowej. Pomaga w gromadzeniu dowodów oraz pozwala prześwietlić oskarżonych i potencjalnych świadków.

W czym tkwi urok OSINT?

OSINT koncentruje się na gromadzeniu publicznie i legalnie dostępnych informacji. Eliminuje to potrzebę korzystania z tajnych czy trudno dostępnych źródeł, do których dotarcie kosztowałoby dużo czasu i środków.

OSINT oferuje cały wachlarz źródeł do wyboru, w tym media społecznościowe, artykuły prasowe, raporty rządowe czy prace naukowe. Dzięki temu zapewnia kompletny obraz sytuacji.

Innym istotnym zagadnieniem jest aktualność informacji. Dzięki możliwości prowadzenia białego wywiadu w czasie rzeczywistym możemy być na bieżąco z najświeższymi wydarzeniami i trendami.

Kolejną zaletą OSINT jako metody pozyskiwania danych wywiadowczych są relatywnie niskie koszty. W odróżnieniu od innych metod, takich jak rozpoznanie osobowe czy elektromagnetyczne, OSINT nie wymaga drogiego sprzętu ani wyspecjalizowanego personelu, co sprawia, że jest to bardzo przystępna opcja.

Dodatkowo OSINT jest niezwykle przejrzysty i łatwy do zweryfikowania. Na dokładności i rzetelności odkrytych danych można polegać.

Jak zatem działa OSINT?

Zapewne nie możesz się doczekać, aby dowiedzieć się, jak działa magia białego wywiadu. Uchylmy więc rąbka tajemnicy:

1. **Zbieranie danych**. Gromadzimy publicznie dostępne informacje z różnych źródeł, takich jak media społecznościowe, artykuły prasowe, sprawozdania rządowe, prace naukowe i komercyjne bazy danych. Można to robić ręcznie lub użyć narzędzi do automatyzacji.
2. **Przetwarzanie danych**. Przesiewamy zebrane informacje, aby pozbyć się danych powielonych, nieistotnych lub niedokładnych. Na tym etapie chcemy przefiltrować i uporządkować dane pod kątem istotności i znaczenia.

3. **Analiza danych**. Na bazie przetworzonych danych szukamy trendów, wzorców i relacji. Narzędzia do wizualizacji danych, głębokiej analizy i przetwarzania języka naturalnego służą tutaj pomocą.
4. **Publikacja wyników**. Ostatni krok polega na podzieleniu się odkryciami z osobami podejmującymi decyzje. Można to zrobić w formie sprawozdania, zestawienia danych czy ostrzeżenia, w zależności od potrzeb danej organizacji.

Sekret OSINT tkwi w tym, że mamy do czynienia z nieprzerwanym cyklem. Za każdym razem doskonalimy proces zbierania, przetwarzania i analizy danych, uzupełniamy go o nowe elementy i informacje zwrotne. W końcu OSINT to nie nauka ścisła. Ma takie same ograniczenia jak inne formy wywiadu. Dlatego wymaga zarówno spostrzegawczości, jak i wyważonej interpretacji ze strony doświadczonego analityka.

Zajrzymy teraz pod maskę naszego nowiuśkiego batmobilu. Te skomplikowane układy to techniki zbierania i analizowania danych. Zobaczmy, z jakich źródeł OSINT czerpie moc:

- **Media społecznościowe**. Portale takie jak Facebook, X czy LinkedIn to coś więcej niż internetowe miejsca spotkań. To również znakomite środowisko do eksploracji trendów, mierzenia nastrojów społecznych, a czasami również wykrywania zagrożeń.
- **Strony internetowe**. Pozyskiwanie danych ze stron internetowych (ang. *web scraping*) przypomina wysłanie współczesnego poszukiwacza w cyfrową dżunglę. Wyspecjalizowane aplikacje wydobywają tony danych ze stron internetowych w sposób szybki i systematyczny.
- **Wyszukiwarki internetowe**. Stare dobre wyszukiwarki internetowe, takie jak Google, umożliwiają użycie zaawansowanych opcji wyszukiwania, aby zawęzić wyniki i szybko zlokalizować potrzebne nam dane. Ten proces nazywa się czasem Google dorkingiem.
- **Rejestry publiczne**. To prawdziwe skrzynie ze skarbami, wśród których aż roi się od cennych informacji. Rejestr beneficjentów rzeczywistych, księgi wieczyste i rejestry handlowe mogą wiele powiedzieć zarówno o osobach, jak i o organizacjach.
- **Serwisy informacyjne**. Tradycyjne kanały, takie jak gazety i czasopisma, oraz internetowe portale informacyjne to istna skarbnica danych. Dzięki nim możemy trzymać rękę na pulsie, jeżeli chodzi o najświeższe wydarzenia, nowe trendy i zagrożenia.
- **Narzędzia do analizy danych**. W przypadku ogromnych zbiorów danych narzędzia takie jak Excel, Tableau czy R to istne dary niebios. Pomagają odsiać nieistotne dane oraz dostrzec wzorce i relacje w pozostałych.

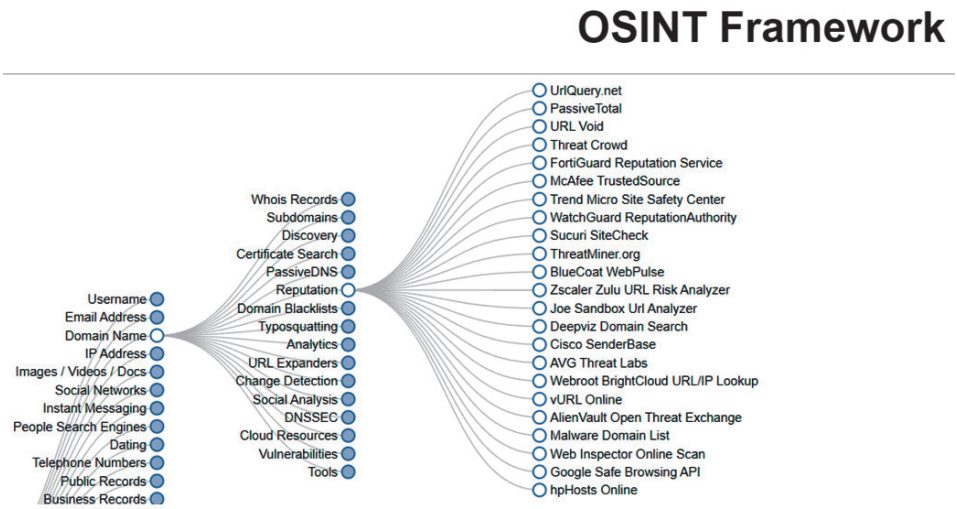
Pamiętajmy jednak o tym, że sytuacja w branży OSINT zmienia się błyskawicznie. Pojawiają się nowe technologie i źródła danych, trzeba więc śledzić i na bieżąco poznawać najnowsze metody oraz narzędzia umożliwiające skuteczne gromadzenie i analizę danych.

Framework OSINT

Strona internetowa dostępna pod adresem *https://osintframework.com*, znana jako framework OSINT, to nieocenione wsparcie dla osób, które zajmują się białym wywiadem. Jest nieustannie zmieniającym się internetowym katalogiem prezentującym nieprzebrane zasoby OSINT w sposób łatwy do zrozumienia i wykorzystania.

To poręczne narzędzie jest owocem pracy Justina Nordine'a, który cieszy się dużym szacunkiem w branży cyberbezpieczeństwa. Z założenia był to projekt ułatwiający ustrukturyzowaną prezentację narzędzi OSINT oraz dzielenie się zasobami. Jako swoiste świadectwo ducha współpracy w dziedzinie cyberbezpieczeństwa przekształcił się w stale aktualizowaną, współtworzoną przez społeczność platformę, która jest powszechnie wykorzystywana przez specjalistów z całego świata.

Odwiedzając stronę frameworku OSINT, zobaczymy, że ma strukturę interaktywnej mapy myśli (rysunek 1.1). Rozpoczynamy od najogólniejszych kategorii, a w miarę jak klikamy dalej, przechodzimy do coraz bardziej konkretnych zasobów i narzędzi. Dzięki temu użytkownicy mogą szybko znaleźć zasoby, których potrzebują, niezależnie od tego, czy są to portale społecznościowe, specjalistyczne wyszukiwarki, bazy z wyciekami danych czy zasoby rządowe.



Rysunek 1.1. Strona frameworku OSINT

Dla specjalistów z branży bezpieczeństwa strona frameworku OSINT to dar niebios. Stanowi doskonały punkt wyjścia do fazy zbierania informacji i rozpoznania w ramach oceny bezpieczeństwa czy dochodzenia. Dzięki kategoryzacji zasobów framework pomaga ekspertom dobrać najlepsze narzędzia do ich potrzeb, co pozwala zaoszczędzić czas na późniejszym etapie badawczym.

Warto zauważyć, że framework OSINT sam w sobie nie jest narzędziem. Bardziej przypomina mapę skarbów, wskazującą drogę do cennych zasobów OSINT. W związku z tym użytkownicy powinni korzystać z poszczególnych narzędzi w sposób odpowiedni i etyczny, zawsze z szacunkiem dla cudzej prywatności i przepisów prawa.

Piękno frameworku OSINT tkwi w jego prostocie i szerokim zakresie. Ponadto regularne aktualizacje sprawiają, że pozostaje istotnym punktem odniesienia dla specjalistów z dziedziny bezpieczeństwa i innych osób zainteresowanych zgłębianiem OSINT. Framework uosabia potęgę współpracy i korzystania z ogólnodostępnych źródeł w społeczności zajmującej się cyberbezpieczeństwem.

Etapy dochodzenia OSINT na konkretnych przykładach

Czy dzięki OSINT bylibyśmy w stanie znaleźć źródło maila phishingowego? Niech odpowiedzią na to pytanie będzie następujący scenariusz:

1. **Analiza wstępna**. Odbiorca e-maila phishingowego zauważył podejrzane elementy i zgłosił e-mail do zespołu ds. bezpieczeństwa.
2. **Metadane e-maila**. Przeanalizowano nagłówek e-maila i uzyskano metadane, takie jak adres IP nadawcy, znacznik czasu oraz informacje o trasowaniu.
3. **Badanie adresu IP**. Adres IP sprawdzono w publicznie dostępnych źródłach OSINT, takich jak bazy danych na temat rejestracji domen, rekordy WHOIS oraz narzędzia do sprawdzania reputacji adresów IP.
4. **Analiza śladu cyfrowego**. Media społecznościowe, fora internetowe oraz inne strony przeszukano pod kątem powiązań z danym adresem IP i innymi adresami e-mailowymi.
5. **Analiza przekrojowa**. Informacje zgromadzone z różnych źródeł OSINT połączono i przeanalizowano, aby ustalić powiązania i wzorce.
6. **Ustalenie autorstwa i publikacja wyników**. Na podstawie zebranych danych badacze byli w stanie określić prawdopodobne źródło e-maila phishingowego. Sporządzono kompleksowy raport, załączając wszystkie istotne szczegóły i zalecenia dotyczące ograniczenia zagrożenia.

A czy moglibyśmy użyć OSINT do znalezienia źródła wycieku danych? Przeanalizujmy kolejny praktyczny przykład:

1. **Wykrycie naruszenia**. Dzięki wewnętrznym zabezpieczeniom lub zgłoszeniu z zewnątrz firma odkrywa wyciek danych.
2. **Zbieranie wskaźników**. Z systemu objętego naruszeniem lub źródeł zewnętrznych zbiera się istotne dowody, takie jak próbki danych objętych naruszeniem czy pseudonimy hakerów.
   - **Próbki danych**. W przypadku wycieków hakerzy często ujawniają próbkę skradzionych danych, aby udowodnić swoją wiarygodność i posiadanie dostępu do informacji. Wykorzystując OSINT, możemy odnaleźć takie

próbki danych na różnych platformach. Może to obejmować publicznie dostępne strony internetowe, fora lub aukcje w dark webie („ciemnej sieci"), na których handluje się takimi danymi lub się je udostępnia. Dzięki narzędziom i technikom OSINT specjaliści ds. cyberbezpieczeństwa mogą zidentyfikować próbki i uzyskać informacje na temat zakresu oraz charakteru naruszenia.

- **Pseudonimy hakerów**. Cyberprzestępcy często wykorzystują różne pseudonimy i wirtualne tożsamości. Dzięki OSINT można zbierać dane na temat tych pseudonimów z różnych źródeł internetowych, w tym mediów społecznościowych, forów i czatów. W wyniki poszukiwań i analiz specjaliści ds. cyberbezpieczeństwa mogą odkryć powiązania, wzorce czy wcześniejsze działania związane z tymi pseudonimami. Takie informacje pomagają określić tożsamość lub możliwe motywy cyberprzestępców.
- **Analiza systemów objętych naruszeniem**. OSINT może pomóc w zidentyfikowaniu istotnych śladów również w zaatakowanych systemach. Poprzez analizę logów systemowych, ruchu sieciowego oraz innych zasobów cyfrowych specjaliści ds. cyberbezpieczeństwa mogą znaleźć ślady pozostawione przez hakerów. Obejmuje to adresy IP, infrastrukturę **dowodzenia i kontroli** (ang. *command and control*, C2) do komunikacji z zaatakowanymi urządzeniami, sygnatury złośliwego oprogramowania czy inne techniczne zasoby, które mogą ujawniać istotne informacje na temat naruszenia. Narzędzia i techniki OSINT umożliwiają sprawdzenie tych tropów w publicznie dostępnych źródłach i odkrycie istotnych wskazówek co do atakujących i ich metod.

3. **Monitorowanie dark webu**. Narzędzia OSINT stosuje się do monitorowania szemranych forów, aukcji czy czatów w dark webie. Celem jest znalezienie wszelkich nawiązań do skradzionych danych lub powiązanych działań.
4. **Monitorowanie mediów społecznościowych**. Publicznie dostępne portale społecznościowe można monitorować pod kątem dyskusji, postów czy komentarzy, które mogłyby dostarczyć informacji na temat naruszenia lub jego sprawców.
5. **Analiza ujawnionych danych**. Jeżeli jakakolwiek część danych pochodzących z wycieku jest publicznie dostępna, techniki OSINT można wykorzystać do analizy powiązanych treści, nazw użytkowników, adresów e-mailowych i czegokolwiek innego, co mogłoby pomóc w dochodzeniu.
6. **Ustalenie sprawców i współpraca**. Wnioskami wysuniętymi dzięki OSINT można podzielić się z organami ścigania, firmami zajmującymi się cyberbezpieczeństwem lub organizacjami branżowymi w celu umożliwienia im współpracy w ramach śledztwa.
7. **Działania prawne lub ograniczenie zagrożenia**. Na podstawie zidentyfikowanych źródeł i dowodów można podjąć odpowiednie kroki prawne lub środki łagodzące skutki naruszenia, aby zminimalizować jego wpływ i zapobiec takim wydarzeniom w przyszłości.

Teraz mamy lepsze pojęcie o tym, jak OSINT może pomóc ludziom i firmom.

Pierwsze kroki i najlepsze praktyki w dziedzinie OSINT

OSINT może być ekscytujący, gdyż daje nam dostęp do cennych informacji i zwiększa wachlarz naszych możliwości w ramach dochodzenia. Oto kilka praktycznych wskazówek, użytecznych spostrzeżeń i sugestii co do zasobów, które mogą pomóc w rozpoczęciu przygody z OSINT i zbudowaniu solidnego warsztatu.

Tajniki skutecznego gromadzenia informacji

Przede wszystkim zdefiniuj swoje cele. Czemu mają służyć zebrane informacje? Odpowiedź na to pytanie pomoże ukierunkować działanie i usprawni proces badawczy. Zanim utkniesz pod górą informacji — a uwierz mi, tak się stanie — opracuj ustrukturyzowaną metodę.

Podziel dochodzenie na logiczne kroki, uwzględniając wszystkie istotne aspekty. Do gromadzenia informacji wykorzystaj różne źródła. Mogą to być wyszukiwarki, media społecznościowe, publiczne rejestry, strony rządowe czy specjalistyczne narzędzia OSINT. Sprawdź informacje w różnych źródłach, aby zwiększyć ich dokładność i zmniejszyć ryzyko pomyłki.

Podszkól się z tworzenia skutecznych zapytań. Zapoznaj się z operatorami, filtrami i zaawansowanymi opcjami wyszukiwania w wyszukiwarkach, które pomagają zawęzić wyniki i zlokalizować konkretne informacje.

Badaj metadane powiązane z plikami cyfrowymi, obrazami i dokumentami. Analizowanie metadanych może dostarczyć cennych informacji, takich jak znaczniki czasowe czy szczegóły na temat lokalizacji, autorstwa i używanych urządzeń.

I jeszcze jedna wskazówka: naucz się podążać za cyfrowym śladem. Obejmuje to badanie profili w mediach społecznościowych, forów internetowych, postów na blogach oraz publicznie dostępnych rejestrów, aby uzyskać wszechstronne informacje na temat obiektu dochodzenia. Wiem, że jest tego sporo, ale nie martw się. Nauczymy się tego później.

Prowadź szczegółowe notatki na temat znalezionych informacji, zawierające znaczniki czasowe, adresy URL, zrzuty ekranów i inne istotne szczegóły. Odpowiednia dokumentacja badań umożliwia wydajną analizę i pozwala łatwo znaleźć odniesienia do informacji, które są nam potrzebne.

Krótka lista użytecznych zasobów

Niezależnie od tego, czy chodzi o sprawdzanie kandydatów na stanowiska, czy o identyfikację potencjalnie niebezpiecznych stron, popularne narzędzia OSINT dają użytkownikom możliwość zbierania informacji dostosowanych do ich specyficznych potrzeb. Wyposażeni w te narzędzia, możemy usprawnić proces badawczy i wysnuć cenne wnioski,

pomocne przy podejmowaniu decyzji. Pamiętaj, że moc OSINT tkwi w przekształcaniu publicznie dostępnych danych w cenne informacje wywiadowcze. Oto moja osobista lista 12 najlepszych narzędzi (z większością z nich zapoznasz się w ramach tej książki):

- Maltego (*https://www.maltego.com*),
- SpiderFoot (*https://intel471.com/attack-surface-documentation*),
- Intelligence X (*https://intelx.io*),
- Shodan (*https://www.shodan.io*),
- framework OSINT (*https://osintframework.com*),
- Metagoofil (*https://github.com/opsdisk/metagoofil*),
- Lampyre (*https://lampyre.io*),
- Spokeo (*https://www.spokeo.com*),
- Recon-ng (*https://github.com/lanmaster53/recon-ng*),
- Mitaka (*https://github.com/ninoseki/mitaka*),
- Babel Street (*https://www.babelstreet.com*),
- Seon (*https://seon.io*.

Uwaga

O frameworku OSINT wspominałem już wcześniej. Ta bardzo często aktualizowana witryna internetowa zapewnia dostęp do całej gamy innych stron i narzędzi. Zaglądaj tam często.

Podsumowanie

Zaczęliśmy od OSINT i zastanawialiśmy się, dlaczego odgrywa dzisiaj tak ogromną rolę. Jak każdej supermocy (czy narzędzie) można go użyć do złych lub dobrych celów. Istnieje też umiejętny i nieumiejętny sposób korzystania z niego. Rozmawialiśmy o najlepszych praktykach, aby móc zbierać i wykorzystywać informacje w sposób odpowiedzialny i etyczny. Nikt w końcu nie został herosem cyberbezpieczeństwa, postępując lekkomyślnie!

Następnie zakasaliśmy rękawy i przeanalizowaliśmy autentyczne przykłady użycia OSINT. Wyjaśniłem, jak OSINT może pomóc wykryć oszustwo w formie phishingu oraz jak wykorzystać go do ustalenia źródła wycieku.

Na koniec zapoznaliśmy się z użytecznymi wskazówkami i zasobami, aby przygotować się do pracy. Był to swoisty pakiet startowy narzędzi OSINT.

Oto rozdział 1. w pigułce — nasz pas startowy do świata OSINT. Za chwilę natomiast zajmiemy się metodami i technikami prowadzenia białego wywiadu.

Rozdział 2

Niewidoczni i nietykalni — znaczenie anonimowości w pracy analityka OSINT

W szybko ewoluującej dziedzinie **OSINT** zabezpieczenie własnej anonimowości jest nie tylko najlepszą praktyką, lecz nieodzownym elementem skutecznego dochodzenia. W tym rozdziale rzucimy nieco światła na priorytetową rolę anonimowości w analizie OSINT. W kolejnych podrozdziałach będziemy zajmować się różnymi aspektami ochrony prywatności w procesie kompleksowego gromadzenia informacji wywiadowczych. Wraz z końcem tego rozdziału będziemy uzbrojeni w wiedzę i umiejętności niezbędne do utrzymania anonimowości, zarządzania swoim cyfrowym śladem i prowadzenia bezpiecznej komunikacji w ramach białego wywiadu.

W tym rozdziale zajmiemy się przede wszystkim następującymi tematami:

- wprowadzenie do anonimowości i prywatności w OSINT;
- ochrona własnego śladu cyfrowego;
- aktualizowanie wiedzy na temat cyberzagrożeń.

Wprowadzenie do anonimowości i prywatności w OSINT

OSINT wymaga głębokiej analizy dużych ilości danych z publicznie dostępnych źródeł. Z wielu ważnych powodów analitycy OSINT muszą jednak zadbać również o swoją prywatność i anonimowość. Powody te możemy podsumować w następujących punktach:

- **Alarm dla podejrzanych**. Jeżeli osoba lub firma zorientuje się, że jest przedmiotem dochodzenia OSINT, jest w stanie podjąć działania utrudniające gromadzenie danych. Może skasować posty w portalach społecznościowych, ograniczyć widoczność profilu, przestać udostępniać witrynę internetową lub zniszczyć dowody. Anonimowość działań odgrywa zatem kluczową rolę w tym, aby nie zaalarmować celu.
- **Niepowodzenie akcji**. Jeżeli cel zorientuje się, że jest obserwowany, może zmodyfikować swoje działania lub zmienić sposób komunikacji, unikając tym samym wykrycia. Może to poważnie zaszkodzić otwartemu dochodzeniu OSINT, jeżeli prowadzący je nie zgromadzili jeszcze danych wywiadowczych wystarczających do podjęcia decyzji. Anonimowość pomaga chronić dochodzenie przed wykryciem.
- **Przerwanie podejrzanych działań**. Jeżeli dochodzenie zostanie wykryte na wczesnym etapie, organy ścigania i inne instytucje mogą nie być w stanie wykryć działalności przestępczej ani zgromadzić dowodów niezbędnych do postawienia winnych przed sądem. Podejrzani mogą unikać wzbudzania podejrzeń. Anonimowość to klucz do rzetelnego monitorowania celów bez ryzyka wykrycia.
- **Konsekwencje prawne i kwestie etyczne**. W niektórych krajach nawet niezamierzone poinformowanie podejrzanych o prowadzonym dochodzeniu może owocować postawieniem nam zarzutów. Anonimowość pozwala uniknąć nieumyślnych naruszeń etyki i prawa.
- **Bezpieczeństwo osób**. Sprawcy, tacy jak hakerzy, terroryści czy inne grupy przestępcze, mogą mścić się na analitykach i źródłach, jeżeli dowiedzą się o prowadzonym dochodzeniu. Anonimowość i prywatność gwarantują, że my analitycy i nasze źródła będziemy bezpieczni.
- **Wycieki danych**. Informacje poufne powinny być chronione przed dostaniem się w niepowołane ręce. Jest to możliwe jedynie dzięki ścisłej kontroli sposobu wykorzystania tych danych i dostępu do nich. W celu uniknięcia katastrofalnych w skutkach naruszeń danych konieczne jest przestrzeganie zasad zachowania prywatności.

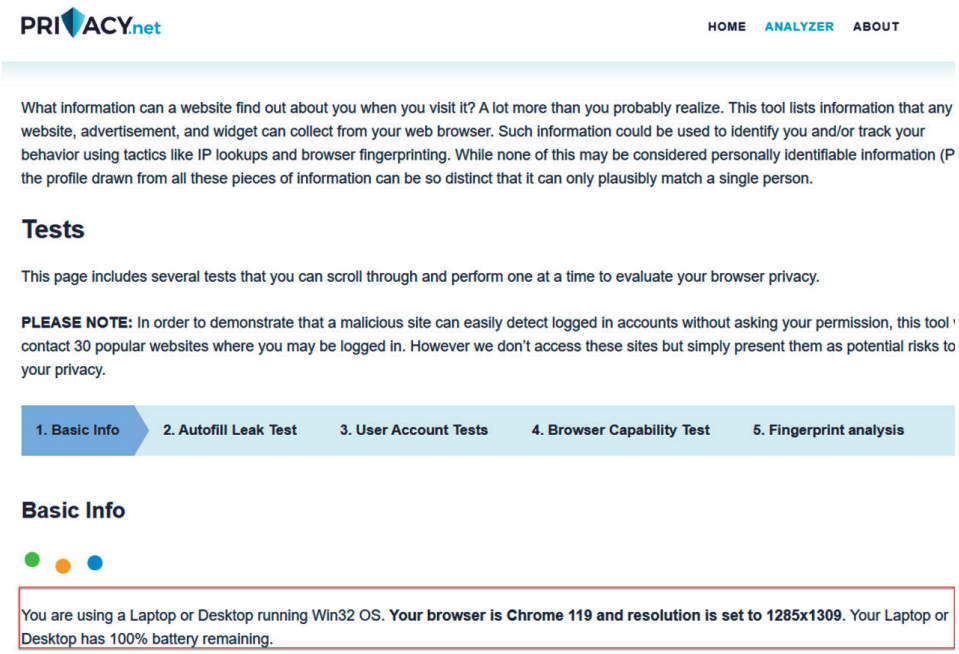
Czynniki prowadzące do utraty anonimowości w OSINT

W jaki sposób możemy zostać wykryci w trakcie dochodzenia? Spójrzmy na kilka przykładów:

- **Ujawnienie adresu IP**. Jednym z najprostszych sposobów na ukrycie się jest nieujawnianie swojego adresu IP. Jeżeli nie korzystamy z **wirtualnej sieci prywatnej** (ang. *Virtual Private Network*, VPN) lub przeglądarki Tor, odwiedzane strony mogą zarejestrować nasz prawdziwy adres IP.

Jako specjalista ds. cyberbezpieczeństwa stanąłem kiedyś w obliczu dużego wyzwania. Potrzebowałem znaleźć informacje na temat cyberataków, które wydawały się pochodzić z konkretnego miejsca. Aby dokonać tego bez wzbudzania podejrzeń atakujących, użyłem **sieci VPN**. Połączyłem się z serwerem z innego kraju, który ukrył mój prawdziwy adres IP i lokalizację. Wyglądało to tak, jakbym przeglądał sieć z lokalizacji powiązanej z tym serwerem, a nie ze swojej własnej. To pozwoliło mi bezpiecznie przeglądać różne strony i fora oraz zbierać informacje bez ujawniania mojej tożsamości. Doświadczenie to uświadomiło mi potęgę sieci VPN, jeżeli chodzi o ochronę cyfrowej tożsamości podczas badania wrażliwych tematów.

- **Pobieranie cyfrowego odcisku palca przeglądarki (ang. *browser fingerprinting*)**. Przeglądarki internetowe zbierają zaskakujące ilości danych, od rozdzielczości ekranu po zainstalowane wtyczki. Wszystkie te informacje mogą stanowić swoisty **odcisk palca** (ang. *fingerprint*). Nie wierzysz? Zrób sobie przerwę i odwiedź stronę *https://privacy.net/analyzer* (rysunek 2.1). A nie mówiłem?



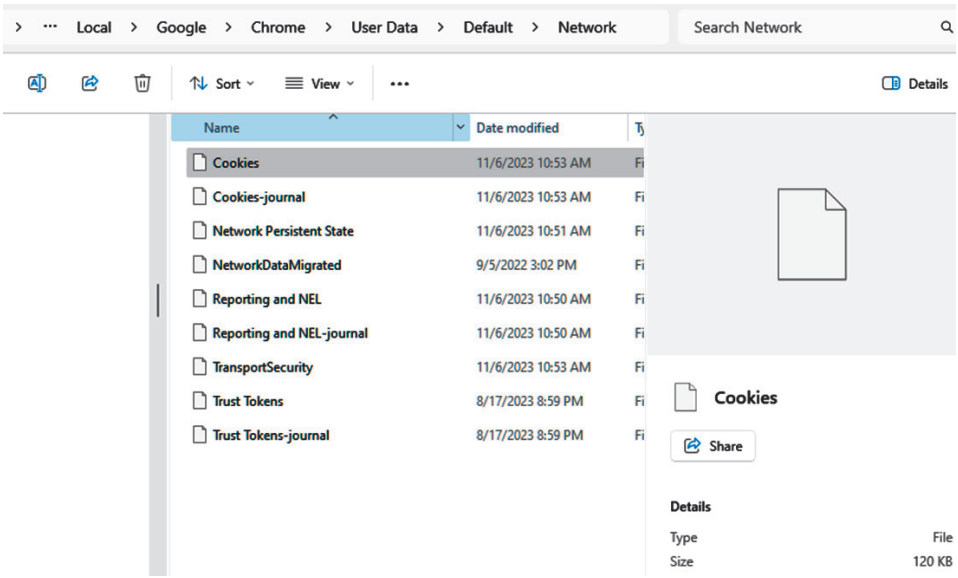
Rysunek 2.1. Moje wyniki z analizatora Privacy.net

Jeżeli myślisz, że tryb incognito Cię ochroni, to niestety się mylisz. Dzięki cyfrowemu odciskowi palca przeglądarki możliwe jest śledzenie działań użytkownika z różnych sesji.

- **Nadmierne zaufanie do technologii**. Poleganie na narzędziach takich jak sieci VPN czy przeglądarka Tor bez pełnego zrozumienia ich ograniczeń

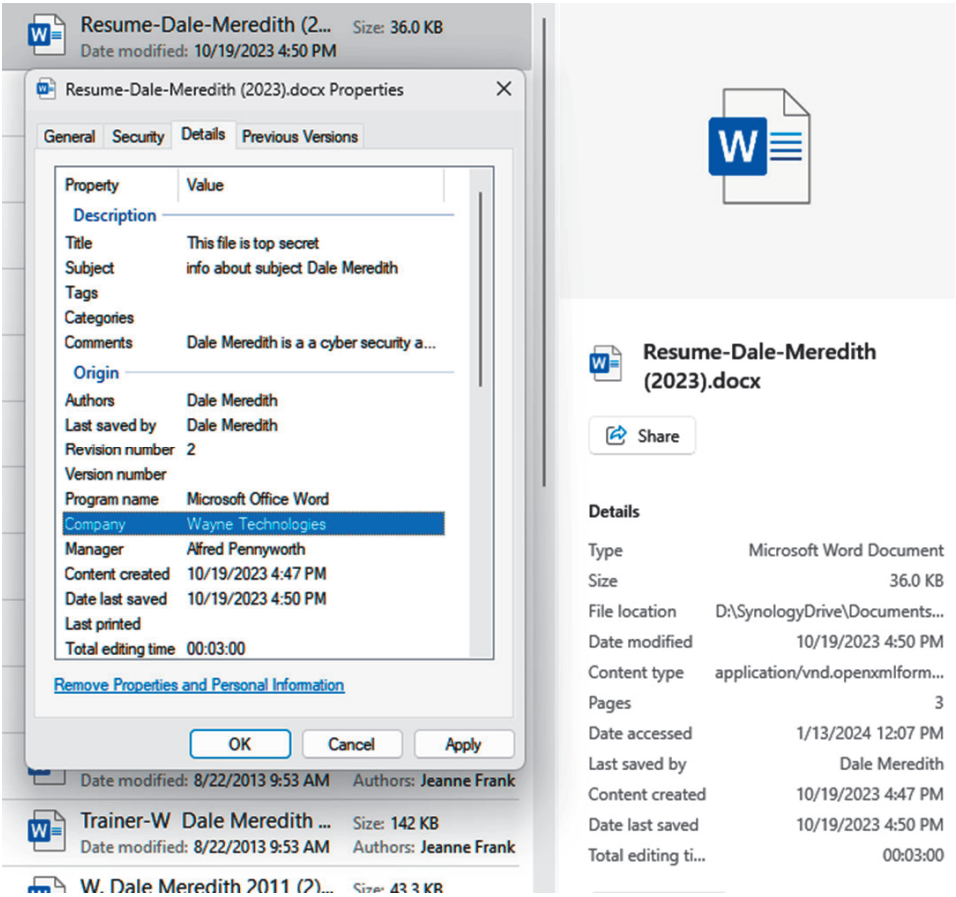
może stworzyć fałszywe poczucie bezpieczeństwa. Na przykład niektóre sieci VPN logują działania użytkownika, adresy IP, znaczniki czasowe i inne informacje pomimo haseł marketingowych, że tego nie robią. Potężni przeciwnicy, tacy jak organy państwowe, w niektórych przypadkach są w stanie zdeanonimizować działania użytkownika korzystającego z przeglądarki Tor. Żadna technologia nie stanowi uniwersalnego rozwiązania w kwestii ochrony anonimowości. Trzeba stosować wiele warstw zabezpieczeń i mieć świadomość słabości każdego z narzędzi lub podejść.

- **Śledzenie za pomocą plików cookie (ang. *cookie tracking*)**. Pliki cookie to niewielkie pliki tekstowe, które strony internetowe zapisują na urządzeniach, aby śledzić i zapamiętywać działania użytkowników (rysunek 2.2). Chociaż są wygodne, gdy pamiętają nasze dane do logowania lub zawartość koszyka, pozwalają firmom tworzyć skomplikowane profile dotyczące zwyczajów, zainteresowań, zachowań i innych aspektów na podstawie danych zgromadzonych z wielu stron i sesji. Regularne usuwanie plików cookie może ograniczyć śledzenie, ale firmy opracowały bardziej zaawansowane technologie, takie jak pobieranie cyfrowego odcisku palca przeglądarki czy identyfikacja na podstawie unikalnych cech elementu *canvas* na danej przeglądarce (ang. *canvas fingerprinting*), dzięki którym pliki cookie nie są niezbędne do śledzenia. Korzystanie z przeglądarek dbających o prywatność użytkownika, takich jak Tor, oraz zacieranie za sobą cyfrowych śladów poprzez niepowtarzanie tych samych wzorców zachowań jest ważne, jeżeli chcemy uniknąć śledzenia.



Rysunek 2.2. Pliki cookie są przechowywane w różnych miejscach i mogą zawierać wiele cennych informacji

- **Wycieki metadanych**. Dokumenty, zdjęcia, pliki audio oraz wideo, mogą zawierać metadane, czyli generowane przez urządzenie informacje na temat samego pliku. Mogą one obejmować znaczniki geograficzne i czasowe, numery seryjne urządzeń czy historię edycji (rysunek 2.3). Podobnie wiadomości takie jak e-maile mają nagłówki, które zawierają adres IP, informacje na temat klienta itp. Wyciek metadanych może dostarczyć informacji na temat tożsamości użytkownika i narazić na szwank jego anonimowość. Dlatego przed udostępnieniem starannie usuwajmy metadane z plików za pomocą odpowiednich narzędzi. Unikajmy też metod komunikacji, które powodują ujawnianie takich metadanych.



Rysunek 2.3. Przykład metadanych dołączonych do pliku

- **Niezabezpieczone publiczne sieci wi-fi**. Publiczne sieci wi-fi w kawiarniach, na lotniskach czy w hotelach często nie są zabezpieczone hasłem ani innymi metodami. Z tego względu każdy w pobliżu może łatwo przechwycić niezaszyfrowaną komunikację przechodzącą przez sieć i obserwować nasze

działania online. Nigdy nie loguj się do ważnych kont, w tym do poczty elektronicznej czy aplikacji bankowej, i nie podawaj poufnych informacji, gdy używasz niezabezpieczonej, publicznej sieci wi-fi. W takich przypadkach korzystaj z zaufanej sieci VPN, aby zaszyfrować komunikację. Najlepszym rozwiązaniem byłoby w ogóle poczekać z przesyłaniem wrażliwych danych do momentu połączenia się ze znaną i zaufaną siecią.

- **Socjotechnika**. Choć dysponujemy coraz lepszymi zabezpieczeniami technicznymi, ludzka natura nadal jest podatna na stare dobre triki socjotechniczne, takie jak phishing. W ochronie przed nimi kluczowe znaczenie ma nieużywanie tych samych haseł do różnych kont, korzystanie z uwierzytelniania wieloskładnikowego, gdy tylko to możliwe, zabezpieczanie komunikacji szyfrowaniem PGP oraz nauczenie się wykrywania oszustwa przed kliknięciem łącza lub załącznika. Żaden zestaw narzędzi do ochrony anonimowości nie pomoże nam, gdy ktoś podstępem wydobędzie od nas dane osobowe.
- **Korzystanie z kont osobistych do celów OSINT**. Jednym z najpoważniejszych błędów w dziedzinie bezpieczeństwa operacyjnego (ang. *operations security*, OPSEC) jest prowadzenie działań OSINT i badań w obszarze cyberbezpieczeństwa z kont, które można powiązać z naszą prawdziwą tożsamością. Gdy gromadzimy informacje wywiadowcze za pomocą wyszukiwarek internetowych, sieci społecznościowych, forów i innych cyfrowych lokalizacji, zawsze używajmy jednorazowych, anonimowych kont i maskujmy adresy IP. Zadbajmy o rygorystyczne rozdzielenie swoich prywatnych działań w internecie od związanych z dochodzeniem.
- **Przypadkowe potknięcia**. Pojedynczy wyciek danych osobowych na czacie, w poście na forum lub podczas rozmowy za pomocą komunikatora może wystarczyć, aby nasza anonimowość legła w gruzach. Musimy zachowywać niezwykłą ostrożność, gdy dzielimy się jakimikolwiek informacjami na swój temat w internecie, gdyż takie szczegóły mogą nas zdemaskować. Musimy również konsekwentnie rozdzielać alternatywne tożsamości. Wielokrotne wykorzystywanie tych samych nazw użytkownika, elementów adresów e-mailowych czy haseł przy tworzeniu kolejnych kont może ułatwiać ich powiązanie. A wystarczy chwila nieuwagi.
- **Nieaktualna wiedza**. Co chwila mamy do czynienia z nowymi technikami hakerskimi i sposobami wykorzystania luk w zabezpieczeniach. Jeżeli nie aktualizujemy swojej wiedzy na temat najnowszych zagrożeń dla prywatności i bezpieczeństwa, nasze dane mogą paść ofiarą tych nowych metod, o których nic nie wiemy i przeciw którym się nie zabezpieczyliśmy. Nigdy nie możemy zakładać, że mamy wystarczającą wiedzę. Aby dotrzymać kroku zmieniającym się zagrożeniom, uczenie się powinno być nieustającym procesem.

W poszukiwaniu złotego środka — prywatność w dochodzeniach OSINT

Technologia zawsze wywraca zasady gry do góry nogami. Chociaż łapanie przestępców, złoczyńców i arcyłotrów brzmi jak świetna przygoda, to jeżeli nie będziemy uważni, może zaszkodzić naszemu życiu prywatnemu.

Potrzebujemy systemu, który zapewnia nadzór, kontrolę, obiektywność i, co najważniejsze, osobistą odpowiedzialność. Nie możemy pozwolić na beztroskie korzystanie z tych potężnych narzędzi, jak się komu żywnie podoba, bez określenia kilku fundamentalnych zasad. Te zasady muszą być przejrzyste, tak aby każdy mógł zgłosić obiekcje, gdy coś jest nie w porządku.

Technologia sama w sobie nie jest wyposażona w moralny kompas. To tylko narzędzie. Musimy działać mądrze, etycznie i przede wszystkim czujnie. W końcu to bardziej maraton niż sprint. Jeżeli będziemy naginać zasady dla krótkoterminowych zwycięstw, sami sobie zgotujemy porażkę w długoterminowej perspektywie. Zawsze musimy mieć z tyłu głowy prawdziwy cel, a mianowicie społeczeństwo, które jest jednocześnie bezpieczne i wolne. Ochrona tej kruchej równowagi, moi drodzy, jest czymś, na co nie należy szczędzić wysiłków. W porządku, myślę, że się rozumiemy. Kazanie zakończone.

Ochrona własnego śladu cyfrowego

Cyfrowy ślad jest jak cień w słoneczny dzień: zawsze nam towarzyszy i zmienia się nieco, w miarę jak idziemy przez życie. Ten cień może jednak czasem powiedzieć na nasz temat więcej, niż byśmy chcieli. Tylko jedno kliknięcie chroni nasze dane osobowe, takie jak miejsce zamieszkania czy numer PESEL, przed ciekawskim wzrokiem. Nie wyrażaliśmy zgody na tak szczegółową obserwację, ale prawda jest taka, że jesteśmy na nią narażeni i wszyscy powinniśmy być tym zaniepokojeni.

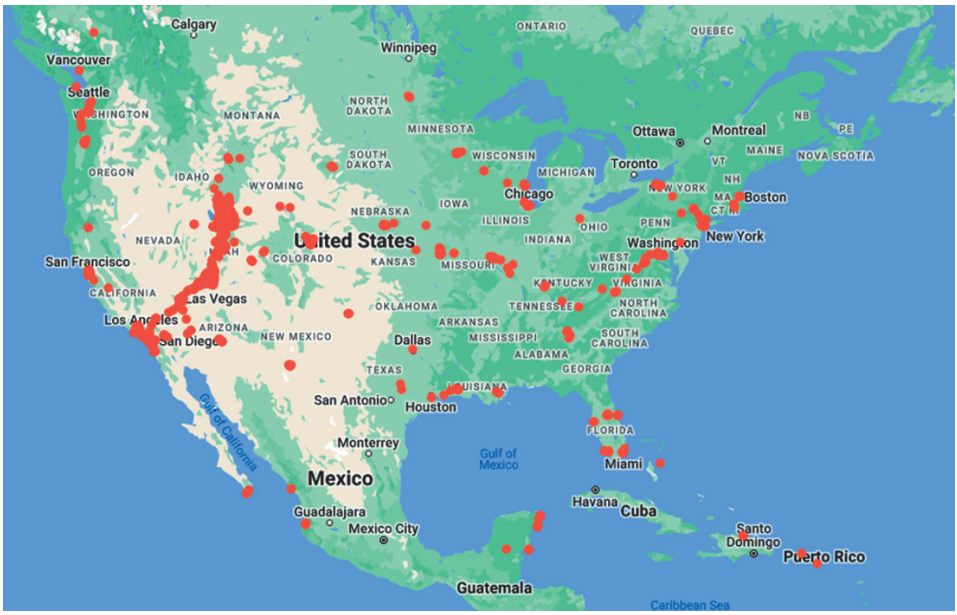
Ograniczanie TWOJEGO cyfrowego śladu

Zanim przejdziemy do prowadzenia dochodzenia OSINT, jako specjaliści z zakresu cyberbezpieczeństwa powinniśmy wiedzieć, jak chronić samych siebie. Czy wiesz, że około 91% przestępstw cybernetycznych rozpoczyna się od prostego e-maila (*https://www.yeoandyeo.com/resource/91-of-cyberattacks-begin-with-a-phishing-email*)?

Na początku atakujący może nawet nie wiedzieć, jak się nazywasz. W miarę zbierania informacji tworzy jednak pełen obraz Twojej cyfrowej tożsamości. W dzisiejszym świecie dane są równie cenne co ropa naftowa. Zdanie sobie sprawy z tego, z jaką łatwością ktoś może zdobyć informacje na nasz temat, jest nie tylko niepokojące, lecz także powinno skłonić nas do działania.

Nasze dane osobowe są wykorzystywane przez cyberprzestępców, stalkerów i szukające korzyści przedsiębiorstwa. Nawet jeżeli sami nie sprzedajemy bezpośrednio tych

informacji, nasze codzienne czynności robią to za nas. Każde zapytanie w wyszukiwarce Google, każdy post w mediach społecznościowych, a nawet każdy produkt, który przeglądamy w sklepie internetowym, uzupełnia nasz profil — profil, którego sami nie stworzyliśmy (rysunek 2.4).



Rysunek 2.4. Firma Google śledzi nas za pomocą naszego telefonu (*https://timeline.google.com*)

Dlaczego ochrona danych osobowych jest obecnie ważniejsza niż kiedyś?

Naruszenia danych stwarzają zagrożenie nie tylko tu i teraz. Mają dalekosiężne konsekwencje, łącznie z ryzykiem kradzieży tożsamości czy nawet naruszenia bezpieczeństwa fizycznego osób. Ich wpływ jest wielowymiarowy. Na przykład podszywający się pod nas oszuści mogą zaciągnąć pożyczkę, realizować nielegalne transakcje, a nawet dokonywać poważniejszych przestępstw. Oczyszczenie się z zarzutów jest nie tylko trudne, lecz również wyniszczające finansowo i emocjonalnie.

Naruszenia danych mogą mieć istotny wpływ na nasze życie prywatne. Na przykład potencjalny pracodawca może znaleźć nierzetelne lub niekorzystne informacje na nasz temat, co może zaszkodzić naszej reputacji, zanim w ogóle będziemy mieć szansę zaprezentować swoje umiejętności.

Stawka jest wysoka, a prawdopodobieństwo nie działa na naszą korzyść. Nie poddawajmy się jednak cyfrowemu przeznaczeniu. Oto kilka wskazówek, które nie tylko

zwiększą naszą cyfrową świadomość, lecz również możliwości. Nasze dane osobowe są cenne. Czas zacząć je traktować w ten sposób.

Przeglądarki internetowe — pierwszy front walki o dane

Przeglądarka to przyjacielsko usposobiony pośrednik, który umożliwia nam swobodne poruszanie się po cyfrowej autostradzie informacyjnej. Tutaj czytamy wiadomości, oglądamy filmy, prowadzimy potyczki w mediach społecznościowych czy co tam nam w duszy gra. Pod tą sympatyczną fasadą czai się jednak aparat gromadzenia danych, który zawstydziłby amerykańską agencję wywiadowczą NSA. Nie, nie chodzi mi o to, żeby napchać Ci głowę teoriami spiskowymi. Niemniej jednak lepiej zapamiętaj moje słowa: „To, że nie widzisz czarnych helikopterów, nie znaczy, że ich tam nie ma!".

Własne i zewnętrzne pliki cookie

Układ pokarmowy przeglądarki wypełniają różne rodzaje ciasteczek:

- **Własne pliki cookie**. Zapisywane przez witrynę internetową, którą odwiedzamy. Pamiętają nasze ustawienia, zawartość koszyka z zakupami i inne tajemnice.
- **Zewnętrzne pliki cookie**. Zdeponowane przez kogoś innego niż witryna internetowa, na której przebywamy, np. przez reklamodawców. Te pliki cookie nie odstępują nas na krok podczas naszej podróży po sieci, podsuwając nam pod nos tę parę butów, którą kiedyś zostawiliśmy w koszyku.

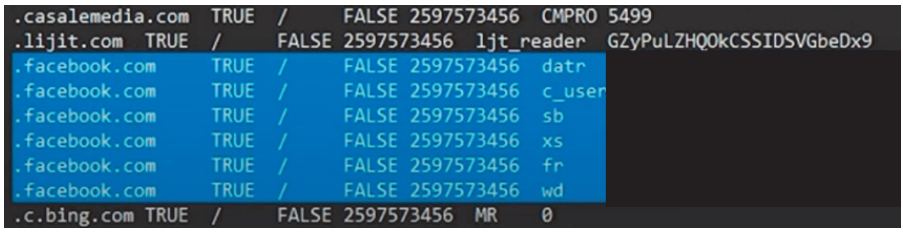
W jaskini ciasteczkowego potwora

Narzędzie nazywane **złodziejem ciasteczek** (ang. *cookie grabber*) zostało stworzone z myślą o przechwytywaniu plików cookie. Czy to groźne? Tak, złodziej ciasteczek może wykradać oba rodzaje ciasteczek, w tym te, które zawierają dane do logowania.

Dajmy na to, że wchodzimy na stronę, na której czyha na nas złodziej ciasteczek. Nieświadomi zagrożenia logujemy się na tej stronie, a nasze sesyjne pliki cookie wędrują do kieszeni złoczyńcy. W ten sposób atakujący zdobył klucz do naszego cyfrowego królestwa i uzyskał dostęp do wszystkich kont na innych platformach, a wszystko dzięki prostemu trikowi, którego nikt nawet nie zauważył.

To jednak nie wszystko. Niektóre witryny internetowe przechowują dane do logowania (tzn. nazwę użytkownika i hasło) w formie niezaszyfrowanego tekstu bezpośrednio w przeglądarce. W takim przypadku, gdy logujesz się w witrynie, przechowuje ona wpis z danymi uwierzytelniającymi w formacie czytelnym dla każdego. Jeżeli Twój komputer dostał się w niepowołane ręce lub pracujesz na współdzielonym urządzeniu, ktoś może użyć prostych narzędzi, takich jak edytor heksadecymalny, aby wykraść te dane. To tak, jakbyśmy zostawili klucze od domu na ławce w parku i poszli sobie dalej.

Wyobraź sobie logowanie na stronie internetowej, która nie podchodzi poważnie do kwestii prywatności. Dane do logowania są przechowywane w pliku cookie w formie niezaszyfrowanej. Nam się do niczego nie przydadzą, ale haker — a nawet wścibski współlokator — może z łatwością wydobyć te informacje i zalogować się na nasze konto jak na swoje własne (rysunek 2.5).



Rysunek 2.5. Dzięki złodziejowi ciasteczek można ukraść cudze konto lub tożsamość

Jak się chronić?

Zarówno sieci VPN, jak i konfigurowanie **łańcuchów serwerów pośredniczących** (ang. *proxy chaining*) to skuteczne sposoby ochrony prywatności w internecie. Dzięki nim można ukryć własny adres IP, utrudniając zewnętrznym plikom cookie śledzenie naszych działań. To szczególnie ważne w dzisiejszym cyfrowym świecie, gdzie śledzenie użytkowników i ochrona danych stanowią istotne zagadnienia. Ważne jest jednak, aby wybrane przez nas sieci VPN i serwery proxy były godne zaufania, ponieważ one również mają dostęp do naszych danych. Zawsze preferuj usługi, które są znane z rygorystycznych zasad ochrony prywatności i zaangażowania na rzecz bezpieczeństwa użytkownika.

DuckDuckGo — cichy bohater ochrony prywatności

Jeżeli przyrównać mainstreamowe przeglądarki do szukających poklasku celebrytów, DuckDuckGo (rysunek 2.6) jest introwertycznym geniuszem, którego nikt nie słucha, choć wszyscy powinni. Misją DuckDuckGo jest uproszczenie ochrony prywatności online. Ta odważna firma zabezpiecza użytkownika przed śledzeniem podczas jego podróży po internecie, a jej zapora sieciowa blokuje próby dostępu do historii przeglądania i danych osobowych.

Produkty DuckDuckGo są stworzone z myślą o tym, aby oddać nam kontrolę nad naszymi danymi. Ta wyszukiwarka nie zbiera historii zapytań ani danych użytkownika. Wszystkie wyszukiwania są domyślnie poufne. Rozszerzenie do przeglądarki i aplikacja mobilna również blokują agresywne skrypty śledzące, które czyhają na nas w sieci.

Szyfrowanie stanowi kolejną warstwę ochrony, która zabezpiecza połączenia między użytkownikiem a stronami internetowymi. Wspólnie te narzędzia tworzą skuteczną tarczę chroniącą prywatność przed profilowaniem ze strony reklamodawców i innych zewnętrznych firm.



Rysunek 2.6. DuckDuckGo to wspaniała przeglądarka pozwalająca użytkownikom zachować prywatność

Działalność biznesowa DuckDuckGo pokrywa się z misją stawiania prywatności na pierwszym miejscu. Firma zarabia dzięki reklamom dobranym na podstawie słów kluczowych — zamiast reklam bazujących na profilach osobowych, które ciągną się za nami jak koszmary z przeszłości.

Gotowi na dobrą zmianę? Doskonale. Nie da się jednak z dnia na dzień zapomnieć o jednym sposobie życia i skoczyć na główkę w inny. Na taką zmianę trzeba się przygotować:

1. **Pobierz i zainstaluj**. Wybierz swoją bezpieczną przeglądarkę.
2. **Zaimportuj ustawienia**. Większość przeglądarek pozwala importować zakładki i ustawienia z innych przeglądarek.
3. **Ustaw jako domyślną**. Ustaw nową przeglądarkę jako domyślną do wszystkich celów.

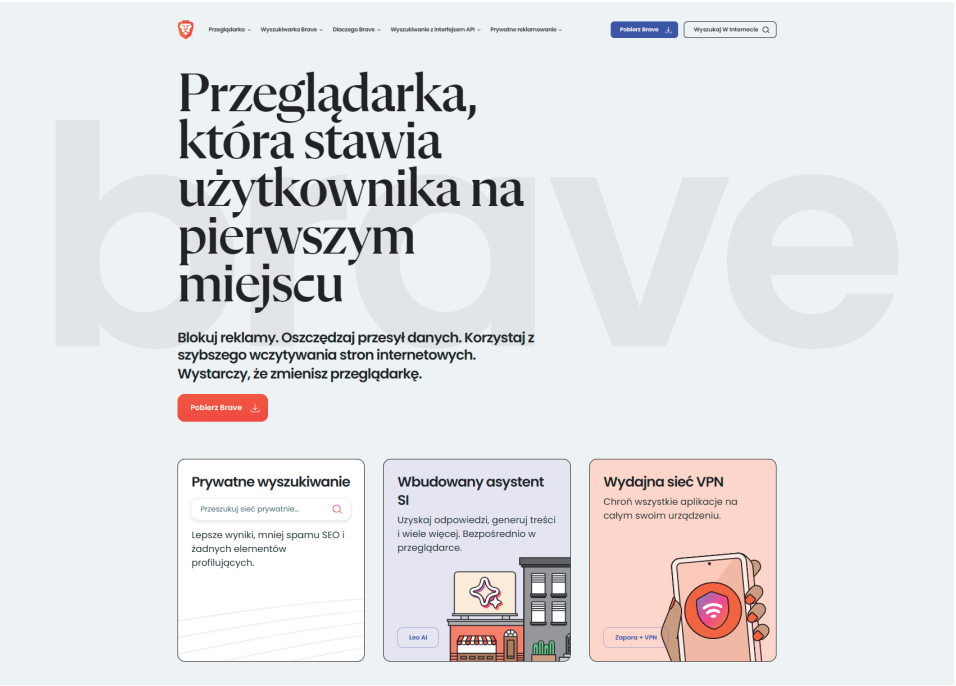
Alternatywne przeglądarki — wady i zalety

DuckDuckGo nie jest jedynym rycerzem na białym koniu, który może pospieszyć nam na ratunek. Są też inne przeglądarki, a każda z nich ma swoje słabe i mocne strony.

Przeglądarka Brave

To tę przeglądarkę polecam wszystkim. Jest to relatywnie nowy produkt na rynku.

Brave (*https://brave.com*) to wspaniały punkt wyjścia do ukrycia naszych działań w internecie przed ciekawskim wzrokiem (rysunek 2.7). Domyślnie blokuje narzędzia śledzące, ograniczając firmom zewnętrznym możliwość śledzenia nas.

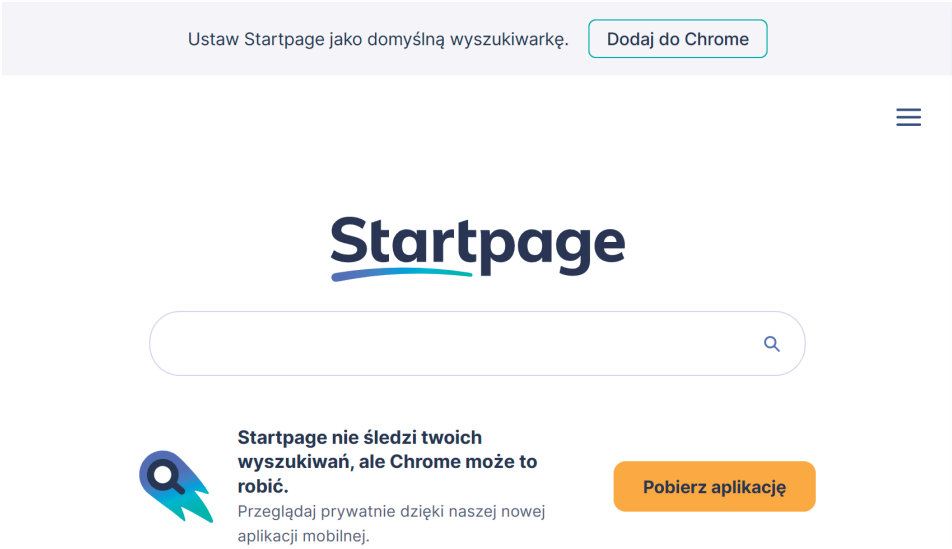


Rysunek 2.7. Przeglądarka Brave — mój osobisty faworyt w dziedzinie ochrony tożsamości

Jeżeli niechętnie podchodzisz do zmiany przeglądarki, dodam, że rozszerzenia takie jak Startpage zapewniają podobne zabezpieczenia.

Startpage wyświetla ocenę prywatności strony na skali od jednego do pięciu, pozwalając użytkownikowi zobaczyć, jak wiele skryptów śledzących i plików cookie uniknięto na każdej stronie (rysunek 2.8). Szczegółowe informacje mogą zaskoczyć, ale są bardzo pomocne. Startpage ukrywa tożsamość użytkownika przed wszelkimi skryptami śledzącymi poprzez maskowanie jego cyfrowego śladu.

Chcemy zablokować skrypty śledzące, ale możemy potrzebować niektórych nieszkodliwych plików cookie, aby umożliwić stronom poprawne funkcjonowanie. Startpage umożliwia zatwierdzanie konkretnych plików cookie bez zezwalania na nieograniczony dostęp. W przypadku wyszukiwania Startpage przesyła zapytanie do wyszukiwarki Google, ale robi to anonimowo, aby nie przyczyniać się do budowy naszego upiornego profilu.



Rysunek 2.8. Rozszerzenie Startpage w Chrome Web Store

Z potężnymi sojusznikami u swego boku, takimi jak zabezpieczenia przeglądarki Brave oraz ułatwiające podejmowanie decyzji informacje z rozszerzenia Startpage, możesz teraz stanąć do walki ze swoim cyfrowym cieniem. Nigdy więcej nie będziesz bezbronną ofiarą dla cybernetycznych mechanizmów śledzących. Podsumujmy wady i zalety tego rozwiązania:

- **Zalety**: domyślnie blokuje reklamy i skrypty śledzące.
- **Wady**: wbudowany system wyświetlania reklam może nie trafić w nasze gusta.

Przeglądarka Tor

Tor to połączona ze sobą społeczność skupiona wokół wspólnego celu, jakim jest zapewnienie prywatności online. Projekt Tor (rysunek 2.9) zrodził się w duchu buntu. Rządy szpiegują, korporacje śledzą, a Tor przybywa nam na odsiecz! To swoisty ruch oporu online, wyposażony w serwery, serwery-przekaźniki (ang. *relays*) i węzły. Tę infrastrukturę utrzymują ochotnicy z całego świata, a żaden pojedynczy punkt nie ma obrazu pełnej ścieżki.

Tor usuwa metadane i maskuje adresy IP. Komunikacja jest wielokrotnie zaszyfrowana, a w miarę kolejnych skoków przez węzły prywatnej sieci stopniowo odszyfrowywana. To jak zdejmowanie kolejnych warstw cebuli. Każdy serwer pośredniczący potrafi określić jedynie następny przystanek, ale nie zna punktu docelowego.

Jest to możliwe jedynie dzięki dużej liczbie węzłów. Tysiące bezinteresownych ochotników użyczają swoich komputerów jako węzłów sieci Tor. Te zróżnicowane punkty wejścia, przejścia i wyjścia stanowią zdecentralizowany trzon tej sieci. Nie poddające się cenzurze połączenia są szyfrowane w sposób chroniący prywatność.



Rysunek 2.9. Strona projektu Tor

Tor to darmowe oprogramowanie (*https://torproject.org*) stworzone przez społeczność wyznawców prywatności. Kod jest dostępny dla wszystkich do kontroli i modyfikowania. Otwartość źródeł pozwala projektowi Tor realizować swoją misję. Te narzędzia nie mają ukrytych luk czy celów. Podsumujmy wady i zalety tego rozwiązania:

- **Zalety**: zapewnia najwyższy poziom anonimowości.
- **Wady**: korzystanie z przeglądarki jest wolniejsze ze względu na przechodzenie przez wiele serwerów pośredniczących.

„Dale, a od których przeglądarek trzymałbyś się z daleka?" — zapytasz. No cóż, lista wygląda mniej więcej tak, przy czym kolejność nie jest zbyt istotna:

- Google Chrome,
- Microsoft Edge,
- Firefox,
- Opera,
- Safari.

Przeglądarka to nasza pierwsza linia obrony przed cyberzagrożeniami. To nie tylko wrota do internetu. To forteca, która chroni nasze dane. Dokonaj zmiany już dziś i ufortyfikuj swoją przeglądarkę. Twoje cyfrowe „ja" będzie Ci wdzięczne za dodatkową ochronę.

Skarpetkowe pacynki — tworzenie person internetowych i zarządzanie nimi

Zanim nasza wyobraźnia pogalopuje zbyt daleko — nie, nie będziemy zajmować się tworzeniem urokliwych pacynek z ulubionej pary skarpetek. Skarpetkowe pacynki (ang. *sock puppets*) to inaczej fikcyjne tożsamości internetowe utworzone do maskowania,

manipulacji i zbierania informacji. Te postaci, niczym pacynki na dłoni lalkarza, pozwalają nam chować się pod różnymi tożsamościami i prowadzić anonimowe interakcje.

Chociaż nie jest w zasadzie nielegalne, używanie pacynek często nie jest mile widziane ze względu na potencjalne nadużycia. Można je wykorzystywać do szerzenia dezinformacji, sztucznie zwiększać wskaźniki popularności, anonimowo napastować innych i infiltrować społeczności incognito. Uzasadnione zastosowania obejmują z kolei dziennikarstwo śledcze i testy penetracyjne.

Istnieje kilka względów, dla których osoby i organizacje mogą korzystać z kont typu *sock puppet*:

- **Anonimowość**. Najważniejszym powodem jest rozdzielenie działań online od prawdziwej tożsamości, co umożliwia gromadzenie informacji bez utraty anonimowości.
- **Podstęp**. Fikcyjne konta pozwalają wpływać na przebieg rozmów, podawać nieprawdziwe informacje i manipulować percepcją. Można je wykorzystać do infiltracji lub socjotechniki.
- **Rozpoznanie**. Dobry kamuflaż jest potrzebny do zbierania informacji na temat osób, organizacji i innych zagadnień bez wzbudzania podejrzeń.
- **Prywatność**. Niektórzy po prostu chronią swoją prywatność poprzez rozdzielenie swojej działalności online na kilka niepowiązanych tożsamości.

Przygotowanie sceny — tworzymy własną pacynkę

Internetowa persona stworzona do ochrony anonimowości i gromadzenia informacji może być potężnym narzędziem w przypadku etycznego użycia. Konta pacynkowe są niczym cyfrowe kameleony: mogą zlać się z otoczeniem i zbierać dane OSINT bez ujawniania prawdziwej tożsamości analityka. Ta praktyka jest szczególnie cenna w przypadkach, gdy ujawnienie tożsamości mogłoby wypaczyć zdobyte informacje lub stanowić ryzyko dla bezpieczeństwa badacza.

Wyobraźmy sobie na przykład, że ekspert ds. cyberbezpieczeństwa ma za zadanie ocenić bezpieczeństwo instytucji finansowej. W etyczny sposób tworzy fikcyjne konto i dzięki temu może wejść w interakcję ze stronami phishingowymi lub potencjalnymi sprawcami, aby lepiej zrozumieć ich taktykę, bez narażania siebie i instytucji na niepotrzebne ryzyko. Przypomina to pracę policjanta pod przykrywką w cyfrowej dzielnicy. Obserwujemy i zdobywamy informacje, ale nie ingerujemy.

Dodatkowo konta pacynkowe mogą odgrywać istotną rolę w śledzeniu zagrożeń dla cyberbezpieczeństwa. Można je wykorzystać do monitorowania forów w dark webie, infiltrowania sieci cyberprzestępców oraz gromadzenia informacji na temat nadciągających zagrożeń, naruszeń czy sprzedaży ukradzionych danych. Pozwala to specjalistom z zakresu cyberbezpieczeństwa ostrzec potencjalne ofiary i wzmocnić zabezpieczenia, zanim dojdzie do szkody.

Etyczne wykorzystanie fikcyjnych kont w OSINT reguluje ścisły kodeks postępowania. Nie należy ich używać do oszustwa ani manipulacji, lecz raczej jako tarczę do ochrony

tożsamości specjalistów ds. bezpieczeństwa podczas zbierania danych potrzebnych do wzmocnienia cyfrowych zabezpieczeń. To peleryna niewidka dla pozytywnych bohaterów, dzięki której mogą obserwować i zgłaszać problemy bez znajdowania się na celowniku.

Oto kilka kwestii do rozważenia przy tworzeniu konta pacynkowego:

- Jasno określ cel fikcyjnego konta. Może to być badanie naukowe, zbieranie danych czy trening z zakresu cyberbezpieczeństwa. Zawsze miej sformułowany jasny i etyczny cel.
- Tworzenie pacynki zaczynamy od przygotowania wiarygodnej persony. Przypomina to tworzenie postaci do sztuki teatralnej. Potrzebujemy jakiejś przeszłości, zainteresowań, a także osobliwości. Narzędzia takie jak Fake Name Generator (*https://www.fakenamegenerator.com*) czy NameFake (*https://namefake.com*) to nasi najlepsi pomocnicy, jeżeli chcemy stworzyć wiarygodnie wyglądającą tożsamość.

  Oprócz imienia i nazwiska nasza pacynka potrzebuje również:

  - daty i miejsca urodzenia,
  - miejsca zamieszkania,
  - wykształcenia i zatrudnienia,
  - zainteresowań i hobby,
  - ulubionych książek, filmów i muzyki,
  - poglądów politycznych,
  - wyznania,
  - zdjęć i obrazów.

  Niektórzy nazwą te kroki **pretextingiem**.

Uwaga

Pretexting polega nie tylko na udawaniu, że jest się kimś innym. Wymyśla się również przeszłość, tło wydarzeń i wypowiedzi, aby uczynić wszystko bardziej wiarygodnym.

- Musimy dysponować zdjęciem lub awatarem persony, aby nasze fikcyjne konto wyglądało możliwie najbardziej wiarygodnie. Strona internetowa pod adresem *https://thispersondoesnotexist.com* to fantastyczne narzędzie do generowania zdjęć osób za pomocą sztucznej inteligencji (rysunek 2.10). W ten sposób nikt nie może wyszukać źródła obrazu w internecie, żeby dowiedzieć się, że go sobie od kogoś pożyczyliśmy.
- Potrzebujemy również specjalnego konta e-mailowego dla naszej persony. Możemy skorzystać z takich usług jak 10 Minute Mail (*https://10minutemail.net*), dzięki którym można stworzyć jednorazowe adresy e-mailowe wygasające po upływie określonego czasu.



Rysunek 2.10. Obraz wygenerowany przez sztuczną inteligencję (*https://thispersondoesnotexist.com*)

- Utwórzmy dla naszej pacynki również jakieś konta i profile w mediach społecznościowych.

Uwaga

Pamiętaj, że kluczem do sukcesu w tym przypadku jest konsekwencja. Ta sama persona powinna istnieć na różnych platformach.

- Korzystaj z sieci VPN (takich jak *https://www.expressvpn.com*) do zamaskowania swojego adresu IP i rozważ użycie przeglądarek, które chronią prywatność, takich jak Tor (*https://www.torproject.org*), aby utrzymać swoją prawdziwą tożsamość ukrytą za kulisami.

  Kiedyś przeprowadzał ze mną wywiad pewien reporter. Wolałem zachować anonimowość, więc zdecydowałem się użyć przeglądarki Tor, która szyfruje komunikację poprzez przekierowanie jej przez kilka serwerów z różnych części świata. Dodatkowo skorzystałem z szyfrowanego komunikatora dostępnego w dark webie. Dzięki temu mogłem bezpiecznie się z nim komunikować. Nasze rozmowy były w pełni prywatne. Nie było ryzyka namierzenia nas.

- Nie zapomnij o numerze telefonu dla swojej pacynki! Używając usługi takiej jak TextFree (*https://textfree.us*), możesz wysyłać i odbierać wiadomości tekstowe bez ujawniania swojego prawdziwego numeru telefonu. To niezłe rozwiązanie.

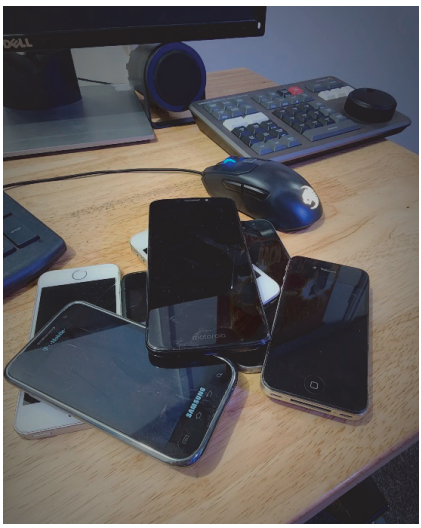
Nawiązywanie anonimowej komunikacji

Aby uniemożliwić powiązanie fikcyjnego konta pacynkowego z jego twórcą, niezbędne są anonimowe kanały komunikacji. Obejmuje to tworzenie niemożliwych do śledzenia adresów e-mailowych oraz przygotowanie telefonów na kartę z tymczasowymi numerami (ang. *burner phone*).

Tworząc adres e-mailowy dla pacynki, weź pod uwagę następujące kwestie:

- Unikaj nietypowych dostawców, którzy mogą wzbudzić podejrzenia.
- Używaj popularnych serwisów, takich jak Gmail czy Outlook.
- Twórz adresy z publicznych sieci wi-fi lub przez sieć VPN, aby zachować anonimowość.
- Adres e-mailowy musi wyglądać wiarygodnie i nie może składać się z przypadkowych znaków.
- Adresu e-mailowego użyjemy do rejestrowania kont, więc anonimowość jest ważna.

Telefony na kartę to ostatni element utrzymania śledztwa w tajemnicy (rysunek 2.11). Trzeba z nich jednak korzystać rozważnie. Używaj takiego telefonu jedynie do spraw bezpośrednio związanych z dochodzeniem: rozmów, wiadomości tekstowych, kodów uwierzytelniających itp.



Rysunek 2.11. Niektóre z moich telefonów na kartę, których używałem w trakcie dochodzeń

Należy też pamiętać, że w Polsce od 2017 r. nie jest możliwe korzystanie z karty SIM w usługach przedpłaconych bez rejestracji z użyciem imienia i nazwiska oraz numeru PESEL. Ogranicza to istotnie poziom anonimowości oferowany przez takie usługi.

Nigdy nie zapisuj poufnych dokumentów, nazw, dat, lokalizacji czy innych danych dotyczących sprawy na tym urządzeniu. Pamiętaj, że takie telefony nadal można podsłuchiwać, zhakować czy przejąć, pomimo że są jednorazowego użytku. W związku z tym podejmij dodatkowe środki ostrożności, a mianowicie korzystaj z komunikatorów szyfrujących wiadomości, takich jak Signal czy WhatsApp, unikaj wiązania telefonów na kartę z prywatnymi kontami, wyłącz GPS, usuń metadane z obrazów i regularnie

czyść pamięć podręczną. Używaj nazw kodowych zamiast prawdziwych do kontaktu ze źródłami.

Podczas dochodzenia OSINT odpowiedzialne zarządzanie telefonami na kartę to istotny etap w cyklu życia sprawy. Gdy dochodzenie zostaje zamknięte lub istnieją wątpliwości co do bezpieczeństwa korzystania z takiego telefonu, należy wycofać urządzenie z użytku w sposób bezpieczny i profesjonalny. Istnieją dwa dopuszczalne podejścia:

- **Odpowiedzialna archiwizacja**. Przypomina to postępowanie z innymi poufnymi materiałami po zakończeniu dochodzenia, gdzie konieczne jest utrzymywanie jasnego łańcucha dowodowego. Należy zdeponować telefon w bezpiecznym miejscu wraz z oprogramowaniem i wszelkimi innymi użytymi narzędziami. Dzięki temu mamy pewność, że zasoby, dane i potencjalne dowody znajdują się w nienaruszonym stanie i pod odpowiednim nadzorem. Nie chodzi tutaj o gromadzenie sprzętu, lecz o staranne rozdzielenie obowiązków i nienaganne utrzymywanie standardów zawodowych.
- **Staranny demontaż**. Zacznij od zresetowania urządzenia do ustawień fabrycznych, aby usunąć wszelkie dane, co jest standardową procedurą w branży. Następnie rozmontuj urządzenie. Usuń kartę SIM i zadbaj o to, aby nie nadawała się do dalszego użytku. Może to obejmować pocięcie jej na kawałki, aby zapobiec odzyskaniu danych. Jest to metoda sugerowana przez protokoły bezpieczeństwa. Dalsze rozmontowanie urządzenia, w tym oddzielenie baterii od innych podzespołów, ma zagwarantować, że żadne komponenty umożliwiające odzyskanie danych nie wpadną w niepowołane ręce. Utylizację należy przeprowadzić dyskretnie i w kilku miejscach, aby ograniczyć ryzyko odtworzenia danych.

To nie jest fragment kryminału, lecz chleb powszedni etycznego hakowania i profesjonalnego prowadzenia cyfrowych dochodzeń. Telefon na kartę to tarcza, która zarówno chroni anonimowość analityka, jak i zapewnia rzetelność jego pracy. Korzystanie z tych urządzeń, a następnie ich utylizacja, to świadectwo zawodowego zaangażowania na rzecz bezpieczeństwa i ochrony danych w dziedzinie, gdzie stawka jest zawsze wysoka.

Pamiętajmy o tym, że wszystkie kroki, jakie podejmujemy, mają na celu zwiększenie bezpieczeństwa i odkrycie podatności, zanim ktoś wykorzysta je do złych celów. Nasze praktyki są przejrzyste dla klientów i nie wykraczają poza granice prawa, dzięki czemu nasza praca jest zawsze spójna z celem ochrony zasobów i informacji w świecie, który jest w coraz większym stopniu zależny od cyfrowej infrastruktury.

Dzięki anonimowym, niepodatnym na śledzenie kanałom komunikacji nie będzie możliwe powiązanie kont pacynkowych z ich twórcami. Konta te będą żyć własnym życiem, gwarantując prywatność i kamuflaż, które mają kluczowe znaczenie w pracy analityka OSINT.

Pociągając za sznurki — agent Pacyna w akcji

Teraz, gdy nasza pacynka jest gotowa pojawić się na cyberscenie, musimy pamiętać o kilku zasadach etyki:

- **Transparentność wobec interesariuszy**. Jeżeli używamy fikcyjnych kont w działalności badawczej lub kontroli w ramach przedsiębiorstwa, musimy zachować transparentność wobec interesariuszy na temat metod i intencji.
- **Ochrona danych**. Bądźmy czempionami ochrony danych. Zbierajmy tylko te dane, które są niezbędne do prowadzenia dochodzenia, i podchodźmy do nich z najwyższą odpowiedzialnością.
- **Dokumentowanie i sprawozdania**. Należy prowadzić szczegółowy rejestr czynności wykonywanych z fikcyjnych kont. To nie tylko ułatwia prezentację wyników, lecz również zapewnia rozliczalność z przeprowadzonych działań.

Wykorzystanie dynamiki płci w działaniach z fikcyjnych kont

Na cybernetycznej scenie wywiadowczej zbudowanie swojego cyfrowego alter ego jest w połowie sztuką, a w połowie nauką i wymaga umiejętnego balansowania na etycznej linie rozciągniętej nad cyfrowym światem, zwłaszcza jeżeli chodzi o dynamikę płci. Tak, internet pełen jest stereotypów na temat płci, ale kiedy tworzymy personę, musimy podchodzić do tych uogólnień z ostrożnością.

Wyobraźmy sobie, że wybraliśmy żeńską postać jako swój kamuflaż. To prawda, że bycie kobietą może okazać się pomocne w niektórych sytuacjach ze względu na sposób, w jaki ludzie prowadzą interakcje społeczne. Pamiętajmy jednak, że nie jesteśmy tutaj po to, aby kogoś oszukiwać dla przyjemności. Musimy działać inteligentnie, a nie podstępnie. Możemy na przykład posłużyć się metodą „na wabia", zachowywać się odrobinę zalotnie i bezradnie, aby zdobyć uwagę celu. W takich przypadkach należy jednak zdecydowanie pamiętać o tym, aby działać etycznie. Chodzi o gromadzenie informacji w sprytny sposób, a nie o zwodzenie lub wykorzystywanie innych.

Gdy chcemy stworzyć wiarygodne konto typu *sock puppet*, diabeł tkwi w szczegółach. Dajmy sobie spokój z powielaniem stereotypów i wyposażmy naszą pułapkę w prawdziwą osobowość. Kilka niepowtarzalnych cech sprawi, że pacynka stanie się czymś więcej niż zbiorem pikseli — zyska głębię i wiarygodność, które mogą wzbudzić zaufanie tam, gdzie to najbardziej potrzebne.

Uwaga

Oto kilka profesjonalnych porad. Całkowicie odseparuj życie swojego fikcyjnego „ja" od życia prywatnego. Używaj maszyn wirtualnych, przeglądarek w trybie piaskownicy i tym podobnych rozwiązań. Mieszanie tych dwóch bytów to jak założenie skarpet do sandałów. Tak się po prostu nie robi. Dzięki temu mamy solidną przykrywkę oddzieloną grubym murem od naszej prawdziwej tożsamości.

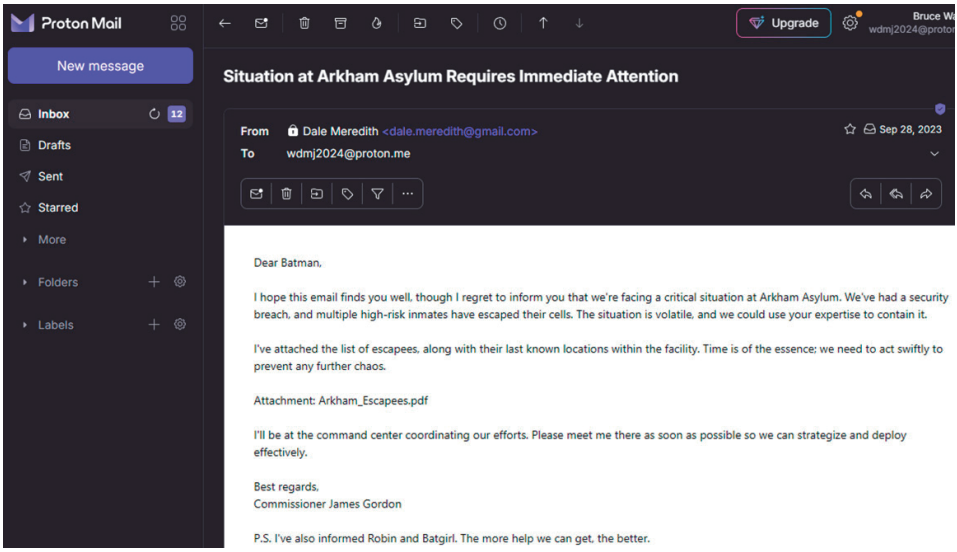
Gdy działamy w słusznej sprawie, te wszystkie pacynkowe akrobacje są jak najbardziej uzasadnione. To sprawdzony sposób na infiltrację podejrzanych cyfrowych klik, wykrywanie cyberzagrożeń, udawanie żółtodzioba we własnej firmie czy sprawdzenie, kto złapie się na phishingową przynętę. Przywdziewamy cybernetyczną pelerynę niewidkę i używamy swoich supermocy w służbie dobra.

Podsumowując: działajmy mądrze i etycznie. Pamiętajmy, że mamy zwalczać przestępców, a nie dołączyć do ich szeregów.

Anonimowe e-maile i wiadomości tekstowe

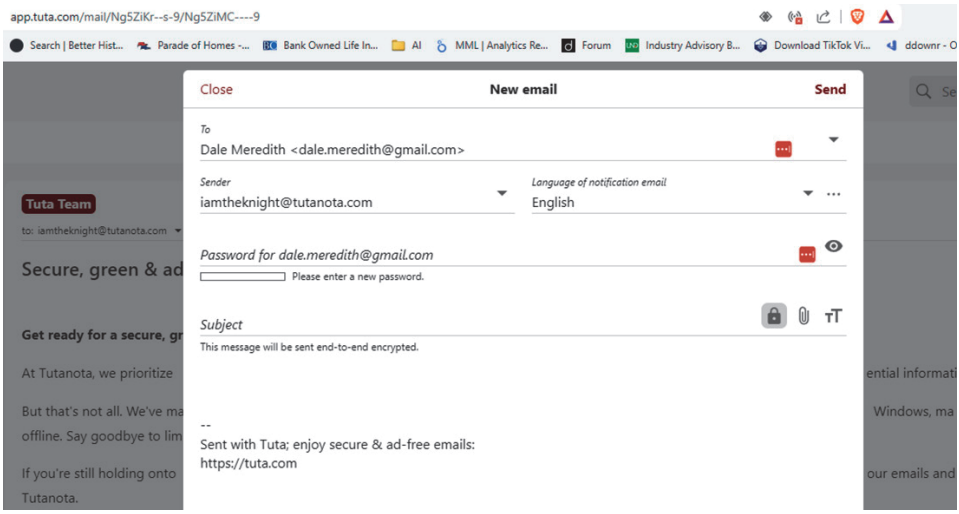
Korzystanie z anonimowych adresów e-mailowych to sprawa najwyższej wagi dla analityków OSINT, którzy pragną ukryć swoją tożsamość i zachować anonimowość w interakcjach online. Adresy e-mailowe często stanowią wrota do prawdziwej tożsamości danej osoby, gdyż dostarczają różnych wskazówek i ujawniają powiązania. Bez dbałości o anonimowość badacze OSINT ryzykują wyciekiem swoich danych osobowych, np. jeżeli ich adres e-mailowy zostanie powiązany z forami, usługami czy mediami społecznościowymi użytymi w ramach dochodzenia. Może to narazić badaczy na ataki hakerskie, nękanie poprzez publikowanie informacji na ich temat (ang. *doxing*), zemstę czy niepożądane powiązania z różnymi grupami i ruchami.

Tworzenie adresów e-mailowych w żaden sposób nie powiązanych z danymi identyfikującymi analityka OSINT ma kluczowe znaczenie dla bezpieczeństwa i prywatności. Z anonimowych adresów e-mailowych nigdy nie należy korzystać do realizowania działań, które mogłyby prowadzić do ujawnienia danych osobowych. Nie może to być adres zarejestrowany w mediach społecznościowych, portalach zawodowych takich jak LinkedIn, sklepach internetowych itd. Użycie odpowiedniej usługi, takiej jak Proton Mail (*https://protonmail.com*), byłoby najlepszym rozwiązaniem (rysunek 2.12).



Rysunek 2.12. Usługa Proton Mail pomaga w ukryciu prawdziwej tożsamości

Inną usługą, z której można skorzystać, jest Tuta (*https://tuta.com*). Do utworzenia konta nie są wymagane żadne prawdziwe dane osobowe (rysunek 2.13).



Rysunek 2.13. Anonimowe konto e-mailowe Tuta

Korzystanie ze specjalnie założonych anonimowych adresów e-mailowych pozwala analitykom OSINT rejestrować się na forach, zadawać pytania i prowadzić rozmowy bez obaw o bezpieczeństwo ich prawdziwej tożsamości. To istotna linia obrony przed utratą anonimowości.

Aktualizowanie wiedzy na temat cyberzagrożeń

Prowadzenie dochodzeń OSINT jest nierozłącznie powiązane z ryzykiem dla cyberbezpieczeństwa. Zachowanie prywatności i anonimowości w internecie to fundamentalne zasady etycznego białego wywiadu. Dlatego zajmujące się nim osoby nie mogą sobie pozwolić na to, aby zostać w tyle za nowymi zagrożeniami technologicznymi. Muszą na bieżąco śledzić nowinki w dziedzinie bezpieczeństwa, uczyć się na cudzych błędach i doskonalić warsztat.

Uzyskiwanie bieżących informacji na temat prywatności i bezpieczeństwa

Monitorowanie wiadomości z zakresu cyberbezpieczeństwa i prywatności pomaga zrozumieć stale zmieniający się profil ryzyka. Zasubskrybuj serwis monitorujący zagrożenia, taki jak jeden z tutaj wymienionych, aby otrzymywać powiadomienia na temat nowych podatności i ataków:

- newsletter ze strony Cybersecurity Threats organizacji Center for Internet Security (CIS) (*https://www.cisecurity.org/cybersecurity-threats*),

- biuletyny Agencji ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury Stanów Zjednoczonych (ang. *Cybersecurity and Infrastructure Security Agency*, CISA) (*https://www.cisa.gov/news-events/bulletins*).

Osobiście polecam biuletyny CISA. Nie tylko nie faworyzują żadnego z dostawców, lecz również są niezwykle drobiazgowe (rysunek 2.14).



Rysunek 2.14. Biuletyny CISA

Jeżeli chcesz być asem cyberbezpieczeństwa, polecam też lekturę branżowych blogów i serwisów informacyjnych, takich jak te:

- *Krebs on Security* (*https://krebsonsecurity.com*),
- *Privacy News* (*https://www.privateinternetaccess.com/blog*),
- *SCHMOOZE OSINT* (*https://www.sangoma.com*).

Dzięki tym zasobom będziesz mieć aktualne informacje o tym, co się dzieje w tej branży.

Należałoby również przysłuchiwać się, co mówią najważniejsze osobistości w dziedzinie bezpieczeństwa informacji w mediach społecznościowych, i w miarę możliwości brać udział w konferencjach, takich jak DEF CON, Black Hat czy BSides.

Uczenie się na podstawie wcześniejszych naruszeń i incydentów

Analizowanie już zakończonych dochodzeń w sprawie dużych naruszeń może owocować ważnymi spostrzeżeniami. Atak na LinkedIn z 2016 r. (*https://www.forbes.com/sites/daveywinder/2024/01/23/massive-26-billion-record-leak-dropbox-linkedin-twitterx-all-named/?sh=2ab1fc93ab58*) pokazuje, w jaki sposób dane ukradzione stronie trzeciej uruchomiły lawinę powiązanych ataków. Kampanie doxingu i innych form prześladowania przeciwko znanym osobom, takie jak Gamergate (*https://www.nytimes*

.com/interactive/2019/08/15/opinion/what-is-gamergate.html), rzucają nieco światła na rzeczywiste szkody, jakie może wyrządzić OSINT, jeżeli użyjemy go jako broni. Badanie praktyk samozwańczych detektywów uwidacznia również ryzyka, związane między innymi ze stosowaniem zabiegów socjotechnicznych, których etyczna praktyka OSINT powinna unikać.

Podsumowanie

Solidne zabezpieczenia własnej anonimowości stanowią pierwszą linię obrony analityka OSINT. Regularnie wyszukuj swoje imię i nazwisko online, aby ocenić swój cyfrowy ślad i usunąć wszelkie wycieki danych osobowych. Korzystaj z narzędzi takich jak przeglądarka Tor, wirtualne numery telefonów i anonimowe konta e-mailowe, aby zabezpieczyć swoją prawdziwą tożsamość. Postaw grubą kreskę między różnymi tożsamościami. Używaj oddzielnych urządzeń i kont do działań OSINT. Uczyń z nieustannego podnoszenia swoich kompetencji w dziedzinie prywatności priorytet — co chwilę bowiem mamy do czynienia z nowymi zagrożeniami.

Etyczni analitycy OSINT potrafią zagwarantować sobie osobiste bezpieczeństwo i prowadzić badania bez zbędnego ryzyka dzięki ostrożności w tym zakresie. Zagrożenia stale ewoluują, więc nie możemy spocząć na laurach, jeżeli nie chcemy pozostać w tyle. Na tym zakończymy na razie temat anonimowości, a za chwilę przedstawię metody i techniki, które mamy do dyspozycji podczas dochodzeń OSINT.

Narzędzia OSINT — metody i techniki gromadzenia i analizowania informacji

Rozdział 3

Rozsiądź się wygodnie w fotelu, ponieważ zaraz wyruszymy w oszałamiającą podróż po tętniącym życiem ekosystemie **OSINT**. W tym rozdziale będziemy odkrywać tajemnice OSINT. Poznamy istotę białego wywiadu, dla którego każdy strzępek informacji to krok milowy na drodze do opanowania sztuki etycznego hakowania.

Od odszyfrowywania języka sieci po wcielenie się w rolę cyfrowego detektywa — to będzie jazda bez trzymanki przez cyberprzestrzeń. Nie martw się jednak. Nie zapomniałem o odrobinie humoru, aby osłodzić nieco proces zdobywania wiedzy.

Jakie ekscytujące atrakcje zaplanowaliśmy na tej trasie? Oto mały przedsmak czekającej nas przygody:

- wstęp do metod i technik OSINT;
- przeszukiwanie i przeglądanie ogólnodostępnych warstw internetu;
- przeszukiwanie i przeglądanie głębszych i mroczniejszych warstw internetu;
- analiza danych przestrzennych i obrazów;
- automatyzacja zbierania i analizy danych OSINT.

W ramach tego rozdziału osiągniesz biegłość w gromadzeniu i analizowaniu danych z ogólnodostępnych źródeł w sposób finezyjny i etyczny. Twoja skrzynka z narzędziami wypełni się po brzegi strategiami i technikami, które pomogą Ci w pełnej zapału eksploracji świata OSINT.

Wstęp do metod i technik OSINT

W branży OSINT dostępne są różnorodne techniki i metody. Te narzędzia umożliwiają współczesnym analitykom wydajne wykorzystywanie ogromnych ilości danych. Niezależnie od tego, czy chodzi o eksplorację mniej znanych obszarów internetu, czy o analizę danych przestrzennych, narzędzia OSINT odgrywają kluczową rolę w odkrywaniu cennych informacji. Zagłębmy się teraz w niektóre z technik niezbędnych dla etycznego hakowania i zbierania informacji.

Zapakuj prowiant na drogę, usiądź wygodnie w fotelu i pozwól mi zabrać się na przejażdżkę, podczas której będziemy podziwiać te techniki. Każda z nich jest niczym gwiazda na migoczącym niebie etycznego hakowania i białego wywiadu. Pasy zapięte?

Różnorodność technik OSINT

W rozległej dziedzinie OSINT istnieje całe mnóstwo technik i metod, które otwierają różne możliwości gromadzenia i analizowania informacji. Te techniki to nasz zestaw narzędzi do etycznego hakowania i prowadzenia wywiadu. Przyjrzyjmy się dokładniej niektórym z nich. W drogę!

Web scraping

Pozyskiwanie danych ze stron internetowych za pomocą oprogramowania (ang. *web scraping*), zwane dosłownie „skrobaniem" sieci, to fundament OSINT. Ta technika umożliwia szybkie i wydajne zbieranie dużych ilości danych.

Oto kilka korzyści, jakie web scraping zapewnia specjalistom w dziedzinie bezpieczeństwa:

- **Wygodna automatyzacja**. Wyobraź sobie, że masz niestrudzonego cyfrowego asystenta, wyposażonego w skrypty w językach programowania takich jak Python. Przegląda on strony internetowe w poszukiwaniu cennych informacji, podczas gdy Ty w tym czasie popijasz kawę. Tak mniej więcej działa web scraping. To prawdziwa supermoc zbierania danych!
- **Tylko najlepsze kąski**. Gdy wyruszamy na poszukiwanie skarbów w bezkresnych odmętach internetu, technika web scrapingu pomaga odnaleźć dokładnie te informacje, których potrzebujemy. Mogą to być dane kontaktowe z katalogów internetowych albo gorące newsy z forów technicznych — niezależnie od tematu web scraping pozwala dotrzeć do tych danych szybko i sprawnie.
- **Stała kontrola**. Web scraping stoi na straży. Korzystając z tej techniki, możemy monitorować strony internetowe i uzyskiwać informacje o wszelkich zmianach. To niezwykle wygodne, gdy chcemy trzymać rękę na pulsie i otrzymywać informacje o aktualizacjach i powiadomieniach ze stron, które nie umożliwiają subskrypcji.

- **Podróż w czasie**. Narzędzia do web scrapingu są niczym wehikuły czasu, jeżeli chodzi o zawartość stron internetowych. Mogą wykonywać regularne migawki, umożliwiając sprawdzenie, co się zmieniło wraz z upływem czasu. To prawdziwe zbawienie, gdy musimy odnieść się do treści, które zostały zaktualizowane lub usunięte.
- **Odkrywanie głębszego sensu**. Gdy już mamy wszystkie te dane na tacy, przywdziewamy prochowiec detektywa i szukamy wskazówek i powiązań. To jak układanie puzzli. Trzeba rozszyfrować, co to wszystko znaczy i jak wiąże się z szerszą perspektywą danej sprawy.
- **Turbodoładowanie procesu badawczego**. Wszystkie niepowiązane szczegóły pochodzące z przeszukiwania sieci można połączyć z innymi danymi, zwiększając efektywność badań. Można to przyrównać do mieszania kolorów w poszukiwaniu idealnego odcienia do obrazu, aby wzbogacić go o głębię i kontekst.

Jeżeli chodzi o narzędzia do web scrapingu, wybór często pada na język programowania Python w połączeniu z takimi bibliotekami jak Beautiful Soup. Możesz zacząć od odwiedzenia strony *https://www.crummy.com/software/BeautifulSoup*. Beautiful Soup pomaga błyskawicznie przemierzać kod HTML i XML stron internetowych w poszukiwaniu potrzebnych informacji. Oto prosty skrypt w Pythonie, który pomoże nam zaznajomić się z procesem web scrapingu z użyciem tej biblioteki:

```
from bs4 import BeautifulSoup
import requests
response = requests.get('https://daledumbsitdown.com')
soup = BeautifulSoup(response.text, 'html.parser')
# Drukuje tytuł strony
print(soup.title.string)
```

Podzielmy kod na mniejsze części i zastanówmy się, co robią:

1. Ta linijka kodu zaprasza na scenę naszego gospodarza — bibliotekę Beautiful Soup:

   ```
   from bs4 import BeautifulSoup
   ```

2. Rolę hostessy odegra bardzo popularna biblioteka *requests*, która wykonuje zapytania HTTP, w tym `GET` i `POST`:

   ```
   import requests
   ```

3. Tutaj hostessa wysyła żądanie GET do strony internetowej *https://daledumbsitdown.com*. Funkcja `requests.get()` to prośba o podzielenie się informacjami, a odpowiedź zostaje zachowana w zmiennej `response`:

   ```
   response = requests.get('https://daledumbsitdown.com')
   ```

4. Teraz pałeczkę przejmuje gospodarz programu. Biblioteka Beautiful Soup interpretuje uzyskaną odpowiedź. Zawartość tekstowa, czyli treść naszego show, zostaje wyłuskana z odpowiedzi. Parser (`'html.parser'`) nadaje strukturze HTML sens. Każdy znacznik zna swoje miejsce w przedstawieniu.

   ```
   soup = BeautifulSoup(response.text, 'html.parser')
   ```

5. Na koniec prosimy Beautiful Soup o podanie tytułu strony internetowej. Biblioteka znajduje element *title* w kodzie w HTML i drukuje tekst między znacznikami. To właśnie tytuł strony. Kurtyna w dół.

```
print(soup.title.string)
```

Podsumowując: ten skrypt to nasza przepustka do web scrapingu. Na razie pobieramy jedynie treść i wyświetlamy tytuł strony. Wiem, że to prosty przykład, ale na początek wystarczy. W miarę zagłębiania się w nowe techniki odkryjemy, że każda z nich ma wiele poziomów złożoności i głębi, co zapewnia liczne możliwości doskonalenia umiejętności i pogłębiania zrozumienia.

Korzystanie z mediów społecznościowych

Platformy takie jak Twitter, Facebook, LinkedIn i Instagram to nie tylko wirtualne centra rozrywki, lecz również bogate źródła danych. W tym rozdziale zajmiemy się nimi nieco dokładniej. Na razie jednak zastanówmy się, dlaczego analizę mediów społecznościowych można uznać za osobną technikę. W ramach OSINT analiza mediów społecznościowych obraca się wokół wydobywania i badania danych z różnych portali, a jej celem jest stworzenie obrazu pracowników i działań organizacji, a czasami również zidentyfikowanie potencjalnych podatności.

Oto lista podejść stosowanych przez profesjonalistów OSINT:

- **Agregacja profilów**. Specjaliści ds. bezpieczeństwa zbierają i łączą dane na temat pracowników, interesariuszy i samej firmy. Używają narzędzi takich jak Pipl czy Spokeo, aby wyszukiwać osoby w różnych portalach społecznościowych i gromadzić na ich temat informacje, które ktoś inny mógłby wykorzystać do tworzenia ukierunkowanych ataków phishingowych. Poszukiwane dane mogą obejmować nazwy stanowisk, zainteresowania oraz inne istotne szczegóły.
- **Analiza treści**. Analizowanie postów, polubień, udostępnień i komentarzy może ujawnić wzorce zachowań. Na przykład pracownik opowiadający o programie wykorzystywanym w pracy lub narzekający na niego na publicznym forum nieświadomie udostępnia informacje o oprogramowaniu wykorzystywanym przez firmę.
- **Geolokalizacja i metadane**. Zdjęcia i posty często zawierają znaczniki, np. dane geolokalizacyjne. Mogą one przypadkiem ujawnić lokalizację kluczowej infrastruktury, takiej jak serwerownie i centra danych. Ponadto metadane w opublikowanych zdjęciach mogą obejmować markę i model urządzenia, potencjalnie oferując wgląd w to, jakiego sprzętu używa się w firmie.
- **Mapowanie relacji**. Istnieją narzędzia, takie jak Maltego, które służą do wizualizowania relacji między różnymi osobami w firmie. Analizowanie sieci kontaktów danej osoby umożliwia wyciąganie wniosków na temat struktury organizacyjnej, a nawet nieoficjalnych powiązań między pracownikami i innymi podmiotami, takimi jak dostawcy i konkurencja.

- **Analiza nastrojów**. Niektóre zespoły ds. bezpieczeństwa idą nawet dalej. Przeprowadzają analizę nastrojów na bazie postów, aby poznać morale pracowników firmy. Złe nastoje mogą wskazywać na wyższe ryzyko zaniedbań lub zagrożeń ze strony personelu, co może wpływać na profil bezpieczeństwa firmy.
- **Wydarzenia i wzorce**. Analitycy ds. bezpieczeństwa szukają wzmianek o aktualizacjach, poprawkach do zaaplikowania czy przerwach. Takie informacje dostarczają wiedzy o okresach, w których systemy organizacji są podatne na ataki. To samo odnosi się do postów dotyczących wydarzeń firmowych. W tych dniach biura mogą być puste, a dział IT może być zajęty zadaniami niezwiązanymi z bezpieczeństwem.
- **Rekrutacje i oferty pracy**. Oferty pracy na portalu LinkedIn i podobnych mogą ujawniać cenne informacje na temat wykorzystywanych technologii, realizowanych projektów czy przyszłych decyzji firmy. Dzięki nim możemy poznać rodzaje systemów w użytku, potencjalne kierunki ekspansji czy planowane zmiany technologiczne.

OSINT w mediach społecznościowych wymaga zachowania równowagi między poszanowaniem prywatności a zdystansowaną obserwacją. Analitycy zazwyczaj nigdy nie wchodzą w bezpośrednie interakcje z celami ani nie naruszają zasad ochrony prywatności. Wręcz przeciwnie — zbierają informacje w sposób pasywny, wykorzystując do tego publicznie dostępne źródła, i na tej podstawie opierają swoje działania.

Zrozumienie czynnika ludzkiego w cyberbezpieczeństwie to priorytet. Nie chodzi tylko o technologie, jakie wykorzystuje firma, lecz także o ludzi, którzy ich używają i o nich rozmawiają. W ten sposób analiza OSINT w mediach społecznościowych skupia się na przekształceniu publicznego cyfrowego śladu pracowników organizacji w cenne źródło informacji.

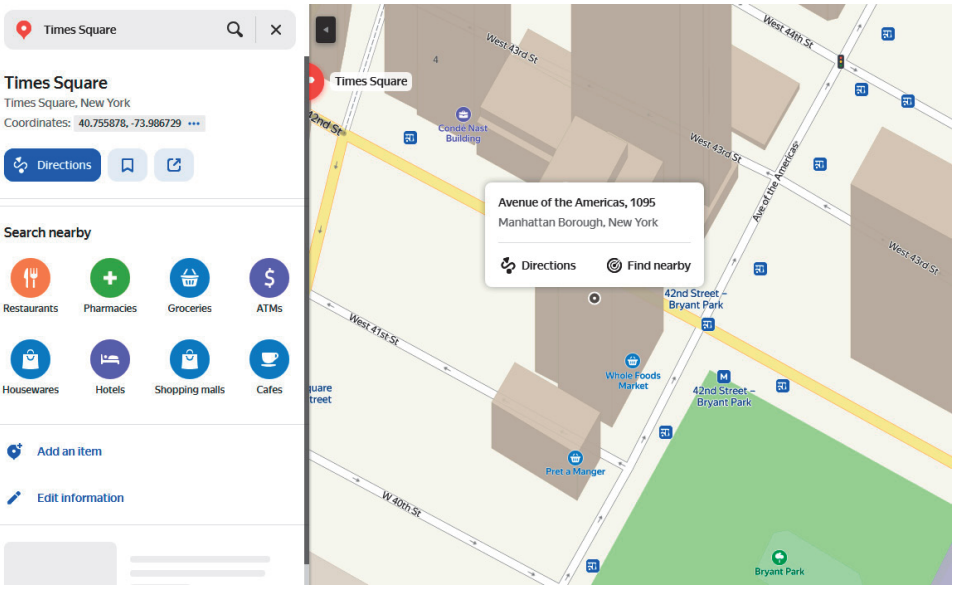
Analiza danych przestrzennych i obrazów

Analiza danych przestrzennych polega na zagłębieniu się w dane geograficzne w celu odnalezienia wzorców i trendów. To istotne narzędzie OSINT, które pomaga wizualizować dane w kontekście geograficznym, co często prowadzi do spostrzeżeń, które mogą umknąć przy bardziej tradycyjnej analizie danych. Analiza danych przestrzennych polega nie tylko na przeglądaniu zachwycających zdjęć satelitarnych, choć muszę przyznać, że nie raz wciągnęło mnie to bardziej, niż wynikałoby to z założonego celu. To również potężne narzędzie, które zapewnia cenne informacje na temat różnych zjawisk — od zmian środowiskowych po ekspansję terenów miejskich.

Na początek porozmawiajmy o uroku zdjęć satelitarnych i lotniczych. Nie chodzi tylko o zwykłe zdjęcia satelitarne, które możemy przeglądać w usłudze Google Earth. Zdjęcia satelitarne mogą być skarbnicą danych na temat wzorców, ruchów, a czasami nawet tajnych obiektów. Aby dokonać interpretacji obrazów i wyciągnąć z nich cenne wnioski, konieczne jest opanowanie platform takich jak Sentinel Hub (*https://www.sentinel-hub.com*).

Przejdźmy do technik geolokalizacyjnych. To tu zaczyna się prawdziwa zabawa, gdyż mówimy o wykorzystaniu narzędzi i platform do znajdowania dokładnej lokalizacji, a czasami nawet zawężenia wyników do dokładnego punktu, z którego zrobiono zdjęcie.

Jakich to wymyślnych narzędzi potrzebujemy? Wyszukiwarki internetowe, takie jak Google, Bing i Yandex, są wyposażone w funkcję mapy. Można ich użyć do przeprowadzenia badania. Istnieją również inne narzędzia zaprojektowane specjalnie do tego celu. Niektóre z nich wyświetlają tylko ruch lotniczy, inne pokazują najnowsze zdjęcia satelitarne regionu, a jeszcze inne — tylko obraz z kamer ulicznych (rysunek 3.1).



Rysunek 3.1. Współrzędne budynku w wyszukiwarce Yandex.com

Organy ścigania mogą używać narzędzi do śledzenia ruchu lotniczego i morskiego, aby monitorować działania przestępców. Źródła danych przestrzennych stanowią bogate zasoby informacji dla różnych zastosowań OSINT.

To jednak nie wszystko! Analiza obrazów pozwala zejść jeszcze głębiej. Dzięki niej możemy uzyskać wskazówki na temat tego, co pozostaje ukryte na widoku. Ta technika obejmuje dogłębną analizę konkretnych elementów. Badając cienie, możemy na przykład uzyskać informacje na temat pory dnia, kiedy wykonano zdjęcie, a dokładne przestudiowanie tła może wykryć istotne znaki lub punkty orientacyjne, które umożliwią wyciągnięcie kolejnych wniosków. Strony internetowe takie jak FotoForensics (*http://fotoforensics.com*) mogą być przydatne na tym etapie, gdyż pomagają przeanalizować obrazy kawałek po kawałku w poszukiwaniu ukrytych informacji.

Analiza deep webu i dark webu

Kolejną wartą wspomnienia techniką jest analiza **deep webu** („głębokiej sieci") i **dark webu** („ciemnej sieci"). Polega ona na podróżowaniu do ukrytych zakątków internetu w poszukiwaniu informacji.

Wiem, że mówienie o dark webie może wzbudzać pewien niepokój. Na razie wspomnę jedynie o tym podejściu, ale obiecuję, że jeszcze w tym rozdziale zajmiemy się tematem ukrytych źródeł bardziej szczegółowo i zapoznamy się z narzędziami, które są potrzebne, aby bezpiecznie zapuścić się w te zakątki internetu.

Pamiętaj, że kluczem do skutecznych działań OSINT jest nie tylko zbieranie danych. Chodzi o wykorzystanie zebranych danych do podejmowania świadomych decyzji i lepszego zrozumienia przedmiotu dochodzenia.

Wybór odpowiedniej metody do zadania

W OSINT wybór najlepszej techniki do danego zadania to rozstrzygająca kwestia. Może na samym wstępie zadecydować o powodzeniu lub porażce przedsięwzięcia. Przyjrzyjmy się kilku przykładom, które to demonstrują:

- **Zapobieganie szpiegostwu przemysłowemu**. Wyobraź sobie, że jesteś konsultantem ds. cyberbezpieczeństwa, który ma zabezpieczyć tajemnice handlowe firmy. Wykorzystanie technik głębokiej analizy danych z mediów społecznościowych mogłoby pomóc w monitorowaniu działań pracowników w internecie, aby zapobiec potencjalnym wyciekom. To właśnie niektórzy z nas opisaliby jako **etyczne hakowanie** (ang. *white hat hacking*).
- **Reagowanie w przypadku klęsk i katastrof**. W obliczu klęsk żywiołowych analiza danych przestrzennych może uratować ludzkie życie. Dzięki analizie obrazów satelitarnych możemy z dużą dokładnością zidentyfikować dotknięte obszary i skutecznie zaplanować akcje ratunkowe.
- **Badania rynkowe**. Jeżeli chcemy wiedzieć, jak ludzie postrzegają produkt lub markę, możemy uzyskać te informacje, badając trendy i nastroje w mediach społecznościowych. W ten sposób możemy trzymać rękę na pulsie.

Uwaga

W każdym z tych scenariuszy niebanalną rolę odgrywa wybór odpowiedniej metody OSINT. Nie chodzi po prostu o gromadzenie danych, lecz o gromadzenie odpowiednich danych. To przywodzi mi na myśl moją mantrę na temat hakowania, a w tym przypadku na temat OSINT: „To, że możesz, nie znaczy, że ci wolno". Prowadząc biały wywiad, zawsze pamiętajmy, aby przestrzegać etycznych praktyk.

OSINT to szybko zmieniająca się i zróżnicowana dziedzina, oferująca wiele użytecznych narzędzi dla osób gromadzących i analizujących dane z ogólnodostępnych źródeł. Niezależnie od tego, czy pozyskujemy dane ze stron internetowych, czy przekopujemy

media społecznościowe w poszukiwaniu złotych grudek informacji, zastosowanie odpowiednich metod to klucz do sukcesu.

Przeszukiwanie i przeglądanie ogólnodostępnych warstw internetu

Sieć powierzchniowa (ang. *surface web*), będąca nieprzebranym zbiorem informacji indeksowanych przez wyszukiwarki, to ważne źródło do celów OSINT. W tym podrozdziale nabędziesz umiejętności i wiedzę niezbędne do skutecznego poruszania się w obrębie tej części sieci dzięki szerokiej gamie technik zbierania danych.

Zaawansowane techniki korzystania z wyszukiwarek internetowych

Wyszukiwarki internetowe to nasi najlepsi sprzymierzeńcy, gdy żeglujemy po sieci powierzchniowej. Aby w pełni wykorzystać ich potencjał, trzeba jednak opanować sztukę zaawansowanego wyszukiwania. Te techniki umożliwiają zawężenie wyników i znalezienie dokładnie tych informacji, których poszukujemy.

Wykorzystanie operatorów, takich jak `site:` do ograniczenia wyszukiwania do konkretnej witryny czy `intext:` do znalezienia stron zawierających konkretną frazę, może całkowicie zmienić zasady gry. Te specjalistyczne techniki dostosowywania zapytań pozwalają skupić się na najbardziej istotnych wynikach bez przedzierania się przez dżunglę niezwiązanych treści.

Jednym z moich ulubionych operatorów jest `site:`. Ten niepozorny pomocnik pozwala zawęzić wyniki wyszukiwania do konkretnej witryny. Dlaczego to pomocne? Ułatwia wyszukiwanie szczegółowych informacji ze znanego źródła. Oto jak to działa:

```
site:daledumbsitdown.com "cyber security"
```

Wyniki wyszukiwania dla tego zapytania wyświetlą tylko te strony z witryny `daledumb` ↪`sitdown.com`, które zawierają frazę `cybersecurity`. Proste, prawda?

Natomiast operator `intext:` pomaga znaleźć strony zawierające konkretną frazę. Usprawnia to proces wyszukiwania. Wypróbujmy to zapytanie:

```
intext:"recent cyber attacks"
```

To zapytanie zwraca strony, które zawierają konkretną frazę `recent cyber attacks` (najnowsze cyberataki), co pozwala szybko znaleźć najświeższe wiadomości na ten temat. Bułka z masłem!

Opanowanie połączeń różnych operatorów może dodatkowo zwiększyć dokładność wyszukiwania, przyspieszając znalezienie ściśle określonych informacji. To cenna

umiejętność w świecie OSINT, gdzie precyzyjne i szybkie lokalizowanie danych jest często na wagę złota.

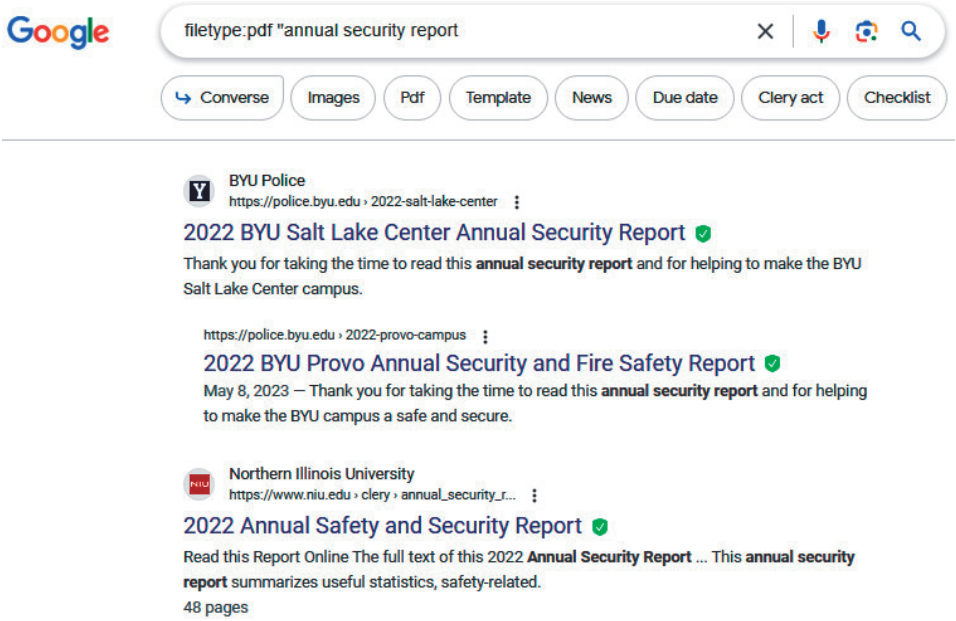
Google hacking

Google hacking, lub też **Google dorking**, to technika wykorzystująca zaawansowane operatory wyszukiwania do znajdowania konkretnych informacji lub ewentualnych podatności na stronach indeksowanych przez Google'a. Jest to jedna z technik stojących u podstaw OSINT. Umożliwia analitykom zlokalizowanie poufnych danych lub wycieków, które mogą być publicznie dostępne w internecie.

Na przykład operator `filetype:` może służyć do znajdowania dokumentów konkretnego rodzaju na zadany temat. Otwórzmy wyszukiwarkę Google i wypróbujmy następujące zapytanie:

```
filetype:pdf "annual security report"
```

To zapytanie zwróci wszystkie dokumenty PDF, które zawierają frazę `annual security report` (roczne sprawozdanie na temat bezpieczeństwa), co potencjalnie może dać nam dostęp do szczegółowych informacji na temat trendów i naruszeń w zakresie bezpieczeństwa (rysunek 3.2). Teraz wcielmy się na chwilę w rolę niezbyt etycznego hakera i pomyślmy, co mógłby chcieć wyszukać na temat naszej organizacji.



Rysunek 3.2. Zaawansowane zapytania mogą zwracać interesujące wyniki

Czujesz już dreszcz niepokoju? Nie? No to daj mi chwilę!

Operator `inurl:` znajduje adresy URL zawierające konkretne słowa kluczowe, co czasami prowadzi do wykrycia ukrytych katalogów i poufnych informacji. Oto jak można go wykorzystać:

```
inurl:admin login
```

To zapytanie zwraca adresy URL, które zawierają słowa `admin` i `login`, co może prowadzić do naprawdę ciekawych znalezisk. Proszę, spróbuj. Poczekam.

W miarę zaznajamiania się z podstawowymi operatorami można je łączyć, tworząc bardziej złożone zapytania. Dzięki temu możemy dokopać się do informacji, których nie dałoby się tak łatwo uzyskać zwykłymi sposobami. Oto kilka zaawansowanych technik i przykładów:

```
intext:"Login" inurl:/secure
```

To zapytanie łączy dwa operatory wyszukiwania Google: `intext:` i `inurl:`. Oto co robi każda z tych części:

- `intext:"Login"` — operatora `intext:` używa się do wyszukiwania konkretnego słowa lub wyrażenia w treści stron internetowych. W tym przypadku szukamy stron, których tekst zawiera słowo `Login`. Może to zwrócić strony, na których znajduje się formularz logowania.
- `inurl:/secure` — operator `inurl:` szuka konkretnych słów lub wyrażeń w adresie URL strony internetowej. Tutaj szukamy adresów URL, które zawierają wyrażenie `/secure`, co mogłoby wskazywać, że strona znajduje się w zabezpieczonej części witryny. Może to być strona logowania lub panel administratora.

Podsumowując: dzięki temu połączeniu możemy znaleźć zabezpieczone strony logowania. To zapytanie można by wykorzystać do wyszukiwania stron z podatnościami, gdyż będzie zwracać strony, które mogą zawierać poufne dane lub funkcjonalności.

Teraz pojedziemy po całości. Co powiesz na to zapytanie?

```
intitle:"index of" ".ssh" OR "ssh_config" OR "ssh_known_hosts" OR
"authorized_keys" OR "id_rsa" OR "id_dsa"
```

Jesteś w stanie zgadnąć, co ono robi? Dam Ci chwilę na zastanowienie, bo tym razem operatorów nie jest mało. Już?

Po połączeniu wszystkich elementów zapytanie wyszukuje wykazy katalogów (za to odpowiedzialne jest wyrażenie `index of` przy operatorze `intitle:`), które zawierają którekolwiek z wymienionych plików konfiguracyjnych lub plików z kluczami protokołu **Secure Shell** (**SSH**). Rozbijmy to na mniejsze części:

- `intitle:"index of"` — operator `intitle:` wyszukuje strony z konkretnymi słowami lub wyrażeniami w tytule. W tym przypadku szukamy stron z tytułem `index of`. Taki tytuł mają często wykazy katalogów w serwerach sieciowych. Lista katalogów jest widoczna w formie strony internetowej.
- `".ssh" OR "ssh_config" OR "ssh_known_hosts" OR "authorized_keys" OR "id_rsa" OR "id_dsa"` — ta część zapytania wyszukuje strony, które zawierają jeden

z kilku ciągów znaków. Każdy z nich jest powiązany z plikami konfiguracyjnymi lub kluczami SSH, których można użyć do uwierzytelniania i zabezpieczania połączeń do serwerów. Podzielmy to na jeszcze mniejsze części:

- `.ssh` — w tym katalogu znajdują się zazwyczaj pliki konfiguracyjne i klucze SSH.
- `ssh_config` — nazwa pliku konfiguracyjnego SSH po stronie klienta.
- `ssh_known_hosts` — ten plik przechowuje klucze publiczne hostów, z którymi klient SSH się łączył, co pozwala na sprawdzenie ich tożsamości przy kolejnym połączeniu.
- `authorized_keys` — ten plik zawiera akceptowane przez serwer klucze publiczne, dzięki którym użytkownik dysponujący odpowiednim kluczem prywatnym może połączyć się z serwerem.
- `id_rsa` — ten plik zawiera prywatny klucz RSA użytkownika, który może posłużyć do uwierzytelnienia klienta na serwerze SSH.
- `id_dsa` — ten plik zawiera prywatny klucz DSA użytkownika, który może posłużyć do uwierzytelnienia klienta na serwerze SSH.
- Operator `OR` służy do łączenia warunków. Dzięki temu wyszukujemy strony, które spełniają jeden z wymienionych warunków. Innymi słowy, zapytanie zwróci strony zawierające przynajmniej jedną z nazw plików lub katalogów.

Osobiście mógłbym napisać całą książkę na temat Google hackingu (dorkingu). To kolejne narzędzie, które może poprowadzić nas niczym Alicję w Krainie Czarów w głąb króliczej nory. I to nie jednej. Dzięki niemu możemy odnaleźć kamery monitoringu, urządzenia **internetu rzeczy** (ang. *Internet of Things*, IoT), strony logowania do platformy SharePoint czy nawet drukarki. O tak, nie ma to jak polecić firmowej drukarce wydrukować *Wojnę i pokój*, aby udowodnić, że podatność istnieje.

Specjalistyczne wyszukiwarki i katalogi

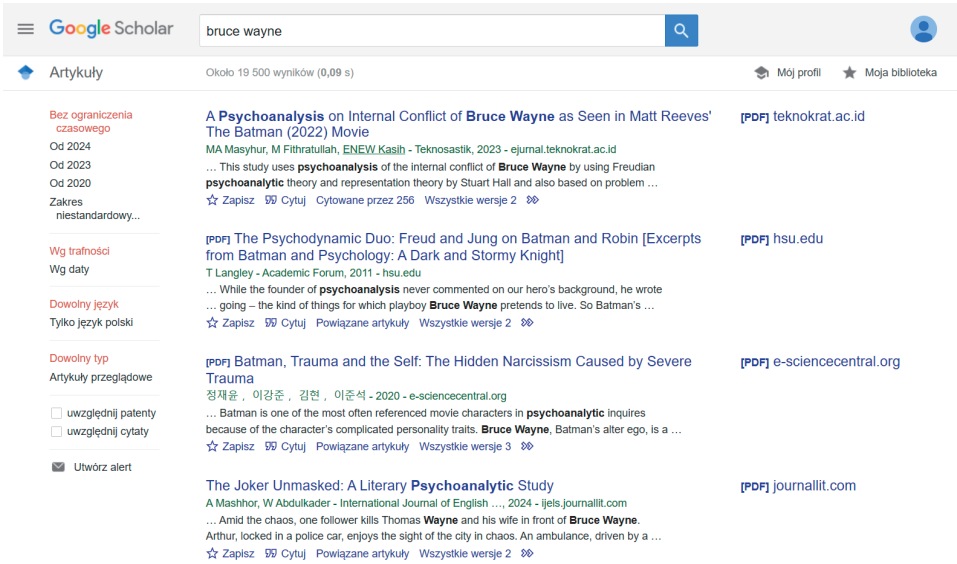
Specjalistyczne wyszukiwarki i katalogi to podstawowe zasoby dla badaczy, zwłaszcza w dziedzinie OSINT. Te narzędzia zostały zaprojektowane z myślą o konkretnych obszarach. Oferują one lepiej dopasowane i bardziej wyspecjalizowane informacje, niż można znaleźć, używając popularnych wyszukiwarek. W tej sekcji omówię różne rodzaje tych platform i sposoby ich skutecznego wykorzystania w analizie OSINT.

Specjalistyczne wyszukiwarki to platformy, które zbierają konkretny rodzaj informacji, oferując bardziej ukierunkowane podejście do gromadzenia danych. Takie narzędzia mają za zadanie zapewnić szczegółowe informacje w danej dziedzinie. Teraz dokonamy przeglądu różnych rodzajów specjalistycznych wyszukiwarek i ich zastosowań w dziedzinie OSINT.

Wyszukiwarki naukowe

Myślmy o wyszukiwarkach naukowych jako o naszej sekretnej przepustce do elitarnej biblioteki cyberwiedzy, gdzie proste zapytanie może zaowocować dostępem do całego uniwersum naukowych plotek, które wynoszą OSINT na nowy poziom. Oto niektóre z takich platform:

- **Google Scholar** (*https://scholar.google.com*). To internetowa strefa VIP dla artykułów i prac naukowych, książek, referatów konferencyjnych i patentów, gdzie spotykają się one na pogawędkę. Możesz tutaj znaleźć niektóre z najrzetelniejszych artykułów naukowych bez przedzierania się przez nienaukową tłuszczę, z którą mielibyśmy do czynienia w zwykłej wyszukiwarce Google (rysunek 3.3).



Rysunek 3.3. Wyniki zapytania o Bruce'a Wayne'a w wyszukiwarce Google Scholar

- **PubMed** (*https://pubmed.ncbi.nlm.nih.gov*). Teraz przywitajmy się z PubMedem. To nieoceniony przewodnik, do którego możemy się zwrócić z wszelkimi zapytaniami dotyczącymi medycyny i biologii. Jego misją jest poprawa zdrowia ludzi na całym świecie. Tak, obejmuje to również Twoje dobre samopoczucie!

  Teraz przejdźmy do statystyk. Ta baza danych zawiera ponad 36 milionów odwołań i streszczeń, co czyni z niej wartościowy zbiór literatury biomedycznej. Chociaż nie da nam na talerzu całego tekstu artykułu naukowego, zawiera odniesienia do pełnych wersji, jeżeli są dostępne. Niezależnie od tego, czy poszukiwany zasób znajduje się na stronie wydawcy, czy na stronie niezawodnego archiwum **PubMed Central** (PMC), jesteśmy tylko jeden krok od tego, aby dać nurka w świat nauki.

- **IEEE Xplore** (*https://ieeexplore.ieee.org/Xplore/home.jsp*). Jest to cyfrowa biblioteka oferująca wszechstronny dostęp do specjalistycznej literatury z dziedziny elektrotechniki, informatyki i elektroniki, ciesząca się uznaniem ze względu na wysoką jakość treści. Stanowi cenny zasób dla fascynatów nowinek technologicznych, którzy szukają szczegółowych badań i artykułów.

Wyszukiwarki kodu

Te platformy nie tylko udostępniają niezliczone projekty o ogólnodostępnym kodzie źródłowym, lecz czasami również stanowią przypadkowe źródło danych poufnych i informacji na temat podatności oprogramowania.

- **GitHub** (*https://github.com*). Ta strona internetowa, będąca jednocześnie wyszukiwarką, przechowuje projekty deweloperów. To prawdziwa kopalnia złota, jeżeli szukamy otwartoźródłowych projektów i fragmentów kodu. Czasami ujawnia jednak również informacje poufne i luki w bezpieczeństwie projektów informatycznych.
- **SourceForge** (*https://sourceforge.net*). To kolejna wspaniała strona połączona z wyszukiwarką. Umożliwia użytkownikom wyszukiwanie, tworzenie i publikowanie oprogramowania o ogólnodostępnym kodzie źródłowym za darmo. Możemy tutaj znaleźć różnorodne projekty informatyczne, a także nawiązać kontakt z innymi programistami.

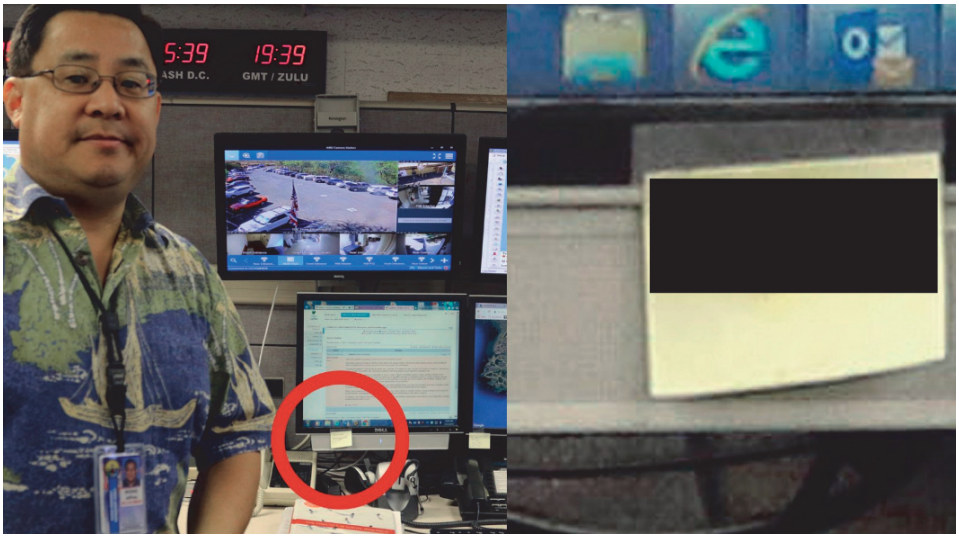
Wyszukiwarki patentów

Tutaj możemy zapoznać się z innowacjami technologicznymi i projektami wynalazków, które kształtują naszą rzeczywistość:

- **Google Patents** (*https://patents.google.com*). Ta witryna zawiera szczegółowe informacje na temat patentów i jednocześnie pozwala lepiej zrozumieć osiągnięcia postępu technologicznego i konkurencję rynkową.
- **Baza danych Urzędu Patentów i Znaków Towarowych Stanów Zjednoczonych** (United States Patent and Trademark Office, USPTO; *https://www.uspto.gov*). To prawdziwy gigant w dziedzinie patentów. Katalog zawiera szczegółowe informacje na temat patentów, w tym opisy, zastrzeżenia patentowe i odwołania, dzięki czemu zapewnia wyjątkowy wgląd w świat wynalazków i innowacji.

Wyszukiwarki obrazów

Wyszukiwarki obrazów mogą odegrać decydującą rolę w identyfikacji podatności i potencjalnych zagrożeń. Są w stanie dostarczyć nam zdjęcia infrastruktury systemu, aplikacji, sieci, a nawet haseł zapisanych na samoprzylepnych karteczkach, jak to miało miejsce podczas wywiadu telewizyjnego na kanale TV5Monde w 2015 r. (rysunek 3.4).



Rysunek 3.4. Wywiad telewizyjny z hasłem zapisanym na samoprzylepnej karteczce w tle

Niezależnie od tego, czy weryfikujemy autentyczność obrazów, czy sprawdzamy powiązane informacje, te narzędzia to podstawa:

- **TinEye** (*https://tineye.com*). Ta przyjazna wyszukiwarka umożliwia użytkownikom odwrotne wyszukiwanie obrazów, co pozwala znaleźć źródło obrazu lub zlokalizować przypadki jego użycia w sieci. Używam tego narzędzia nieustannie. Pomaga mi, gdy potrzebuję sprawdzić autentyczność zdjęcia lub znaleźć więcej informacji na temat konkretnego obrazu.
- **Grafika Google** (*https://images.google.com*). To najpopularniejszy wybór, jeżeli chodzi o wyszukiwarki, ze względu na wygodny dla użytkownika interfejs i bogate repozytorium obrazów. Narzędzie korzysta z przepastnej bazy danych firmy Google, która może okazać się żyłą złota, gdy chcemy zidentyfikować cele podatne na cyberataki. Osoby o złych intencjach mogą użyć wyszukiwarek obrazów i filmów do monitorowania działań sieci w czasie rzeczywistym, pozyskując aktualne informacje na temat zmieniających się cech celu. Ten stały dostęp do danych umożliwia szybkie wykrycie zmian w systemie i sieci, a przez to przygotowanie się i szybkie reagowanie.

Fajnie było poszperać w wynikach wyszukiwania, prawda? Czasami naprawdę trudno przewidzieć, co czai się zaledwie parę kliknięć od nas. No ale to tylko część przygody. Teraz przygotujmy się na przejażdżkę przez dżunglę mediów społecznościowych. To tutaj tętni życie — informacje są nieustannie aktualizowane i dodawane. To nie jakiś odgrzewany kotlet, lecz show na żywo! W mediach społecznościowych mamy dostęp do relacji na bieżąco na temat ludzi i firm — prawdziwe informacyjne eldorado. Udajmy się więc tam i zobaczmy, jakie smaczne kąski znajdziemy na kanałach mediów społecznościowych.

Badanie mediów społecznościowych do celów OSINT

Rozpoznanie w mediach społecznościowych (ang. *social media intelligence*, SOCMINT) umożliwia zbieranie informacji z tętniącego życiem świata mediów społecznościowych. Podczas gdy w ramach OSINT skupiamy się na przeglądaniu ogólnodostępnych danych, w przypadku SOCMINT zapuszczamy się nieco głębiej, zyskując dostęp do informacji, którymi podzielono się początkowo z węższym gronem osób w mediach społecznościowych.

Media społecznościowe przekształciły się w gwarne węzły informacyjne, gdzie osoby i organizacje publikują opinie, przesyłają aktualizacje i dzielą się wiadomościami. Te platformy stały się też ważnym instrumentem dla białego wywiadu. Zapewniają niezliczone ilości danych, które można analizować do różnorodnych celów. Zapuśćmy się nieco głębiej w ten gąszcz informacji i zobaczmy, jakie perełki możemy tam znaleźć dzięki OSINT:

- **X, dawniej Twitter** (*https://x.com*):
  - **Cyfrowy bazar**. X to swoiste centrum informacyjne, gdzie można zapoznać się z najnowszymi plotkami i wiadomościami. Analitycy OSINT zaglądają tutaj, aby zasięgnąć języka na dowolny aktualny temat.
  - **Wyszukiwanie z klasą**. X jest wyposażony w użyteczne opcje wyszukiwania, które umożliwiają przesiewanie tweetów przez różnego rodzaju filtry, dzięki czemu analitycy OSINT nie mają najmniejszych problemów ze znalezieniem informacji, których szukają.
  - **Wygodne API**. No i jakby tego było mało, integracja z API serwisu X pozwala zaoszczędzić mnóstwo czasu, dzięki czemu badacze mogą gromadzić ogromne ilości informacji bez dużego wysiłku.
- **Facebook** (*https://www.facebook.com*):
  - **Szeroki wybór czatów**. Facebook to gigantyczne miejsce spotkań z milionami grup i forów, na których ludzie dzielą się informacjami na wszelkie tematy. Dla analityków OSINT to kolejna kura znosząca złote jajka.
  - **Społecznościowe targowisko**. Marketplace Facebooka tętni życiem. Ludzie kupują i sprzedają rzeczy na prawo i lewo. Dla analityków to świetne miejsce, aby zaznajomić się z najświeższymi trendami i zachowaniami konsumentów.
  - **Wydarzenia w pobliżu**. Wydarzenia na Facebooku to poręczne narzędzie do tworzenia i promocji różnorodnych imprez. Ta prosta funkcjonalność pozwala badaczom gromadzić informacje na temat wydarzeń i osób w nich uczestniczących.
- **LinkedIn** (*https://www.linkedin.com*):
  - **Ośrodek networkingu**. LinkedIn to przede wszystkim miejsce nawiązywania kontaktów zawodowych. Z tego względu to skarbnica informacji na temat firm, branż oraz grubych ryb w świecie biznesu.

- **Portal rekrutacyjny**. To również miejsce, w którym można sprawdzić oferty pracy oraz uzyskać wgląd w trendy branżowe i zmiany na rynku pracy.

Uwaga

Oferty pracy to moja ulubiona sekcja. Na podstawie tych ogłoszeń uzyskuję zawsze mnóstwo informacji na temat swoich celów.

- **Skarbnica treści**. Użytkownicy serwisu LinkedIn dzielą się z innymi różnorodnymi treściami, od artykułów po prezentacje, co stanowi cenne źródło informacji dla analityków OSINT.

- **Instagram** (*https://www.instagram.com*):
  - **Magiczna kraina obrazów**. Instagram kręci się wokół treści graficznych, zapewniając dostęp do istnego oceanu obrazów i filmów, które idealnie nadają się do wszelkiego rodzaju analiz, w tym badania trendów i nastrojów.
  - **Magia znaczników**. Instagram oferuje ciekawe funkcjonalności, takie jak hasztagi i znaczniki geograficzne, które pozwalają kategoryzować treści. Zdecydowanie ułatwia to życie analitykom OSINT poszukującym konkretnych informacji.
  - **Obserwatorium influencerów**. Instagram to również miejsce aktywności wielu influencerów, którzy mają duży wpływ na kształtowanie opinii. Warto mieć na oku publikowane przez nich treści i strategie, gdyż dają wgląd w trendy w mediach społecznościowych i opinię publiczną.

No dobrze, skoro wiesz już, z jakiego rodzaju informacjami mamy do czynienia, zobaczmy, co możemy z nimi zrobić.

Pojęcia z zakresu SOCMINT — szczegółowa analiza

Niezwykle ważne jest rozumienie różnych pojęć i terminów, które stanowią fundament SOCMINT. Zacznijmy od tych:

- **Profil użytkownika**. Zawiera statyczne dane stanowiące krótkie podsumowanie informacji, jakie użytkownik prezentuje online na temat samego siebie, z perspektywy osobistej lub zawodowej. Profil użytkownika w serwisie LinkedIn może obejmować informacje o aktualnym zatrudnieniu na stanowisku „Administrator Windows", wykształceniu oraz zestawie umiejętności, takich jak „Exchange 2013" czy „SharePoint". Z kolei z portalu X możemy się dowiedzieć, jakie są zainteresowania użytkownika i z jakimi informacjami wchodzi zazwyczaj w interakcje, co zapewnia wgląd w osobowość i preferencje danej osoby.
- **Interakcje**. Ten aspekt obejmuje różnorodne czynności, w jakie angażują się użytkownicy w mediach społecznościowych. Na przykład na Facebooku użytkownik może aktywnie uczestniczyć w grupie dyskusyjnej na temat

najnowszych wydarzeń w dziedzinie cyberbezpieczeństwa, dzielić się spostrzeżeniami i udostępniać zasoby. Na platformach takich jak Instagram interakcje mogą obejmować komentarze pod postami na temat narzędzi z zakresu bezpieczeństwa połączeń bezprzewodowych. Może to być też udostępnienie relacji na temat ostatniego webinaru dotyczącego etycznego hakowania. Te interakcje to wspaniałe źródło bieżących informacji na temat opinii, rozmów i treści, które interesują danego użytkownika.

- **Metadane**. W tym przypadku chodzi o dane kontekstowe, które towarzyszą głównej treści opublikowanej w mediach społecznościowych. Na przykład udostępnione zdjęcie może zawierać różnego rodzaju metadane, takie jak lokalizacja geograficzna, czas i data opublikowania zdjęcia, a także rodzaj urządzenia użytego do wgrania treści. Te metadane umożliwiają wyciąganie daleko idących wniosków na temat zachowań i zwyczajów użytkownika, pomagając badaczom zbudować dokładniejszy profil osób i grup.

Uwaga

To, jakie informacje ludzie nieświadomie udostępniają w mediach społecznościowych, przyprawia o zawroty głowy. Niektórzy podają wszystkie dane: imiona i nazwiska, płeć, adresy e-mailowe, a nawet imiona dzieci. Najbardziej przeraża mnie, gdy ktoś publikuje zdjęcia swoich dzieci online. Dlaczego? Pierwsza zasada internetu brzmi, że jeżeli coś raz się w nim znajdzie, to *nie da się* już tego cofnąć. Rodzice natomiast uwielbiają mówić o swoich dzieciach. Zdjęcia często zawierają informacje, które wydają się niegroźne, lecz mogą narazić je na niebezpieczeństwo. Wyobraźmy sobie zdjęcie zrobione pierwszego dnia szkoły. Dziecko stoi przed domem, na którym widnieje numer. Dobra, już schodzę z ambony.

Na świecie istnieją dwa rodzaje danych

Technicznie rzecz biorąc, możemy mieć do czynienia z dwoma rodzajami informacji:

- **Informacje jawne**. Tym rodzajem danych użytkownicy chętnie dzielą się w mediach społecznościowych. To przekazywane w sposób bezpośredni informacje, które nie wymagają dodatkowej obróbki i stanowią widoczną warstwę internetowej tożsamości użytkownika. Na przykład użytkownik może otwarcie dzielić się swoimi poglądami na temat najnowszych wydarzeń w dziedzinie cyberbezpieczeństwa na platformie X czy opublikować post w serwisie LinkedIn na temat nowo uzyskanego certyfikatu z zakresu etycznego hakowania. Ta kategoria informacji obejmuje dane profilowe, takie jak stanowisko, wykształcenie oraz przynależność do grup lub społeczności. Informacje jawne stanowią bezpośrednie okno na życie zawodowe, zainteresowania i opinie użytkownika, przekazując tym samym bezpośredni obraz jego działań i zaangażowania.
- **Informacje niejawne**. To bardziej subtelny rodzaj danych, które użytkownicy często ujawniają nieświadomie. Przyjrzyjmy się przykładowi. Analizując wzorce polubień i udostępnień na platformach takich jak Facebook, analitycy

mogą wysnuwać wnioski na temat preferencji, przynależności i nastawienia do pewnych tematów czy społeczności. Metadane dołączone do udostępnianych treści, takie jak znaczniki geograficzne i rodzaje urządzeń, mogą oferować wskazówki na temat zwyczajów, odwiedzanych miejsc oraz używanych urządzeń. Informacje niejawne stanowią istotne źródło spostrzeżeń, które mogą pomóc badaczom zbudować bardziej precyzyjny i kompleksowy profil danej osoby, często ujawniając wzorce i szczegóły, które nie są widoczne na pierwszy rzut oka.

Dzięki wykorzystaniu zarówno informacji jawnych, jak i niejawnych analitycy SOCMINT mogą stworzyć szczegółową sieć spostrzeżeń, pomocnych w prowadzeniu bardziej wnikliwego dochodzenia. To jak układanie puzzli, z których każdy dopełnia ogólny obraz.

„Rozszerlokuj" to!

Moje dzieci nienawidzą, kiedy używam tego słowa. Za każdym razem gdy zadają mi pytanie, które w mojej ocenie wymaga jedynie odrobiny zdrowego rozsądku, aby znaleźć odpowiedź, mówię im: „Rozszerlokuj to!". Nie wyobrażacie sobie, jaka była moja radość, gdy pojawiło się na rynku to narzędzie.

Sherlock to poręczny program, który wyszukuje nazwę użytkownika lub firmy w różnych mediach społecznościowych. Działa niczym prywatny detektyw, któremu podrzucasz karteczkę z imieniem i nazwiskiem, a on przeczesuje internet w poszukiwaniu wszelkich profilów w mediach społecznościowych, które mogą być powiązane z tak nazywającą się osobą.

Przetestujmy, jak to działa. Na początek zapoznaj się z krótką instrukcją instalacji tego narzędzia w dystrybucji Kali Linux, która jest moim domyślnym systemem do działań OSINT:

1. **Zaktualizuj**. Zanim zaprosimy Sherlocka w cyfrową gościnę, upewnijmy się, że wszystko jest w idealnym porządku. Otwórz terminal i uruchom następujące polecenie, aby zaktualizować system:

   ```
   sudo apt update && sudo apt upgrade -y
   ```

2. **Zainstaluj**. Po zaktualizowaniu informacji o dostępnych pakietach i ogólnej aktualizacji oprogramowania użyjemy menadżera pakietów APT, aby wprowadził naszego wybitnego gościa i zainstalujemy program:

   ```
   sudo apt install sherlock
   ```

3. **Sprawdź**. Jeszcze tylko standardowa wymiana uprzejmości. Upewnij się, że instalacja przebiegła pomyślnie:

   ```
   sherlock --version
   ```

4. **Start**. Teraz Sherlock jest gotowy do pracy. Podsuńmy mu jakiś trop. W tym celu możemy użyć tego prostego polecenia:

   ```
   sherlock <nazwa użytkownika>
   ```

Pamiętajmy, że wyniki mogą być trafione albo nie. Rysunek 3.5 przedstawia niewielką próbkę wyników z wyszukiwania nazwy użytkownika *dalemeredith*.

```
┌──(kali㉿kali)-[~]
└─$ sherlock dalemeredith
[*] Checking username dalemeredith on:

[+] About.me: https://about.me/dalemeredith
[+] Audiojungle: https://audiojungle.net/user/dalemeredith
[+] Behance: https://www.behance.net/dalemeredith
[+] Disqus: https://disqus.com/dalemeredith
[+] Facebook: https://www.facebook.com/dalemeredith
[+] Fiverr: https://www.fiverr.com/dalemeredith
[+] Flipboard: https://flipboard.com/@dalemeredith
[+] GeeksforGeeks: https://auth.geeksforgeeks.org/user/dalemeredith
[+] Gravatar: http://en.gravatar.com/dalemeredith
[+] Houzz: https://houzz.com/user/dalemeredith
[+] Instagram: https://www.instagram.com/dalemeredith
[+] Issuu: https://issuu.com/dalemeredith
[+] NationStates Nation: https://nationstates.net/nation=dalemeredith
[+] NationStates Region: https://nationstates.net/region=dalemeredith
[+] Periscope: https://www.periscope.tv/dalemeredith/
[+] Reddit: https://www.reddit.com/user/dalemeredith
[+] SlideShare: https://slideshare.net/dalemeredith
[+] Smule: https://www.smule.com/dalemeredith
[+] Snapchat: https://www.snapchat.com/add/dalemeredith
[+] Strava: https://www.strava.com/athletes/dalemeredith
[+] ThemeForest: https://themeforest.net/user/dalemeredith
[+] TrashboxRU: https://trashbox.ru/users/dalemeredith
```

Rysunek 3.5. Wyniki wyszukiwania nazwy użytkownika dalemeredith z użyciem narzędzia Sherlock

Niezależnie od tego, czy szukamy wskazówek na temat nazwy użytkownika, czy staramy się powiązać fakty, nie zapominajmy o Sherlocku. To proste, pozbawione udziwnień narzędzie stanowi naprawdę wielką pomoc dla każdego cybernetycznego detektywa.

Hasztagi i znaczniki geograficzne

Gdy chodzi o wydobywanie cennych informacji z internetu, umiejętność korzystania z hasztagów i znaczników geograficznych może oznaczać różnicę między sukcesem a porażką. Są niczym drogowskazy na tajnej mapie, które prowadzą nas prosto do skarbu.

Te niepozorne, opatrzone symbolem krzyżyka (*#*) wyrażenia oświetlają naszą drogę ku bieżącym rozmowom i popularnym tematom. Wyobraź sobie następującą sytuację. Śledzisz najświeższe plotki — dajmy na to — na temat największego superbohatera wszech czasów. Wybierzmy kogoś, kto nie ma supermocy. Kogoś, kto biega po nocy w płaszczu. Znalazłem! Niech to będzie Batman. Wejdźmy na naszą ulubioną platformę mediów społecznościowych i wyszukajmy hasztag *#Batman*. Tadam! W mgnieniu oka przenosimy się do epicentrum aktualnych rozmów na ten temat. To fantastyczny sposób na to, aby trzymać rękę na pulsie i zbierać informacje w czasie rzeczywistym. Oto kilka wskazówek, jak skutecznie używać hasztagów:

- **Analiza trendów**. Narzędzia takie jak **Hashtagify** (*https://hashtagify.me*) i **RiteTag** (*https://ritetag.com*) mogą być naszymi gwiazdami przewodnimi po hasztagowym uniwersum. Pomagają odnaleźć popularne hasztagi, a nawet sugerują optymalne sposoby na poszerzenie zasięgu. To przepustka za kulisy, umożliwiająca poznanie najgorętszych tematów, które wstrząsają internetem.
- **Interakcje ze społecznościami**. Platformy takie jak **X Pro** (wcześniej TweetDeck; *https://pro.twitter.com*) mogą stać się naszym centrum dowodzenia, jeżeli chodzi o monitorowanie społeczności skupionych wokół konkretnych hasztagów oraz interakcję z nimi. Umożliwiają przysłuchiwanie się niszowym dyskusjom i bycie świadkiem ważnych rozmów.
- **Odkrywanie treści**. Platforma **BuzzSumo** (*https://buzzsumo.com*) to kolejne ciekawe narzędzie, które może pomóc w wyszukiwaniu popularnych treści na podstawie hasztagów. Jest jak lupa, która pozwala dokładniej przyjrzeć się tematom, które wzbudzają duże zainteresowanie w wybranym przez nas obszarze.

Nie zapomnijmy o znacznikach geograficznych

Znacznik geograficzny to cyfrowy równoważnik krzyżyka na mapie. Dzięki niemu możemy określić współrzędne geograficzne (długości i szerokość) dowolnego urządzenia podłączonego do internetu. Przez dowolne urządzenie rozumiem również telefon, tablet i inteligentny zegarek. Ta fascynująca technologia dzieli się na trzy rodzaje: informacje zbierane przez serwer, informacje zbierane przez urządzenie i informacje połączone.

- **Informacje zbierane przez serwer — tajniak od IP**

  To podejście przypomina wynajęcie cyfrowego detektywa, który śledzi fizyczne lokalizacje powiązane z adresami IP na podstawie wielu lat zbierania danych. Rzetelność informacji zależy od jakości danych dostarczonych przez serwisy stron trzecich, co czasem sprawia, że nie możemy mieć absolutnej pewności. Znaczniki na mapie cały czas się zmieniają, a dostawcy usług dyktują standardy i oferują niestandardowe rozwiązania geolokalizacyjne.

- **Informacje zbierane przez urządzenie — zaklinacz GPS**

  W tym przypadku można powiedzieć, że to my nosimy w kieszeni minidetektywa, który po cichu przekazuje położenie naszego urządzenia. Metoda ta opiera się na systemie GPS i sieciach komórkowych. Zapewnia to większą dokładność w gęsto zaludnionych obszarach. W rzadziej zaludnionych miejscach mogą pojawić się problemy, prowadząc do opóźnień i luk w przekazywaniu informacji. Aby ta metoda działała możliwie najlepiej, konieczne jest uruchomienie wykrywania lokalizacji, ale pamiętajmy, że zawsze dobrze mieć z tyłu głowy kwestie prywatności.

- **Połączone informacje – optymalne rozwiązanie**

  W tym przypadku współpracujemy nie z jednym, ale z dwoma detektywami. Dzięki wykrywaniu lokalizacji na podstawie danych zbieranych przez serwer

i przez urządzenie możemy uzyskać bardziej kompleksowy obraz. Zapewnia to lepsze doświadczenia użytkownika, ponieważ gdy jedna metoda zawiedzie, mamy zapasową opcję. To dobre rozwiązanie w przypadku stron stawiających na interakcję z użytkownikiem.

- **Śledzenie lokalizacji w prawdziwym świecie**

  Po ataku na Kapitol, który miał miejsce 6 stycznia 2021 r. w Stanach Zjednoczonych, firma Google aktywnie współpracowała z organami ścigania i pomagała w dochodzeniach. Nakazy sądowe dotyczące geofencingu, które pozwalają tym organom żądać informacji na temat urządzeń znajdujących się w konkretnej lokalizacji o konkretnej porze, ułatwiają tę współpracę. Chociaż ta technologia pomogła w zlokalizowaniu podejrzanych, wzbudziła także obawy o poszanowanie prywatności, gdyż umożliwia zbieranie informacji również o osobach postronnych. Google prowadzi negocjacje w tej trudnej sytuacji, starając się zapewnić równowagę między pomocą w dochodzeniach a ochroną prywatności użytkowników.

  Ten przypadek podkreśla kluczową rolę, jaką firmy technologiczne mogą odgrywać w dochodzeniach w erze cyfrowej. Równie istotny jest temat delikatnej równowagi między pomocą organom ścigania a ochroną prywatności użytkowników. Zapewnienie tej równowagi jest niezbędne do utrzymania publicznego zaufania i współpracy. Konieczne jest osiągnięcie harmonii w miarę rozwoju technologii, aby zagwarantować, że dążenie do sprawiedliwości nie zagraża prywatności. Dla mnie oznacza to przyszłość, w której firmy technologiczne i organy ścigania częściej łączą siły, lecz w której istnieją też mechanizmy chroniące prawa człowieka. Mam nadzieję, że tak będzie. Nadal jednak z dużą obawą podchodzę do wszelkich doniesień o współpracy rządów z branżą technologiczną.

Magiczny świat danych EXIF

EXIF (Exchangeable Image File Format) to standard metadanych dla plików graficznych. Metadane EXIF to prawdziwa gwiazda wieczoru. Ten mały geniusz przenika do zdjęć, które robimy telefonem lub cyfrowym aparatem, i przechowuje bogactwo informacji, w tym współrzędne GPS, które można wykorzystać do dokładnego prześledzenia naszych kroków. To istne szaleństwo, prawda? Jest jeden haczyk: w celu zapewnienia prywatności użytkowników większość stron internetowych i mediów społecznościowych usuwa te dane. Z tego względu obraz z pełnymi danymi EXIF to prawdziwy biały kruk. Jeżeli nam się jednak uda wyszukać taki egzemplarz, jest co świętować. Aby wydobyć ze zdjęcia dane EXIF, możemy użyć narzędzi takich jak **Jimpl** (*https://jimpl.com*). Rysunek 3.6 pokazuje przykładowe wyniki.

Zauważ, że informacje na temat lokalizacji nie są dostępne. Wynika to z tego, że wyłączyłem wykrywanie lokalizacji do celów robienia zdjęć, w tym dla tego zdjęcia, które zostało zrobione na konferencji Black Hat. Mój telefon jest nieźle zabezpieczony. Niemniej jednak sporo danych i tak zostało zebranych (rysunek 3.7).

Jimpl

IMAGE METADATA | CAMERA SETTINGS | LOCATION | FULL METADATA

UPLOAD ANOTHER IMAGE



Metadata takes **2.57 KB (0.2%)** of this image and may include sensitive info. To protect your privacy, download this image without metadata by clicking the button below.

Image metadata

Name	20220810_111727.jpg
File size	1.05 MB (1097976 bytes)
File type	JPEG
MIME type	image/jpeg
Image size	1500 x 2821 (4.2 megapixels)
Color space	sRGB
Created	August 10, 2022 11:17

Location

This photo doesn't include location data.
We can't find where it was taken.

Rysunek 3.6. Informacje o moim zdjęciu pozyskane narzędziem Jimpl

Camera settings

Make	samsung
Model	SM-S908U
Focal length	3.8 mm
Aperture	2.2
Exposure	1/20
ISO	1000
Flash	No Flash

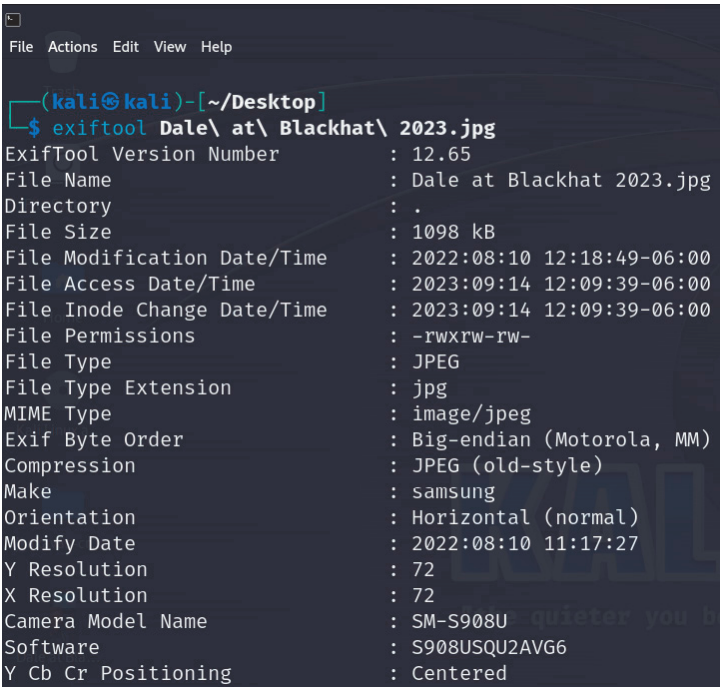
Rysunek 3.7. Informacje o aparacie i jego ustawieniach wykryte przez narzędzie Jimpl

ExifTool to popularny program używany przez osoby potrzebujące przeglądać i edytować metadane plików multimedialnych. Obecnie to narzędzie jest wbudowane w dystrybucję Kali Linux. Odpalmy więc nasz system i zobaczmy, co potrafi ExifTool.

Pierwszym krokiem w posługiwaniu się tym nowym źródłem jest nauczenie się, jak odczytywać istniejące metadane pliku. Możemy to zrobić za pomocą prostej komendy:

```
exiftool moje_arcydzieło.jpg
```

To polecenie ujawni wszystkie sekretne metadane, jakie przechowuje plik *moje_arcydzieło.jpg*, w tym użyte ustawienia aparatu oraz datę utworzenia zdjęcia (rysunek 3.8).



Rysunek 3.8. Wyniki z narzędzia ExifTool dla pliku graficznego Dale at Blackhat 2023.jpg

W miarę korzystania z narzędzia ExifTool odkryjemy całe mnóstwo zaawansowanych funkcjonalności czekających na odkrycie. Możliwości są szerokie: od analizy wielu zdjęć naraz po kopiowanie metadanych między plikami. Polecam zagłębienie się w dokumentację albo wpisanie `man exiftool`, aby poznać więcej funkcjonalności.

Rozumienie ukrytych źródeł

Przede wszystkim musimy rozumieć, co mamy na myśli, mówiąc o **ukrytych źródłach**. Mogą to być niejawne fora, strony internetowe lub bazy danych, które nie zostały zindeksowane przez najpopularniejsze wyszukiwarki. Z tego względu nie są łatwo dostępne. Możemy też mieć do czynienia z danymi, które leżą na widoku, ale często pozostają niezauważone. Należą do nich na przykład niezabezpieczone lub słabo zabezpieczone

urządzenia podłączone do internetu. Te nisze mogą zawierać nieocenione dane, które prowadzą do dalszych odkryć lub umożliwiają sformułowanie danych wywiadowczych niedostępnych z poziomu sieci powierzchniowej.

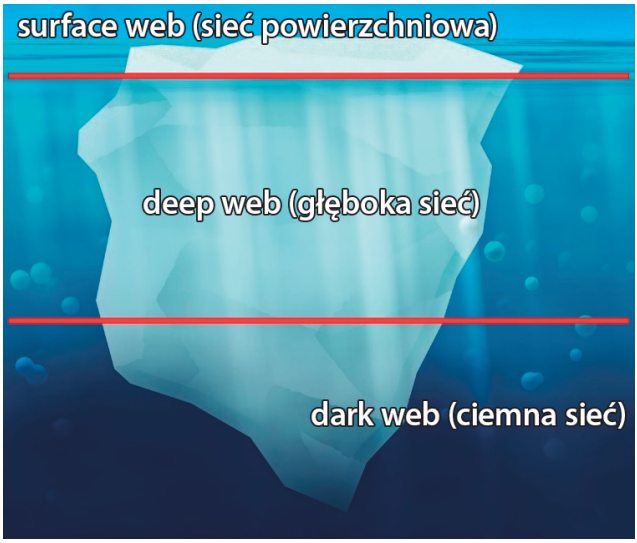
Przeszukiwanie i przeglądanie głębszych i mroczniejszych warstw internetu

Trzymaj się mocno, ponieważ za chwilę wkroczymy w głęboką i ciemną sieć, czyli dwa regiony internetu, które są relatywnie słabo poznane. Większość treści z głębokiej sieci nie jest dostępna za pośrednictwem tradycyjnych wyszukiwarek. Nie należy jednak zakładać, że w głębokiej sieci mamy do czynienia jedynie z podejrzanymi interesami. Takie rzeczy też mają tu miejsce, ale bez przesady. Większość treści to bazy danych, informacje poufne lub dostępne za opłatą.

Upewnijmy się, że rozumiemy internet

Zacznijmy od podstaw. Muszę mieć pewność, że rozumiesz, iż internet jest podzielony na *warstwy*. Tak. Internet to coś więcej niż wpisanie adresu *www.daledumbsitdown.com* w przeglądarkę Google Chrome, aby poczytać sobie o technologii, czy robienie zakupów w sklepie Amazon.

Internet jest jak góra lodowa. Ten obszar, z którego zazwyczaj korzystamy, to jedynie jej czubek — ta część, która jest widoczna nad wodą. Z kolei **głęboka sieć** (ang. *deep web*) i **ciemna sieć** (ang. *dark web*) to masywne, ukryte części internetu, które aż roją się od tajemnic. Rysunek 3.9 zapewnia graficzne przedstawienie tego podziału.



Rysunek 3.9. Warstwy internetu: sieć powierzchniowa, głęboka sieć i ciemna sieć

Nie musisz jednak lękać się nieznanego. Masz we mnie przewodnika.

- **Warstwa pierwsza: sieć powierzchniowa**

  Wyobraź sobie, że siedzisz na brzegu i chłodzisz stopy w ocenie. Sieć powierzchniowa jest właśnie jak taka olśniewająca i tętniąca życiem publiczna plaża. YouTube, Wikipedia, bogactwo obrazów, treści i interakcji — wszystko to dostępne po wpisaniu prostego zapytania w wyszukiwarkę Google. I wszystko pod czujnym nadzorem botów indeksujących tradycyjnych wyszukiwarek.

- **Warstwa druga: głęboka sieć**

  W miarę jak odpływamy od brzegu, wkraczamy w sieć głęboką. Tutaj wszystko jest nieco bardziej tajemnicze. Ta część internetu jest jak archiwum ogromnej biblioteki. Zawiera bazy danych, prywatne konta e-mailowe, usługi na subskrypcję i poufne dane. Jest to część o wiele rozleglejsza niż sieć powierzchniowa i nie jest zindeksowana przez zwykłe wyszukiwarki. Wkraczając do głębokiej sieci, możemy się czuć, jakbyśmy dostali przepustkę do tajnego klubu, do którego dostęp mają tylko wtajemniczeni.

- **Warstwa trzecia: ciemna sieć**

  Teraz odpłyniemy jeszcze dalej i głębiej, w najbardziej odosobnione zakątki internetu — do ciemnej sieci. Wyobraź sobie dark web jako przypominający labirynt targ w ustronnym miejscu miasta, którego wąskie uliczki aż roją się od tajemnic. To niewielka część sieci głębokiej, celowo ukryta i niedostępna za pośrednictwem tradycyjnych przeglądarek. Tutaj liczy się anonimowość, a użytkownicy korzystają głównie z przeglądarek takich jak Tor, aby ukryć swoją tożsamość i działania. Pamiętajmy jednak, że wielka moc pociąga za sobą wielką odpowiedzialność. Ta warstwa internetu jest również kolebką różnorodnej nielegalnej działalności, więc konieczna jest ostrożność i etyczne podejście.

Jeżeli chodzi o OSINT, sieć powierzchniowa jest punktem wyjścia, gdyż pęka w szwach od łatwo dostępnych, gotowych do wykorzystania informacji. Jest to obszar zindeksowany przez wyszukiwarki, dzięki czemu każdy z zacięciem do eksploracji ma szansę w prosty sposób znaleźć to, czego szuka. Gdy chcemy wybrać się do ciemnej sieci, warto się jednak nieco przygotować. Oto co powinniśmy zrobić, aby móc sprawnie poruszać się po tym obszarze i bezpiecznie gromadzić cenne informacje:

1. **Użyj sieci VPN.**

   Zacznij od wyposażenia się w **wirtualną sieć prywatną** (ang. *Virtual Private Network*, VPN), aby ukryć swoje działania online. Dzięki temu zachowasz swój adres IP w tajemnicy, co przełoży się na lepszą ochronę prywatności.

2. **Pobierz przeglądarkę.**

   Następnie ściągnij z internetu przeglądarkę, której można użyć do poruszania się po dark webie. Może to być między innymi Tor, Waterfox bądź Freenet. Te przeglądarki umożliwiają dostęp do stron w domenie *.onion*, charakterystycznej dla dark webu.

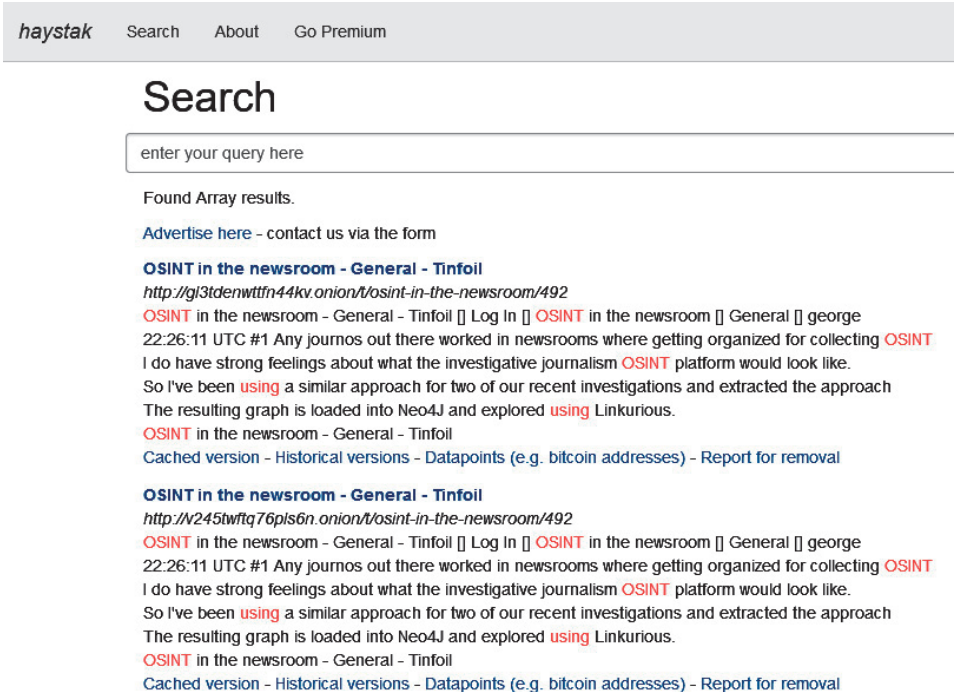
3. **Zacznij podróż od wyszukiwarki.**

   Jesteśmy gotowi i możemy zacząć eksplorację! Ale chwila, Google nam w tym nie pomoże. Musimy mieć wyszukiwarkę, która specjalizuje się w znajdowaniu stron z domeny *.onion*. Popularnym wyborem jest DuckDuckGo (*https://duckduckgo.com*). Nowa wyszukiwarka będzie naszym zaufanym przewodnikiem po niezbadanych obszarach.

4. **Odwiedzaj witryny z domeny *.onion*.**

   Gdy masz już odpowiednią przeglądarkę i wyszukiwarkę, możesz odwiedzać strony z domeny *.onion*. Stąpaj jednak uważnie. Nie wszystkie zakątki dark webu są bezpieczne. Trzymaj się utartych ścieżek, odwiedzaj znane strony i unikaj podejrzanych linków. To istny dziki zachód, więc zachowaj rozsądek!

Rysunek 3.10 pokazuje przykład, jak możemy korzystać z zasobów dark webu. Używając przeglądarki Tor, wyszukuję termin OSINT w wyszukiwarce *haystak*. Zwróć uwagę na domenę *.onion* w adresach.



Rysunek 3.10. Wyszukiwanie w zasobach dark webu

W miarę jak zapuszczamy się coraz głębiej, nie zapominajmy o bezpieczeństwie. Pamiętajmy, że eksploracja ciemnej sieci nie jest dla osób o słabych nerwach. Z odpowiednimi zabezpieczeniami i narzędziami możemy jednak dość bezpiecznie podróżować po odmętach internetu.

Zbieranie danych narzędziem theHarvester

Narzędzie **theHarvester** to niestrudzony cybernetyczny żniwiarz. Dołączony standardowo do dystrybucji Kali Linux program zbiera adresy e-mailowe, nazwy subdomen, hostów i dane pracowników z różnego rodzaju źródeł, w tym wyszukiwarek internetowych, serwerów kluczy PGP oraz deep webu. Jest często wykorzystywany przez specjalistów ds. bezpieczeństwa i badaczy na wczesnych etapach testów penetracyjnych lub dochodzeń do prowadzenia rozpoznania i gromadzenia informacji. Aby uruchomić program theHarvester, otwórz terminal i posłuż się następującą składnią:

```
theHarvester -d <domena> -l <limit> -b <źródło>
```

Podzielmy to na mniejsze części:

- `-d` — określa domenę, którą chcemy przeszukać.
- `-l` — ogranicza liczbę wyników.
- `-b` — określa źródło wyszukiwania. Dopuszczalne wartości obejmują Google'a, Binga, PGP, LinkedIna i X. Warto w tym miejscu zauważyć, że w przypadku niektórych z tych źródeł konieczne jest zainstalowanie kluczy API. W przeciwnym wypadku dla tych źródeł pojawiają się błędy.

Oto konkretny przykład:

```
theHarvester -d hackthissite.org -l 500 -b all
```

Wynik użycia polecenia prezentuje rysunek 3.11.

Muszę nadmienić, że wyników było więcej, niż pomieściło się na zrzucie ekranu. Prawdziwe zatrzęsienie!

Shodan

Shodan (*https://shodan.io*) jest tym dla urządzeń internetu rzeczy, czym Google dla stron internetowych. Shodan umożliwia odnalezienie wszelkiego rodzaju podłączonych do internetu urządzeń i usług, a także łączenie się z nimi. Chociaż większość osób korzysta z wyszukiwarki Shodan, aby sprawdzić, czy nie zhakowano im kamerki internetowej, specjaliści ds. bezpieczeństwa używają jej do innych celów. My przeszukujemy tę witrynę, aby znaleźć podatności w różnych urządzeniach podłączonych do internetu, w tym serwerach WWW i systemach automatyki przemysłowej.

Shodan sprawia, że jesteśmy w stanie znaleźć rzesze potencjalnych celów do ataku, nie ruszywszy się sprzed ekranu laptopa. Zacznijmy od wpisania w interfejsie aplikacji nazwy domeny do przeskanowania (rysunek 3.12).

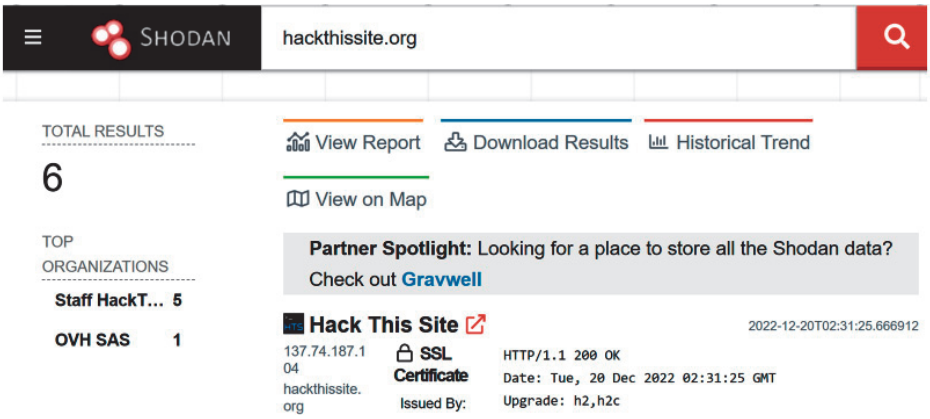
Większość wyników dla domeny *hackthissite.org* dotyczy certyfikatów SSL, ale gdyby powiązane z nią były urządzenia IoT, takie jak kamery czy czujniki, oprogramowanie do udostępniania zdalnego pulpitu albo jakikolwiek niepoprawnie skonfigurowany system podłączony do internetu, byłyby tutaj widoczne. Teraz kolejna sugestia. Wpisz w wyszukiwarkę Shodan zapytanie **`os:windows 7`**, a znajdziesz dzięki temu urządzenia z systemem Windows 7 (rysunek 3.13).

```
[*] Interesting Urls found: 13
------------------
http://mail-old.hackthissite.org
https://hackthissite.org/
https://mail.hackthissite.org/
https://mail.hackthissite.org/?r=/login
https://stats.hackthissite.org/
https://www.hackthissite.org/
https://www.hackthissite.org/?adlt=strict
https://www.hackthissite.org/missions/
https://www.hackthissite.org/missions/basic/11/
https://www.hackthissite.org/missions/basic/11/e/l/t/o/n/
https://www.hackthissite.org/missions/realistic/12/cgi-bin/internet.pl
https://www.hackthissite.org/missions/realistic/2/
https://www.hackthissite.org/missions/realistic/9/

[*] LinkedIn Links found: 0
---------------------

[*] IPs found: 45
-------------------
67.21.66.227
67.21.66.228
67.21.66.229
67.21.66.230
89.41.169.49
89.106.200.1
137.74.187.100
137.74.187.101
```

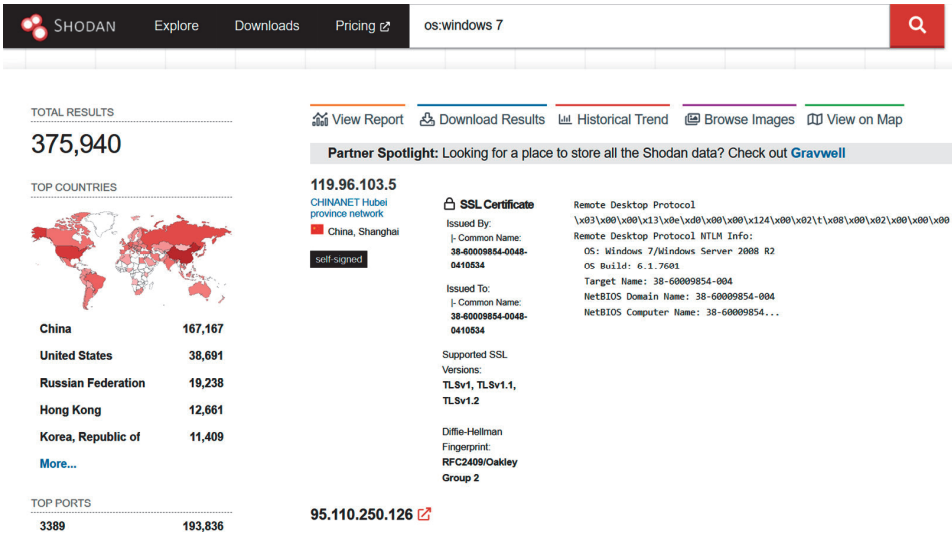
Rysunek 3.11. Wyniki wyszukiwania w narzędziu theHarvester



Rysunek 3.12. Użycie wyszukiwarki Shodan do przeszukania domeny hackthissite.org

To odrobinę zaskakujące zobaczyć na własne oczy, że w 2023 r. aż 375 940 urządzeń używało Windowsa 7 jako systemu operacyjnego. Każde z nich to potencjalny cel ataku.

Jedną z funkcjonalności wyszukiwarki Shodan jest możliwość monitorowania witryn i adresów IP pod kątem pojawienia się nowo zainstalowanych urządzeń. Funkcja monitorowania pozwala specjalistom ds. cyberbezpieczeństwa obserwować i śledzić działania w obrębie konkretnego zakresu adresów IP. Ma to kluczowe znaczenie z kilku powodów:

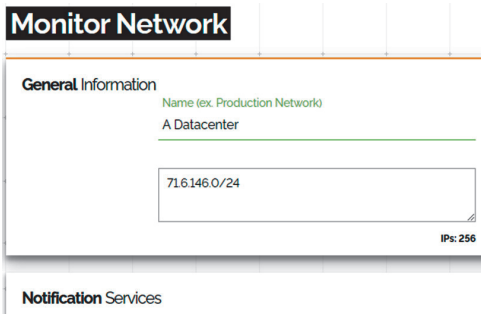


Rysunek 3.13. Znaleźliśmy w internecie ponad 375 tysięcy urządzeń z systemem operacyjnym Windows 7

- **Wykrywanie nowych urządzeń**. Dzięki monitorowaniu danego zakresu możemy określić, kiedy do sieci podłączono nowe urządzenie. Pozwala to upewnić się, że w sieci znajdują się tylko uprawnione urządzenia, i wykryć te, które podłączono bez zezwolenia i które mogą stanowić zagrożenie dla bezpieczeństwa.
- **Wykrywanie podatności**. Shodan może dostarczyć informacji na temat znanych luk w zabezpieczeniach urządzeń w konkretnym zakresie adresów IP. Umożliwia to usuwanie takich podatności, zanim zostaną wykorzystane.
- **Śledzenie zmian i anomalii**. Monitorowanie pozwala obserwować zmiany w konfiguracji i zachowaniu sieci. Obejmuje to zmiany w otwartych portach, usługach uruchomionych na urządzeniach oraz aktualizacje wersji oprogramowania sprzętowego. Anomalie w tych obszarach mogą wskazywać na naruszenia bezpieczeństwa.
- **Analiza danych historycznych**. Shodan przechowuje historyczne dane, co może być pomocne w analizowaniu trendów w obrębie danego zakresu adresów IP w czasie. Dzięki temu można zrozumieć zmiany w stanie zabezpieczeń sieci.
- **Powiadomienia**. Shodan pozwala również ustawić powiadomienia, gdy w ramach zakresu IP spełnione zostaną pewne warunki. Można na przykład skonfigurować powiadomienie przy pojawieniu się nowego urządzenia lub wykryciu nowej usługi.

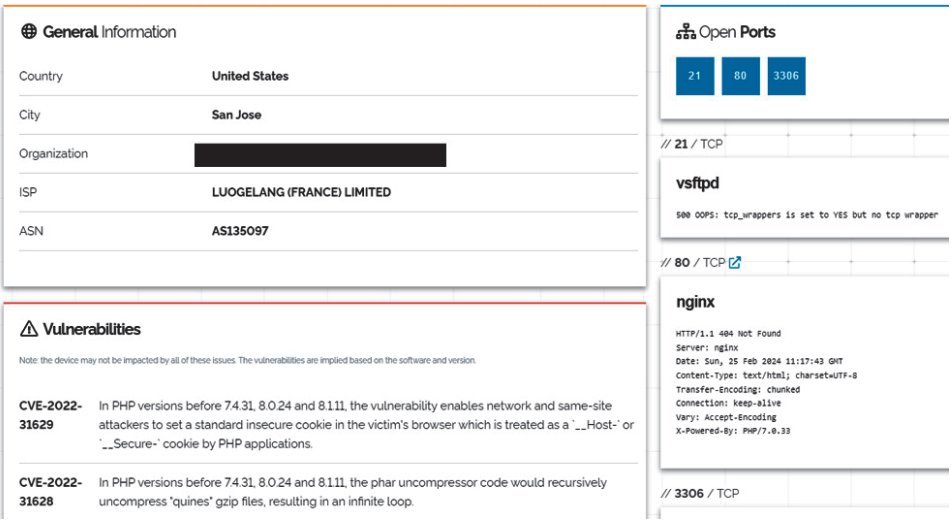
Gdybyśmy chcieli użyć wyszukiwarki Shodan do monitorowania zakresu *71.6.146.0/24*, musielibyśmy wykonać następujące kroki:

1. **Określ zakres**. Aby s`konfigurować monitorowanie dla adresów IP z zakresu *71.6.146.0/24*, trzeba podać ten zakres w ustawieniach monitorowania (rysunek 3.14).



Rysunek 3.14. Shodan ma rozbudowaną funkcjonalność śledzenia zmian

2. **Zdefiniuj powiadomienia**. Określ kryteria wysyłania powiadomień zgodne z Twoimi potrzebami. Mogą one obejmować pojawienie się nowych urządzeń, udostępnienie podatnych usług czy nieoczekiwane zmiany w konfiguracji urządzeń.
3. **Przeglądaj sprawozdania**. Na podstawie wyników monitorowania Shodan generuje raporty. Regularne przeglądanie tych raportów pozwala śledzić stan sieci i wykrywać potencjalne zagrożenia dla bezpieczeństwa (rysunek 3.15).



Rysunek 3.15. Shodan wykrywa usługi, porty i podatności

4. **Reaguj na alerty**. Po otrzymaniu powiadomienia należy je zbadać, aby określić, czy jego źródłem jest realne zagrożenie, czy nieszkodliwa zmiana.

Skuteczne korzystanie z funkcji monitorowania, jakie zapewnia Shodan, pozwala utrzymać wysoką świadomość na temat stanu sieci w danym zakresie adresów IP i wykazywać aktywną postawę względem ewentualnych zagrożeń dla cyberbezpieczeństwa.

Automatyzacja zbierania i analizy danych OSINT

Teraz przyjrzymy się temu, w jaki sposób sztuczna inteligencja (SI) wstrząsnęła światem OSINT. Sztuczna inteligencja może zapewnić turbodoładowanie dla naszego gromadzenia i analizy danych. Wszystko dzieje się szybciej, inteligentniej i — bądźmy szczerzy — po prostu łatwiej.

W jakie obszary wkracza SI? Istnieje wiele zadań, które może ona uprościć:

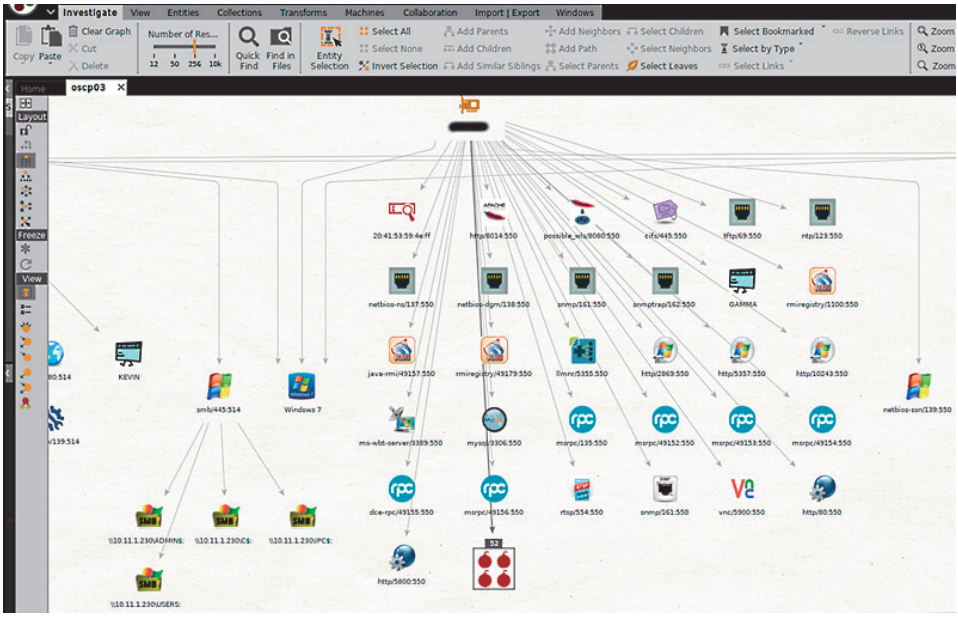
- **Web scraping**. Zaprząc sztuczną inteligencję do wydobywania danych z różnych miejsc, takich jak serwisy z wiadomościami czy fora społecznościowe, to eleganckie rozwiązanie.
- **Analiza nastrojów**. Polega na wysnuwaniu wniosków na temat ogólnych odczuć w odniesieniu do jakiegoś tematu poprzez przekopywanie się przez tony danych tekstowych.
- **Rozpoznawanie obrazów**. Sztuczna inteligencja opanowała również tę umiejętność. Potrafi wyciągnąć istotne informacje z grafiki i filmów.
- **Rozpoznawanie wzorców**. To kolejny nowy obszar, w którym zaczynamy odczuwać wpływ sztucznej inteligencji. SI przekopuje się przez przepastne zbiory danych, aby dostrzec tendencje i wzorce. Dzięki temu jesteśmy w stanie zauważyć rzeczy takie jak kampanie dezinformacyjne czy działania przestępcze szybciej i precyzyjniej, niż gdybyśmy robili to sami.
- **Podsumowywanie tekstów**. Sztuczna inteligencja potrafi analizować tony tekstu i śledzić zmiany w opinii publicznej na różne tematy.

Nie chodzi tylko o przyspieszenie pracy. SI wynosi analizę danych na zupełnie nowy poziom, pomagając rozwiązywać złożone problemy i gromadzić informacje z różnych źródeł.

Jednym z cieszących się dużą popularnością narzędzi OSINT jest Maltego (*https://www.maltego.com*). Stanowi klasyczne wyposażenie każdego analityka OSINT. Jest to graficzne środowisko, które pomaga w wizualizacji sieci i cyberzagrożeń. Niczym lupa pokazuje szczegóły i uwidacznia powiązania między różnymi elementami, zapewniając kompleksowy obraz informacji zdobytych podczas dochodzenia.

Niezależnie od tego, czy badamy cyfrowe ślady osoby, czy analizujemy cyberataki, Maltego maksymalnie to upraszcza dzięki szerokiemu spektrum wtyczek i rozszerzeń, które zapewniają bezproblemową integrację z SI. To bardzo użyteczne narzędzie w pracy OSINT, gdyż umożliwia dogłębną i kompleksową analizę danych. Zbiera fragmenty różnych informacji i integruje je w spójną całość. Wykresy i badania powiązań dają jasny obraz relacji między podmiotami, dzięki czemu mamy wrażenie, że wątki same się

układają na cyfrowej planszy. Przyjrzyjmy się przykładowi takich powiązań i relacji (rysunek 3.16).



Rysunek 3.16. Wyniki badania w programie Maltego

W mojej opinii OSINT wspomagany sztuczną inteligencją to nie tylko fajny trend. Niedługo nie będzie można się bez tego obejść. Stare sposoby zbierania danych odejdą do lamusa, gdyż nie radzą sobie z otaczającym nas bezmiarem danych.

Podsumowanie

Warto zapamiętać, że chociaż w internecie roi się od danych, nie wszystkie są wartościowe. Każdą z takich informacji musimy ocenić krytycznym okiem i oddzielić ziarno od plew. Pomyśl o tym jako o formie cyfrowej samoobrony. Zanim przyswoisz sobie jakąś informację jako prawdę, poddaj ją próbie. Sprawdź ją w zaufanych źródłach. Nie chodzi tylko o ostrożność. Chodzi o działanie w sposób inteligentny i o to, aby nie dać się oszukać. Widzieliśmy zasoby takie jak obrazy, metadane, a także urządzenia IoT, które mogą ujawniać cenne dane na temat firmy lub celu dochodzenia. Nawet zasoby, których nigdy byśmy o to nie podejrzewali, ujawniają informacje. Musimy jednak pamiętać o tym, aby te informacje sprawdzić dwa albo nawet trzy razy. Bądźmy ostrożni i miejmy świadomość, że w cyberświecie odrobina sceptycyzmu może nam dużo dać. Dzięki temu będziemy dysponować pewnymi informacjami, a nasze wnioski będą poprawne.

W następnym rozdziale przyjrzymy się narzędziom do pozyskiwania danych. Spróbujemy też za ich pomocą znaleźć w internecie parę informacyjnych perełek.

Wyprawa w nieznane — narzędzia do eksploracji ukrytych danych

Rozdział 4

Ten rozdział zawiera szczegółową prezentację programów i platform służących do odkrywania ukrytych informacji. Narzędzia te zwiększają nasze możliwości w zakresie prowadzenia **białego wywiadu** i mają kluczowe znaczenie dla każdego, kto pragnie wyjść poza podstawowe zapytania i odkryć prawdziwe bogactwo dostępnych informacji.

Ponieważ te specjalistyczne narzędzia dają nam możliwość znalezienia danych, które są ukryte lub trudne do zlokalizowania, pomagają prowadzić dochodzenie w sposób kompleksowy i wnikliwy. Ich znajomość nie jest opcjonalna. To raczej podstawa dla każdego specjalisty OSINT. Niezależnie od tego, czy badamy potencjalne zagrożenia, konkurencję w branży czy inny interesujący nas temat, narzędzia pozwalające na eksplorację ukrytych danych to absolutny mus.

W tym rozdziale zajmiemy się następującymi tematami:

- wprowadzenie do narzędzi do eksploracji ukrytych danych;
- analiza domen i adresów IP;
- rozpoznanie witryn internetowych i zgłębianie ich niewidocznych warstw;
- analiza dokumentów i metadanych;
- wizualizacja danych w analizie OSINT;
- najlepsze praktyki korzystania z narzędzi do eksploracji ukrytych danych.

Lektura tego rozdziału sprawi, że będziesz lepiej rozumieć rolę narzędzi do pozyskiwania danych w ramach OSINT. Dowiesz się, jak z nich korzystać do skutecznego zbierania, analizowania i interpretowania informacji. Dzięki temu wyniesiesz swoje umiejętności OSINT na nowy poziom.

A teraz do dzieła! Poznaj niezbędnik analityka OSINT.

Wprowadzenie do narzędzi do eksploracji ukrytych danych

Narzędzia do eksploracji ukrytych danych odgrywają niezwykle istotną rolę w dochodzeniach OSINT. Pozwalają analitykom odkrywać niejawne informacje z publicznie dostępnych źródeł, które w przeciwnym razie mogłyby pozostać w cieniu. Specjaliści OSINT korzystają z szerokiej gamy takich technik i narzędzi, dzięki czemu mogą zgłębiać niejasne tematy, znajdować powiązania między danymi i generować nowe tropy.

Istnieje bardzo wiele rodzajów narzędzi do eksploracji ukrytych danych, dopasowanych do różnych potrzeb badawczych. Narzędzia do analizy domen i adresów IP pozwalają zgłębić takie sekrety jak dane rejestracyjne witryny oraz historia własności stron internetowych i sieci. Narzędzia do web scrapingu oraz archiwa stron internetowych umożliwiają wyciąganie treści, kodu i metadanych. Analiza dokumentów wydobywa na światło dzienne metadane i inne cenne wskazówki ukryte w plikach. Z kolei techniki wizualizacji danych pomagają zobrazować powiązania w złożonych zbiorach informacji.

Umiejętne korzystanie z tych narzędzi pozwala analitykom OSINT przejść od prostych zapytań w wyszukiwarce Google do wyciągania nieoczywistych wniosków na podstawie publicznie dostępnych danych. Tak jak wykrywacze metalu lokalizują ukryte skarby, te narzędzia wydobywają na wierzch informacje, które mogą rzucić zupełnie nowe światło na sprawę. Analitycy muszą jednak korzystać z nich w sposób legalny i etyczny.

Mistrzowskie opanowanie narzędzi do eksploracji ukrytych danych umożliwia specjalistom ds. bezpieczeństwa odnajdowanie kluczowych informacji na temat osób, organizacji, miejsc i wydarzeń.

Obnażanie sekretów sieci

Cyfrowy ślad to istna skarbnica informacji — akta naszego cyfrowego „ja". W miarę rozrastania się cyfrowego uniwersum kluczowe znaczenie dla osób i organizacji ma zrozumienie, jak rozległe ślady za sobą pozostawiają.

Dlaczego podążanie za cyfrowym śladem jest takie ważne? Wynika to z tego, że w erze cyfryzacji dane są nową walutą. Informacje dają władzę — możliwość tworzenia skutecznych strategii, wprowadzania innowacji, a czasami również dominowania.

Skoro rozumiemy w ogólnym zarysie, w jaki sposób narzędzia do eksploracji ukrytych danych wspomagają dochodzenia OSINT, przejdźmy do bardziej szczegółowych i praktycznych zastosowań. Skupmy się na początek na jednej z najbardziej istotnych umiejętności analityka OSINT, a mianowicie na analizie domen i adresów IP. To fascynujące, ile można się dowiedzieć na temat historii i powiązań witryny internetowej, mając dostęp do tych informacji. Zacznijmy od tego, jak działa analiza domen i adresów IP oraz dlaczego to taki ważny atut dla specjalisty ds. bezpieczeństwa.

Analiza domen i adresów IP

Zacznijmy od **WHOIS**, czyli od mechanizmu, który oświetla ciemne zakamarki cyfrowego świata, obnażając dane rejestracyjne domen. Nazwy domen, na które się natykamy, gdy odwiedzamy stronę internetową lub wysyłamy wiadomość e-mailową, to coś więcej niż cyfrowy adres. To wrota do archiwum informacji, a WHOIS to klucz, który te wrota otwiera.

DNA protokołu WHOIS — definicja i cele

Wyszukanie WHOIS polega na wysłaniu zapytania do jednego z wielu serwerów WHOIS odpowiedzialnych za zarządzanie bazą danych **domen najwyższego poziomu** (ang. *Top-Level Domain*, TLD). W odpowiedzi serwer WHOIS sprawdza informacje w swojej bazie danych i wysyła rekord tekstowy zawierający dostępne dane rejestracyjne dla przedmiotu zapytania. Obejmuje to informacje na temat rejestratora domeny, danych kontaktowych abonenta, serwerów nazw, daty rejestracji i wygaśnięcia oraz statusu. Oto dokładny przebieg zdarzeń:

1. Wydajemy polecenie WHOIS. Za kulisami zapytanie jest przekierowywane do serwera WHOIS, który specjalizuje się w domenie najwyższego poziomu, o którą pytamy. Domeny najwyższego poziomu to na przykład *.com*, *.org* czy *.net* albo domeny krajowe, takie jak *.pl* czy *.uk*. Każda domena najwyższego poziomu ma swój serwer WHOIS.
2. Serwer WHOIS otrzymuje zapytanie i je przetwarza. Wyszukuje w swojej bazie danych informacje dotyczące nazwy domeny lub adresu IP, który wskazaliśmy.
3. Jeżeli serwer WHOIS znajdzie dopasowanie, komponuje odpowiedź zawierającą różne dane. Mogą one obejmować następujące pola:
   - ***Registrant* (*Abonent*)**: imię i nazwisko lub nazwa, adres oraz dane kontaktowe właściciela domeny;
   - ***Registrar* (*Rejestrator*)**: nazwa podmiotu, który prowadzi rejestrację domen;
   - ***Name Servers* (*Serwery nazw*)**: serwery odpowiedzialne za zarządzanie rekordami DNS domeny;
   - ***Creation Date* (*Utworzona*) i *Registry Expiry Date* (*Koniec okresu rozliczeniowego*)**: data rejestracji domeny oraz data, do której opłacona jest domena;
   - ***Domain Status* (*Status*)**: informacja, czy domena jest aktywna, zablokowana czy może znajduje się w jeszcze innym stanie;
   - ***DNSSEC***: informacja, czy domena korzysta z rozszerzenia bezpieczeństwa systemu DNS (ang. *DNS Security Extensions*, DNSSEC), które zapewnia dodatkową ochronę.

4. Serwer WHOIS formatuje informacje w ustrukturyzowaną odpowiedź i wysyła na nasz komputer. Format może się różnić w zależności od serwera WHOIS oraz domeny najwyższego poziomu, ale zazwyczaj przypomina niesformatowany tekst.
5. Na koniec nasz komputer wyświetla odpowiedź WHOIS na ekranie. Jako specjaliści ds. cyberbezpieczeństwa analizujemy te informacje, aby uzyskać wgląd w historię rejestracji domeny, jej własność oraz inne istotne szczegóły.

Zobaczmy, jak to wygląda w praktyce. Łączę się z terminalem i wita mnie czarny ekran, oczekujący na moje polecenia. Wpisuję proste zapytanie i budzę bestię:

```
whois daledumbsitdown.com
```

Wynik użycia polecenia prezentuje rysunek 4.1.

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: daledumbsitdown.com
Registry Domain ID: 1972026533_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.eu
Registrar URL: http://www.registrar.eu
Updated Date: 2023-09-26T19:42:16Z
Creation Date: 2015-10-26T17:41:51Z
Registrar Registration Expiration Date: 2024-10-26T17:41:51Z
Registrar: Hosting Concepts B.V. d/b/a Registrar.eu
Registrar IANA ID: 1647
Registrar Abuse Contact Email: abuse@registrar.eu
Registrar Abuse Contact Phone: +31.104482297
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Whois Privacy Protection Foundation
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Zuid-Holland
Registrant Postal Code: REDACTED FOR PRIVACY
```

Rysunek 4.1. Wyniki zapytania WHOIS dla domeny daledumbsitdown.com

Ekran ożywa. Jak potok płyną kolejne wiersze z informacjami na temat domeny. To coś więcej niż dane rejestracyjne — to historia, biografia i odcisk palca w jednym.

WHOIS to nie tylko narzędzie. Służy za publiczny rejestr cyfrowych nieruchomości. Zapewnia podstawowe informacje na temat domeny lub adresu IP. Kto jest właścicielem domeny? Kiedy została zarejestrowana? Kiedy wygasa rejestracja? Rejestry WHOIS pozwalają usłyszeć bicie serca domeny — cichy puls w tle, często niedostrzegany, ale którego znaczeniu nie da się zaprzeczyć.

Zakres zastosowań — nie tylko domeny, lecz również bloki adresów IP

Możliwości wyszukiwania w bazach danych WHOIS wykraczają poza weryfikację domen. Tak jak każda strona internetowa ma swoją domenę, każde urządzenie w sieci ma swój adres IP — unikalny zestaw liczb, który odróżnia go od milionów innych. Niektóre firmy są właścicielami bloków adresów IP, co może być źródłem interesujących informacji.

Gdy wyślemy zapytanie WHOIS na temat bloku adresów IP, możemy zdobyć informacje na temat alokacji i dystrybucji adresów IP oraz podmiotów, które je kontrolują.

Zapytanie o adres IP *8.8.8.8* szybko pokazuje, że cały blok adresów IP należy do firmy Google (rysunek 4.2).

```
NetRange:       8.8.8.0 - 8.8.8.255
CIDR:           8.8.8.0/24
NetName:        GOGL
NetHandle:      NET-8-8-8-0-2
Parent:         NET8 (NET-8-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Google LLC (GOGL)
RegDate:        2023-12-28
Updated:        2023-12-28
Ref:            https://rdap.arin.net/registry/ip/8.8.8.0


OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2019-10-31
```

Rysunek 4.2. Wyniki zapytania WHOIS pokazujące blok adresów IP zarządzanych przez firmę Google

WHOIS odgrywa kluczową rolę w mapowaniu cyfrowego krajobrazu. Określa granice, rejestruje zmiany i — mimo że cyfrowy świat wydaje się przepastny i nieprzewidywalny — gwarantuje każdej witrynie miejsce na mapie.

Cyfrowa lupa — popularne platformy zapytań WHOIS

Cyberprzestrzeń pełna jest tych, którzy mówią językiem protokołu WHOIS, ale niewielu rozumie jego istotę. Oto niektóre prominentne figury w tej dziedzinie.

DomainTools

DomainTools (*https://www.domaintools.com*) to użyteczne narzędzie do obsługi zapytań WHOIS, które zapewnia szczegółowe informacje rejestracyjne na temat domeny o wskazanej nazwie. Gdy wpiszemy nazwę domeny w pasku wyszukiwania, wyświetli się status rejestracji domeny, rejestrator, serwery nazw oraz dane kontaktowe abonenta. Najważniejsze informacje, jakie wyświetla narzędzie DomainTools, to:

- data rejestracji domeny i koniec okresu rozliczeniowego;
- rejestrator, który dokonał rejestracji domeny;
- nazwa, numer telefonu i adres abonenta;
- dane kontaktowe osoby ds. administracyjnych i technicznych dla danej domeny;
- serwery nazw dla domeny oraz informacje DNS.

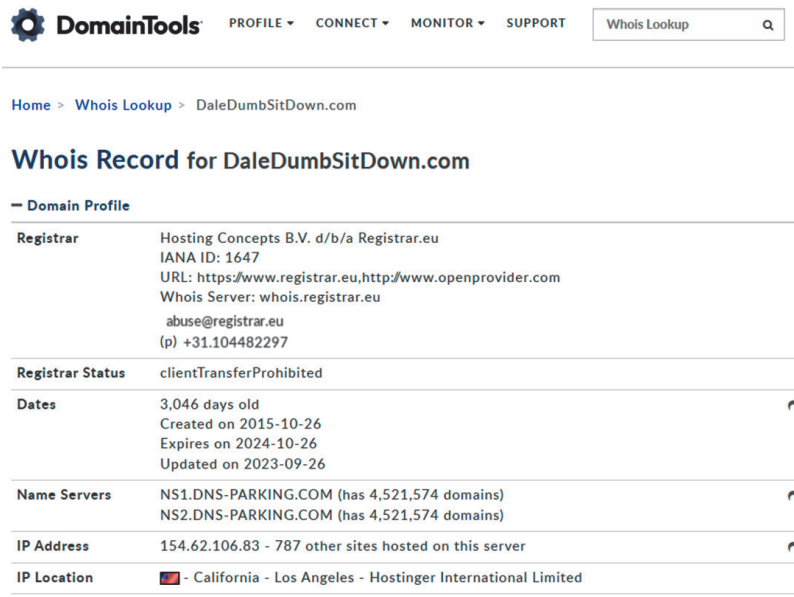
Zapytanie WHOIS wykonane narzędziem DomainTools pobiera dane z odpowiedniej bazy danych WHOIS dla każdej domeny najwyższego poziomu. W szybki i prosty sposób udostępnia bogactwo informacji na temat właściciela i szczegółów technicznych domeny (rysunek 4.3). Narzędzie jest użyteczne w analizie domeny, monitorowaniu rejestracji i badaniu domen do celów bezpieczeństwa.

Whois.com

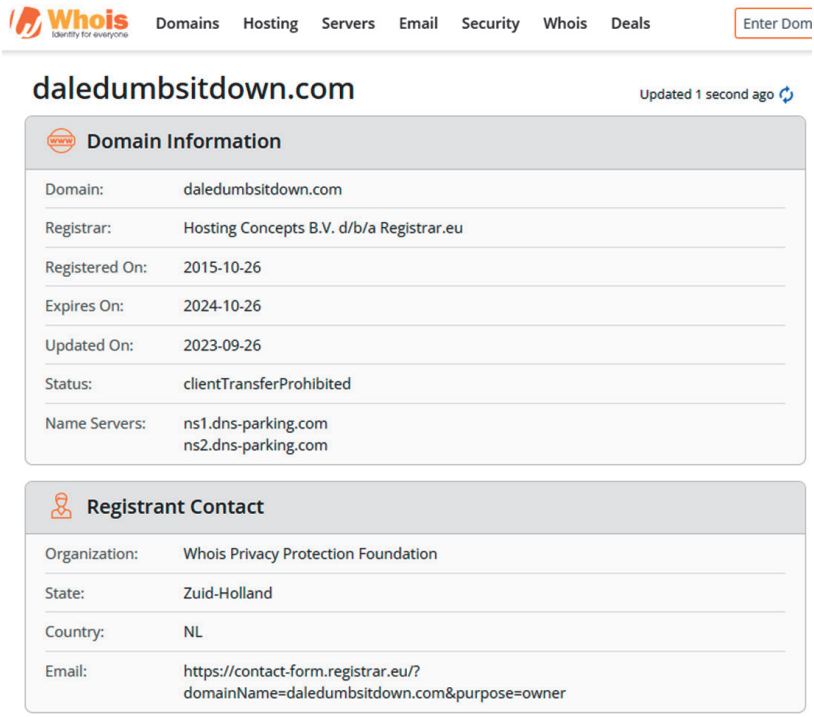
Strona internetowa Whois.com jest zgrabna i prosta. Bez zbędnych upiększeń rozwiewa cyfrową mgłę i pokazuje esencję informacji na temat domeny (rysunek 4.4).

Chociaż zapytania WHOIS dają wgląd w szczegółowe dane na temat rejestracji domeny, wielu abonentów ukrywa dzisiaj swoje dane osobowe przed publicznym wzrokiem, korzystając z usług pośredniczących, które chronią ich prywatność. Takie usługi zastępują nazwę lub imię i nazwisko, adres, numer telefonu oraz adres e-mailowy abonenta w publicznym rejestrze WHOIS danymi kontaktowymi pośrednika. Pozwala to właścicielom domen zachować anonimowość.

W tym miejscu należy jednak zauważyć, że nie daje to stuprocentowej gwarancji anonimowości. Usługodawcy są prawnie zobowiązani do udostępnienia danych chronionego przez siebie klienta, jeżeli otrzymają wezwanie lub nakaz sądowy. Organy ścigania i właściciele praw własności intelektualnej mogą wnosić do sądów o ujawnienie danych rzeczywistych właścicieli nielegalnych lub zwodniczych stron, jeżeli chowają się oni za pośrednikami. Podsumowując: anonimowość oferowana przez takie usługi ma swoje granice.



Rysunek 4.3. Interfejs do wysyłania zapytań WHOIS w narzędziu DomainTools



Rysunek 4.4. Wyniki ze strony Whois.com dla domeny daledumbsitdown.com

Gdyby tylko istniał sposób, aby cofnąć się w czasie! Wcześniej ludzie nie mieli takiej obsesji na punkcie prywatności. Rzecz w tym, że taki sposób istnieje. Witryna WHOXY (*https://www.whoxy.com*) udostępnia historyczne rejestry domen. Zobaczmy, co właściciel domeny *https://www.daledumbsitdown.com* chciał ukryć (rysunek 4.5).



Rysunek 4.5. Wyniki ze strony Whoxy.com dla domeny daledumbsitdown.com

Każde z zaprezentowanych tutaj narzędzi ma swoje zalety, które pozwalają niezłomnym badaczom uzyskać lepszy wgląd w strukturę sieci. To różne soczewki mikroskopu, pokazujące warstwy, niuanse i aspekty, które inaczej pozostałyby w ukryciu.

Odnajdywanie połączeń

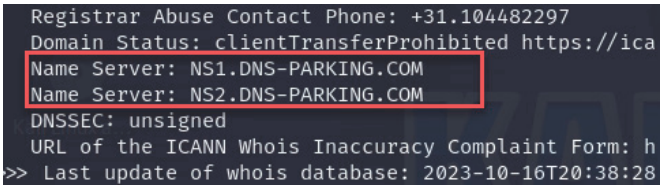
Wykrywanie powiązań domen i ich właścicieli w bazach danych WHOIS to cenny element dochodzeń w dziedzinie cyberbezpieczeństwa, zwłaszcza jeżeli chcemy odkryć nieoczywiste związki między podmiotami. Oto jak się za to zabrać:

1. **Zacznij od domeny głównej**. W bazie danych WHOIS wyszukaj główną domenę, będącą obiektem zainteresowania. Tutaj mamy przykład takiego polecenia:

   ```
   whois daledumbsitdown.com
   ```

   Zwróci ono informacje na temat właściciela i rejestracji głównej domeny.

2. **Poszukaj serwerów nazw**. W wynikach zapytania WHOIS odnajdźmy serwery nazw domeny. Te serwery są odpowiedzialne za przechowywanie rekordów DNS dla danej domeny. Wpisy często wyglądają tak jak na rysunku 4.6.



Rysunek 4.6. Serwery nazw dla domeny daledumbsitdown.com

3. **Zbadaj serwery nazw**. Teraz wykonaj zapytania WHOIS dla każdego ze zidentyfikowanych serwerów nazw. Dla przykładu z rysunku 4.6 będą one wyglądały następująco:

```
whois ns1.dns-parking.com
whois ns2.dns-parking.com
```

Uwaga

Te zapytania zwrócą informacje na temat serwerów nazw i mogą wskazać na inne domeny, które używają tych samych serwerów nazw. To cenna wskazówka, która może pomóc zidentyfikować powiązane domeny.

4. **Sprawdź często pojawiających się abonentów**. W wynikach WHOIS dla serwerów nazw poszukaj abonentów, których nazwy często się powtarzają. Abonenci to organizacje lub osoby prywatne, które zarejestrowały domenę. Jeżeli znajdziesz nazwę lub dane kontaktowe tego samego abonenta w danych dla wielu domen, możesz założyć, że mają tego samego właściciela.
5. **Zbadaj subdomeny i wszelkie inne tropy**. Możesz wysłać szczegółowe zapytania nie tylko na temat serwerów nazw, lecz także na temat subdomen oraz wszelkich innych domen powiązanych z domeną główną. Zapytania mogą wyglądać tak:

```
whois subdomain.daledumbsitdown.com
whois additional-daledumbsitdown.com
```

Ciemna strona mocy — użycie rekordów WHOIS do przeprowadzania ataków

Wyobraź sobie taki scenariusz: za pomocą baz WHOIS hakerzy zbierają użyte do rejestracji adresy e-mailowe i dane właścicieli, aby wykorzystać je do swoich niecnych planów obejmujących przekręt phishingowy. Któż potrafi się oprzeć odruchowi otworzenia e-maila, którego nadawca wygląda tak dziwnie znajomo? To idealna przynęta.

To jednak nie wszystko. Hakerzy często wyszukują domeny, dla których zbliża się koniec okresu rozliczeniowego. Jeżeli rejestracja wygaśnie, przejmują domenę szybciej, niż bylibyśmy w stanie powiedzieć „cyberbezpieczeństwo". Po co? Takie przejęte domeny mogą rozprowadzać złośliwe oprogramowanie lub przekierowywać nieświadomych niczego użytkowników internetu do niebezpiecznych stron.

Bywa jeszcze gorzej. Stosując socjotechniczne sztuczki, cybernetyczni naciągacze potrafią nakłonić właścicieli do przekazania im własności domeny. Podstępne zawłaszczenie cyfrowego aktu własności umożliwia im przejęcie kontroli nad witryną.

Nie zapominajmy o serwerach nazw. Rejestry WHOIS bez zająknięcia zwracają te istotne informacje o infrastrukturze, wręcz zapraszając do ataków DDoS lub ataków przechwytywania DNS (ang. *DNS hijacking*). Dzięki sprytnie spreparowanym rekordom DNS cybernetyczni oszuści mogą tworzyć cyfrowe iluzje, prowadzące nieświadomych internautów na manowce.

Aby ukryć swoje prawdziwe intencje, atakujący używają często serwerów pośredniczących i prowadzą nieustające ataki na serwery WHOIS, aby wykryć podatności i zidentyfikować kolejne cele. Dla nich dane WHOIS to nie mglista wskazówka, lecz gotowy przepis na atak.

Analiza rekordów DNS i adresów IP — wiązanie domen z infrastrukturą

Techniki OSINT umożliwiają wykorzystanie rekordów DNS i adresów IP do wykrywania ukrytych powiązań między domenami a infrastrukturą. Zapytanie DNS dotyczące domeny *hackthissite.org* (wpisz `dig hackthissite.org` w terminalu) ujawnia powiązane z nią adresy IP (rysunek 4.7).

Możemy również wykonać odwrotne zapytanie DNS dla adresu IP (wpisz `dig -x 137.74.187.102`), aby znaleźć nazwy hostów powiązanych ze wskazanym adresem (rysunek 4.8).

W tym przypadku nie widzimy żadnych innych domen, ponieważ na tym hoście ich nie ma, ale w niektórych przypadkach wyniki mogłyby wyglądać mniej więcej tak:

```
;; ANSWER SECTION:
host1234.examplehosting.com. 3600 IN A 93.184.216.34
site1.com. 3600 IN CNAME host1234.examplehosting.com.
site2.net. 3600 IN CNAME host1234.examplehosting.com.
site3.org. 3600 IN CNAME host1234.examplehosting.com.
```

Gdy korzystamy z systemu operacyjnego Windows, najlepszym wyborem do analizy rekordów DNS będzie narzędzie wiersza poleceń `nslookup`. Składnia polecenia wygląda następująco:

```
nslookup hackthissite.org
```

```
┌──(kali㉿kali)-[~]
└─$ dig hackthissite.org

; <<>> DiG 9.19.17-1-Debian <<>> hackthissite.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13300
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;hackthissite.org.              IN      A

;; ANSWER SECTION:
hackthissite.org.       3600    IN      A       137.74.187.102
hackthissite.org.       3600    IN      A       137.74.187.100
hackthissite.org.       3600    IN      A       137.74.187.101
hackthissite.org.       3600    IN      A       137.74.187.104
hackthissite.org.       3600    IN      A       137.74.187.103
```

Rysunek 4.7. Wyniki użycia polecenia dig hackthissite.org

```
┌──(kali㉿kali)-[~]
└─$ dig -x 137.74.187.102

; <<>> DiG 9.19.17-1-Debian <<>> -x 137.74.187.102
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;102.187.74.137.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
102.187.74.137.in-addr.arpa. 21600 IN   PTR     hackthissite.org.

;; Query time: 220 msec
;; SERVER: 10.10.10.1#53(10.10.10.1) (UDP)
;; WHEN: Mon Oct 16 16:17:15 MDT 2023
;; MSG SIZE  rcvd: 86
```

Rysunek 4.8. Polecenie dig zwraca rekord PTR dla adresu IP 137.74.187.102

Wynik pokazałem na rysunku 4.9.

```
Non-authoritative answer:
Name:   hackthissite.org
Address: 137.74.187.102
Name:   hackthissite.org
Address: 137.74.187.100
Name:   hackthissite.org
Address: 137.74.187.104
Name:   hackthissite.org
Address: 137.74.187.101
Name:   hackthissite.org
Address: 137.74.187.103
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:102
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:100
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:104
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:103
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:101
```

Rysunek 4.9. Wyniki polecenia nslookup dla domeny hackthissite.org

To nie wszystko!

W ramach dochodzeń OSINT rekordy DNS dostarczają mnóstwa informacji. Pytając o różne rodzaje rekordów, analityk może poznać istotne informacje na temat zasobów internetowych i infrastruktury organizacji. W tym punkcie poznasz kilka ważnych typów rekordów DNS i wykorzystasz je do zebrania informacji wywiadowczych.

Rekordy A i AAAA

Rekordy A i **AAAA** łączą nazwy domen z powiązanymi adresami IPv4 i IPv6. Sprawdzenie rekordu A domeny pokazuje adres IP, pod którym dostępna jest domena, co umożliwia zdobycie kolejnych informacji poprzez odwrotną translację adresów DNS (ang. *reverse DNS lookup*) i poznanie innych domen dostępnych pod tym samym adresem IP.

Do wygenerowania zapytania o rekordy A możemy użyć narzędzia `nslookup`:

```
nslookup
> set type=A
> daledumbsitdown.com
```

Wyniki obrazuje rysunek 4.10.

Rekordy MX

Rekordy wymiany poczty (ang. *mail exchange record*, MX) określają serwery poczty elektronicznej odpowiedzialne za dostarczanie wiadomości na adresy e-mailowe z danej domeny. Wylistowanie rekordów MX domeny ujawnia główną infrastrukturę poczty

```
PowerShell 7.3.8
PS C:\Users\dalem> nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set type=A
> daledumbsitdown.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    daledumbsitdown.com
Address:  84.32.84.227

>
```

Rysunek 4.10. Zapytanie o rekord A dla domeny daledumbsitdown.com

elektronicznej, która może być celem przyszłych ataków socjotechnicznych lub kampanii hakerskich. Narzędzia takie jak `nslookup` umożliwiają zawężenie zapytania do tych konkretnych rekordów. Przyda się przećwiczyć to w praktyce.

Najpierw wpisz `nslookup` i naciśnij klawisz *Enter*. Następnie określ rodzaj rekordu do wyszukania i nazwę domeny:

```
nslookup
> set type=MX
> daledumbsitdown.com
```

Na ekranie pojawi się wynik podobny do tego z rysunku 4.11.

```
> set type=mx
> daledumbsitdown.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
daledumbsitdown.com     MX preference = 10, mail exchanger = mx2.hostinger.com
daledumbsitdown.com     MX preference = 5, mail exchanger = mx1.hostinger.com
>
```

Rysunek 4.11. Wyniki zapytania o rekordy MX wygenerowane narzędziem nslookup

Na zrzucie ekranu widzimy dwa serwery poczty elektronicznej dla domeny *daledumbsitdown.com* z przypisanym priorytetem.

Uwaga

Priorytet (`preference = X`) pokazuje, z którym serwerem najpierw zostanie nawiązane połączenie. Zasada jest taka, że im niższa liczba, tym wyższy priorytet. W tym przypadku serwer o priorytecie równym 5 (`mx1.hostinger.com`) będzie pierwszy w kolejce.

Rekordy TXT

Rekordy TXT pozwalają dołączyć dowolny tekst dla administratorów domeny (rysunek 4.12). W tym miejscu można opublikować dane konfiguracyjne, takie jak rekordy specyfikacji Sender Policy Framework (SPF), które identyfikują autoryzowane serwery poczty elektronicznej dla domeny. Zebranie danych SPF z rekordów TXT może ujawnić zatwierdzoną infrastrukturę do wysyłania e-maili dla danej organizacji.

```
> set type=txt
> daledumbsitdown.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
daledumbsitdown.com     text =

        "google-site-verification=FZnGQZA-xR4TrUjCak_3zyPfhSc8BTM1zVOw2X80LAE"
daledumbsitdown.com     text =

        "v=spf1 include:_spf.mail.hostinger.com ~all"
daledumbsitdown.com     text =

        "pinterest-site-verification=881a39213331c0b4ead786126f31d959"
daledumbsitdown.com     text =

        "google-site-verification=7NNP3Uqgi8cVyDGbcpy8BOGItDFQV1Ug0YFVBsiWlaU"
>
```

Rysunek 4.12. Wyniki zapytania o rekordy TXT wygenerowane narzędziem nslookup

Rekordy CNAME

Rekordy nazwy kanonicznej (ang. *canonical name record*, CNAME) łączą aliasy domeny z jej prawdziwą nazwą (rysunek 4.13). Rekordy te mogą pokazywać powiązania między domenami a dostawcami usług wyższego rzędu.

```
> set type=cname
> hackthissite.org
Server:  dns.google
Address:  8.8.8.8

hackthissite.org
        primary name server = c.ns.buddyns.com
        responsible mail addr = admin.hackthissite.org
        serial  = 2023040305
        refresh = 3600 (1 hour)
        retry   = 900 (15 mins)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
>
```

Rysunek 4.13. Sprawdzenie aliasów dla domeny hackthissite.org

Wykorzystując znajomość tych i innych typów rekordów DNS, analitycy OSINT mogą opracować schemat kluczowych zasobów sieciowych i zrozumieć powiązania w obrębie organizacji lub domeny. W następnym rozdziale zajmiemy się dodatkowymi technikami gromadzenia informacji wywiadowczych na temat infrastruktury.

Mapowanie cyfrowego śladu — wykorzystanie analizy rekordów DNS i adresów IP

Technika analizy rekordów DNS i adresów IP pozwala rzucić nieco światła na infrastrukturę sieciową organizacji i jej powiązania. Oto kilka sposobów, w jakie można wykorzystać tę wiedzę:

- **Opracowanie schematu infrastruktury**. Zapytania DNS dotyczące domen zwracają informacje na temat powiązanych adresów IP, serwerów nazw, serwerów poczty elektronicznej i innych hostów. Odwrotna translacja domen na adresy IP dostarcza danych o dodatkowych domenach i zasobach związanych z celem. Na podstawie tych elementów analityk może stworzyć diagram cyfrowego śladu celu.
- **Wykrycie współdzielonej infrastruktury hostingowej**. Zapytania DNS często pokazują, że na tym samym serwerze lub pod tym samym adresem IP dostępnych może być wiele domen. Może to sugerować, że te domeny należą do tej samej organizacji, nawet jeżeli dane rejestracyjne WHOIS się różnią.
- **Potwierdzenie powiązań domeny**. Analiza rekordów DNS sprawdza powiązania między domenami poprzez weryfikację podsieci, serwerów nazw, adresów IP oraz innych dopasowań w rekordach DNS. Możesz znaleźć witryny stron zależnych, subdomeny, domeny partnerów itp.
- **Wykrywanie nowo utworzonych domen**. Monitorowanie rekordów DNS w czasie informuje o rejestracji nowych domen w istniejącej infrastrukturze. Jest użyteczne do wykrywania nowych zasobów.
- **Śledzenie zmian infrastruktury**. Zmiany w rekordach DNS informują o migracjach, restrukturyzacjach, zamknięciach lub przejęciach domen.
- **Pozyskiwanie informacji geograficznych na temat hostingu**. Geolokalizacja adresów IP umożliwia określenie fizycznego regionu, gdzie znajdują się serwery, a przez to również geograficznego kontekstu.
- **Identyfikacja usług stron trzecich**. Badanie rekordów DNS i adresów IP informuje o użyciu zewnętrznych usług, takich jak sieci dostarczania treści (ang. *content delivery network*, CDN), ochrona przed atakami DDoS czy usługi chmurowe na bazie nazw hostów.
- **Weryfikacja autentyczności domeny**. Można potwierdzić, że adres IP odpowiada prawdziwej stronie i nie prowadzi do podrobionej domeny.

Analiza rekordów DNS i adresów IP rzuca światło na cyfrowy ślad organizacji, jej infrastrukturę, powiązania, lokalizacje, usługi i zmiany. Jeżeli zastosujemy ją w procesie zbierania wywiadu, może zapewnić nieoceniony wgląd w cyfrowy ślad celu.

Traceroute i mapowanie sieci — kartografowie cybernetycznych mórz

Bez właściwych narzędzi żeglowanie po złożonych sieciach może być nie lada wyzwaniem. ***Traceroute*** oraz narzędzia do **mapowania sieci** to niezbędne instrumenty, które pozwalają nam poruszać się po zawiłych ścieżkach przepływu danych i rozumieć je z dużą dozą precyzji i jasności. Stanowią kluczowy element, który przekształca enigmatyczny taniec pakietów w możliwe do uchwycenia wzorce.

Traceroute

Program *traceroute* to sieciowe narzędzie diagnostyczne używane do mapowania ścieżki między systemem źródłowym a systemem docelowym w sieci IP. Wysyła pakiety UDP lub ICMP, stopniowo zwiększając tzw. **czas życia pakietu** (ang. *Time To Live*, TTL), czyli liczbę dopuszczalnych przeskoków (ang. *hop*) na trasie, i rejestruje źródło pakietów przychodzących w odpowiedzi.

Po wysłaniu pakietu przez *traceroute* pierwszy router na trasie danego pakietu zmniejsza wartość pola TTL o 1 i przekazuje go do kolejnego routera. Gdy wartość TTL osiągnie zero, router odrzuca pakiet i wysyła komunikat ICMP o błędzie przekroczenia czasu do nadawcy pakietu.

Pozwala to narzędziu *traceroute* poznać wszystkie routery na trasie po źródłowym adresie IP otrzymanego pakietu ICMP. Program *traceroute* zaczyna od małej wartości TTL, a następnie stopniowo ją zwiększa, co pozwala mu zarejestrować każdy kolejny router na trasie do celu.

Na przykład śledzenie trasy pakietu z hosta *A* do hosta *B* wyglądałoby w ten sposób:

1. Host *A* wysyła pakiet UDP z wartością TTL ustawioną na 1 i hostem *B* jako systemem docelowym.
2. Pierwszy router na trasie (*R1*) otrzymuje pakiet i zmniejsza wartość TTL do 0, odrzuca pakiet i wysyła komunikat ICMP do hosta *A*. W ten sposób zidentyfikowano router *R1*.
3. Host *A* wysyła nowy pakiet z wartością TTL ustawioną na 2. Router *R1* zmniejsza wartość TTL do 1, a potem przesyła pakiet do routera *R2*. Router *R2* zmniejsza wartość TTL do 0, odrzuca pakiet i wysyła ICMP do hosta *A*. W ten sposób zidentyfikowano router *R2*.
4. Proces przebiega dalej, a wartość TTL jest stopniowo zwiększana, dopóki pakiet nie dotrze do celu, tzn. do hosta *B*.

Po drodze *traceroute* (lub ***tracert*** dla użytkowników systemu Windows) rejestruje adresy IP i opóźnienia sieci przy każdym przeskoku. W ten sposób powstaje mapa ścieżki i jej jakości między źródłem a miejscem docelowym w sieci. Z tego względu *traceroute* to ważne narzędzie do rozwiązywania problemów z siecią i tworzenia jej topologii.

Narzędzie *traceroute* jest używane z poziomu wiersza poleceń. Do polecenia należy dołączyć argument w postaci docelowej nazwy hosta lub adresu IP. Podstawowa składnia w systemach Linux i macOS wygląda następująco:

```
traceroute [miejsce docelowe]
```

Gdybyśmy na przykład chcieli prześledzić trasę do domeny `daledumbsitdown.com`, polecenie wyglądałoby tak:

```
traceroute daledumbsitdown.com
```

Pakiety UDP pomkną przez sieć, a my zobaczymy mniej więcej takie wyniki jak na rysunku 4.14.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ traceroute daledumbsitdown.com
traceroute to daledumbsitdown.com (191.96.144.104), 30 hops max,
 1  firewalla.lan (10.10.10.1)  0.365 ms  0.401 ms  0.359 ms
 2  192.168.1.1 (192.168.1.1)  8.908 ms  8.899 ms  8.828 ms
 3  lo0.mar1.slc.xmission.net (166.70.255.53)  11.686 ms  11.642
 4  br2.core.xmission.net (166.70.1.22)  11.490 ms  11.473 ms  1
 5  ae-15.a03.lsanca07.us.bb.gin.ntt.net (129.250.195.105)  45.1
 6  ae-13.r24.lsanca07.us.bb.gin.ntt.net (129.250.3.141)  44.811
 7  ae-3.r22.dllstx14.us.bb.gin.ntt.net (129.250.7.68)  60.907 m
 8  ae-15.r21.dllstx14.us.bb.gin.ntt.net (129.250.2.58)  64.911
 9  ae-4.r25.atlnga05.us.bb.gin.ntt.net (129.250.4.117)  86.958
10  129.250.4.67 (129.250.4.67)  86.739 ms  82.010 ms  81.878 ms
```

Rysunek 4.14. Wyniki polecenia traceroute z nazwą domeny daledumbsitdown.com jako argumentem

Każda linia zawiera numer porządkowy przeskoku, adres IP oraz opóźnienie.

Symbol gwiazdki (*) w wynikach oznacza, że od danego routera na trasie nie otrzymano odpowiedzi. Istnieje kilka możliwych powodów:

- **Blokada przez zaporę sieciową (ang. *firewall*)**. Router może być chroniony zaporą sieciową, która blokuje wysyłanie komunikatów ICMP o błędzie dla pakietów z zerowym TTL lub blokuje pakiety UDP/TCP narzędzia *traceroute*. Z tego względu odpowiedź nigdy nie nadchodzi.
- **Ograniczenie przepustowości**. Aby zapobiec przeciążeniu, niektóre routery ograniczają liczbę pakietów do śledzenia ścieżki, na którą odpowiadają. W przypadku przekroczenia limitu przestają reagować.
- **Utrata pakietów**. Gdy sieć jest przeciążona lub następuje utrata pakietów po drodze, pakiety wysyłane przez *traceroute* mogą nie dotrzeć do kolejnego routera. W takim przypadku również na próżno czekamy na odpowiedź.
- **Niewłaściwy adres**. Adres IP routera może być źle skonfigurowany lub nieosiągalny, przez co pakiet sondujący nigdy nie dotrze do celu.

- **Awaria routera**. Router może być niesprawny, odłączony od sieci lub z innego powodu niedostępny. W takim przypadku nie obsłuży pakietu i nie wygeneruje odpowiedzi.

Możemy również doprecyzować działanie narzędzia *traceroute*, na przykład aby korzystało z protokołu TCP poprzez dodanie opcji `-T`, ograniczyło liczbę przeskoków z użyciem opcji `-m` albo prześledziło ścieżkę w odwrotnej kolejności dzięki opcji `-r`. Na przykład:

```
traceroute -T -m 50 -r daledumbsitdown.com
```

W tym przypadku *traceroute* będzie wysyłać pakiety TCP i będzie stopniowo zmniejszać czas ich życia, a liczbę wyświetlonych wyników ograniczy do co najwyżej 50 skoków.

Mapowanie sieci

Mapowanie sieci to kluczowa technika OSINT, która pomaga poznać cyfrowy ślad organizacji będącej celem dochodzenia. Analitycy OSINT wykorzystują różne narzędzia do wizualizacji tras sieciowych, identyfikowania kluczowej infrastruktury oraz wykrywania związków między zasobami podłączonymi do internetu.

Nmap

Nmap umożliwia sondowanie aktywnych hostów oraz listowanie usług i systemów operacyjnych. Przeanalizujmy kilka przykładów użycia:

```
nmap 192.168.1.1
```

To polecenie wykonuje podstawowe skanowanie SYN na danym hoście, aby znaleźć otwarte porty TCP.

```
nmap -sU -p 123,161 10.0.0.0/24
```

W tym przypadku Nmap wykona skanowanie UDP w tej podsieci, obierając za cel porty obsługujące protokoły NTP i SNMP.

Zastanawiasz się, jakiego systemu operacyjnego używa urządzenie? Sprawdźmy:

```
nmap -O hackthissite.org
```

Jeżeli chcesz dowiedzieć się więcej, ale nieco bardziej dyskretnie, użyj trybu ninja:

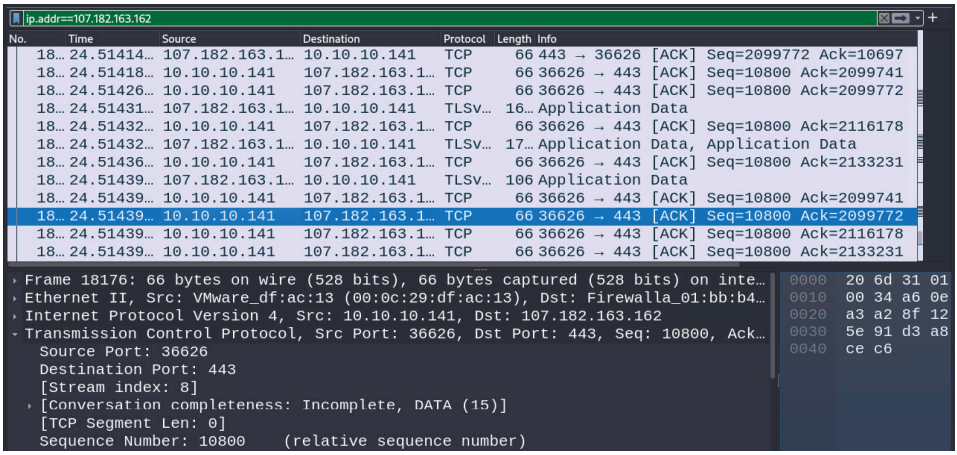
```
nmap -sS hackthissite.org
```

Jeżeli chodzi o program Nmap, można by napisać niejedną książkę o tym wspaniałym narzędziu. W internecie na pewno znajdziesz sporo materiałów do wyboru.

Wireshark

Wireshark to analizator pakietów o ogólnodostępnym kodzie źródłowym umożliwiający dogłębną inspekcję ruchu sieciowego, komunikacji i protokołów. Działa niczym wielozadaniowy mikroskop sieciowy, pozwalając użytkownikom przechwytywać pakiety przechodzące przez przewodowe, bezprzewodowe i wirtualne interfejsy. To kolejne narzędzie, któremu poświęcono całe książki. Zacznijmy jednak od czegoś prostego:

1. Uruchom Wiresharka i zacznij przechwytywać pakiety z wybranego interfejsu. Zastosuj filtr wyświetlania, taki jak `ip.addr==154.41.250.193`, aby wyodrębnić ruch płynący do tego adresu IP lub z niego.
2. Sprawdź przechwycone pakiety i zwróć uwagę na wszelkie inne adresy IP komunikujące się ze wskazanym adresem. Mogą to być serwery, klienty lub sąsiednie routery.
3. Zastosuj dodatkowe filtry, aby wyodrębnić ruch z wynikowych adresów IP. Wpisz na przykład `ip.src==192.168.1.105`, aby przejrzeć wszelki ruch z nowo znalezionego adresu IP.
4. Przeanalizuj ten ruch i zidentyfikuj nazwy hostów na podstawie zapytań i odpowiedzi DNS. Określ otwarte porty na podstawie portów docelowych i określ usługi dzięki analizie protokołów.
5. Kliknij prawym przyciskiem myszy na strumień komunikacji i wybierz opcję *Follow TCP Stream* (obserwuj strumień TCP), aby odtworzyć przepływ i odnaleźć wszelkie możliwe do odczytania pakiety danych, które mogą dostarczać wskazówek na temat ich funkcji i celu (rysunek 4.15).



Rysunek 4.15. Przeglądanie połączeń do domeny daledumbsitdown.com narzędziem Wireshark

Użyj funkcji filtrowania, analizy TCP oraz dekodowania Wiresharka, aby poszerzyć mapę sieci zaczynającą się od adresu IP *154.41.250.193*. Odkrywaj nowe adresy IP, nazwy hostów, relacje i role sąsiednich hostów.

Analizę przeprowadzoną za pomocą Wiresharka uzupełnij dzięki innym wyszukiwaniom, takim jak odwrotna translacja adresów DNS, zapytania do bazy danych WHOIS czy skany narzędziem Nmap, aby wzbogacić znalezione dane o adresach IP i nazwach hostów.

Jak widzisz, Wireshark może być potężnym sojusznikiem w odkrywaniu warstw sieciowej komunikacji oraz skrywanych przez nie sekretów. Nasza eksploracja na tym się jednak nie kończy. Po utworzeniu mapy sieci czas na rozpoznanie witryn internetowych.

Rozpoznanie witryn internetowych — zgłębianie niewidocznych warstw

System Kali Linux zapewnia użytkownikom wiele narzędzi z zakresu rozpoznania witryn internetowych, stworzonych z myślą o gromadzeniu i szczegółowej analizie danych.

W tym podrozdziale lepiej poznasz ten zestaw narzędzi. Nauczysz się, w jaki sposób automatycznie pozyskiwać dane ze stron internetowych, analizować je w narzędziu **Metagoofil**, sprawdzać historię strony w archiwum **Wayback Machine** oraz szukać ukrytych katalogów i plików. Te techniki stanowią podstawę analizy stron internetowych. Ich użycie zapewni Ci dobry start.

Pozyskiwanie danych ze stron internetowych i ich analiza

Web scraping odnosi się do automatycznego wydobywania i zbierania danych ze stron internetowych. Obejmuje użycie narzędzi i skryptów do systematycznego pozyskiwania i przetwarzania treści, metadanych oraz innych informacji ze stron internetowych.

Web scraping umożliwia gromadzenie na dużą skalę treści tekstowych, obrazów, dokumentów i ustrukturyzowanych danych z internetu. Te surowe dane można potem analizować, aby formułować nieoczywiste wnioski, monitorować zmiany w czasie, przekształcać je w zbiory danych oraz używać ich do innych celów.

Skoro wiesz już, w jaki sposób web scraping pomaga zbierać duże zbiory danych, przyjrzymy się narzędziu Metagoofil.

Metagoofil

Chociaż metadane mogą dostarczać cennych informacji na temat dokumentu, ich obecność może również stwarzać ryzyko dla bezpieczeństwa. Gdy dokumenty zawierające metadane są publikowane w sieci lub udostępniane szerokiemu gronu odbiorców, tracimy nad tymi informacjami kontrolę. Pomysłowi napastnicy mogą zbierać metadane technikami OSINT i wykorzystywać je do złych celów.

W tym miejscu wkraczają na scenę narzędzia takie jak Metagoofil. Metagoofil zbiera metadane z dokumentów publikowanych na stronach internetowych, dostarczając informacji na temat użytkowników czy oprogramowania organizacji. Zebranych metadanych można użyć do badań z zakresu bezpieczeństwa lub testowania, w tym do:

- projektowania skuteczniejszych ataków socjotechnicznych;
- ustalenia wersji oprogramowania w celu znalezienia luk w zabezpieczeniach;
- określenia imion, nazwisk i adresów e-mailowych pracowników.

Metagoofil był kiedyś domyślnie dołączany do dystrybucji Kali Linux, ale czasami zdarza się, że pewne narzędzia znikają ze standardowej wersji. Dobra nowina jest taka, że zawsze można go łatwo pobrać i zainstalować, używając menedżera pakietów APT.

Otwórz terminal i wpisz następujące polecenie:

```
sudo apt install metagoofil
```

Po zainstalowaniu narzędzia możemy go użyć do wydobywania metadanych. W tym przykładzie będziemy gromadzić dane z domeny *packtpub.com*.

Wykonamy takie oto polecenie:

```
metagoofil -d packtpub.com -t doc,pdf -l 20 -n 10 -o packt -f html
```

Rozbijmy to na mniejsze części:

- `-d packtpub.com` — określa domenę będącą przedmiotem badania.
- `-t doc,pdf` — określa typ pliku do wyszukania.
- `-l 20` — ogranicza wyszukiwanie do 20 wyników.
- `-n 10` — ogranicza liczbę plików do pobrania do 10.
- `-o packt` — wskazuje *packt* jako katalog docelowy.
- `-f html` — wskazuje HTML jako wynikowy format.

Po paru minutach Metagoofil zaczyna wyświetlać wyniki na terminalu (rysunek 4.16).

```
┌──(kali㉿kali)-[~]
└─$ metagoofil -d packtpub.com -t doc,pdf -l 20 -n 10 -o packt -f hmtl
[*] Searching for 20 .doc files and waiting 30.0 seconds between searches
[*] Results: 0 .doc files found
[*] Searching for 20 .pdf files and waiting 30.0 seconds between searches
[*] Results: 20 .pdf files found
https://www.packtpub.com/sites/default/files/downloads/6572OT_ColoredImages.pdf
https://www.packtpub.com/sites/default/files/downloads/Reinforcement_Learning.pdf
https://www.packtpub.com/sites/default/files/downloads/8420OT_Bonus_Chapter.pdf
https://www.packtpub.com/sites/default/files/downloads/2901OS_ColoredImages.pdf
```

Rysunek 4.16. Użycie narzędzia Metagoofil do pozyskania plików .doc i .pdf ze strony packtpub.com

Aby obejrzeć wyniki w bardziej uporządkowany sposób, możemy otworzyć plik `/root/➥packt/index.html`, który zawiera czytelnie sformatowaną tabelę z metadanymi wydobytymi z dokumentów. W niektórych przypadkach Metagoofil może znaleźć nawet oprogramowanie lub wiadomości e-mailowe. To więcej niż można by oczekiwać.

Wiem, o czym teraz myślisz. Wszyscy tego kiedyś doświadczyliśmy — beztrosko wydobywaliśmy sobie dane, aż tu nagle Google jak nie zacznie rzucać błędem HTTP 429!

Wysłaliśmy zbyt wiele zapytań, więc nasz adres IP został zablokowany. Bardzo irytujące! Z odpowiednimi narzędziami możemy jednak ominąć tę blokadę i kontynuować pracę. Kluczem jest użycie serwerów pośredniczących (ang. *proxy*).

Najpierw zatrudnijmy narzędzie *proxychains* do przekierowywania zapytań przez wiele serwerów. Jeżeli nie jest już domyślnie zainstalowane, w systemie Kali Linux możemy je zainstalować, używając tego polecenia:

```
sudo apt install proxychains4 -y
```

Następnie dostosujmy plik konfiguracyjny programu *proxychains*, do którego prowadzi ścieżka `/etc/proxychains4.conf`. Możesz go otworzyć w edytorze Vim:

```
vim /etc/proxychains4.conf
```

Włącz tryb *Round Robin*, aby używać po kolei serwerów pośredniczących z listy. Pomijając komentarze, treść pliku powinna wyglądać mniej więcej tak:

```
round_robin_chain
chain_len = 1
proxy_dns
remote_dns_subnet 224
tcp_read_time_out 15000
tcp_connect_time_out 8000
[ProxyList]
socks4 [adres IP i port serwera pośredniczącego]
socks4 [adres IP i port serwera pośredniczącego]
```

Uwaga

Przykładowy wpis w części `[ProxyList]` wygląda następująco: `socks4 192.168.0.1 8000`. Pamiętajmy, że działa tutaj zasada, wedle której im więcej serwerów pośredniczących, tym lepiej.

Dzięki *proxychains* narzędzie Metagoofil będzie zmieniać serwery pośredniczące i dzięki temu dłużej pracować bez przeszkód. W przypadku większej puli adresów IP do rotacji możemy również zmniejszyć opóźnienie między połączeniami. Pamiętaj jednak, żeby przestrzegać warunków korzystania ze stron internetowych, ograniczeń przesyłu danych oraz wytycznych z pliku `robots.txt`. Postępujmy etycznie, a dzięki *proxychains* będziemy mogli wydobywać dane bez obaw, że nastąpi blokada.

Analiza i wnioski

Kolejnym krokiem po zdobyciu danych jest ich analiza. Narzędzia takie jak ***grep*** pozwalają przekopać się przez treść i odnaleźć konkretne wyrażenia, słowa kluczowe i fragmenty informacji. Umiejętność filtrowania i znajdowania informacji przekształca proste zbieranie danych we wnikliwą analizę.

```
grep -ri "wyrażenie" /ścieżka/do/pobranych/danych/stron_internetowych
```

Za dużo nowości naraz? Podzielmy to polecenie na kawałki:

- `grep` — narzędzie wiersza poleceń do wyszukiwania wyrażeń tekstowych w plikach. Jego nazwa pochodzi od angielskiego ***global regular expression print*** (globalne wyszukiwanie wyrażeń regularnych).
- `-ri` — dwie opcje w jednym:
  - `-r` (lub `--recursive`) — informuje narzędzie *grep* o tym, że powinno szukać wyrażenia nie tylko w konkretnym katalogu, lecz również w jego podkatalogach.
  - `-i` (lub `--ignore-case`) — dzięki tej opcji narzędzie ignoruje wielkość liter, więc przy wyszukiwaniu słowa *wyrażenie* zwróci nie tylko wpisy zawierające *wyrażenie*, lecz również *Wyrażenie*, *wYrAżEnIe* itp.
- `"wyrażenie"` — to wyrażenie tekstowe wyszukujemy w treści plików. Oczywiście zastąp ten fragment tekstem, który chcesz wyszukać.
- `/ścieżka/do/pobranych/danych/stron_internetowych` — katalog, w którym prowadzimy wyszukiwanie. Opcja *-r* zapewnia, że narzędzie *grep* przeszuka nie tylko ten katalog, lecz również jego podkatalogi.

Gdy uruchomimy to polecenie, `grep` wyszuka podane wyrażenie we wszystkich plikach tekstowych z katalogu `/ścieżka/do/pobranych/danych/stron_internetowych` oraz podkatalogów, a następnie wyświetli pasujące wiersze.

Wayback Machine i archiwa stron internetowych

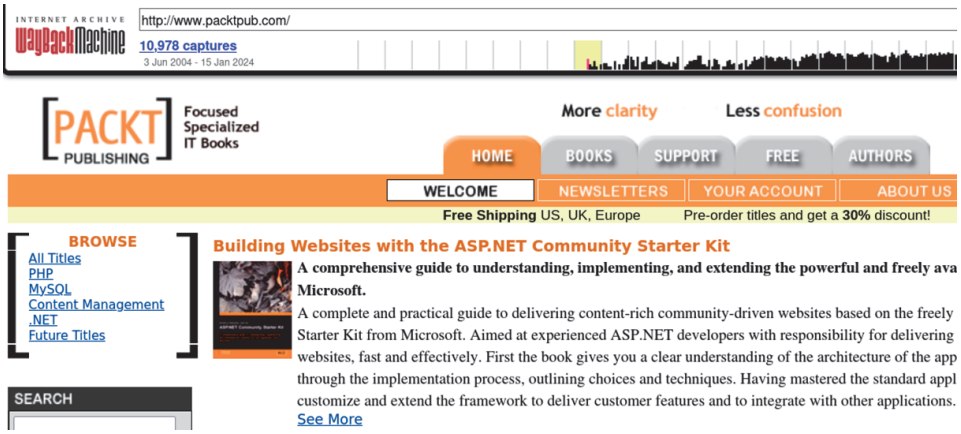
Archiwum Wayback Machine pozwala sprawdzić, jak wyglądały wcześniej strony internetowe. Okresowo zapisuje zawartość stron oraz zapewnia dostęp do ich starszych wersji i treści, które mogą już nie być dostępne w sieci.

To archiwum może być niezwykle użyteczne do web scrapingu i celów OSINT. Oto kilka powodów:

- **Dostęp do skasowanych lub zmienionych treści stron**. Archiwum Wayback Machine przechowuje wersje stron, które są już niedostępne. Dzięki temu można wydobyć stąd treść, która została usunięta ze strony.
- **Analiza zmian na stronie**. Porównując różne wersje kodu i struktury strony, można zidentyfikować zmiany.
- **Badanie domen**. Dzięki archiwum możemy przeglądać historyczne informacje na temat własności strony, witryn powiązanych z adresami e-mailowymi lub nazwiskami oraz wcześniejsze domeny.
- **Odkryj ukryte i zapomniane strony**. Archiwum zawiera strony, które zniknęły z żywej sieci. Można tu odkryć prawdziwe ukryte skarby.
- **Tworzenie zbiorów danych**. Możemy wydobywać dane z aktualnych i historycznych źródeł w sposób hurtowy.

Odkrywanie ukrytych informacji

Każdy zarchiwizowany adres URL to element skomplikowanej układanki, zapewniający wgląd w stan zabezpieczeń strony, ewolucję treści i zmiany w strukturze. Analizując te dane, można wykryć wzorce, odkryć podatności oraz znaleźć rzeczy, które często są ukryte w aktualnych wersjach strony (rysunek 4.17).



Rysunek 4.17. Pierwsza wersja strony wydawnictwa Packt (2004 r.)

Retrospektywna analiza danych z archiwum Wayback Machine to nieodzowna część oceny bezpieczeństwa strony internetowej. Pozwala specjalistom zrozumieć historyczne podatności, śledzić poprawki i przewidzieć ewentualne przyszłe zagrożenia. Każde archiwum, każdy adres URL to zasób, który uzupełnia kompleksową analizę, stojącą u podstaw świadomych, strategicznych decyzji z zakresu cyberbezpieczeństwa.

Listowanie katalogów i plików

Witryny internetowe udostępniają różnego rodzaju nieopublikowane katalogi i pliki, które mogą zawierać cenne informacje. Trzeba tylko umieć je odnaleźć. Badacze ds. bezpieczeństwa mają do dyspozycji narzędzie **DirBuster** (*https://gitlab.com/kalilinux/packages/dirbuster*), które bardzo im w tym pomaga. Wysyła ono żądania do witryny, wykorzystując zmyślną listę terminów, co pozwala im odkryć to, co właściciele strony woleliby ukryć. Wypróbowuje setki tysięcy ścieżek i nazw katalogów, szukając odpowiedzi innej niż komunikat o błędzie.

Gdy DirBuster znajdzie istniejącą ścieżkę, loguje ją do późniejszej weryfikacji przez użytkownika. Może to prowadzić do wykrycia prywatnych zasobów, które właściciel witryny zostawił w jakimś niepozornym miejscu, myśląc, że nikt ich nie znajdzie.

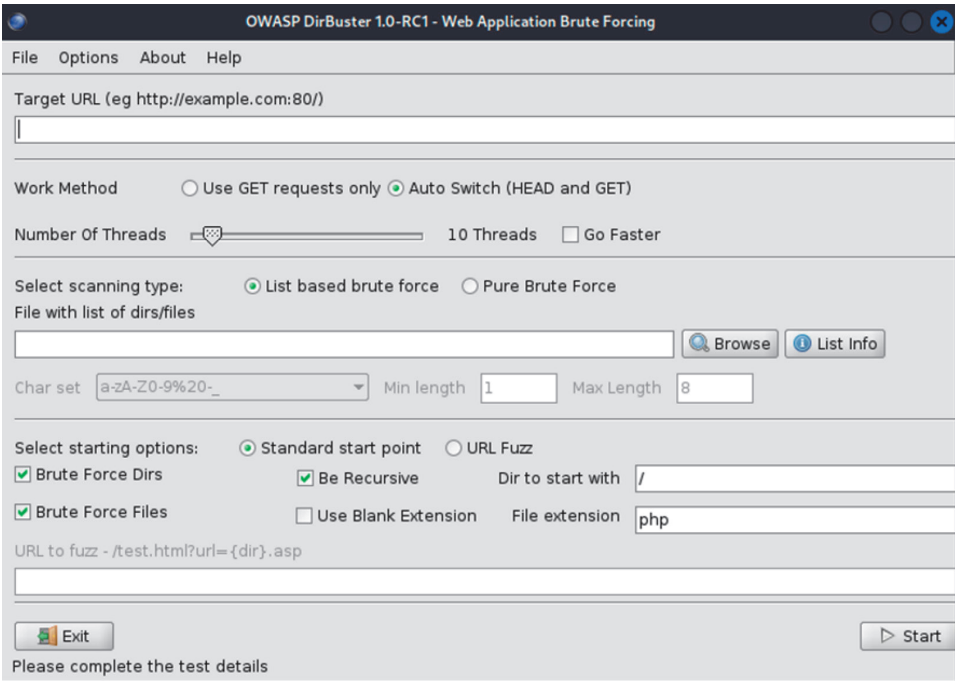
Dogłębna analiza wymaga wytrwałości oraz bogatych słowników dostosowanych do charakterystyki witryny. DirBuster metodycznie przekopuje się przez trzewia witryn internetowych, aby dobrać się do tych ukrytych zasobów. To jak wykopaliska archeologiczne, które pozwalają odkryć dawno zapomniane skarby.

Uruchamianie i używanie DirBustera jest relatywnie proste. Narzędzie ma intuicyjny graficzny interfejs użytkownika, który umożliwia wygodne ustawienie parametrów do kompleksowego i precyzyjnego poszukiwania.

Uruchom DirBustera z terminala:

```
dirbuster
```

I bum! Na ekranie pojawia się interfejs graficzny (rysunek 4.18).



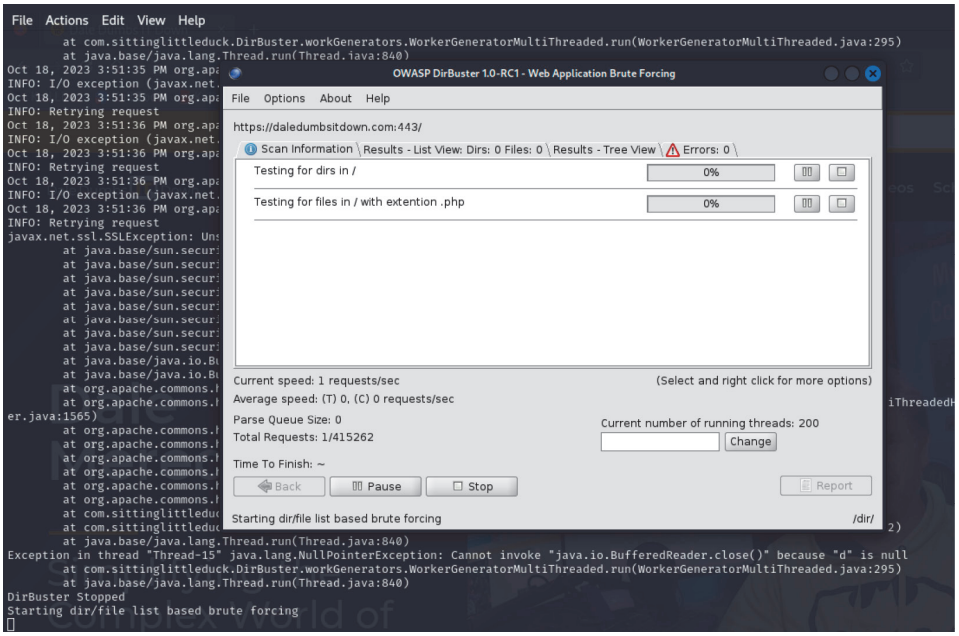
Rysunek 4.18. Interfejs narzędzia DirBuster w systemie Kali Linux

Konfiguracja DirBustera obejmuje określenie docelowego adresu URL oraz wybranie odpowiedniej listy słów, takiej jak ta: `/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt`. Po wybraniu słownika i określeniu rozszerzenia pliku rozpocznij wyszukiwanie, zmieniając DirBustera w detektywa szukającego ukrytych uliczek i przejść.

Kliknij przycisk *Start* (rozpocznij), widoczny na rysunku 4.18, a DirBuster zacznie węszyć i wyświetlać wyniki (rysunek 4.19).

Analiza pliku robots.txt

W uzupełnieniu do wyników uzyskanych z DirBustera możemy przeprowadzić analizę pliku `robots.txt`. Pomoże nam ona zrozumieć, które części witryny są celowo chronione przed indeksowaniem przez wyszukiwarki. Plik `robots.txt` to standardowe



Rysunek 4.19. Narzędzie DirBuster skanuje witrynę daledumbsitdown.com

rozwiązanie stosowane przez witryny do przekazywania instrukcji botom internetowym i crawlerom. Plik określa strony lub pliki, które właściciel witryny chce wyłączyć z indeksowania i dostępu. Oto kilka informacji na temat pliku `robots.txt`:

- Jest to plik tekstowy, który musi mieć dokładnie tę nazwę i znajdować się w katalogu głównym witryny.
- Plik zawiera zbiór reguł określających, które aplikacje klienckie (ang. *user agents*), czyli boty lub inaczej crawlery, mogą uzyskiwać dostęp do stron w witrynie.
- Zasady te muszą mieć format zgodny z mechanizmem REP (Robot Exclusion Protocol).

Rzućmy okiem na zawartość przykładowego pliku `robots.txt`:

```
curl -s https://www.apple.com/robots.txt | less
```

Wynik powinien przypominać ten z rysunku 4.20. Widać na nim listę katalogów, których wyszukiwarki nie powinny indeksować.

Treść pliku `robots.txt` w czytelnym formacie ujawnia sekrety dotyczące struktury witryny. Wymienione tutaj ścieżki i katalogi można dalej eksplorować, zapewniając sobie wgląd w potencjalnie wrażliwe lub poufne części strony internetowej.

```
File  Actions  Edit  View  Help
# robots.txt for http://www.apple.com/

User-agent: *
Disallow: /*/includes/*
Disallow: /*retail/availability*
Disallow: /*retail/availabilitySearch*
Disallow: /*retail/pickupEligibility*
Disallow: /*shop/signed_in_account*
Disallow: /*shop/sign_in*
Disallow: /*shop/sign_out*
Disallow: /*shop/answer/vote*
Disallow: /*shop/bag*
Disallow: /*shop/browse/overlay/*
Disallow: /*shop/browse/ribbon/*
Disallow: /*shop/browse/campaigns/mobile_overlay*
Disallow: /*shop/button_availability*
Disallow: /*shop/favorites*
Disallow: /*shop/iphone/payments/overlay/*
Disallow: /*shop/mobile/olss_error*
Disallow: /*shop/mobilex/*
Disallow: /*shop/np/order*
Disallow: /*shop/np/giftorguestorder*
Disallow: /*shop/np/sign_in*
```

Rysunek 4.20. Wynik pokazujący zasady indeksowania katalogów przez wyszukiwarki

Synergia narzędzia DirBuster i pliku robots.txt

Integrując siłowe, lecz precyzyjne możliwości narzędzia DirBuster ze wstępnym rozpoznaniem dzięki analizie pliku `robots.txt`, badacze dysponują dwutorowym podejściem do wyszukiwania ukrytych danych. Plik `robots.txt` zarysowuje wstępnie strukturę katalogów, a DirBuster, niczym niezłomny wędrowiec, eksploruje jej niezbadane zakamarki, aby odkryć dane, zasoby i pliki konfiguracyjne. To podejście jest integralną częścią kompleksowej analizy i oceny bezpieczeństwa witryn internetowych.

Synergia między rygorystycznym przeczesywaniem struktury przez DirBustera i podstawowymi informacjami z pliku `robots.txt` pomaga dotrzeć do ukrytych warstw strony internetowej. Każde z tych rozwiązań przyczynia się do stworzenia całościowego obrazu architektury witryny i rozmieszczenia treści.

Uwaga

Pamiętaj o motcie superbohatera: „Z wielką mocą wiąże się wielka odpowiedzialność", a przy okazji również o moim własnym: „To, że możesz, nie znaczy, że ci wolno".

Dobrze się bawiliśmy, listując katalogi i pliki oraz odkrywając porozrzucane po witrynie zapomniane zasoby. Teraz zmienimy nieco temat i zagłębimy się w analizę dokumentów i metadanych. Będziemy się przyglądać danym o danych, które o tych pierwszych mogą nam sporo powiedzieć.

Analiza dokumentów i metadanych

Dokumenty i powiązane z nimi metadane to ukryte skarby — każdy z nich może dostarczyć bogactwo informacji, które ludzie często przeoczają. Pliki takie jak dokumenty PDF, dokumenty Worda czy arkusze kalkulacyjne nie tylko zawierają swoją jawną treść, lecz nasycone są też metadanymi, które mogą wiele powiedzieć na temat autorstwa oraz czasu utworzenia i modyfikacji. Niekiedy kryją również wrażliwe informacje nieprzeznaczone dla publicznych oczu.

Identyfikacja ukrytych informacji w dokumentach i plikach

Znajdowanie ukrytych informacji w dokumentach i plikach cyfrowych przypomina odkopywanie skarbów. Te dane, zapisane celowo lub nie, mogą dostarczyć istotnych informacji do celów cyberbezpieczeństwa bądź kryminalistyki. Wyposażona w bogaty zestaw narzędzi dystrybucja Kali Linux to nieodłączny sojusznik specjalistów w tych dziedzinach.

Strategiczne wydobywanie metadanych

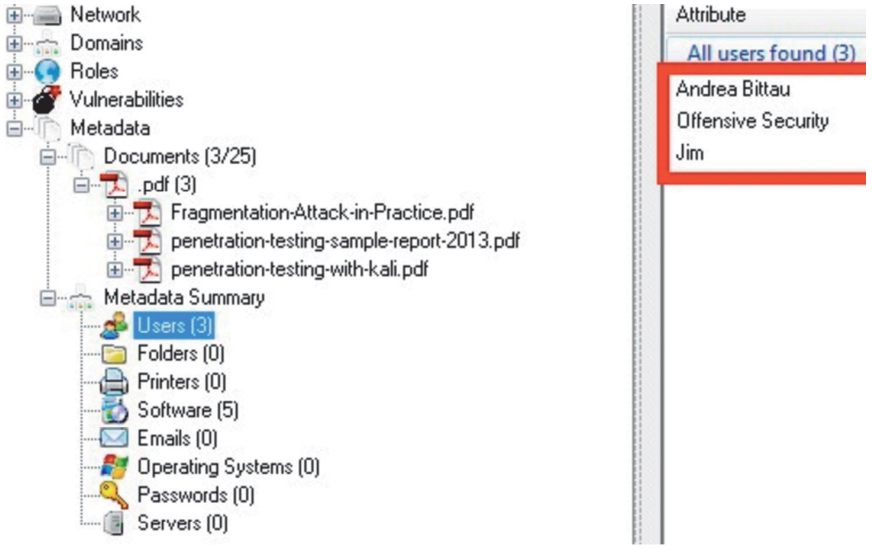
Każdy format pliku zawiera unikalny zestaw metadanych, a umiejętność ich skutecznego wydobywania to klucz do sukcesu. Specjaliści muszą wiedzieć, które narzędzie pasuje do danego formatu, aby zagwarantować, że pozyskane metadane będą kompletne i rzetelne.

Dzięki temu wyrafinowanemu zestawowi umiejętności analitycy nie tylko zdobywają dane, lecz również wiążą cyfrowe pliki i dokumenty w złożoną sieć powiązań. Każdy fragment metadanych to wskazówka, która może doprowadzić do istotnych odkryć i zwieńczyć dochodzenie OSINT.

FOCA

Mam dla Ciebie jeszcze jedno doskonałe narzędzie. Wypróbuj program **FOCA**. Jego nazwa to akronim od angielskiego **Fingerprinting Organizations with Collected Archives** (tworzenie cyfrowych odcisków organizacji na podstawie zebranych danych), a narzędzie dostępne jest pod adresem *https://github.com/ElevenPaths/FOCA*. Służy ono do pobierania dokumentów ze stron internetowych w celu analizowania metadanych. Ukryte dane o pliku mogą zawierać cenne szczegóły, takie jak nazwiska lub nazwy użytkowników edytujących dokument (rysunek 4.21), wersje oprogramowania użytego do utworzenia pliku, ścieżki pokazujące, gdzie znajduje się dany plik, i wiele, wiele więcej!

Chociaż istnieją prawdopodobnie bardziej zaawansowane aplikacje niż FOCA, to darmowe narzędzie jest wyjątkowo proste do użycia w systemie Windows. Realizuje swoją misję, po cichu wypytując wyszukiwarki Google, Bing i DuckDuckGo o różne rodzaje dokumentów, takich jak pliki tekstowe, arkusze kalkulacyjne, prezentacje PowerPointa czy dokumenty



Rysunek 4.21. Dane użytkowników odnalezione za pomocą narzędzia FOCA

PDF — cokolwiek, co można wyciągnąć ze wskazanej domeny. Najlepsze jest to, że dzieje się to pasywnie w tle, bez robienia dużego hałasu czy alarmowania badanej witryny.

Wszystkie metadane, które FOCA wydobywa, mogą zawierać cenne wskazówki lub oferować nowy punkt wyjścia do analizy w ramach dochodzenia. To naprawdę ekscytujące! Możemy na przykład wziąć znalezione przez to narzędzie nazwy użytkownika i zapytać o nie na różnych platformach, aby zobaczyć, czy są powiązane w inny sposób z daną osobą. W metadanych możemy też podejrzeć wersję oprogramowania i sprawdzić, czy występują w nim znane podatności, które mogłyby zostać wykorzystane przez kogoś z mniej kryształowymi zamiarami. Możliwości eksploracji są niemalże nieograniczone!

Analiza dokumentów w poszukiwaniu cennych wskazówek

Istotne dane i fakty zakopane w plikach, takich jak dokumenty PDF, pliki edytorów tekstu czy pliki tekstowe, mogą dostarczyć ważnych wskazówek na temat działań, planów oraz współpracowników organizacji lub jednostek. Techniki takie jak wydobywanie tekstu, analiza metadanych i zaznaczanie fragmentów mogą przyczynić się do systematycznego wyszukiwania istotnych nazw, dat, miejsc, zdarzeń i innych szczegółów, które można przeoczyć, przeglądając dokument po raz pierwszy. Ponadto dokumenty często zawierają ukryte metadane, takie jak informacje na temat miejsca, autora czy zmian, które mogą dostarczyć kontekst dotyczący utworzenia i historii dokumentu. Drobiazgowo sprawdzając treść tekstową i metadane dokumentów zebranych w ramach dochodzenia OSINT, możemy znaleźć subtelne wskazówki i połączyć je w bardziej kompleksowy obraz wywiadowczy.

Zebraliśmy właśnie nieco interesujących danych dzięki węszeniu w dokumentach — różne nazwy, daty i miejsca. Teraz czas zebrać to wszystko razem i połączyć w większy obraz. Na tym etapie możemy wspomóc się narzędziami OSINT do wizualizacji danych. Gdy nadamy wynikom graficzny format, nie tylko prościej będzie nam to wszystko zrozumieć, lecz także ułatwimy sobie wyciąganie odkrywczych wniosków.

Wizualizacja danych w OSINT

W ramach OSINT wizualizacja danych jest procesem przekształcającym surowe i skomplikowane dane w interaktywny i łatwy do zrozumienia format graficzny. Wykorzystuje się na tym etapie różne narzędzia i techniki do tworzenia wykresów, map cieplnych, diagramów sieci i innych graficznych reprezentacji. W ten sposób wykrywanie wzorców, trendów i innych powiązań staje się łatwiejsze. W świecie OSINT wizualizacja to klucz do interpretacji dużych ilości danych i pozyskiwania użytecznych informacji wywiadowczych. Dzięki graficznemu formatowi analitycy szybko dostrzegają powiązania, anomalie i cenne informacje, które trudno byłoby zidentyfikować w surowym tekście.

Dlaczego wizualizacja jest nieodzowna w analizie OSINT?

- **Jasność i zrozumiałość**. Wizualizacja zapewnia jasność. Przekształca abstrakcyjne, złożone dane w namacalną formę, w możliwe do interpretacji obrazy. Dzięki temu wzorce, tendencje i inne powiązania zaczynają być widoczne dla obserwatora jak na dłoni.
- **Wydajność i szybkość**. Wizualizacja na osi czasu pozwala obserwatorom sprawnie przekopywać się przez góry danych, szybko dostrzegać wzorce oraz dochodzić do cennych wniosków z prędkością nieosiągalną w przypadku analizy surowych danych.
- **Podejmowanie decyzji i działań**. Decyzje są równie istotne co dane, na podstawie których są podejmowane. Wizualizacja łączy dane z decyzjami, a wnioski z akcjami. Każda wizualizacja to soczewka powiększająca niejasne, zaciemnione szczegóły i rzucająca na dane światło, które stanowi podstawę do podejmowania decyzji, działań i reakcji.

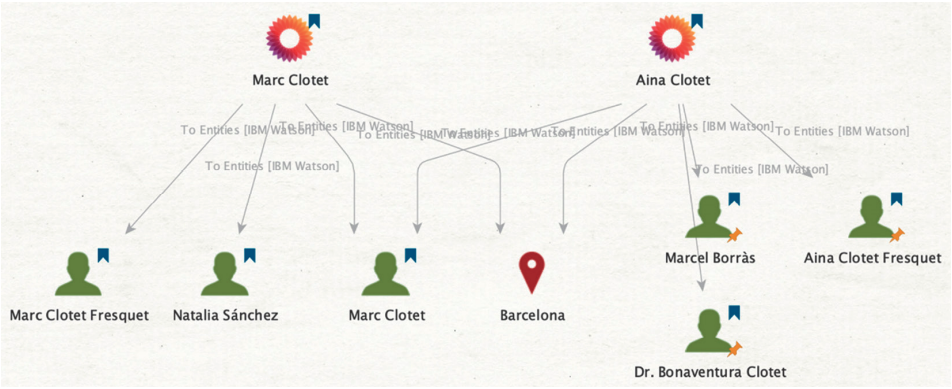
Siedzę przed komputerem otoczony górą danych OSINT, które zebrałem. Patrząc na ten stos profili w mediach społecznościowych, rejestrów publicznych i kodu stron internetowych, wiem, że wizualizacja danych za chwilę przekształci te skrawki w epickie odkrycie!

Prawdziwa moc wizualizacji danych tkwi w zdolności wydobywania na wierzch ważnych spostrzeżeń z wielu pozornie mało istotnych szczegółów. W miarę jak abstrakcyjne punkty danych przekształcają się w bogate sieci powiązań, osie czasu, mapy geograficzne i wykresy, ich znaczenie krystalizuje się w objawienie.

Narzędzia i techniki wizualizacji danych w OSINT

Prowadzenie białego wywiadu wymaga narzędzi i technik, które pomagają wydobyć na światło dzienne ukryte fakty. Oto niektóre z moich ulubionych programów (z częścią z nich zapoznam Cię dokładniej w następnym rozdziale):

- **Maltego**. Dostępny na stronie *https://www.maltego.com* program tworzy graficzny model powiązań między różnymi podmiotami, osobami, stronami internetowymi, domenami, adresami IP i organizacjami (rysunek 4.22).



Rysunek 4.22. Maltego pokazuje powiązania między adresami e-mailowymi a nazwami użytkowników w portalu LinkedIn

  Powiązania są generowane poprzez automatyczne wyszukiwanie, filtrowanie i zestawianie danych ze źródeł otwartych i prywatnych. To jedno z moich ulubionych narzędzi.

- **Gephi**. Jest to napisany w Javie, otwartoźródłowy zestaw narzędzi do tworzenia wykresów i analizy danych. Często używa się go do analizy i wizualizacji powiązań w ramach takich sieci jak media społecznościowe, mapy infrastruktury czy wykresy relacji. Gephi można pobrać za darmo ze strony *https://gephi.org*. Działa w systemach Windows, macOS i Linux.

- **CaseFile**. Czym jest CaseFile firmy Maltego? Posłuchaj krótkiej historyjki. Wyobraź sobie, że prowadzisz cyberdochodzenie i przekopujesz się przez hałdy danych zgromadzonych w ramach różnych spraw — arkuszy kalkulacyjnych transakcji finansowych, zapisów rozmów telefonicznych, podejrzanych e-maili itp. W jaki sposób podejść do całej tej góry danych? Tutaj pomocny jest CaseFile, który pozwala przekształcić dane offline w graficzne mapy relacji w czasie krótszym, niż trwa zaparzenie porannej kawy.

  CaseFile pomaga tchnąć życie w dane offline oraz znaleźć powiązania i wzorce bez połączenia z internetem.

Każde z przedstawionych tutaj narzędzi OSINT jest na swój sposób wyjątkowe. Przekształcają one niejasny kod i niejednoznaczne dane w symfonię odkrywczych wizualizacji.

Najlepsze praktyki korzystania z narzędzi do eksploracji ukrytych danych

Dane żyją. Nie chodzi tylko o ich istnienie, lecz również o nieustanną ewolucję. To, co dzisiaj jest pożytecznym narzędziem, może szybko stać się reliktem przeszłości. Każdy dzień mojej pracy z OSINT przypomina mi, że czujność jest nie tylko pożądana, lecz wręcz nieodzowna. Wprowadziłem w życie nowy zwyczaj, albo raczej rytuał. Nieustannie poszukuję najnowszych, najlepszych i najbardziej zaawansowanych narzędzi i metod pozyskiwania danych. Dla mnie kanały RSS, fora i miejsca wymiany informacji w ramach społeczności to coś więcej niż platformy. Pozwalają mi zdobywać aktualne informacje na temat zmian w zestawie narzędzi OSINT.

Zazwyczaj radzę początkującym, aby używali wielu narzędzi, zamiast specjalizować się tylko w jednym. Każde narzędzie ma swoje wyjątkowe zalety, szuka danych w różnych źródłach — w mediach społecznościowych, rejestrach publicznych czy technicznych bazach danych. Wykorzystanie różnych narzędzi zapewnia bardziej kompleksowy obraz sytuacji.

Ważne jest również, aby używać różnych słów kluczowych, synonimów, powiązanych pojęć, błędnej pisowni — czegokolwiek, co może nam pomóc spojrzeć na sprawę z nowej perspektywy. Korzystaj również z wbudowanych filtrów, takich jak data, miejsce czy rodzaj źródła, aby zawęzić wyniki wyszukiwania. Dzięki temu możesz dotrzeć do najbardziej istotnych danych.

Gdy już zaczniesz uzyskiwać jakieś wyniki, ważne jest, aby ocenić wiarygodność i ewentualną tendencyjność każdego źródła. Uwzględnij takie rzeczy jak kompetencje, reputacja i dodatkowe dowody. Dobrze jest również pomyśleć o organizacji wyników pracy w formie map myśli, wykresów z relacjami czy osi czasu, aby dostrzec powiązania.

Nie zapomnij też zatrzeć za sobą śladów. Używaj serwerów pośredniczących, sieci VPN i anonimowych kont, aby utrudnić wykrycie przez cel dochodzenia. Oczywiście musisz również przestrzegać warunków korzystania z usług poszczególnych platform oraz przepisów prawa w zakresie ochrony prywatności. Etyka pracy w OSINT odgrywa dużą rolę w mojej książce.

Jest jeszcze wiele tematów, które moglibyśmy poruszyć, w tym monitorowanie zmian dotyczących celu dochodzenia, zabezpieczenie własnych działań oraz nieustanne podnoszenie swoich kwalifikacji. Niemniej jednak już samo zastosowanie najlepszych praktyk, takich jak sprawdzanie źródeł, stosowanie różnych słów kluczowych, dobra organizacja wyników i etyczne podejście, powinno pomóc Ci w osiągnięciu sukcesu w dziedzinie OSINT.

Podsumowanie

Jestem pewien, że w tym punkcie naszej podróży czujesz w sobie nowo zyskane supermoce OSINT. Zdobyliśmy praktyczne doświadczenie w wydobywaniu ukrytych danych z domen, rekordów, adresów IP, stron internetowych i dokumentów. Z nowym zestawem technik wykrywania danych możesz przekształcić rozproszone punkty w żywą opowieść. Internet wita nowego detektywa.

Następny nasz krok to poznanie dalszych narzędzi, które automatyzują niektóre działania OSINT z zakresu gromadzenia danych, a także systemu operacyjnego zaprojektowanego specjalnie z myślą o białym wywiadzie.

Rozdział 5

Od Recon-ng po Trace Labs — wycieczka objazdowa po najlepszych narzędziach OSINT

Ten rozdział pomoże Ci odnaleźć się w złożonym ekosystemie dodatkowych narzędzi **OSINT**, które odkryją przed nami ukryte na widoku dane. Zrozumienie tych narzędzi i skuteczne posługiwanie się nimi jest ważne dla specjalistów z różnych dziedzin, w tym z obszaru cyberbezpieczeństwa i dziennikarstwa śledczego, gdyż pomaga przekopać się przez cyfrowe góry danych i zdobyć istotne informacje.

W tym rozdziale poruszymy następujące tematy:

- Recon-ng — potężny framework narzędzi OSINT;
- Maltego — narzędzie do wizualizacji danych i powiązań OSINT;
- Shodan — wyszukiwarka **internetu rzeczy** (ang. *Internet of Things*, IoT);
- Trace Labs — zaawansowany system operacyjny zaprojektowany do działań OSINT;
- przegląd pakietu narzędzi Aircrack-ng;
- dodatkowe otwartoźródłowe narzędzia OSINT;
- nadążanie za tempem zmian w dziedzinie OSINT.

Po zapoznaniu się z tym rozdziałem będziesz dysponować jeszcze większym zestawem narzędzi OSINT, które ułatwią Ci prowadzenie badań. Zdobędziesz też trochę praktycznego doświadczenia w korzystaniu z nich.

Recon-ng — potężny framework narzędzi OSINT

Recon-ng to wielozadaniowy kombajn do celów rozpoznania stron internetowych, którego użyteczne funkcjonalności umożliwiają sprawniejsze prowadzenie wywiadu. Ma modułową architekturę, więc można łatwo poszerzyć jego możliwości, instalując nowe moduły z wbudowanego rynku. Społeczność cały czas rozwija nowe moduły, dzięki czemu Recon-ng pozostaje w czołówce najnowocześniejszych narzędzi OSINT.

Recon-ng wykorzystuje interaktywny interfejs wiersza poleceń, co sprawia, że narzędzie jest proste w użyciu nawet dla początkujących. Nie dajmy się jednak zwieść prostemu interfejsowi. Framework Recon-ng umożliwia zaawansowane zarządzanie danymi i automatycznie zapisuje zebrane informacje w ustrukturyzowanej bazie danych, ułatwiając dostęp i eksport.

Podsumowując: Recon-ng łączy w sobie elastyczną, modułową architekturę, utrzymywany przez społeczność rynek modułów, intuicyjny interfejs, solidny mechanizm zarządzania danymi oraz rozszerzalne API, co sprawia, że jest to naprawdę potężny otwartoźródłowy framework do prowadzenia rozpoznania stron internetowych.

Zainstalujmy i skonfigurujmy framework Recon-ng w systemie Kali Linux:

1. Otwórz terminal.
2. Sklonuj repozytorium Recon-ng. Git, czyli popularny program do kontroli wersji, powinien być domyślnie zainstalowany w Twoim systemie. Za jego pomocą sklonujesz repozytorium Recon-ng z GitHuba (powiedzmy, że jest to miejsce, gdzie nasz cyfrowy detektyw trzyma swoje narzędzia). Aby przystąpić do klonowania, użyj następującego polecenia:

   ```
   git clone https://github.com/lanmaster53/recon-ng.git
   ```

3. Przejdź do katalogu ze sklonowanym repozytorium:

   ```
   cd recon-ng
   ```

4. Zainstaluj wymagane zależności:

   ```
   pip3 install -r REQUIREMENTS
   ```

5. Uruchom narzędzie Recon-ng:

   ```
   ./recon-ng
   ```

Uruchamianie modułów Recon-ng i zbieranie informacji

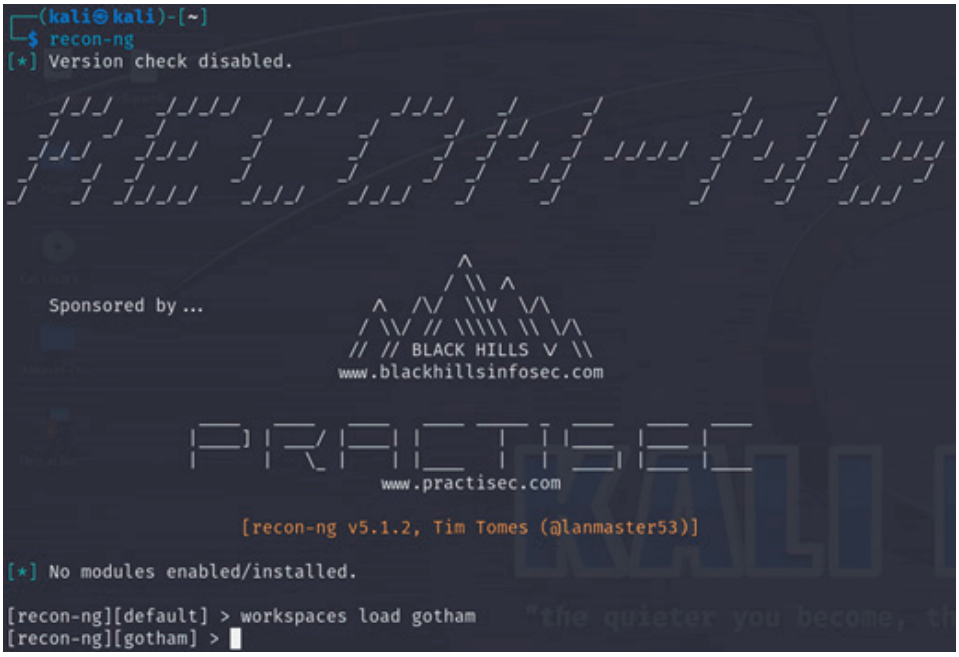
Nasz informacyjny kombajn łączy w sobie całą gamę narzędzi i technik oraz ułatwia korzystanie z nich dzięki dobrze zorganizowanemu systemowi modułów. Moduły służą specyficznym celom — od profilowania domeny po ekstrakcję informacji z mediów społecznościowych.

Po zainstalowaniu Recon-ng musimy najpierw się upewnić, że rozumiemy koncepcję obszarów roboczych (ang. *workspaces*).

Aby utworzyć nowy obszar roboczy, użyj następującego polecenia:

```
workspaces create [nazwa_obszaru_roboczego]
```

Po utworzeniu obszaru roboczego zostajemy do niego automatycznie przeniesieni. Aby zmienić obszar roboczy, możemy użyć polecenia `workspaces load [nazwa_obszaru_robo↪czego]`. Wynik jest przedstawiony na rysunku 5.1.



Rysunek 5.1. Załadowanie obszaru roboczego o nazwie gotham

Obszary robocze w Recon-ng przypominają oddzielne katalogi przeznaczone na pojedynczy projekt. Ta funkcjonalność pozwala użytkownikom oddzielić dane i konfiguracje dotyczące różnych spraw. Podział na obszary robocze jest ważny z kilku powodów:

- **Odizolowanie od siebie różnych projektów**. Każdy obszar roboczy w Recon-ng funkcjonuje jako oddzielny katalog na dane konkretnego projektu. Oznacza to, że jeżeli pracujemy nad różnymi sprawami, każda z nich będzie mieć własną przestrzeń roboczą z danymi, modułami i konfiguracjami. Nie ma ryzyka niepożądanego przepływu materiałów dowodowych między projektami, co należy do podstawowych zasad prawidłowego prowadzenia dochodzenia.
- **Zachowanie skupienia**. Dzieląc dane na obszary robocze, możemy utrzymać wysoki poziom skupienia na konkretnym zadaniu. Niepowiązane dane nie będą

nas rozpraszać. To szczególnie istotne, gdy pracujemy z dużymi ilościami informacji, gdyż pomaga uniknąć zamieszania i gwarantuje, że widzimy jedynie te dane, które są istotne dla aktualnego śledztwa.

- **Rzetelność danych i brak interferencji**. Użycie oddzielnych obszarów roboczych pomaga zapewnić rzetelność danych. Jeżeli na przykład potrzebujemy wrócić do wcześniejszego projektu, aby dokonać dalszej analizy lub potwierdzić wnioski, musimy być pewni, że dane nie zmieniły się na skutek innych działań.
- **Wydajne raportowanie**. Gdy przychodzi czas na opracowanie wyników w formie raportu, dysponujemy wszystkimi istotnymi danymi w obrębie pojedynczego obszaru roboczego, co usprawnia proces. Nie ma potrzeby przedzierania się przez gąszcz niepowiązanych informacji. Bezpośrednio z tego obszaru roboczego można wyeksportować lub udostępnić wnioski.
- **Elastyczność przy współpracy**. Jeżeli pracujemy w zespole, możemy udostępniać obszary robocze członkom zespołu, co umożliwia współpracę bez ryzyka zmiany danych w innych lub prywatnych projektach. Każdy współpracownik może przechodzić między obszarami roboczymi zgodnie z potrzebami, pracować równolegle nad różnymi aspektami tego samego projektu lub nad zupełnie innymi sprawami.

Obok obszarów roboczych kolejnym ważnym zagadnieniem w pracy z Recon-ng są moduły. Wbudowany rynek (ang. *marketplace*) oferuje ogromną liczbę modułów, które obejmują szeroki zakres taktyk rozpoznania. Dzięki sprytnemu wyszukiwaniu znalezienie tego, czego potrzebujemy, to bułka z masłem. Aby zainstalować nowy moduł, wystarczy wpisać: `marketplace install [fragment_nazwy_modułu]`.

Uwaga

Dodawanie kluczy API też jest niewiarygodnie proste. Po prostu użyj polecenia `keys add [nazwa] [wartość]`, aby zacząć korzystać z takich usług jak Shodan. To istotne ułatwienie!

Zrozumienie i skuteczne używanie poleceń do zarządzania modułami jest konieczne do sprawnego poruszania się po tej złożonej platformie. Przyjrzyjmy się kilku poleceniom:

- **Wyszukiwanie modułów**

  Aby przeszukać rynek pod kątem modułu, wpisz:

  ```
  marketplace search
  ```

- **Przeglądanie zainstalowanych modułów**

  Następujące polecenie wyświetli wszystkie aktualnie zainstalowane moduły. Pełna nazwa każdego modułu pokazuje, jakiej kategorii danych dotyczy dany moduł (domen, lokalizacji, profili itd.):

  ```
  modules search
  ```

- **Wybór i użycie modułu**

  Aby pobrać i zainstalować moduł z rynku, wpisz:

  ```
  marketplace install [nazwa_modułu]
  ```

  Teraz możemy załadować gotowy do użycia moduł. Jeżeli na przykład zainstalowaliśmy moduł o nazwie *hackertarget*, załadujemy go poleceniem `modules load hackertarget` (rysunek 5.2). Analogicznie postępujemy w przypadku innych modułów.

```
[recon-ng][gotham] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][gotham] > modules load hackertarget
[recon-ng][gotham][hackertarget] >
```

Rysunek 5.2. Instalacja i ładowanie modułu

- **Konfiguracja opcji dla modułu**

  Każdy moduł ma specyficzne opcje, które należy skonfigurować. Zazwyczaj obejmują one ustawienie interesującej nas domeny lub adresu IP. Zacznijmy od sprawdzenia, jakie opcje są dostępne:

  ```
  options list
  ```

  Teraz możemy ustawić odpowiednią wartość dla danej opcji:

  ```
  options set SOURCE example.com
  ```

- **Uruchamianie modułu**

  Po ustawieniu opcji jesteśmy gotowi do działania. Moduł uruchamiamy następującym poleceniem:

  ```
  run
  ```

  Teraz — niczym za sprawą magii — moduł ściągnie informacje, których pozyskanie jest jego celem. Gdy zakończy działanie, będziemy mogli przeglądać różne kategorie zapisanych wyników, używając następującego polecenia:

  ```
  show [kategoria]
  ```

  Kategorie wyników odpowiadają nazwom tabel w bazie danych Recon-ng. Ich listę uzyskasz, gdy uruchomisz polecenie `show`. Na przykład aby przejrzeć wykryte hosty, wpisz:

  ```
  show hosts
  ```

  Przykładowy wynik takiego polecenia jest widoczny na rysunku 5.3.

Piękno Recon-ng tkwi w iteracyjnym podejściu. Każdy cykl rozpoznania ujawnia kolejne szczegóły na temat celu. Obszerna biblioteka modułów tego narzędzia jest jego istotną zaletą. Pokazane tutaj kroki zapewniają jedynie ogólny ogląd, ale każdy moduł ma swoje niepowtarzalne cechy. Warto regularnie sprawdzać rynek Recon-ng w poszukiwaniu nowych cennych dodatków.

```
[recon-ng][gotham][hackertarget] > show hosts

+-------------------------------------------------------------------+
| rowid |              host                |    ip_address         |
+-------------------------------------------------------------------+
| 1     | data.packtpub.com                | 52.215.120.22         |
| 2     | salesdb.packtpub.com             | 83.166.169.242        |
| 3     | hub.packtpub.com                 | 172.67.31.83          |
| 4     | datahub.packtpub.com             | 172.67.31.83          |
| 5     | epic.packtpub.com                | 52.19.26.156          |
| 6     | staging-epic.packtpub.com        | 52.48.37.122          |
| 7     | dev-epic.packtpub.com            | 52.18.34.177          |
| 8     | subscription-rc.packtpub.com     | 172.67.31.83          |
| 9     | dtc.packtpub.com                 | 192.168.0.110         |
```

Rysunek 5.3. Dane na temat hostów w domenie packtpub.com znalezione narzędziem Recon-ng

Maltego — narzędzie do wizualizacji danych i powiązań

Maltego to narzędzie do wizualizacji danych i znajdowania powiązań, które pomaga ekspertom ds. cyberbezpieczeństwa wydobyć na światło dzienne i zrozumieć złożone sieci powiązań między informacjami. Przydaje się do śledzenia cyfrowych działań i analizowania cyberzagrożeń.

Tym, co wyróżnia Maltego, jest jego zdolność zbierania wyników wielu różnych zadań wywiadowczych w ramach spójnego interfejsu. Ponadto użytkownicy dystrybucji Kali Linux mogą skorzystać z wersji społecznościowej, która oferuje szereg skanów bez konieczności ponoszenia początkowych kosztów.

Dzięki Maltego użytkownicy mogą wydobywać szeroki zakres informacji: dane osobowe (takie jak nazwiska, adresy e-mailowe i pseudonimy), dane organizacji, firm i stron internetowych, informacje na temat infrastruktury internetowej, w tym domen, adresów IP i powiązanych sieci, a także dokumenty i pliki.

Czołowe agencje rządowe, w tym amerykańska agencja wywiadowcza **National Security Agency** (**NSA**), wykorzystują narzędzia takie jak Maltego do wizualizacji powiązań i skutecznego monitorowania zagrożeń.

Początek pracy z Maltego

Maltego to kluczowe narzędzie w branży OSINT, zaprojektowane głównie do wizualizacji danych. Prezentując złożone dane w prostszy i lepiej ustrukturyzowany sposób, Maltego zapewnia jasność w cyfrowym chaosie.

Dystrybucja Kali Linux najczęściej zawiera już zainstalowane narzędzie Maltego. Jeżeli jednak musisz je zainstalować, użyj po prostu instalatora APT:

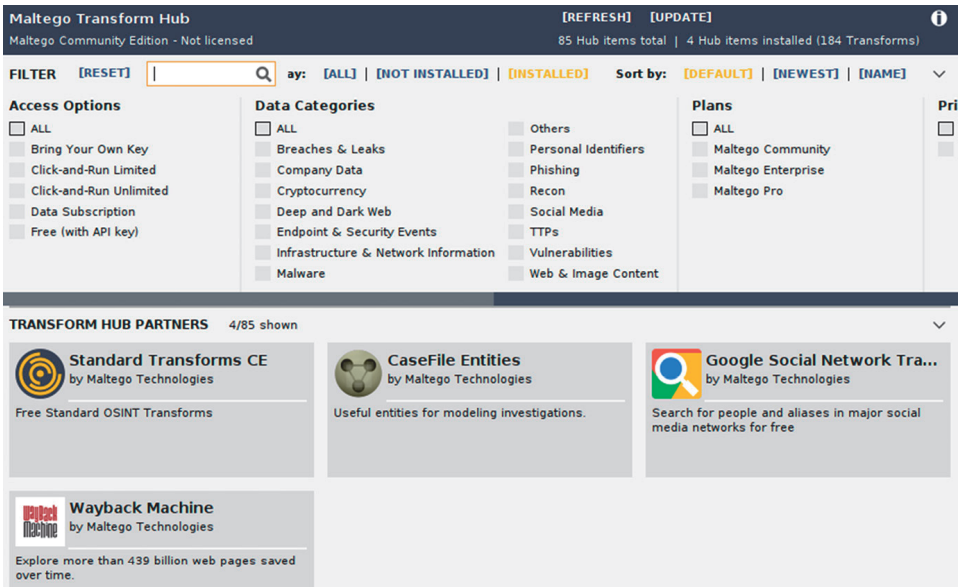
```
sudo apt install maltego
```

Po zakończeniu instalacji wpisz `maltego` w wierszu poleceń. Przy pierwszym uruchomieniu Maltego przeprowadza użytkownika przez kreatora ustawień. Obejmuje to utworzenie konta Paterva i zalogowanie się do niego, co jest niezbędne do uzyskania dostępu do niektórych funkcjonalności i rozszerzeń.

Po rejestracji i logowaniu możemy określić na przykład mechanizm analizy, tak zwaną **maszynę** (ang. *machine*). W kontekście Maltego maszyna określa głębokość i rodzaj rozpoznania, jakie ma zostać przeprowadzone względem wybranego celu.

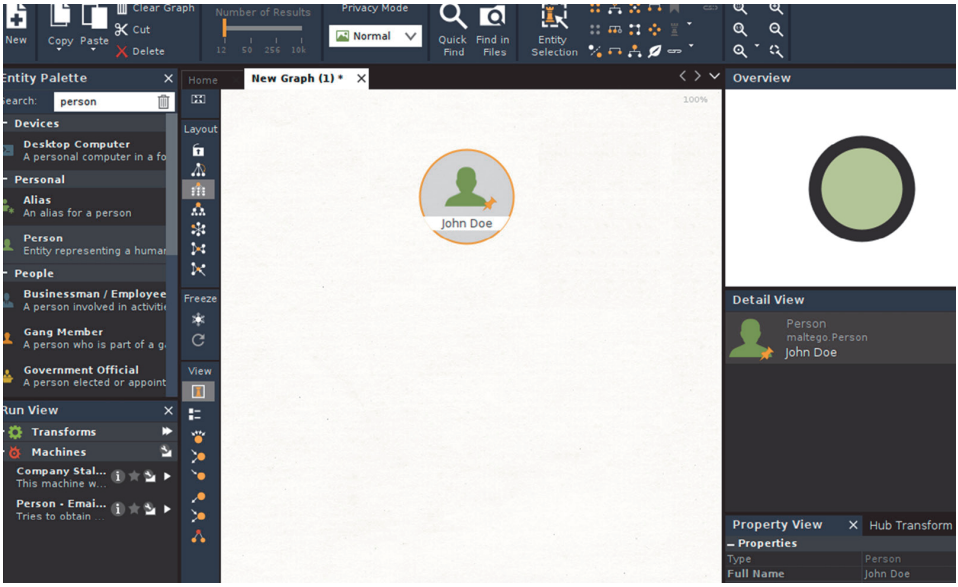
Aby wyciągnąć z Maltego jak najwięcej, musimy dodać **transformacje** (ang. *transforms*), które są zasadniczo rozszerzeniami pozwalającymi na dostęp do usług zewnętrznych pobierających dane. Niektóre transformacje są bezpłatne, a za część lepszych trzeba zapłacić. W ramach tego demo będę starał się korzystać tylko z darmowych wtyczek.

Na ekranie głównym wybierz opcję ***Free (with API key)*** (bezpłatne z kluczem API), aby usunąć z wyników wyszukiwania wszystkie płatne transformacje. Transformacje, które mam zainstalowane w swoim systemie Kali Linux, pokazuje rysunek 5.4.



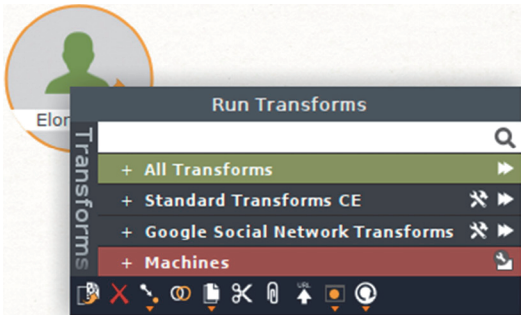
Rysunek 5.4. Transformacje zainstalowane w moim systemie

Następnie utwórzmy nowy graf. Kliknij ikonę *New* (nowy) na pasku menu. Teraz dodamy encję (ang. *entity*), czyli obiekt, który będzie podlegał transformacjom. Przewinę listę po lewej stronie nieco w dół, z dostępnych opcji wybiorę *Person* (osoba) i przeciągnę tę ikonę do obszaru edytora (rysunek 5.5).



Rysunek 5.5. Ikona encji na obszarze grafu

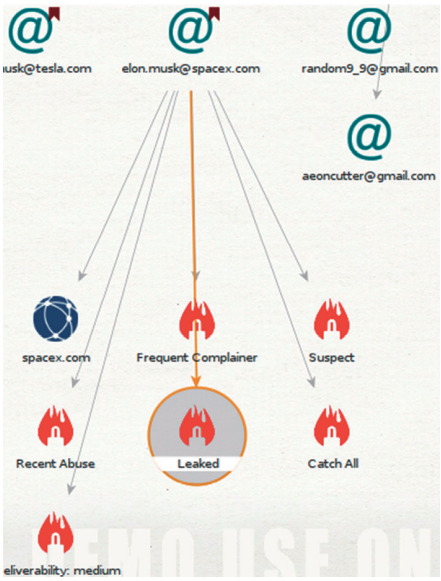
Zauważysz od razu, że domyślnym imieniem i nazwiskiem jest John Doe, ale taki Jan Kowalski za bardzo mnie nie interesuje. O kim byłoby ciekawiej wyszukiwać informacje? Dwukrotnie kliknij ikonę osoby i zmień dane. Wpiszmy dla zabawy `Elon Musk`. Zaakceptuj zmianę przyciskiem *OK*. Teraz kliknij prawym przyciskiem ikonę. Zobaczysz listę dostępnych transformacji (rysunek 5.6).



Rysunek 5.6. Widok możliwych do uruchomienia transformacji po kliknięciu obiektu prawym przyciskiem myszy

Możemy je sobie po kolei uruchamiać.

Na wykresie zaczynają się pojawiać adresy e-mailowe. Niektóre mogą być prawdziwymi adresami Elona Muska (np. *elon.musk@spacex.com*), a inne mogą należeć do kogoś innego lub nawet do spamerów. Kliknijmy prawym przyciskiem myszy adres *elon.musk@spacex.com* i ponownie uruchommy dostępne transformacje (rysunek 5.7).



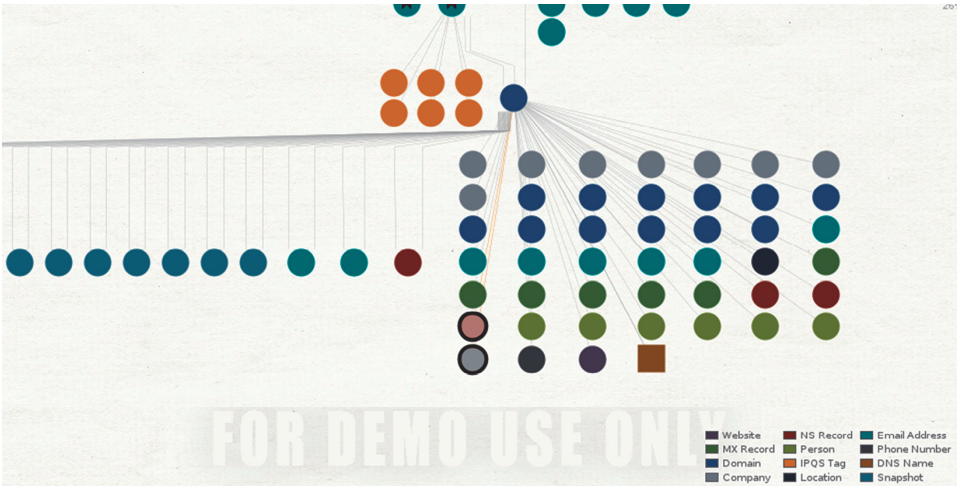
Rysunek 5.7. Interesujące informacje po wykonaniu transformacji na adresie e-mailowym elon.musk@spacex.com

Jeżeli wybierzemy ikonę *Leaked* (wyciek), zobaczymy po lewej stronie, że ten adres był powiązany z wyciekiem z bazy danych (rysunek 5.8).



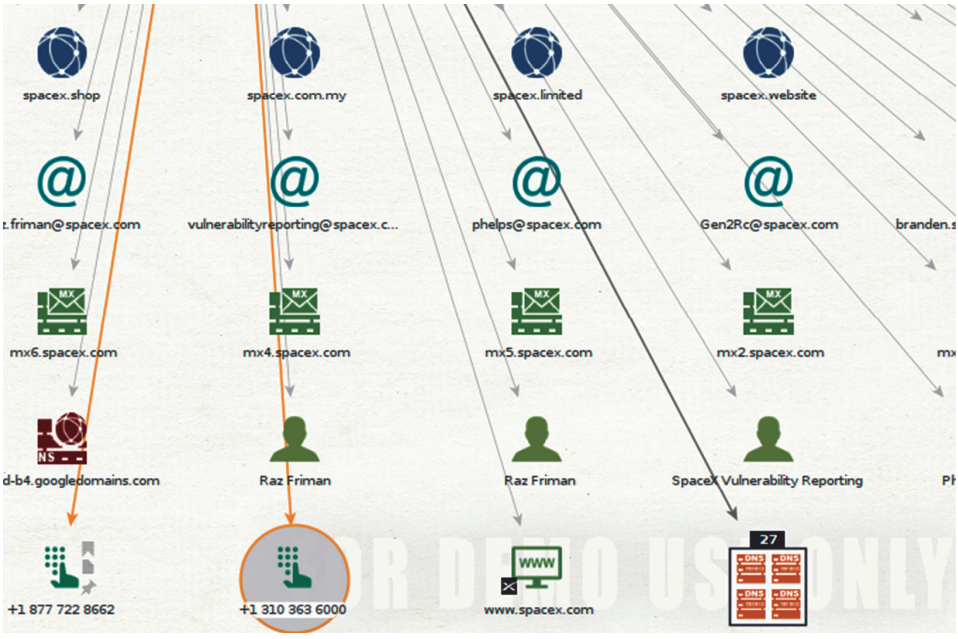
Rysunek 5.8. Szczegółowe dane pokazują, że adres e-mailowy był przedmiotem naruszenia

Możemy kopać głębiej, wyszukując dalsze informacje o każdym nowo odkrytym obiekcie. Dzięki temu nasza wiedza o celu rośnie. Możemy na przykład uruchomić transformację na domenie *spacex.com* (rysunek 5.9). Zapytanie zwróciło tak wiele obiektów, że widok został pomniejszony. Możemy go z powrotem powiększyć i szukać dalej.



Rysunek 5.9. Wyniki transformacji dla domeny spacex.com

Zauważ, że w miarę jak zwiększam przybliżenie, zaczynam dostrzegać imiona i nazwiska oraz numery telefonów. To może zaprowadzić mnie ku nowym tropom (rysunek 5.10).



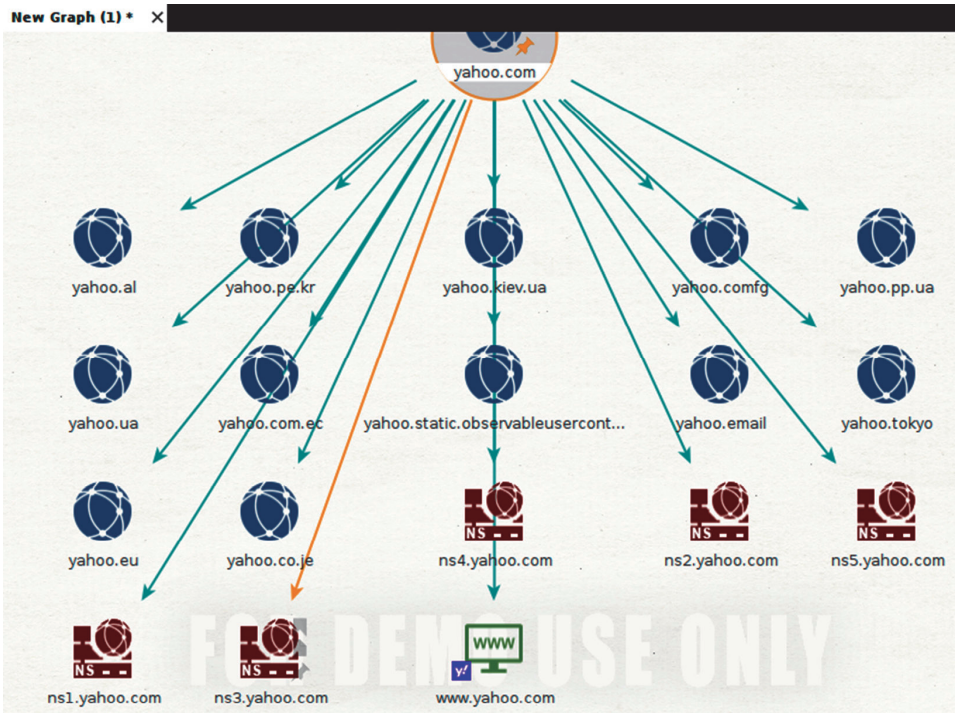
Rysunek 5.10. Na ekranie pojawiają się imiona i nazwiska oraz numery telefonów osób

Rozpracowywanie infrastruktury

Aby zacząć, wybierz domenę i przyjrzyj się dostępnym transformacjom, które reprezentują zasadniczo różne dostępne funkcje i zadania. Zacznijmy na przykład od analizy DNS. Kilka innych transformacji również wygląda interesująco. Możemy zbierać informacje o serwerach poczty elektronicznej, serwerach nazw, domenach najwyższego poziomu oraz witrynach internetowych.

Na początku przeprowadźmy transformację *To Website [Quick lookup]*, która zwróci nam witryny internetowe powiązane z domeną. Następnie kliknij prawym przyciskiem myszy ikonę domeny i wybierz transformację *To DNS Name - NS (name server)*, aby uzyskać informacje na temat serwerów nazw. Teraz moglibyśmy z kolei wylistować subdomeny lub zbadać usługi poczty elektronicznej, aby zrozumieć, w jaki sposób jest obsługiwana, i zdobyć dane odpowiedzialnych za to serwerów.

W ramach kolejnego przykładu przeanalizujmy domeny najwyższego poziomu powiązane z domeną *yahoo.com*. Transformacja *To Domain (Find other TLDs) [WhoisXML]* zwraca domeny takie jak *yahoo.au*, *yahoo.email* i *yahoo.tokyo* (rysunek 5.11).



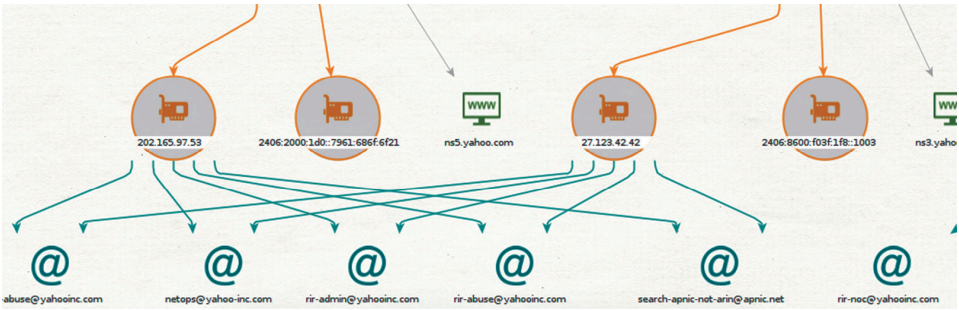
Rysunek 5.11. Wyniki wyszukiwania domen najwyższego poziomu, serwerów nazw i witryn

Następnie zobaczmy, czy możemy zdobyć informacje na temat niektórych adresów e-mailowych. Możemy spróbować pozyskać dane z rejestrów WHOIS (*To Email address*

[From whois info]), baz danych PGP (*To Email Addresses [PGP]*) lub wyszukiwarek internetowych (*To Email addresses [using Search Engine]*). Jeżeli nie znajdziemy żadnych adresów e-mailowych w wyszukiwarkach, nie ma problemu.

Sprawdźmy, czy wyciągniemy jakieś adresy IP z serwerów nazw (*To IP Address [DNS]*). Możemy też zbadać witryny i domeny obsługiwane przez te same serwery nazw. Pozyskawszy adresy IP, możemy zweryfikować ich właścicieli i poszukać ich adresów e-mailowych w różnych źródłach.

Możemy tu znaleźć takie adresy jak *admin@yahooinc.com*, co jest całkiem użyteczne. Po zbadaniu domen możemy je zgrupować i sprawdzić, na jakie serwery nazw wskazują. Zazwyczaj są to standardowe serwery Yahoo. Dzięki pogrupowaniu serwerów nazw możemy odkryć inne domeny aktualnie obsługiwane przez te serwery (rysunek 5.12).



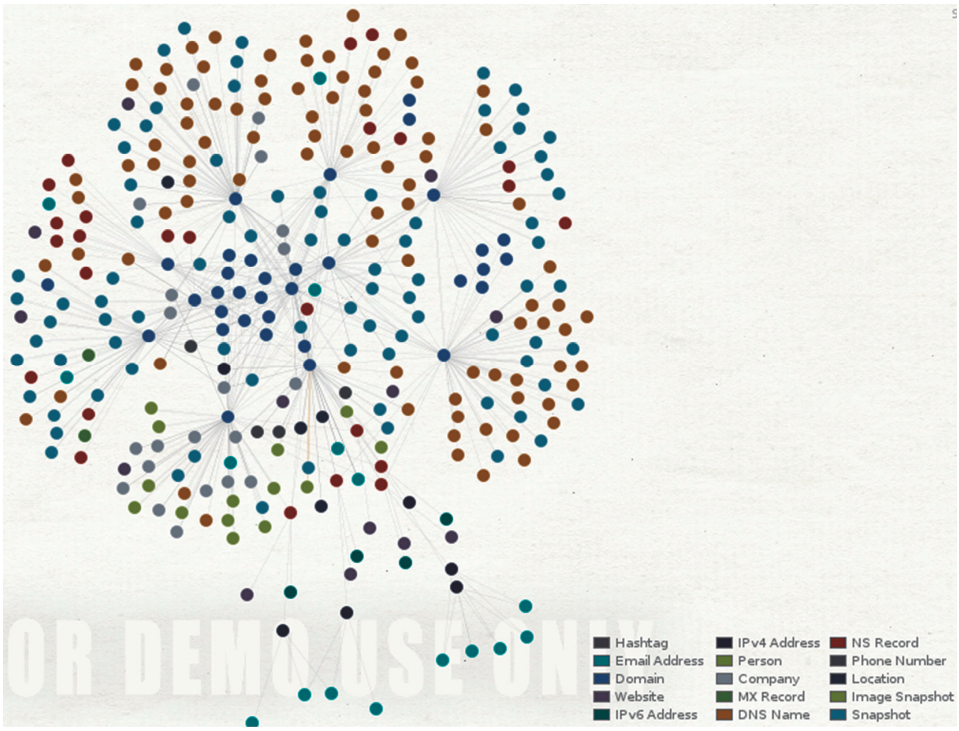
Rysunek 5.12. Dodatkowe informacje w postaci adresów e-mailowych, adresów IP oraz witryn internetowych

Proces ten może chwilę zająć, ale na końcu dysponujemy kompleksowym obrazem struktury, obejmującej witryny takie jak Yahoo, *yahoologins.com*, *yahoochatrooms* czy *rocketmail.ru* (rysunek 5.13).

Dzięki temu mamy do dyspozycji wygodną reprezentację wszystkich zgromadzonych informacji oraz powiązań z innymi domenami, serwerami nazw, serwerami e-mailowymi itp. Istne szaleństwo, prawda?

Shodan — wyszukiwarka internetu rzeczy

Shodan nie jest typową wyszukiwarką. Zamiast wyszukiwać strony, skanuje internet w poszukiwaniu urządzeń. Od kamer internetowych po sygnalizację świetlną — jeżeli urządzenie jest podłączone do internetu, Shodan je znajdzie. Biorąc pod uwagę gwałtowny wzrost liczby urządzeń internetu rzeczy, kluczowe dla każdej osoby działającej w branży cyberbezpieczeństwa i OSINT jest zrozumienie oraz umiejętne używanie tego narzędzia.



Rysunek 5.13. Niewielki przegląd informacji na temat infrastruktury yahoo.com

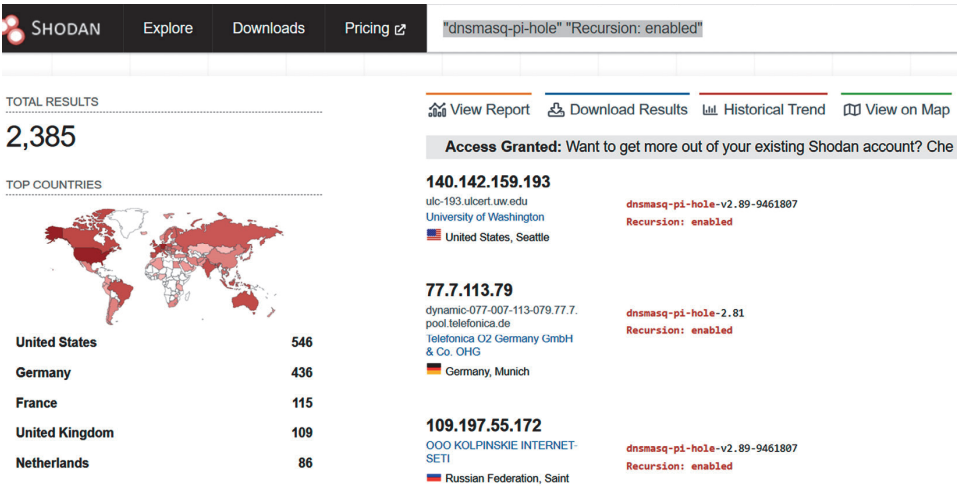
Google wyszukuje strony internetowe, Shodan — urządzenia. Ta nietypowa wyszukiwarka patrzy na internet z perspektywy dostępnych w nim urządzeń. Niezależnie od tego, czy mamy do czynienia z inteligentną lodówką, **przemysłowymi systemami sterowania** (ang. *Industrial Control System*, ICS) czy nawet miejską infrastrukturą energetyczną — jeżeli urządzenia nie są odpowiednio zabezpieczone, najprawdopodobniej Shodan je wykryje.

Początek pracy z narzędziem Shodan

Aby poznać możliwości wyszukiwarki Shodan, zacznijmy od następujących kroków:

1. Odwiedź stronę narzędzia Shodan (*https://www.shodan.io*) i utwórz konto.
2. Po zarejestrowaniu uzyskasz dostęp do interfejsu wyszukiwania. Możesz tutaj wpisać konkretne wyrażenie, adres IP lub filtr, aby rozpocząć wyszukiwanie.
3. Proste zapytanie o kamery internetowe w wyszukiwarce Shodan zwróci informacje o niezliczonych kamerach z całego świata, ale prawdziwa zabawa polega na wykorzystaniu filtrów. Na przykład możemy zapytać o kamery w Chicago, wpisując `country: US city:Chicago webcam`. I tyle!

Możliwości Shodana wykraczają poza przeszukiwanie obszarów geograficznych. Powiedzmy, że interesują nas urządzenia Pi-Hole. Wystarczy wpisać `"dnsmasq-pi-hole" "Recursion: enabled"`, a Shodan pokaże nam, gdzie na świecie znajdziemy takie urządzenia (rysunek 5.14).



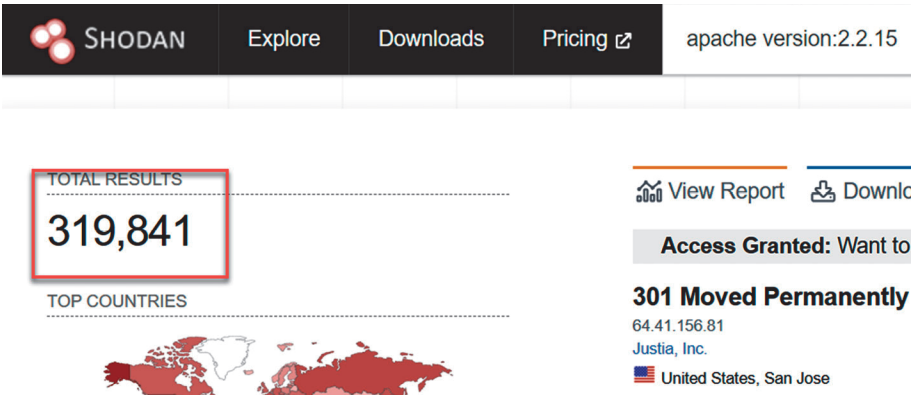
Rysunek 5.14. Wyniki zapytania o urządzenia Pi-Hole w wyszukiwarce Shodan

To narzędzie jest niewiarygodnie użyteczne dla specjalistów ds. bezpieczeństwa, zwłaszcza w przypadku prowadzenia ocen zabezpieczeń dla firm. Możemy na przykład chcieć zobaczyć wszystkie urządzenia danej firmy, takiej jak Microsoft. Wystarczy użyć filtra `org: Microsoft`, a uzyskamy odpowiednią listę.

A co, gdybyśmy chcieli znaleźć serwery z konkretną usługą lub oprogramowaniem? Shodan sprawia, że to dziecinnie proste. Jeżeli szukamy serwerów z usługą SSH, która zazwyczaj działa na porcie 22, wystarczy wpisać `port: 22`. A jeżeli jesteśmy zainteresowani serwerami z oprogramowaniem w wersji podatnej na zagrożenia, takim jak serwer Apache w wersji 2.2.15, możemy użyć filtra *version* (rysunek 5.15). Ta funkcjonalność jest szczególnie przydatna do wykrywania zagrożeń bezpieczeństwa.

Shodan to nie tylko sposób na znajdowanie kamer internetowych czy serwerów. To również wrota do eksploracji przemysłowych systemów sterowania ICS. W tym przypadku użyjemy filtra `tag: ics`. Osobom zainteresowanym bezpieczeństwem Shodan może pomóc wyszukać urządzenia, które nadal używają domyślnych haseł, co jest częstą luką w wielu systemach.

Jednym z fascynujących aspektów Shodana jest możliwość odnalezienia baz danych podłączonych do internetu. Proste wyszukiwanie terminu *MongoDB* może wykryć tysiące takich baz danych dostępnych online. Jest to poważny problem z punktu widzenia bezpieczeństwa danych. Naszym celem jako działających etycznie specjalistów ds. bezpieczeństwa jest zabezpieczenie tych systemów, a nie ich wykorzystywanie. Pamiętaj

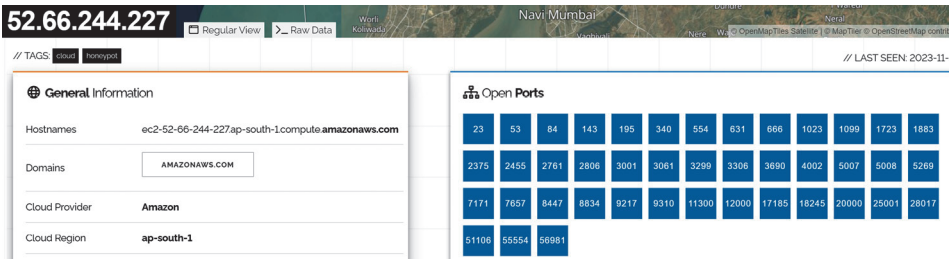


Rysunek 5.15. Ponad 319 000 serwerów Apache z podatnością wciąż jest online

o motcie: „To, że możesz, nie znaczy, że ci wolno". Jeżeli natrafisz na niezabezpieczoną bazę danych, dobrą praktyką jest poinformowanie o podatności organizacji odpowiedzialnej za zasób.

Shodan pozwala również na monitorowanie danych w czasie rzeczywistym, np. obrazów ze zdalnych kamer NetWave, które można filtrować przez kryteria geograficzne.

Jeszcze więcej informacji możemy uzyskać po kliknięciu nazwy urządzenia w wynikach wyszukiwania. Widok urządzenia zapewnia dostęp do kolejnych pokładów informacji (rysunek 5.16).



Rysunek 5.16. Kliknięcie zdalnej kamery ujawnia jeszcze więcej informacji

Kolejną niesamowitą funkcjonalnością Shodana jest możliwość zlokalizowania inteligentnych urządzeń i systemów IoT. Wyszukanie `tag: iot` może zapewnić przegląd podłączonych do sieci inteligentnych urządzeń w konkretnym obszarze, co pokazuje wszechobecność i podatność tych urządzeń.

Jednak możliwości Shodana nie kończą się na tym. Możemy również wyszukiwać specyficzne rodzaje błędów na serwerach sieciowych, takich jak zwracające nagłówki `hacked`, co jest niesamowicie przydatne dla programistów i administratorów.

Shodan znajduje również urządzenia, o których zwykle byśmy nie pomyśleli, takie jak dostępne publicznie drukarki. Może to mieć kluczowe znaczenie dla firm starających

się zapobiec wyciekom poufnych danych. Dla miłośników cyberbezpieczeństwa Shodan to skarbnica informacji na temat konfiguracji serwerów, ustawień zapór sieciowych i zabezpieczeń. To aktualizowany w czasie rzeczywistym obraz stanu zabezpieczeń w internecie.

Korzystanie z interfejsu API wyszukiwarki Shodan

Dla tych, którzy pragnęliby wykorzystać możliwości Shodana w swoich aplikacjach lub zautomatyzować zadania, narzędzie to oferuje interfejs programowania aplikacji (ang. *Application Programming Interface*, API).

Swój klucz API możesz znaleźć na ekranie głównym Shodana po rejestracji.

Pozwala on zautomatyzować wyszukiwanie, zintegrować Shodana z niestandardowymi narzędziami, takimi jak Maltego, lub nawet stworzyć nową aplikację wykorzystującą funkcjonalność wyszukiwania urządzeń.

Trace Labs — zaawansowany system operacyjny zaprojektowany do działań OSINT

Przygotuj się na całkowite zanurzenie we wspaniałym świecie OSINT dzięki systemowi operacyjnemu Trace Labs! Ta niesamowita platforma jest jak wesołe miasteczko zaprojektowane właśnie dla takich entuzjastów białego wywiadu jak my. Od momentu zalogowania wszystko skupia się na tym, aby ułatwić nam prowadzenie dochodzenia. Trace Labs bazuje na nieco okrojonej wersji dystrybucji Kali Linux, więc interfejs jest bardzo podobny (rysunek 5.17). Jest też intuicyjny i prosty, co pozwala nam skupić się na poszukiwaniach, zamiast walczyć z instalacją narzędzi. Wszelkie niezbędne wyposażenie do zdobywania informacji wywiadowczych mamy na wyciągnięcie ręki.

Poczekaj jednak, bo to nie koniec! To podrasowane narzędzie zawiera wszystko, czego potrzebujesz, aby wyciągnąć maksimum ze swoich zapytań. Programiści naprawdę zadbali o każdy szczegół i przewidzieli niestandardowe potrzeby różnych grup użytkowników.

Nie zapominajmy także o wsparciu ze strony społeczności! Zespół doświadczonych użytkowników chętnie współpracuje, daje wskazówki oraz dba o to, żebyśmy mogli w pełni wykorzystać tę platformę. Z tym wspaniałym zespołem u boku zaskoczy Cię, jak szybko rozwiniesz swoje umiejętności.

Organizacja Trace Labs opracowała model wykorzystania crowdsourcingu do współpracy w sprawach zaginięć, w odniesieniu do których organy ścigania zaapelowały



Rysunek 5.17. Pulpit systemu Trace Labs

o pomoc społeczeństwa. Organizacja zrzesza setki wykwalifikowanych badaczy w ramach konkursów typu „**zdobądź flagę**" (ang. *Capture The Flag*, CTF) oraz otwartych dochodzeń, aby pomóc w znalezieniu w sieci nowych tropów, polegając wyłącznie na OSINT.

Witryna Trace Labs to bardzo przydatne miejsce. Możesz stamtąd pobrać gotową maszynę wirtualną (*https://www.tracelabs.org/initiatives/osint-vm*), uzyskać dostęp do użytecznych narzędzi, a także zaangażować się w ciekawe inicjatywy.

Przegląd pakietu narzędzi Aircrack-ng

Aircrack-ng to nie tylko zestaw narzędzi do testowania bezpieczeństwa wi-fi, lecz również duża pomoc w prowadzeniu białego wywiadu, gdyż pomaga zbierać informacje z publicznie dostępnych źródeł, takich jak sieci bezprzewodowe.

W branży OSINT ważne jest znajdowanie słabych punktów w sieciach. Aircrack-ng pomaga zidentyfikować takie luki i pokazuje, które sieci mogą stanowić łatwy cel dla hakerów. W ten sposób możemy dowiedzieć się więcej na temat ewentualnych zagrożeń i sposobów ochrony przed nimi.

Dzięki monitorowaniu funkcjonowania sieci Aircrack-ng pomaga odkryć pewne wzorce. Na przykład możemy się dowiedzieć, kiedy dana sieć jest najbardziej aktywna, i dostrzec ewentualne anomalie.

Tego narzędzia można również użyć do mapowania sieci wi-fi w danym obszarze. Pozwala to zrozumieć, w jaki sposób sieci rozwijają się w różnych miejscach, takich jak miasta i dzielnice.

Osobom zajmującym się cyberbezpieczeństwem Aircrack-ng dostarcza całe mnóstwo praktycznych informacji. Zbierając dane z różnych sieci, badacze mogą lepiej zrozumieć, w jaki sposób tworzyć silniejsze i bezpieczniejsze sieci wi-fi.

Uwaga

Trzeba pamiętać, że chociaż Aircrack-ng jest w stanie zbierać ogromne ilości informacji, zawsze należy je wykorzystywać w sposób odpowiedzialny i etyczny. Tak jak wszystkie zaawansowane narzędzia powinien być używany do nauki i poprawy bezpieczeństwa, a nie do szkodliwych lub nielegalnych działań.

W ramach pakietu Aircrack-ng mamy dostępne różne narzędzia do różnych zadań. Można ich używać oddzielnie lub w połączeniu z innymi do prowadzenia analizy bezpieczeństwa sieci bezprzewodowych. Będziemy korzystać przede wszystkim z następujących narzędzi:

- *airmon-ng* — włącza tryb monitorowania w karcie bezprzewodowej, aby umożliwić przechwytywanie ruchu sieciowego;
- *airodump-ng* — przechwytuje ruch sieciowy, a następnie wyszukuje sieci bezprzewodowe i pakiety danych;
- *airgraph-ng* — tworzy graficzną reprezentację ruchu sieciowego;
- *aireplay-ng* — generuje ruch sieciowy i wykonuje ataki, takie jak atak anulowania uwierzytelnienia (ang. *deauthentication*) czy atak wstrzyknięcia złośliwych pakietów (ang. *packet injection*), aby zmodyfikować zachowanie sieci;
- *aircrack-ng* — główne narzędzie pakietu, które służy do łamania kluczy szyfrowania **Wired Equivalent Privacy (WEP)** i **Wi-Fi Protected Access (WPA)/WPA2**, co pozwala ocenić bezpieczeństwo sieci;
- *airbase-ng* — tworzy fałszywe **punkty dostępowe** wi-fi do przeprowadzania **ataków typu „człowiek pośrodku"** (ang. *Man-in-the-Middle*, MitM) oraz ataków socjotechnicznych.

Istnieją też inne narzędzia, takie jak `airdecap-ng`, `airdecloak-ng` i `airtun-ng`, ale nie będziemy się na nich koncentrować w tej książce.

Uwaga

Ważne jest dostrzegać różnicę między pakietem Aircrack-ng oraz narzędziem `air` ↪`crack-ng`.

Na ten moment dystrybucja Kali Linux obejmuje pakiet Aircrack-ng, ale to może się zmienić w przyszłości. Jeżeli chcemy zainstalować Aircrack-ng w dystrybucji Kali Linux lub innej, oto potrzebne polecenie:

```
sudo apt-get install aircrack-ng
```

Teraz, gdy pakiet Aircrack-ng mamy już zainstalowany, zabierzmy się do pracy.

Airmon-ng

Co zatem robi `airmon-ng`? Działa niczym przełącznik — przełącza kartę wi-fi, czyli tę rzecz w komputerze, która łączy go z wi-fi, w tryb supernasłuchiwania. Zazwyczaj karta wi-fi zwraca jedynie uwagę na te informacje, które są przeznaczone dla naszego komputera. Z narzędziem `airmon-ng` zaczyna jednak nasłuchiwać wszystkich sygnałów wi-fi z otoczenia, nawet tych, które nie są przeznaczone dla nas. To właśnie **tryb monitorowania** (ang. *monitor mode*).

Dlaczego tryb monitorowania jest istotny? Wyobraź sobie, że jesteś specjalistą ds. cyberbezpieczeństwa lub kimś, kto potrzebuje sprawdzić, czy sieć wi-fi jest bezpieczna. Korzystając z `airmon-ng`, możesz nasłuchiwać wszystkiego dookoła i zorientować się, czy sieć ma jakieś luki albo czy ktoś nie próbuje się do niej włamać.

Korzystanie z `airmon-ng` jest dość proste. Przede wszystkim musimy się dowiedzieć, jak nazywa się nasza karta wi-fi (nazwa zazwyczaj brzmi podobnie do `wlan0`). Możemy to zrobić za pomocą prostych poleceń komputerowych. Znając nazwę, możemy użyć `airmon-ng` do przełączenia karty w tryb nałogowego podsłuchiwacza. Tryb zarządzany (ang. *managed mode*) to domyślny tryb działania kart wi-fi, w którym karta otrzymuje jedynie pakiety przeznaczone dla konkretnego adresu MAC. Tryb monitorowania umożliwia karcie otrzymywanie dowolnych pakietów w zasięgu, nawet jeżeli nie są zaadresowane do adresu MAC naszego urządzenia. Przełączmy teraz naszą kartę wi-fi w tryb monitorowania.

1. Aby sprawdzić nazwę interfejsu, uruchom następujące polecenie:

   ```
   ifconfig
   ```

   Zanotujmy nazwę interfejsu, gdyż będzie nam za chwilę potrzebna.

2. Sprawdźmy również stan interfejsów bezprzewodowych:

   ```
   sudo airmon-ng
   ```

3. Teraz chcemy się dowiedzieć, czy jest coś, co może zakłócić działanie pakietu Aircrack-ng:

   ```
   sudo airmon-ng check
   ```

4. Jeżeli pojawią się jakieś wyniki, będziemy chcieli zamknąć te procesy:

   ```
   sudo airmon-ng check kill
   ```

5. Następnie, aby zacząć aktywnie monitorować i podejrzeć, co się dzieje na karcie sieciowej, wpisujemy:

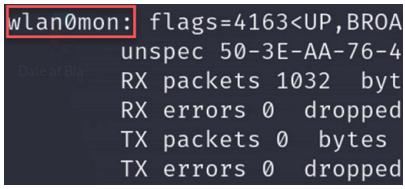
   ```
   sudo airmon-ng start <znaleziona wcześniej nazwa karty sieciowej>
   ```

6. I na koniec:

   ```
   ifconfig
   ```

Teraz możemy zobaczyć, że adapter zmienił nazwę z `wlan0` na `wlan0mon` (rysunek 5.18).

Oprócz wcześniej wspomnianych poleceń narzędzia `airmon-ng` istnieje jeszcze kilka, które mogą okazać się pomocne. Jednym z nich jest polecenie `airmon-ng stop`, które



Rysunek 5.18. Program airmon-ng zmienił nazwę karty sieciowej

wyłączy tryb monitorowania w danym interfejsie. Z kolei polecenie `airmon-ng --channel` ustawia domyślny kanał przy włączaniu trybu monitorowania.

Gdy **karta sieciowa** (ang. *network interface card*, NIC) jest już w trybie monitorowania, możemy zacząć przechwytywać niezbędne dane i przeprowadzać kontrole bezpieczeństwa sieci bezprzewodowej. To dopiero pierwszy akt sztuki, w którym pakiet Aircrack-ng odgrywa główną rolę.

Airodump-ng

Program `airodump-ng` to kolejne narzędzie z pakietu Aircrack-ng — niezwykle użyteczne dla każdej osoby zainteresowanej bezpieczeństwem sieci bezprzewodowych. Zostało zaprojektowane, aby pomóc zbierać informacje o otaczających nas sieciach wi-fi.

Oto co robi `airodump-ng`:

- **Przechwytuje dane wi-fi**. Nasłuchuje danych z sieci i je przechwytuje. Może zobaczyć cały ruch sieci odbywający się dookoła, a nie tylko ten, który jest przeznaczony dla naszego urządzenia.
- **Widzi szczegółowe informacje na temat sieci**. Pokazuje listę wszystkich sieci wi-fi, które jest w stanie znaleźć, wraz z informacjami o tym, jak silny jest sygnał, jaki kanał obsługują oraz jakiego rodzaju zabezpieczeń używają.
- **Śledzi urządzenia**. Może również dowiedzieć się, jakie urządzenia (telefony, laptopy) są podłączone do każdej sieci wi-fi.

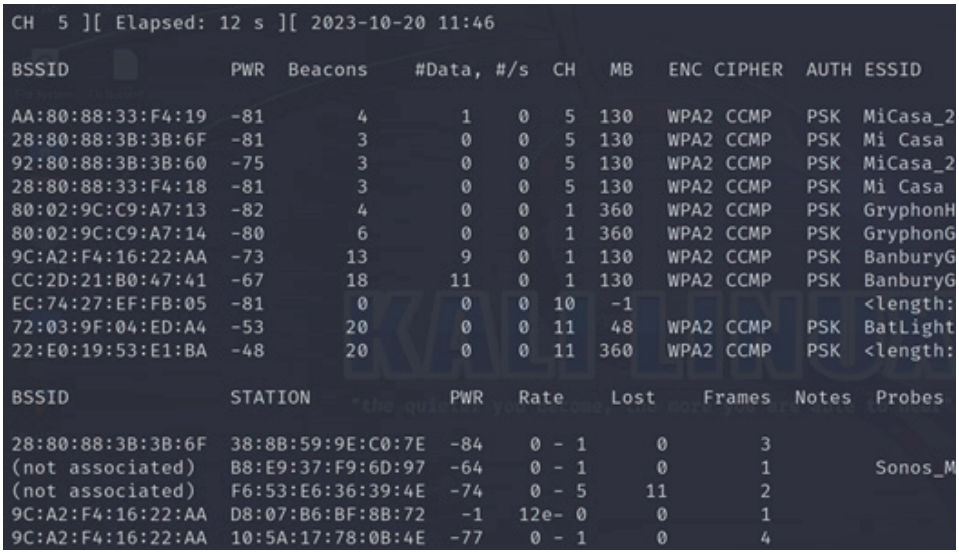
Korzystanie z programu `airodump-ng` wymaga wcześniejszego uruchomienia narzędzia `airmon-ng`, który to proces opisałem w poprzednim punkcie. Gdy jesteśmy gotowi, wpisujemy:

```
sudo airodump-ng wlan0mon
```

Wynik użycia polecenia można zobaczyć na rysunku 5.19.

Istnieje też kilka poleceń, które pozwolą nam ograniczyć zakres przechwytywania za pomocą `airodump-ng`. Obejmują one:

- `--channel` — wybór kanału do nasłuchiwania;
- `--bssid` — ograniczenie wyników do konkretnego identyfikatora **BSSID** (ang. *Basic Service Set Identifier*);
- `-w` — określenie przedrostka plików wynikowych;



Rysunek 5.19. Narzędzie airodump-ng identyfikuje sygnały wi-fi

- `--encrypt` — ograniczenie wyników do konkretnego rodzaju szyfrowania;
- `--showack` — pokazywanie statystyk ACK dla klientów w celu wykrycia podatności z kategorii wstrzykiwania.

Oto przykład użycia niektórych z tych opcji:

```
sudo airodump-ng wlan0mon --channel 6 --bssid <AA:BB:CC:DD:EE:FF> -w
output
```

Dzięki *airodump-ng* możemy gromadzić informacje takie jak adresy MAC punktów dostępowych i systemów klienckich do dalszej analizy oraz konfiguracji zaawansowanych ataków, które możemy zrealizować za pomocą pakietu Aircrack-ng.

Aireplay-ng

Ataki anulowania uwierzytelnienia (ang. *deauthentication*), wykonywane przez `aire`
`↪play-ng`, stanowią istotny element w arsenale testowania bezpieczeństwa sieci. Takie ataki zakłócają komunikację między klientem a punktem dostępowym, zmuszając je do rozłączenia się. Ta technika wykorzystuje pakiety anulujące uwierzytelnienie, które stanowią część protokołu wi-fi, ale mogą być również wykorzystywane do zakończenia połączenia. Ten proces ma kluczowe znaczenie w testowaniu odporności sieci na **ataki blokady usług** (ang. *Denial of Service*, DoS) oraz przejmowanie sygnałów negocjacji (ang. *handshakes*) w przypadku WPA/WPA2.

Aby użyć narzędzia `aireplay-ng`, należy podać:

- rodzaj ataku poprzez użycie odpowiedniej opcji, np. `--deauth`;
- docelową sieć za pomocą opcji `-a` wraz z identyfikatorem BSSID celu;

- informacje na temat interfejsu monitorującego, takiego jak `wlan0mon`, a także adresów MAC docelowych punktów dostępowych i klientów.

Oto przykład kompletnego polecenia dla narzędzia `aireplay-ng`:

```
sudo aireplay-ng --deauth 100 -a <AA:BB:CC:DD:EE:FF> -c
<11:22:33:44:55:66> wlan0mon
```

Niektóre popularne opcje polecenia `aireplay-ng` obejmują:

- `--deauth` — przeprowadzenie ataku anulowania uwierzytelnienia;
- `--fakeauth` — przeprowadzenie ataku nieprawidłowego uwierzytelnienia;
- `--arpreplay` — przeprowadzenie ataku metodą powtórzenia żądania protokołu **Address Resolution Protocol** (**ARP**);
- `-a` — określenie identyfikatora BSSID docelowego punktu dostępowego;
- `-c` — określenie adresu MAC docelowego klienta.

Możliwości programu `aireplay-ng` obejmują szerokie spektrum zastosowań testowych. Dzięki symulowaniu różnych wektorów ataku — od podstawowych ataków anulowania uwierzytelnienia po złożone ataki wstrzykiwania pakietów ARP — program umożliwia dogłębną analizę bezpieczeństwa sieci. To narzędzie ma istotne znaczenie w identyfikowaniu podatności, testowaniu reakcji sieci na wrogie działania oraz potwierdzaniu skuteczności zabezpieczeń.

Aircrack-ng

Program `aircrack-ng` odgrywa ważną rolę w testowaniu bezpieczeństwa sieci dzięki łamaniu kluczy kryptograficznych. To ważne, aby wiedzieć, jak złamać szyfrowanie WEP i WPA/WPA2. Standard szyfrowania WEP łatwiej złamać, gdyż jest starszy i mniej bezpieczny ze względu na swoje podatności. Standardy WPA i WPA2 są trudniejsze do złamania, choć nadal jest to możliwe, zwłaszcza w przypadku słabych haseł i zaawansowanych technik prowadzenia ataku.

Aby złamać szyfrowanie WPA/WPA2, program `aircrack-ng` wykorzystuje przede wszystkim dwie metody: ataki słownikowe i ataki siłowe. Ataki słownikowe wypróbowują hasła z wcześniej opracowanej listy, a ataki siłowe sprawdzają wszystkie kombinacje znaków, aż do odnalezienia właściwej. Powodzenie tych metod zależy od siły hasła oraz jakości słownika.

Przy łamaniu szyfrowania WPA/WPA2, oprócz stosowania ataków słownikowych i siłowych, ważne jest również wykorzystanie pliku `.cap`, który zawiera pakiety danych przechwycone z sieci. Na podstawie analizy tych pakietów, zwłaszcza tych, które dotyczą procesu negocjacji, program `aircrack-ng` podejmuje próby złamania klucza sieciowego. Powodzenie złamania hasła zależy od informacji zawartych w pliku `.cap`, który zawiera dane z procesu negocjacji potrzebne do odszyfrowania klucza kryptograficznego sieci.

Oto niektóre z opcji często używanych z poleceniem `aircrack-ng`:

- `-w` — określenie pliku z listą słów lub słownikiem;
- `-b` — określenie identyfikatora BSSID docelowego punktu dostępowego;
- `-e` — określenie identyfikatora ESSID (ang. *Extended Service Set Identifier*);
- `-a` — określanie trybu ataku, np. `2` dla szyfrowania WPA/WPA2 ze wstępnie udostępnionym kluczem (ang. *Pre-Shared Key*, PSK).

Przykład użycia niektórych z tych opcji pokazuje następujące polecenie:

```
sudo aircrack-ng -w dictionary.txt -b <AA:BB:CC:DD:E:FF> output-01.cap
```

Po znalezieniu ewentualnego klucza program `aircrack-ng` sprawdza, czy jest w stanie odszyfrować dane z sieci. To bardzo ważne, aby wiedzieć, jak silne jest szyfrowanie, i móc wykryć luki w bezpieczeństwie. Pomaga to również zrozumieć, jakie hasła są łatwiejsze do złamania, co przydaje się przy opracowywaniu zasad tworzenia silnych haseł.

Airbase-ng

Program `airbase-ng` to kolejne ciekawe narzędzie z pakietu Aircrack-ng, które pozwala tworzyć fałszywe punkty dostępowe. Dzięki `airbase-ng` możemy zastawić sprytną pułapkę i sprawdzić zarówno odporność sieci, jak i to, czy użytkownicy są w stanie wykryć podstęp. Z tym narzędziem zarzucenie przynęty nie nastręcza specjalistom zbyt wielu problemów, a możliwość obserwowania interakcji między ludźmi i sieciami jest bezcenna i może nas wiele nauczyć o zabezpieczaniu sieci wi-fi.

Jak wspomniałem, tworzenie fałszywych hotspotów jest dziecinnie proste. Wybierasz kanał i podajesz nazwę wi-fi (tzn. identyfikator ESSID), która brzmi wiarygodnie. Sami decydujemy, czy chcemy, żeby nasza fałszywa sieć pytała o hasło, czy nie. Najważniejsze, żeby nie wzbudzać podejrzeń.

To jednak nie wszystko! Fałszywe hotspoty nie mają tylko ładnie wyglądać. Mogą być punktem wyjściowym do ataków MitM. Polegają one na tym, że haker niezauważenie przechwytuje wiadomości przesyłane między osobami, które myślą, że rozmawiają ze sobą bezpośrednio. Ustanowiwszy fałszywy hotspot, haker dostaje się między rozmówców i może ich podsłuchiwać, a nawet modyfikować przesyłane dane.

Ustanowienie fałszywego punktu dostępowego za pomocą `airbase-ng` wymaga podania konkretnych informacji. Wybieramy identyfikator ESSID, czyli nazwę sieci, kanał oraz to, czy komunikacja będzie zaszyfrowana, czy nie. Musimy również skonfigurować swoje urządzenie do monitorowania bezprzewodowego ruchu sieciowego za pomocą interfejsu `wlan0mon`, który utworzyliśmy narzędziem `airmon-ng`. Polecenie trzeba nieco dostosować, aby nasz punkt dostępowy wyglądał na prawdziwy:

```
sudo airbase-ng -a <AA:BB:CC:DD:EE:FF> --essid <nazwa fałszywego punktu
↪dostępowego>
--channel <numer kanału> wlan0mon
```

Oto kilka dodatkowych opcji programu `airbase-ng`, dzięki którym można spersonalizować przynętę:

- `-a` — ustawienie identyfikatora BSSID fałszywego punktu dostępowego;
- `--essid` — ustawienie identyfikatora ESSID fałszywego punktu dostępowego;
- `--channel` — określenie kanału;
- `-W 1` — włączenie obsługi WEP;
- `-z` — włączenie obsługi WPA/WPA2.

Dzięki swojej elastyczności i szerokiemu zakresowi opcji `airbase-ng` jest bardzo przydatnym narzędziem dla każdego testującego bezpieczeństwo sieci.

Airgraph-ng

Program `airgraph-ng` to kolejny istotny element pakietu Aircrack-ng. To narzędzie pomaga lepiej zrozumieć daną sieć bezprzewodową. Przekształca złożone informacje sieciowe w grafy, które łatwo się czyta. Pokazują one wiele ważnych szczegółów na temat sieci, takich jak ilość przechodzących przez nią danych, podłączone urządzenia i ewentualne zagrożenia bezpieczeństwa.

Aby skorzystać z `airgraph-ng`, trzeba najpierw zebrać dane sieciowe za pomocą `airo↪dump-ng`. Tych danych użyjemy do tworzenia grafów. Polecenie `airgraph-ng` wymaga wskazania pliku CSV uzyskanego po uruchomieniu `airodump-ng` oraz pliku wynikowego na gotowy graf. Jeżeli chcemy wygenerować graf **relacji między klientami a punktami dostępowymi** (ang. *Client to AP Relationship*, CAPR), który pokazuje połączenia i pakiety danych, użyjemy tego polecenia:

```
sudo airgraph-ng -i output-01.csv -o output.png -g CAPR
```

Oto najużyteczniejsze opcje do zbierania danych:

- `-i` — wskazanie wejściowego pliku CSV;
- `-o` — wskazanie wyjściowego pliku z grafem;
- `-g` — określenie typu grafu.

Grafy wykonane programem `airgraph-ng` pomagają zrozumieć badaną sieć. Przekształcają złożone dane i upraszczają je, pomagając dostrzec wzorce i wykryć problemy. Możemy na przykład sprawdzić, czy przez sieć o jakichś porach przechodzi dużo danych albo czy w sieci znajdują się urządzenia, których nie powinno tam być. Te grafy są szczególnie użyteczne do wyszukiwania nietypowej aktywności, która może świadczyć o zagrożeniu.

Znajdowanie ukrytych sieci

Zrozumienie podstaw pakietu Aircrack-ng to nieodzowny krok do odkrywania ukrytych sieci. Powinniśmy pamiętać o tym, że nawet jeżeli sieć jest ukryta, nie jest całkowicie niewidoczna. Pomyśl o kiepskim magiku, który na przyjęciu urodzinowym dla

dzieci sprawia, że coś znika, ale uważny obserwator dostrzeże, gdzie to coś się podziało. W tym przypadku nazwy i identyfikatory SSID ukrytych sieci nie są publicznie udostępniane, ale z właściwymi narzędziami możemy odkryć to, co miało pozostać tajemnicą. Zidentyfikowanie ukrytej sieci nie jest niemożliwe, a przy odpowiednim podejściu — wręcz proste.

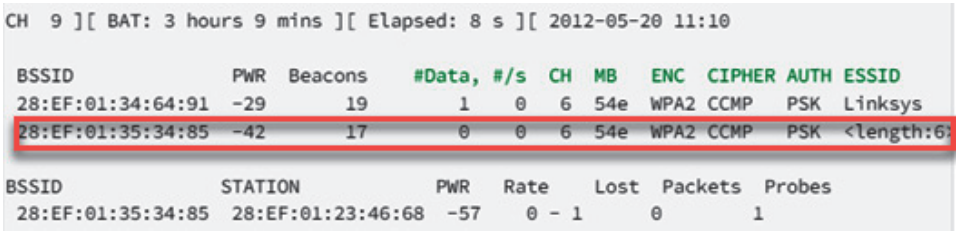
Najpierw chcemy przełączyć kartę sieciową w tryb monitorowania, aby zobaczyć wszystkie tajne sygnały wi-fi przepływające w powietrzu:

```
airmon-ng start wlan0
```

Teraz jesteśmy gotowi, aby zacząć monitorować wszystkie sieci w najbliższej odległości. Robimy to następującym poleceniem:

```
airodump-ng wlan0mon
```

Na ekranie pojawi się lista, na której identyfikatory SSID ukrytych sieci będą widoczne jako `<length: x>`, gdzie `x` oznacza długość nazwy (rysunek 5.20). Jest jednak coś, co pomoże nam ujawnić tę nazwę. Otóż każde urządzenie podłączone do ukrytej sieci wysyła ramki sondujące (ang. *probe requests*) z prośbą o ponowne połączenie. Każde takie żądanie podaje nam ukryty identyfikator SSID na talerzu!



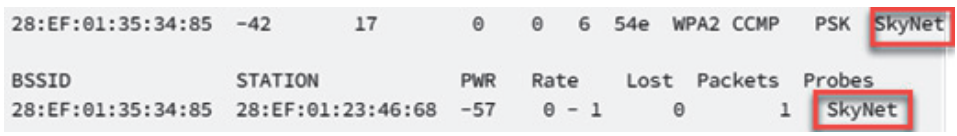
Rysunek 5.20. Program airodump-ng podaje identyfikator ESSID punktu dostępowego jako <length: 6>

Musimy jedynie zmusić podłączone urządzenie do wysłania takiej ramki poprzez chwilowe odłączenie go od sieci. Użyjemy do tego następującego polecenia:

```
aireplay-ng -0 30 -a [adres MAC punktu dostępowego] -c [adres MAC klienta]
↪wlan0mon
```

Flaga `-0` wysyła sygnał rozłączenia, a wartość 30 wskazuje liczbę pakietów do wysłania.

Po anulowaniu uwierzytelnienia u klienta przejdźmy do programu `airodump-ng` i zobaczmy, jak ukryty identyfikator SSID pojawia się niczym za dotknięciem czarodziejskiej różdżki! Bajecznie proste.



Rysunek 5.21. Program airodump-ng pokazuje, że identyfikator SSID sieci to SkyNet

Chociaż ukrycie identyfikatora wydaje się pomysłowe, dla hakera poznanie go to bułka z masłem. Niech nie daje to nam złudnego poczucia bezpieczeństwa! Używajmy silnego szyfrowania, złożonych haseł i innych zabezpieczeń.

Atak anulowania uwierzytelnienia może nam również posłużyć do przeprowadzenia ataku MitM, który prowadzi do przechwycenia danych. To poważne zagrożenie, przed którym należy się dobrze zabezpieczyć.

Na początku haker wysyła sygnał rozłączenia, aby zmusić urządzenie do rozłączenia z prawdziwą siecią wi-fi. To może być bardzo frustrujące!

Następnie haker konfiguruje router o takiej samej nazwie sieciowej jak prawdziwy. Nazywamy go „złym bliźniakiem" (ang. *Evil Twin*). Urządzenie łączy się z fałszywą siecią, ale nie jest tego świadome.

Teraz dochodzimy do ataku MitM — wszelkie dane przesyłane przez fałszywą sieć zostają przechwycone przez hakera. Obejmuje to wrażliwe dane, takie jak hasła, wiadomości i adresy e-mailowe. Scenariusz jak z koszmaru.

Dodatkowe otwartoźródłowe narzędzia OSINT

Narzędzia OSINT oferują szeroki wachlarz możliwości, które obejmują zdobywanie informacji o domenach czy monitorowanie mediów społecznościowych. Te narzędzia, dostępne dla każdego, można też często dostosowywać do swoich potrzeb dzięki ich otwartoźródłowej naturze. Za chwilę przedstawię kolejną porcję wyjątkowych narzędzi OSINT o ogólnodostępnym kodzie źródłowym wraz z ich funkcjonalnościami oraz zastosowaniem w środowisku Kali Linux.

SpiderFoot

SpiderFoot to potężne narzędzie do automatyzacji działań OSINT, które łączy różne źródła danych, aby zbierać i centralizować informacje o konkretnym celu. Mogą to być adresy IP, nazwy domen, adresy e-mailowe czy nawet nazwy użytkowników. Dzięki ponad 200 modułom SpiderFoot łączy w sobie dużą część funkcjonalności z zakresu cyfrowego wywiadu, co ułatwia śledczym analizowanie i interpretowanie danych.

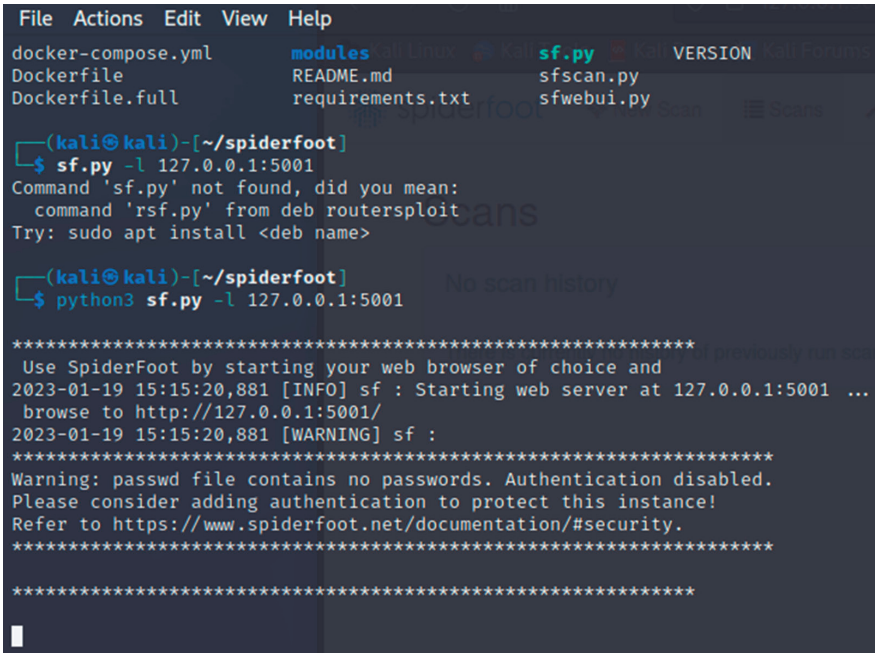
Aby zainstalować SpiderFoota, otwórz terminal i wpisz:

```
sudo apt install spiderfoot
```

Aby uruchomić narzędzie, musimy określić adres IP i port:

```
spiderfoot -l 127.0.0.1:5001
```

Wynik użycia polecenia zaprezentowałem na rysunku 5.22.



Rysunek 5.22. Uruchamianie aplikacji SpiderFoot

Po uruchomieniu usługi SpiderFoot otwórz przeglądarkę i wpisz następujący adres:

```
127.0.0.1:5001
```

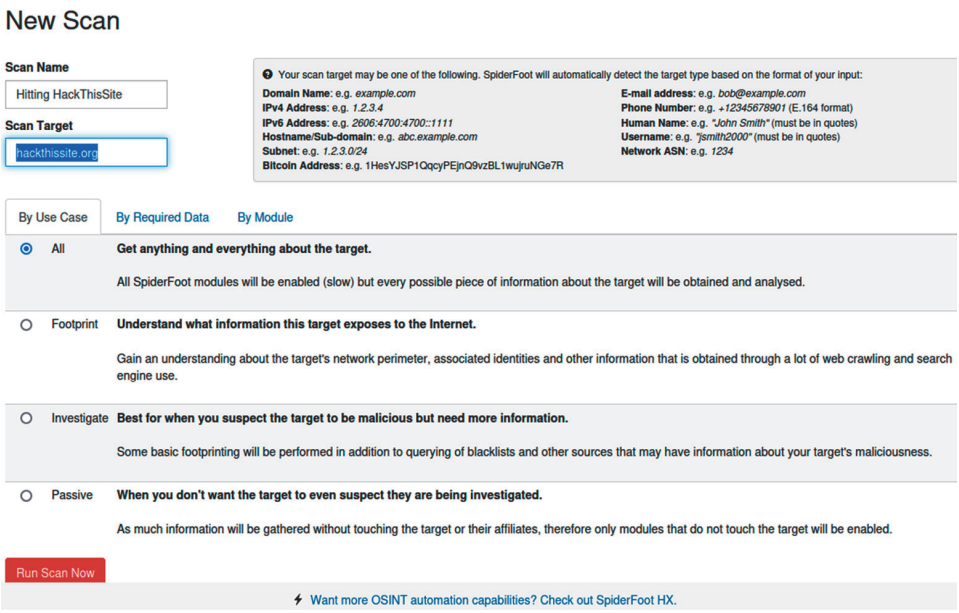
Na ekranie powinien pojawić się interfejs w formie strony internetowej (rysunek 5.23). Kliknijmy zakładkę *New Scan* (nowy skan) i wprowadźmy informacje potrzebne do określenia celu. Użyjemy *hackthissite.org* jako przykładu.

Kliknij przycisk *Run Scan Now* (uruchom skan teraz) i poczekaj na zakończenie procesu. Może to trochę potrwać, ale w nagrodę za cierpliwość dostaniemy całe mnóstwo danych na temat domeny. To prawdziwa kopalnia informacji, jak zwykłem mawiać (rysunek 5.24).

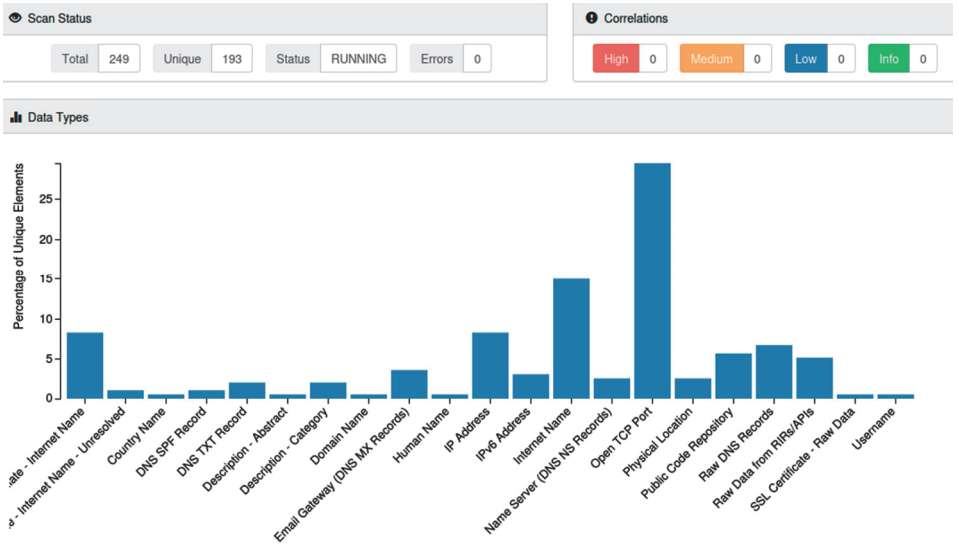
Bardzo przydatną funkcjonalnością w aplikacji SpiderFoot jest możliwość skupienia się na wynikach z jednej kolumny, aby uzyskać więcej informacji. Dzięki temu można łatwo eksplorować i szczegółowo analizować dane. Po prostu klikamy dowolną kolumnę, która przyciąga naszą uwagę, a narzędzie automatycznie wyświetli wszystkie istotne informacje z tej kategorii. Ta niesamowicie pomocna i łatwa w użyciu funkcjonalność sprawia, że analiza danych to czysta przyjemność!

Końcowe przemyślenia na temat narzędzi

Wiem, że mówiliśmy dużo o narzędziach, ale przy okazji jedna myśl mrozi mi krew w żyłach. Chodzi o ilość informacji, które nieświadomie ujawniamy, czy to w mediach społecznościowych, czy podczas rejestracji w aplikacjach i usługach online. Nasze dane



Rysunek 5.23. Konfiguracja nowego skanu w narzędziu SpiderFoot

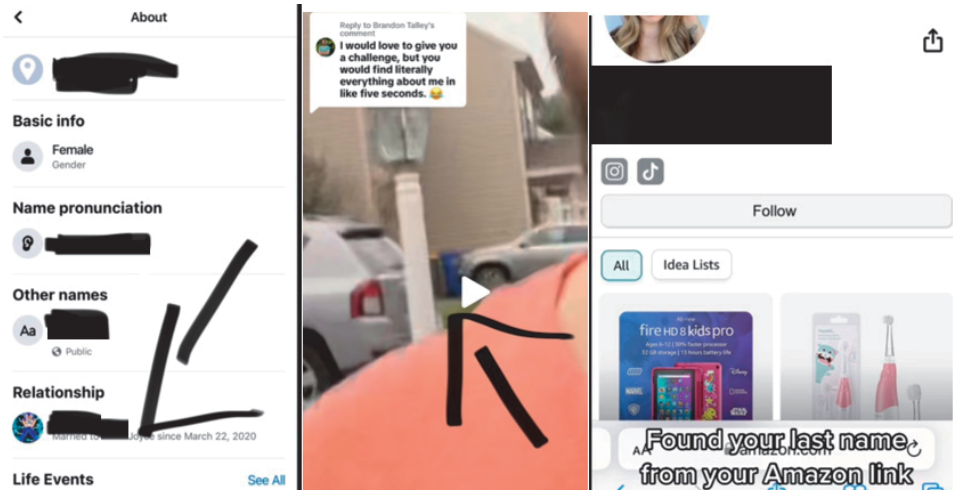


Rysunek 5.24. Wynik skanu w narzędziu SpiderFoot

są wszędzie. Te informacje są łatwo dostępne nawet bez narzędzi. Wystarczy umiejętność wyciągania wniosków i zdrowy rozsądek.

Jednym z najciekawszych detektywów działających na TikToku jest Shay, znana pod nazwą użytkownika *@shay.nanigans87*. Przy ponad 410 000 obserwujących (stan

z października 2024 r.) Shay zdobyła sławę dzięki umiejętności identyfikowania zupełnie obcych sobie osób na podstawie minimalnej ilości danych. Na filmikach pokazuje, jak sprawdza drobne szczegóły na zdjęciach, odszyfrowuje zamazane fragmenty i łączy w całość rozmaite informacje, aby zidentyfikować osoby, które rzuciły jej wyzwanie (rysunek 5.25).



Rysunek 5.25. Użytkowniczka TikToka @shay.nanigans87 nie używa żadnych narzędzi do odnalezienia celów

W jednym z filmików Shay pokazuje, w jaki sposób wykorzystuje częściowo zasłonięty napis na pojemniku z czyjegoś zdjęcia, aby znaleźć adres tej osoby. W innym skupia się na zamazanym rachunku ze sklepu i odczytuje z niego dane klienta. Jej filmiki są porywającym pokazem pracy cyfrowego detektywa.

Chociaż Shay zapewnia, że wykorzystuje swoje umiejętności jedynie w sposób etyczny, jej filmiki przypominają, że nasza prywatność w erze cyfryzacji jest bardziej krucha, niż nam się wydaje.

Po wypróbowaniu wszystkich tych narzędzi kolejnym pytaniem, które się nasuwa, jest to, jak nadążyć za zmianami w narzędziach i technikach OSINT. Opowiem o tym za chwilę.

Nadążanie za tempem zmian w dziedzinie OSINT

W miarę rozwoju technologii narzędzia i techniki wykorzystywane w tej dziedzinie zmieniają się, aby mogły pozostać skuteczne. Pojawiają się też nowe platformy i supernowoczesne narzędzia. Dla specjalistów OSINT dotrzymanie kroku tym zmianom jest szczególnie ważne.

Blogi i witryny internetowe

Wielu badaczy, specjalistów i entuzjastów w dziedzinie wywiadu i cyberbezpieczeństwa prowadzi blogi lub witryny, gdzie omawiają najnowsze techniki, narzędzia i sprawy OSINT. Regularne czytanie takich źródeł zapewnia wgląd w najnowsze trendy i najlepsze praktyki. Witryny takie jak *Bellingcat*, *OSINT Essentials* i *OSINT Techniques* to istne kopalnie informacji.

- **Bellingcat** (*https://www.bellingcat.com*). Witryna poświęcona dziennikarstwu śledczemu, która specjalizuje się w sprawdzaniu faktów i analizie OSINT. Często publikowane są tam informacje na temat metodologii prowadzenia śledztwa, które stanowią doskonały materiał do nauki.
- **OSINT Curious** (*https://www.osintcurio.us*). Projekt skupiony na nowościach i zasobach z branży OSINT. Oferuje spotkania online i blogi, a także narzędzia i wskazówki dla społeczności OSINT.
- **Week in OSINT z witryny Sector035** (*https://sector035.nl/articles/category:week-in-osint*). Oferuje cotygodniowe podsumowanie interesujących wiadomości dla społeczności OSINT wraz z linkami.
- **IntelTechniques** (*https://inteltechniques.com*). Witryna prowadzona przez Michaela Bazzella, byłego śledczego FBI do spraw cyberprzestępczości. Strona zapewnia szeroki wachlarz narzędzi, szkoleń i zasobów związanych z OSINT.
- **OSINT Essentials** (*https://www.osintessentials.com*). Witryna oferuje wiele zasobów z narzędziami, odniesieniami i przewodnikami dla specjalistów i miłośników OSINT.
- **OSINT Techniques** (*https://www.osinttechniques.com*). To użyteczna witryna z treściami edukacyjnymi, zasobami i narzędziami OSINT podzielonymi na kategorie.

Konferencje i warsztaty

Odbywające się co roku duże konferencje z dziedziny cyberbezpieczeństwa, takie jak DEF CON, Black Hat i BSides, oferują specjalne panele poświęcone OSINT. Te wydarzenia stanowią wspaniałą okazję, aby poznać OSINT w praktyce. Często możemy tam spotkać najlepszych instruktorów w tej dziedzinie. Ponadto konferencje to doskonałe miejsce na poznanie innych osób, które pracują w cyberbezpieczeństwie, mogą nas czegoś nauczyć, a nawet pomóc nam w rozwoju kariery zawodowej.

Ocena nowych narzędzi

Gdy wypróbowujemy nowe narzędzia OSINT, powinniśmy pamiętać o kilku rzeczach:

- **Kto jest autorem?** Sprawdź, kto stworzył dane narzędzie. Dowiedz się, jak nazywał się deweloper lub firma, aby ocenić, czy są znani w środowisku OSINT i czy cieszą się zaufaniem.

- **Co zyskam?** Zadaj sobie następujące pytania: Czy to narzędzie robi coś, czego nie mogę zrobić za pomocą dotychczasowych? Czy jest szybsze albo dokładniejsze? Jeżeli robi dokładnie to samo co inne narzędzia, może nie warto go używać.
- **Co mówią inni?** Poszukaj recenzji i komentarzy osób, które używały tego narzędzia. Odwiedź fora, media społecznościowe i witryny poświęcone narzędziom OSINT. Czy łatwo się go używa? Czy dobrze działa? Czy były z nim jakieś problemy?
- **Co z aktualizacjami?** Dobre narzędzia są regularnie aktualizowane przez twórców. Dzięki temu błędy są naprawiane, a narzędzia są z czasem coraz lepsze. Są też dostosowywane do nowych wyzwań w dziedzinie OSINT. Sprawdź stronę lub forum internetowe poświęcone narzędziu, aby dowiedzieć się, jak często wychodzą aktualizacje i czy rzeczywiście coś usprawniają.

Mając te kwestie z tyłu głowy, możemy wybrać najlepsze narzędzia OSINT, które są bezpieczne, użyteczne i dostosowane do zmian w świecie cyberbezpieczeństwa.

Przynależność do społeczności OSINT

Społeczność OSINT jest liczna i zróżnicowana. Obejmuje specjalistów z różnych dziedzin i o różnych poziomach doświadczenia. Przynależność do tej społeczności może przynieść nam następujące korzyści:

- **Nauka przez współpracę**. Dzielenie się doświadczeniami, wyzwaniami i rozwiązaniami może prowadzić do rozwoju wszystkich zaangażowanych stron.
- **Nowe perspektywy**. Różne osoby mogą odmiennie podchodzić do różnych problemów. Współpraca z innymi może zaowocować nowym spojrzeniem lub poznaniem nowej techniki.
- **Budowanie sieci kontaktów**. Nawiązywanie relacji w ramach społeczności może stanowić szansę na rozpoczęcie współpracy, znalezienie mentora czy otrzymanie oferty pracy.

Podsumowanie

W tym rozdziale przyjrzeliśmy się różnym niesamowitym narzędziom OSINT, takim jak Recon-ng, Maltego, Shodan oraz system operacyjny Trace Labs. Każde z tych narzędzi w inny sposób pomaga nam zrozumieć i lepiej wykorzystywać OSINT. Na przykład Maltego pozwala dostrzec powiązania między fragmentami danych, a Shodan oferuje wgląd w internet rzeczy. Rozmawialiśmy również o innych narzędziach, takich jak Aircrack-ng, SpiderFoot i Twint, a także o znaczeniu nieustannego poszerzania swojej wiedzy i o współpracy ze społecznością OSINT.

Za chwilę dowiesz się, w jaki sposób mądre użycie OSINT może wykryć ryzyka dla cyberbezpieczeństwa i zapobiegać im, zapewniając osobom i firmom bezpieczeństwo w internecie.

Oczy i uszy analizy zagrożeń — jak OSINT ogranicza ryzyka cybernetyczne

Rozdział 6

W tym rozdziale nastąpi zwrot akcji. Przejdziemy od teorii do prawdziwych zastosowań **OSINT** w dziedzinie cyberbezpieczeństwa. Przyszedł czas na to, żeby wykorzystać zdobyte podstawy i zaprząc je do praktycznego wsparcia analizy zagrożeń.

W tym rozdziale poruszymy następujące aspekty:

- wprowadzenie do OSINT w analizie zagrożeń;
- zagrożenia cybernetyczne a OSINT;
- platformy do analizy zagrożeń cybernetycznych i ich zastosowanie w OSINT;
- tworzenie strategii analizy zagrożeń na bazie OSINT;
- studium przypadku, czyli rola OSINT w prawdziwych incydentach z zakresu cyberbezpieczeństwa.

Zanim dotrzesz do końca rozdziału, osiągniesz biegłość w dziedzinie OSINT. Zrozumiesz jej znaczenie dla wykrywania potencjalnych zagrożeń dzięki połączeniu wiedzy technicznej i spostrzegawczości. Ponadto nauczysz się wykorzystywać te umiejętności w sposób strategiczny w odniesieniu do wszystkich aspektów cyberbezpieczeństwa, które są powiązane z ludzkimi interakcjami, czyli praktycznie we wszystkich przypadkach. Czas przekuć teorię w praktykę. Do dzieła!

Wprowadzenie do OSINT w analizie zagrożeń

Najpierw musisz się dowiedzieć, dlaczego OSINT odgrywa tak ważną rolę w analizie cyberzagrożeń. W cyfrowym świecie informacje to potęga, a OSINT zapewnia mnóstwo informacji z publicznie dostępnych źródeł. Niezależnie od tego, czy chodzi o media społecznościowe, fora, wyszukiwarki czy bazy danych, OSINT pozwala wykorzystać te zasoby i wyciągnąć wnioski, które inaczej można by przeoczyć. To ważne, ponieważ

umożliwia nam zabezpieczenie się przed zagrożeniami, zanim będą miały szansę się urzeczywistnić.

Jak dokładnie używa się OSINT do ochrony przed cyberzagrożeniami? Polega to na zbieraniu fragmentów cyfrowej układanki i łączeniu ich w całość. OSINT może na przykład zidentyfikować potencjalne podatności w oprogramowaniu i systemach, które mogliby wykorzystać hakerzy. Można go również użyć do śledzenia cyfrowych śladów cyberprzestępców, aby zrozumieć ich taktykę i wzorce postępowania. Ten rodzaj wywiadu jest nieoceniony nie tylko w przypadku reagowania na zagrożenia, lecz również wtedy, gdy chcemy na nie aktywnie się przygotować.

Jednym z najbardziej ekscytujących aspektów OSINT, czyli białego wywiadu, jest to, jak uzupełnia inne formy wywiadu, takie jak **HUMINT** (*Human Intelligence*, **rozpoznanie osobowe**) czy **SIGINT** (*Signal Intelligence*, **rozpoznanie elektromagnetyczne**). HUMINT polega na zrozumieniu zagrożeń poprzez rozmowy z ludźmi i obserwowanie tego, co robią. Zapewnia wgląd w to, dlaczego ataki się zdarzają. Z kolei SIGINT polega na podsłuchiwaniu komunikacji, takiej jak wiadomości e-mailowe, aby zdobyć dokładne informacje na temat zagrożeń.

Łącząc te trzy metody, otrzymujemy pełen obraz zagrożeń cybernetycznych. Dzięki temu łatwiej przewidywać problemy, ograniczać ryzyko i reagować na niebezpieczeństwo.

Nie zapomnijmy jednak o wyzwaniach. Zastosowanie OSINT w ramach analizy cyberzagrożeń nie polega wyłącznie na zbieraniu informacji. Chodzi o wydajne ich analizowanie. Ogrom danych potrafi przytłoczyć, a nie wszystkie są istotne lub rzetelne. Dlatego potrzebni są wykwalifikowani analitycy, którzy przekopią się przez gąszcz nieistotnych detali i wydobędą te, które pomogą podjąć właściwe decyzje. To umiejętność, która wymaga ustawicznego uczenia się i dostosowywania, zwłaszcza biorąc pod uwagę szybką ewolucję cyfrowego otoczenia i zagrożeń.

Zagrożenia cybernetyczne a OSINT

Nowe zagrożenia cybernetyczne nieustannie rzucają wyzwanie naszym wirtualnym zabezpieczeniom. Hakerzy i cyberprzestępcy to kreatywni, szybko dostosowujący się do zmian napastnicy, zawsze na tropie nowych podatności do wykorzystania dla zarobku lub siania chaosu. Cyberzagrożenia czekają tylko na okazję, aby zaszkodzić internetowej rzeczywistości. Naszym światem wstrząsają też globalne wydarzenia, takie jak poważne konflikty polityczne, a hakerzy wykorzystują ten chaos, aby wprowadzać jeszcze więcej zamieszania i realizować swoje niecne zamiary. Ponadto cyberprzestępcy coraz sprytniej obchodzą zabezpieczenia, takie jak dodatkowe kody do logowania.

To nie wszystko! Kradzieże prywatnych informacji, w tym danych osobowych i tajemnic przedsiębiorstw, są coraz częstsze. Cyfrowi kieszonkowcy przywłaszczają sobie nasze dane, a my nie jesteśmy tego nawet świadomi. Gdy tylko pojawią się nowe zabezpieczenia, przestępcy opracowują nowe sposoby ich obchodzenia. Musimy być czujni i uświadamiać innym obecność zagrożeń. To niekończąca się bitwa o ochronę naszej

cyfrowej przestrzeni. Phishing i socjotechnika to niektóre z największych zagrożeń, z jakimi mierzą się organizacje. Te taktyki wykorzystują ułomności ludzkiej natury, co sprawia, że trudniej je wykryć i zapobiegać im niż w przypadku ataków na podatności techniczne. OSINT zapewnia potężne narzędzia i techniki pozwalające wykrywać i analizować zagrożenia sprawniej, co czyni z niego nieocenioną pomoc dla organizacji w walce z cyberprzestępcami.

OSINT staje się również superbohaterem walki z fałszywymi informacjami (tzw. fake newsami). W czasach powszechnej dezinformacji narzędzia OSINT pomagają odróżnić kłamstwa od prawdy.

Jednym z godnych uwagi wydarzeń ostatnimi czasy było użycie narzędzi OSINT do zdemaskowania fałszywych informacji rozprzestrzenianych z użyciem wizerunku prezydenta Ukrainy, Wołodymyra Zełenskiego. Nagranie wykonane techniką deepfake przedstawiało Zełenskiego, jak ogłaszał koniec konfliktu z Rosją i kapitulację Ukrainy. Film odrzucono później jako nieprawdziwy. Techniki analityczne, wykrywające niespójności w oświetleniu, cieniach i ruchu, pomogły zakwestionować autentyczność filmu. W miarę jak coraz więcej osób ma świadomość cyberzagrożeń, rośnie też zapotrzebowanie na narzędzia OSINT pomagające dbać o bezpieczeństwo online.

Phishing

Wyobraź sobie, że przeglądasz pocztę i natrafiasz na wiadomość, która wygląda, jakby pochodziła z dobrze znanej instytucji. Dajmy na to — z Twojego banku. Proszą o kliknięcie linku i zaktualizowanie danych osobowych. Bez chwili zastanowienia klikasz link, żeby mieć to z głowy. Właśnie tak działa phishing! Te ataki sprawiają dużo problemów, gdyż mogą prowadzić do ujawnienia poufnych informacji lub — co gorsza — pobrania złośliwego oprogramowania na urządzenie.

Tutaj następuje mały zwrot akcji. Te sprytne kampanie phishingowe nie pojawiają się znikąd. Często zostawiają cyfrowe ślady rozrzucone po całym internecie. Tutaj nasze umiejętności OSINT mogą wkroczyć do akcji. Dzięki nim możemy ustrzec się przed fałszywymi stronami internetowymi, które wyglądają łudząco podobnie do prawdziwych. Możemy analizować adresy e-mailowe w poszukiwaniu śladów podszywania się pod kogoś innego (tzw. **spoofing**). Możemy też przeczesywać fora internetowe lub nawet dark web, aby znaleźć wycieki danych sugerujące szerzej zakrojoną akcję phishingową.

Porozmawiajmy o użytecznych narzędziach OSINT, takich jak theHarvester. Pamiętasz, jak w rozdziale 3. „Narzędzia OSINT – metody i techniki gromadzenia i analizowania informacji", nazwaliśmy go „cybernetycznym żniwiarzem"? Dzięki programowi theHarvester analitycy ds. bezpieczeństwa mogą znaleźć tony informacji — adresy e-mailowe, subdomeny, dane pracowników, a nawet otwarte porty — z publicznych źródeł, takich jak wyszukiwarki internetowe czy media społecznościowe. Na przykład polecenie `theHarvester -d packtpub.com -b all` wyciąga te wszystkie rodzaje danych z konkretnej domeny (rysunek 6.1). To bardzo pożyteczne w wykrywaniu potencjalnych pułapek phishingowych. Możemy znaleźć fałszywą stronę, która wygląda kubek w kubek jak legalna, ale służy do wykradania danych uwierzytelniających.



Rysunek 6.1. Narzędzie theHarvester wyszukuje dane na temat domeny packtpub.com

W prawdziwym życiu, zwłaszcza w dużych organizacjach, po wykryciu kampanii phishingowej, fałszywe domeny są zazwyczaj szybko usuwane. To jak gra w *Whack a Mole* — zręcznościówkę, która polega na uderzaniu plastikowymi młotkami w pojawiające się figurki chomików: gdy tylko dopadniesz jednego, znika, a w innym miejscu pojawia się kolejny. Dlatego tak ważne jest, aby zespoły ds. cyberbezpieczeństwa działały szybko i używały narzędzi takich jak theHarvester, by wykrywać próby ataków phishingowych, zanim znikną bez śladu.

Socjotechnika

Socjotechnika to złożone i nieustannie ewoluujące zagrożenie w cyberświecie. Nie chodzi tylko o kradzież adresu IP. Obejmuje to szeroki zakres taktyk — od tworzenia mylących nazw użytkowników i adresów e-mailowych po wykorzystanie podłączonych do internetu urządzeń, takich jak kamery. Powszechność i różnorodność tych ataków przyprawia o zawrót głowy. Często też wpasowują się w nasze cyfrowe życie tak idealnie, że ich nawet nie dostrzegamy.

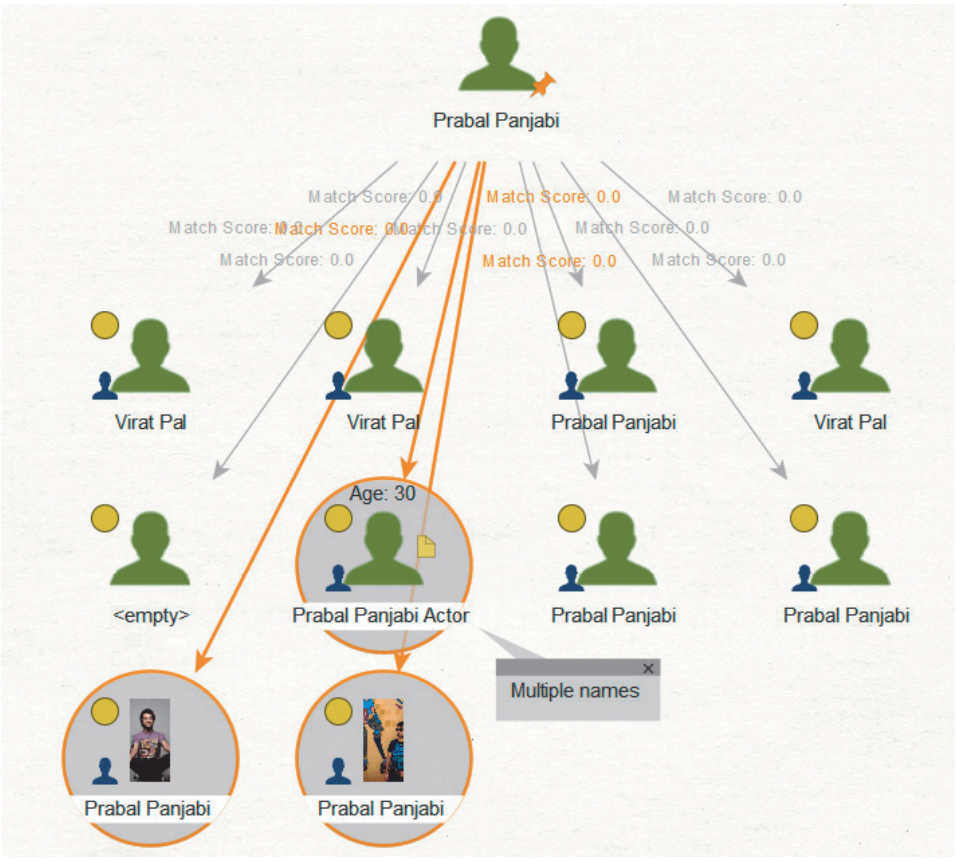
Zrozumieć otoczenie

Aby poradzić sobie z atakami socjotechnicznymi, specjaliści ds. cyberbezpieczeństwa sięgają często po OSINT, by sprawdzić, czego dowiedzieli się atakujący. Cybernapastnicy czasami również zachowują się nieuważnie. Mogą zostawiać cyfrowe tropy lub nawet chwalić się swoimi osiągnięciami. Dlatego sprytny analityk ma na oku różne miejsca, w których pojawiają się powiązane słowa kluczowe lub hasztagi, a także tematy dotyczące phishingu i socjotechniki. Na przykład nagły wzrost narzekań na podejrzane wiadomości e-mailowe w mediach społecznościowych może sugerować, że ma miejsce atak.

Branżowe narzędzia

Jednym z potężnych sojuszników w tej bitwie jest **SpiderFoot**. Ten cyfrowy detektyw automatyzuje wyszukiwanie informacji z różnych źródeł. Analitycy mogą rozpocząć kompleksowy skan za pomocą polecenia takiego jak `spiderfoot -l 127.0.0.1:5001 -s packtpub.com`. Analiza zwraca mnóstwo cennych informacji: adresy e-mailowe, nazwy domen, profile w mediach społecznościowych — wszystko to mogłoby posłużyć do przygotowania ataku socjotechnicznego.

W socjotechnice chodzi jednak nie tylko o to, co widać gołym okiem, lecz przede wszystkim o to, co ukryte. Tu przychodzą z pomocą narzędzia takie jak Maltego. Maltego sięga głębiej, ujawnia ukryte powiązania między osobami, firmami i infrastrukturą internetową, które nie są takie proste do znalezienia (rysunek 6.2).



Rysunek 6.2. Maltego pokazuje nieoczywiste powiązania między osobami

Może na przykład przeanalizować pozornie nieszkodliwy adres e-mailowy, aby znaleźć podłączone do internetu urządzenia, a może nawet kamerkę, nad którą ktoś przejął kontrolę.

Łatanie luk w zabezpieczeniach dzięki OSINT

Nie chodzi tylko o przyszłe czy aktualne zagrożenia. Czasami niebezpieczeństwo tkwi w atakach socjotechnicznych, które już miały miejsce. Strony takie jak Have I Been Pwned służą jako system wczesnego ostrzegania, pozwalając użytkownikom sprawdzić, czy ich dane padły ofiarą naruszenia. To tylko czubek góry lodowej. Prawdziwy zakres socjotechniki obejmuje dużo więcej. Porzucone strony, niezabezpieczone kamery, urządzenia sieciowe, a nawet zapory sieciowe, które nadal straszą w internecie — to wszystko są potencjalne punkty wyjścia do ataków.

Kolejnym aspektem badań OSINT w tym kontekście jest analiza danych ujawnionych w ramach wycieków oraz raportów na temat takich wycieków. Strony takie jak Have I Been Pwned (*https://haveibeenpwned.com*) pozwalają użytkownikom sprawdzić, czy ich dane były częścią znanego wycieku. Te informacje mają kluczowe znaczenie, gdyż tak ujawnione dane stają się często podstawą do przeprowadzenia ataku socjotechnicznego.

Media społecznościowe to dla atakujących kopalnie informacji. Hakerzy wyszukują dane, aby wzbudzać zaufanie lub podszywać się pod osoby w ramach kampanii phishingowych ukierunkowanych na konkretną osobę lub firmę (tzw. spear phishing). W tym kontekście techniki OSINT obejmują dokładne monitorowanie wiadomości, połączeń i wzorców działania, aby wykryć potencjalne podatności.

Szerszy obraz

Systematyczne stosowanie metod OSINT pozwala specjalistom ds. cyberbezpieczeństwa prześledzić rozwój strategii socjotechnicznych. Mogą zrozumieć nie tylko, *jak* doszło do ataku, lecz również *kto* i *dlaczego* za nimi stoi. Te informacje mają kluczowe znaczenie w tworzeniu solidnych zabezpieczeń, w tym kampanii uświadamiających, które pokazują często stosowane techniki phishingowe, oraz procedur zwiększających bezpieczeństwo często atakowanych sektorów.

Dzięki dogłębnej analizie możemy zidentyfikować rodzaje organizacji, które są zagrożone, obszary geograficzne, gdzie najczęściej pojawiają się ataki, oraz poziom złożoności użytych metod. Ten rodzaj wywiadu może zmienić bieg wydarzeń i przekształcić potencjalne ofiary socjotechnicznych sztuczek w świadomych i dobrze przygotowanych obrońców.

Złośliwe oprogramowanie i oprogramowanie wymuszające okup

Złośliwe oprogramowanie jest coraz bardziej zaawansowane i destrukcyjne. Szczególnie szybki rozwój możemy zaobserwować w kategorii oprogramowania wymuszającego okup (ang. *ransomware*). Skupmy się na razie na dwóch kwestiach:

- **Ewolucja złośliwego oprogramowania**. Złośliwe oprogramowanie, początkowo w postaci prostych wirusów i robaków, rozwinęło się w dużo

bardziej złożone formy, obejmujące oprogramowanie szpiegujące (ang. *spyware*), konie trojańskie i rejestratory klawiszy (ang. *keyloggers*). Ich zadaniem jest kradzież danych, zakłócanie działania lub nieuprawniony dostęp do systemu.

- **Trendy w zakresie oprogramowania wymuszającego okup**. Nowoczesne ataki z wykorzystaniem oprogramowania wymuszającego okup obejmują zaszyfrowanie danych i żądanie okupu za klucz do ich odszyfrowania. Atakujący biorą na cel osoby prywatne, przedsiębiorstwa, a nawet urzędy państwowe, okupu zaś żądają w kryptowalutach.

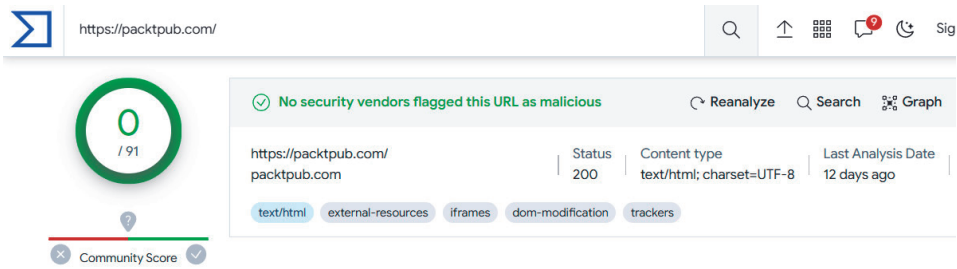
OSINT w zwalczaniu złośliwego oprogramowania

Analiza złośliwego oprogramowania i oprogramowania wymuszającego okup może mieć duże znaczenie w branży OSINT. Oto jak możemy się za to zabrać:

- **Zrozumienie sprawców**. Sprawcy, którzy tworzą złośliwe oprogramowanie lub infekują nim urządzenia, mogą być pojedynczymi hakerami, grupami przestępczymi lub grupami sponsorowanymi przez państwa. Analizując elementy złośliwego oprogramowania, analitycy OSINT mogą gromadzić informacje na temat **taktyk, technik i procedur** (ang. *Tactics, Techniques and Procedures*, TTP) tych sprawców. Może to obejmować zrozumienie celów oraz metod ataku, a także ewentualne określenie pochodzenia lub powiązań.
- **Trendy w cyberbezpieczeństwie**. Analiza złośliwego oprogramowania przyczynia się do lepszego zrozumienia aktualnych zagrożeń i trendów w cyberbezpieczeństwie. Jest to istotne z punktu widzenia OSINT, gdyż umożliwia przewidzenie przyszłych ataków, zrozumienie ewolucji cyberzagrożeń oraz bycie o jeden krok przed sprawcami, jeżeli chodzi o gromadzenie informacji wywiadowczych.
- **Cyfrowe ślady**. Złośliwe i wymuszające okup programy często pozostawiają za sobą cyfrowy ślad. Jego analiza może prowadzić do odkrycia domen, adresów IP i innych cyfrowych wskazówek powiązanych z atakującymi. Te informacje można sprawdzić w publicznie dostępnych bazach i narzędziach, aby pogłębić swoje zrozumienie krajobrazu zagrożeń.
- **Dzielenie się wynikami**. Informacje zdobyte na podstawie analizy złośliwego oprogramowania mogą być bardzo cenne dla całej społeczności związanej z cyberbezpieczeństwem. Takie oparte na współpracy podejście może pomóc innym w zabezpieczeniu się przed zagrożeniami i przyczynić się do zgromadzenia większej puli informacji z otwartych źródeł.
- **Przeciwdziałanie i ograniczanie ryzyka**. Szczegółowe zrozumienie mechanizmu działania różnych rodzajów złośliwego oprogramowania pozwala na opracowanie skuteczniejszych środków zaradczych i strategii ograniczających ryzyko. To istotne dla organizacji starających się chronić swoje zasoby i może być kluczowym elementem strategii z zakresu cyberbezpieczeństwa opartych na OSINT.

Narzędzia OSINT takie jak VirusTotal umożliwiają analizę próbek złośliwego oprogramowania, co zapewnia wgląd w ich zachowanie, źródło i potencjalny wpływ.

Dzięki monitorowaniu rejestracji adresów IP i domen specjaliści ds. cyberbezpieczeństwa mogą znaleźć infrastrukturę wykorzystywaną do prowadzenia ofensywnych kampanii z użyciem złośliwego oprogramowania. Powiedzmy, że napotkamy witrynę internetową — dajmy na to *packtpub.com* — i mamy wątpliwości co do jej bezpieczeństwa. Dzięki narzędziu VirusTotal wystarczy wprowadzić adres URL *https://packtpub.com* w wyszukiwarce, aby sprawdzić wiarygodność witryny (rysunek 6.3).



Rysunek 6.3. Wyniki skanowania domeny packtpub.com narzędziem VirusTotal

VirusTotal skanuje adres URL pod kątem obecności znanych zagrożeń ze swojej bazy danych. Wyniki skanowania pokazują, czy witryna jest powiązana ze szkodliwą działalnością, taką jak rozprzestrzenianie złośliwego oprogramowania czy udział w kampaniach phishingowych. Błyskawiczna ocena pomaga użytkownikom unikać potencjalnie szkodliwych witryn i informuje zespoły ds. cyberbezpieczeństwa o konieczności podjęcia niezbędnych działań po wykryciu zagrożenia.

Wiem, że to było sporo do przyswojenia, więc spójrzmy na przykład. Wyobraźmy sobie, że zauważyliśmy nietypową aktywność sugerującą atak złośliwego oprogramowania na monitorowaną przez nas sieć. Do analizy decydujemy się użyć narzędzia OSINT, takiego jak VirusTotal. W praktyce wygląda to następująco:

1. **Gromadzenie danych**. Najpierw zbierz podejrzane pliki lub adresy URL z analizy ruchu sieciowego. Mogą to być pliki pobrane przez użytkowników lub łącza, które kliknęli.
2. **Analiza narzędziem VirusTotal**. Załaduj pliki lub wprowadź adresy URL do narzędzia VirusTotal. Przeskanuje ono pliki lub strony internetowe, korzystając z bazy danych znanych sygnatur i zachowań złośliwego oprogramowania.
3. **Przegląd wyników**. VirusTotal zwraca szczegółowy raport na temat każdego pliku lub adresu URL, informując o podejrzanym zachowaniu, powiązaniu ze znanymi rodzajami złośliwego oprogramowania lub komunikacji z podejrzanymi adresami IP.
4. **Sprawdzenie informacji**. Na podstawie informacji uzyskanych z narzędzia VirusTotal możemy sprawdzić **wskaźniki zagrożenia** (ang. *Indicators of Compromise*, IoC), takie jak adresy IP, nazwy domen czy hasze plików,

w innych bazach danych OSINT. Pomaga to zrozumieć, czy te wskaźniki są częścią większych kampanii.

5. **Podjęcie działań**. Na bazie odkryć możemy zaktualizować ustawienia bezpieczeństwa sieci. Może to obejmować zablokowanie złośliwych adresów IP, zaaplikowanie uaktualnień usuwających luki lub prowadzenie szkoleń użytkowników.
6. **Dzielenie się odkryciami**. Na koniec przygotuj krótkie sprawozdanie na temat swojego dochodzenia, skupiając się na użyciu narzędzi OSINT do wykrycia zagrożenia związanego ze złośliwym oprogramowaniem oraz ograniczenia jego skutków. Podzielenie się tymi informacjami ze społecznością zajmującą się cyberbezpieczeństwem zwiększa ogólną zdolność do obrony przed zagrożeniami.

Monitorowanie ruchu sieciowego w celu wykrycia złośliwego oprogramowania

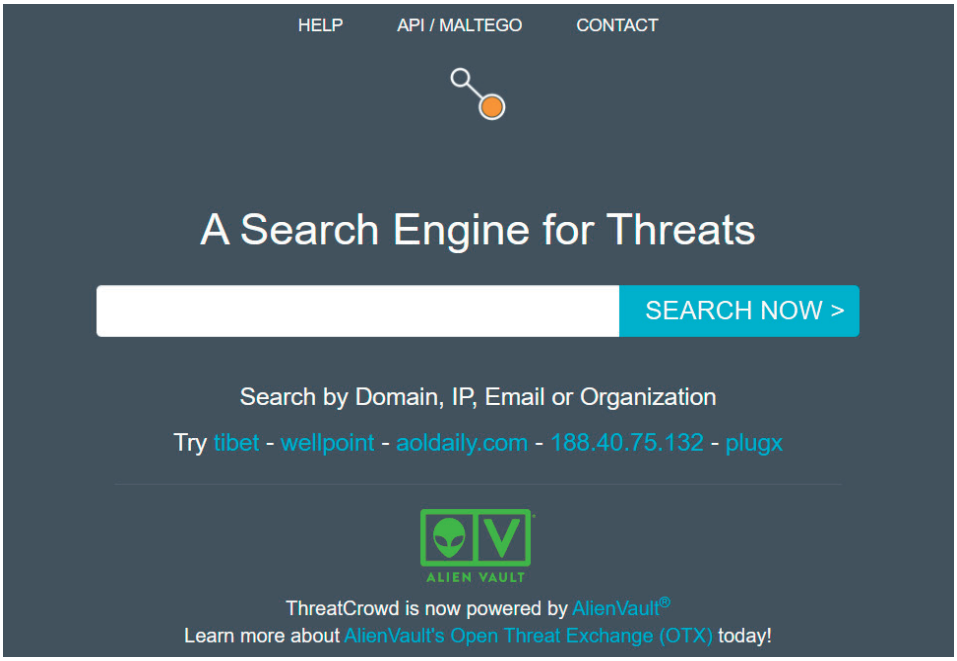
Analizowanie ruchu sieciowego to doskonały sposób na wykrycie złośliwego oprogramowania, w tym oprogramowania wymuszającego okup, zanim spowoduje szkody. Przyglądając się dokładnie danym płynącym przez sieć, analitycy mogą wykryć nietypową aktywność, która wskazuje, że system został zainfekowany. Na przykład nagły wzrost ilości danych przesyłanych do nieznanej witryny może sugerować aktywność botnetu albo kradzież. Użycie narzędzi do inspekcji pakietów, takich jak Wireshark (*https://www.wireshark.org*), pozwala na stałe i szczegółowe monitorowanie ruchu sieciowego. Należy sprawdzić wszelkie dziwne połączenia, protokoły i treści.

Dzięki monitorowaniu sieci problemy można szybko wychwycić i ograniczyć, zanim się rozprzestrzenią. Żadna pojedyncza organizacja nie może jednak kontrolować całego internetu. W takich przypadkach pomocne są platformy oparte na współpracy, takie jak VirusTotal. Dzięki umożliwieniu specjalistom ds. bezpieczeństwa pobrania próbek złośliwego oprogramowania i przeskanowania podejrzanych plików nowe zagrożenia można szybko zidentyfikować i udostępnić ich sygnatury. Tworzone zbiorowo bazy danych, takie jak wspomniany wcześniej VirusTotal czy ThreatCrowd (*http://ci-www.threatcrowd.org*), stanowią systemy wczesnego ostrzegania o nowych atakach (rysunek 6.4).

Połączenie monitorowania sieci i społecznościowej analizy zagrożeń zapewnia organizacjom najlepsze szanse na ochronę przed cyberzagrożeniami, takimi jak na przykład oprogramowanie wymuszające okup. Aktywne podejście w tym zakresie oznacza zarówno obserwowanie własnych systemów, jak i koordynowanie wysiłków z innymi podmiotami z branży.

Kanały informacyjne z zakresu analizy zagrożeń

Kanały informacyjne z zakresu analizy zagrożeń przypominają kanały wiadomości w mediach społecznościowych, lecz zamiast aktualizacji dotyczących zdjęć czy statusów zawierają najnowsze informacje na temat zagrożeń cybernetycznych. Te kanały



Rysunek 6.4. ThreatCrowd pozwala sprawdzić adres IP, domenę lub adres e-mailowy

informacyjne gromadzą dane z wielu miejsc, takich jak fora dotyczące bezpieczeństwa, strony hakerskie czy nawet tweety ekspertów w tej dziedzinie. Zapewniają na bieżąco aktualizacje na temat nowych rodzajów złośliwego oprogramowania.

- Dlaczego to ważne?

  Dysponowanie tymi informacjami ma kardynalne znaczenie dla osób zajmujących się ochroną komputerów i danych przed hakerami. Tak jak aplikacje pogodowe ostrzegają nas o nadchodzących burzach, kanały informacyjne alarmują zespoły ds. cyberbezpieczeństwa o nadciągających cyberzawieruchach w postaci nowych ataków.

- W jaki sposób pomagają?
  - **Wczesne ostrzeganie**. Kanały informacyjne ostrzegają nas o nowych wirusach lub nagłym wzroście ataków hakerskich. Daje to czas na przygotowanie się i zabezpieczenie systemów, zanim problem do nas dotrze.
  - **Analiza trendów**. Obserwując prawidłowości w tych kanałach informacyjnych, eksperci mogą określić, jakie ataki się upowszechniają. Pomaga to przewidzieć, co może się wydarzyć w dziedzinie cyberbezpieczeństwa, i się na to przygotować.

Wyobraźmy sobie, że nasz zespół ds. cyberbezpieczeństwa monitoruje platformę AlienVault OTX, aby nie dać się zaskoczyć nowym cyberzagrożeniom. Pewnego dnia zauważamy ostrzeżenie o nowym wariancie oprogramowania wymuszającego okup

rozsyłanym w ramach kampanii phishingowej. Kanały informacyjne zapewniają szczegółowe wskaźniki IoC, takie jak niebezpieczne adresy IP, tematy wiadomości e-mailowych czy hasze plików powiązane z tym oprogramowaniem.

Uzbrojeni w te informacje, szybko aktualizujemy filtry poczty elektronicznej, aby zablokować wiadomości z podejrzanymi tematami lub pasujące do wymienionych wskaźników. Szybko konfigurujemy też systemy zabezpieczeń, aby wykrywały komunikację z podejrzanych adresów IP i poddawały ją kwarantannie. Podejmując działania na podstawie bieżących informacji z platformy AlienVault OTX, zapobiegamy przedostaniu się złośliwego oprogramowania do sieci, co demonstruje kluczową rolę, jaką odgrywają takie kanały informacyjne w aktywnej ochronie.

Zaawansowane trwałe zagrożenia

Zaawansowane trwałe zagrożenia (ang. *Advanced Persistent Threats*, APT) to jeden z najniebezpieczniejszych typów zagrożeń cybernetycznych. Grupy APT sponsorowane przez państwa prowadzą długoterminowe tajne działania mające na celu zbieranie informacji, obserwację i sabotaż. W dynamicznie zmieniającym się świecie cyberbezpieczeństwa analiza OSINT to kluczowe narzędzie wykorzystywane do demaskowania tych nieuchwytnych przeciwników i zrozumienia ich sposobu działania.

Czym są zaawansowane trwałe zagrożenia?

Zaawansowane trwałe zagrożenia polegają na tym, że wysoko wykwalifikowani hakerzy używają złożonych technik do infiltracji sieci i komputerów. Od zwykłych hakerów odróżnia ich wytrwałość, gdyż potrafią działać w ukryciu przez długi czas. Celem jest spowodowanie szkód, wykradzenie kluczowych danych, zwłaszcza biznesowych bądź rządowych, lub też zakłócenie działania infiltrowanych organizacji.

OSINT na ratunek

Eksperci OSINT zaczynają od przeczesywania internetu w poszukiwaniu wszelkich skrawków informacji, jakie ataki APT mogły po sobie zostawić. Patrzenie na to, co oczywiste, w tym przypadku nie pomoże. Trzeba szukać informacji ukrytych w przepastnym morzu internetowych danych. Podejrzenia może wzbudzić na przykład dziwna nazwa domeny, która wydaje się nie należeć do żadnej znanej firmy, lub seria postów na forum hakerskim, która sugeruje planowany atak cybernetyczny. Takie niewielkie skrawki informacji są jak trop pozostawiony na miejscu zbrodni i odgrywają nieocenioną rolę przy identyfikacji atakujących.

Łączymy kropki, aby uzyskać szerszy obraz

Następnym krokiem jest połączenie elementów tej gigantycznej układanki. W tej dziedzinie eksperci OSINT nie mają sobie równych. Biorą fragment informacji, analizują i łączą go z innymi. Wyobraź sobie tablicę dochodzeniową, na której sznurki łączą różne znalezione w sieci tropy. Nietypowa próba logowania z innego kraju połączona z wyciekiem dokumentu znalezionego na innej stronie internetowej może na przykład

wskazywać na specyficzną aktywność będącą częścią ataku APT. Łącząc ze sobą różne tropy, eksperci OSINT mogą zacząć rozpoznawać wzorce i strategie działań atakujących. To drobiazgowy i powolny proces, wymagający dużej cierpliwości i szczegółowości.

Cyberpościg, czyli śledzenie cyfrowych śladów

W cyfrowym świecie nawet najprzebieglejsi napastnicy APT pozostawiają za sobą ślady. Mogą być subtelne, ale istnieją — w formie cyfrowych rekordów, logów transakcji albo pewnych anomalii w ruchu sieciowym. Eksperci OSINT używają różnych metod, aby badać te ślady. Mogą analizować logi serwerów, aby zobaczyć, czy dochodziło do nietypowej aktywności, lub podejrzeć metadane zhakowanego dokumentu, aby dowiedzieć się, gdzie i kiedy został utworzony. Wszystkie te ślady to cenne poszlaki, pomagające zrozumieć nie tylko, kto jest źródłem zaawansowanego trwałego zagrożenia, lecz również jak działa.

Zrozumieć szerszy kontekst

Jednym z najważniejszych elementów OSINT jest nie tylko zbieranie danych, lecz także rozumienie ich kontekstu. Oznacza to, że musimy przyjrzeć się *powodom* i *sposobom działania* grup APT.

Na przykład w przypadku ataku APT na spółki energetyczne eksperci OSINT próbowaliby określić przyczynę. Czy istnieją motywy polityczne? Czy chodzi o zakłócenie dostaw energii w danym kraju? Zrozumienie tego kontekstu pomaga przewidywać przyszłe cele ataków APT oraz określić ich przyczyny.

Przypadki prawdziwych ataków APT

Przyjrzyjmy się przykładom prawdziwych spraw, w których OSINT pomógł lub mógłby pomóc pochwycić cyberszpiegów.

- **Atak Stuxnet**. W 2010 r. było o tym głośno. Robak komputerowy o nazwie Stuxnet został użyty do sabotowania irańskiego programu nuklearnego. Był to wysoce zaawansowany atak i uważa się, że został zlecony przez inny kraj, przy czym nawet obecnie nie ma stuprocentowej pewności który. Mogąc analizować budowę robaka, eksperci wykorzystali techniki OSINT, aby dowiedzieć się, jak działał, kto był celem i ile szkód mógł spowodować.
- **Ataki na DNC z 2016 r.** W tym przypadku hakerzy zdobyli dostęp do wiadomości e-mailowych Krajowego Komitetu Partii Demokratycznej (*Democratic National Committee*, DNC) w Stanach Zjednoczonych. Sprawdzając pozostawione przez nich cyfrowe ślady, takie jak to, skąd pochodziły adresy e-mailowe hakerów, czy rodzaj złośliwego oprogramowania użytego do ataków, specjaliści OSINT pomogli ustalić, że za atak najprawdopodobniej odpowiedzialna była rosyjska grupa APT.
- **Atak na sieć hoteli i kasyn MGM Resorts International**. W 2023 r. grupa hakerska znana jako **Scattered Spider** („rozproszony pająk") wzięła na celownik sieć MGM Resorts International. Atak doprowadził do wyłączenia części systemów w hotelach i kasynach sieci w Stanach Zjednoczonych, w tym

Bellagio i Cosmopolitan. Z powodu użycia oprogramowania wymuszającego okup obiekty nie mogły korzystać ze swoich komputerów, co drastycznie ograniczyło ich możliwości działania. Nadal *do końca* nie znamy rozmiaru szkód, ale zapewniam, że eksperci ds. bezpieczeństwa korzystają z narzędzi i technik OSINT i dalej prowadzą dochodzenie w sprawie tego ataku.

Biorąc pod uwagę te przykłady, już dzisiaj możemy powiedzieć, że w przyszłości złożoność cyberzagrożeń będzie rosnąć. Aby nie zostać w tyle, eksperci ds. bezpieczeństwa muszą posiłkować się technikami OSINT, nieustannie dostosowując się do nowych wyzwań i walcząc z grupami zagrażającymi naszemu bezpieczeństwu online.

Łączenie OSINT z wewnętrznymi systemami bezpieczeństwa

Gdy myślisz o łączeniu OSINT z wewnętrznymi systemami bezpieczeństwa, wyobraź sobie detektywa, który skrupulatnie zbiera poszlaki z różnych źródeł. Powiązania są w tym procesie najważniejsze i mają kluczowe znaczenie dla zapewnienia bezpieczeństwa. Zastanówmy się teraz, jak połączyć OSINT z wewnętrznymi ramami bezpieczeństwa, aby wzmocnić zabezpieczenia.

- **Integracja z systemami SIEM**. **Systemy zarządzania informacjami i zdarzeniami z zakresu bezpieczeństwa** (ang. *Security Information and Event Management*, SIEM) mają za zadanie zapewniać całościowy obraz stanu zabezpieczeń w organizacji poprzez zbieranie i analizowanie danych z różnych źródeł. Dzięki integracji z OSINT te systemy zyskują dostęp do dodatkowej warstwy kontekstu, co może zwiększyć ich zdolność wykrywania zagrożeń i reagowania na nie. Wyobraźmy sobie na przykład, że system SIEM wykrywa niezwykły wzrost ruchu sieciowego z konkretnej lokalizacji geograficznej. Samo w sobie może to być niepokojące, ale nie dowodzi jeszcze cyberataku. Po połączeniu tego faktu z danymi uzyskanymi z białego wywiadu, które wskazują na aktualne cyberzagrożenia lub inne działania z tej samej lokalizacji, systemy SIEM mogą dokładniej ocenić ryzyko i zastosować odpowiednie procedury bezpieczeństwa.
- **Synergia z systemami EDR**. **Systemy wykrywania zagrożeń punktów końcowych i reagowania na nie** (ang. *Endpoint Detection and Response*, EDR) koncentrują się na identyfikowaniu zagrożeń punktów końcowych sieci i zarządzaniu nimi. Integracja z OSINT może znacznie zwiększyć możliwości takich systemów, zwłaszcza w zakresie wykrywania i rozumienia nowych, ewoluujących zagrożeń. „W jaki sposób?" — możemy zapytać. Wyobraźmy sobie, że system EDR odkrywa nowy rodzaj złośliwego oprogramowania na firmowym laptopie. Chociaż EDR może ograniczyć i wyeliminować zagrożenie, integracja z OSINT zapewnia wgląd w pochodzenie i charakter złośliwego oprogramowania. Być może prowadzona jest kampania z wykorzystaniem tego oprogramowania, o czym mogą informować źródła OSINT, takie jak fora zajmujące się cyberbezpieczeństwem lub kanały

informacyjne dotyczące analizy zagrożeń. Te informacje mogą pomóc zespołowi ds. bezpieczeństwa we wzmocnieniu zabezpieczeń przed podobnymi atakami w przyszłości.

- **Aktywna obrona dzięki połączeniu systemów SIEM i EDR z OSINT**. Prawdziwa potęga integracji OSINT z wewnętrznymi narzędziami bezpieczeństwa tkwi w zmianie podejścia z reaktywnego na proaktywne. Dzięki wykorzystaniu ogromnych ilości publicznie dostępnych informacji organizacje mogą przewidywać ewentualne zagrożenia i przygotowywać się na nie, zanim do nich dojdzie.

Na przykład system SIEM dzięki wykorzystaniu OSINT może natrafić na forum w dark webie, po którym krążą pogłoski na temat planowanego ataku na przedsiębiorstwa z danej branży. Taki wywiad pozwala zespołom ds. bezpieczeństwa z wyprzedzeniem wzmocnić zabezpieczenia i monitorować sygnatury ataków. Jednocześnie można zaktualizować system EDR, aby wykrywał wczesne sygnały naruszeń w punktach końcowych.

Opracowywanie strategii cyberbezpieczeństwa opartej na danych

Jak przekłada się to połączenie wysiłków na solidną strategię cyberbezpieczeństwa? Trzeba umieć zarówno reagować, jak i przewidywać. Nie chodzi o to, żeby czekać, aż włączy się alarm. Trzeba przewidywać, gdzie i kiedy będzie mieć miejsce kolejny atak. Łącząc informacje z analizy OSINT na temat nadciągających zagrożeń i trendów z bieżącymi informacjami z systemów wewnętrznych, uzyskujemy panoramiczny obraz stanu cyberbezpieczeństwa.

Połączone podejście umożliwia opracowywanie strategii, które nie tylko reagują na aktualne zagrożenia, lecz również przewidują przyszłe. Na przykład jeżeli OSINT odkryje wzrost liczby ataków z użyciem oprogramowania wymuszającego okup w danej branży, możemy zapobiegawczo wzmocnić zabezpieczenia przed tym konkretnym zagrożeniem. Jednocześnie dane wewnętrzne mogą pomóc w wykryciu podatności naszych systemów, które mogłyby stanowić punkty wyjścia do takich ataków.

Ustawiczna nauka i adaptacja w dziedzinie cyberbezpieczeństwa

Cyberzagrożenia stale ewoluują, więc strategie cyberbezpieczeństwa też nie powinny stać w miejscu. Dla specjalistów ds. cyberbezpieczeństwa regularne szkolenia i podnoszenie kwalifikacji to konieczność. Poznawanie nowych narzędzi, technik i zagrożeń odgrywa fundamentalną rolę.

Kontakt ze społecznością zajmującą się cyberbezpieczeństwem za pośrednictwem forów i grup to dodatkowy kanał zdobywania wiedzy. Te platformy umożliwiają wymianę spostrzeżeń, omówienie nowych zagrożeń oraz uczenie się na doświadczeniach innych. Dzięki stałym interakcjom i nauce specjaliści ds. cyberbezpieczeństwa nieustannie doskonalą swoje strategie, dbając o to, aby zawsze być kilka kroków przed potencjalnymi cyberzagrożeniami.

Platformy do analizy zagrożeń cybernetycznych i ich integracja z OSINT

Platformy do analizy cyberzagrożeń to zaawansowane technologicznie wieże strażnicze cyfrowego świata. Zespoły ds. cyberbezpieczeństwa używają tych narzędzi, aby wypatrywać potencjalnych cyberzagrożeń. Mają za zadanie zbieranie dużych ilości informacji z internetu, analizowanie ich oraz komunikowanie wniosków. Pomagają organizacjom zrozumieć ataki i lepiej przygotować się na nie, zanim do nich dojdzie.

Przeanalizujmy różne funkcje realizowane przez te platformy:

- **Gromadzenie danych**. Platformy skanują różne źródła, takie jak blogi, witryny informacyjne, a nawet rzadziej odwiedzane obszary internetu. Szukają wszystkiego, co mogłoby świadczyć o cyberzagrożeniach, takich jak podejrzane oprogramowanie czy wzmianki o cyberataku.
- **Analizowanie danych w czasie rzeczywistym**. Wyobraźmy sobie superinteligentny system, który potrafi odczytać i zrozumieć wszystkie te dane w momencie ich otrzymania. To właśnie robią te platformy. Wykorzystują specjalną technologię do szybkiego analizowania informacji i określania, czy wskazują na zagrożenie. Oto kilka kluczowych technik, których te systemy mogą używać:
  - **Uczenie maszynowe**. Platformy często wykorzystują algorytmy uczenia maszynowego do analizowania wzorców w danych. Uczenie maszynowe umożliwia uczenie się na podstawie wcześniejszych przypadków, co zwiększa zdolność wykrywania i przewidywania nowych rodzajów cyberzagrożeń. Na przykład, analizując dane historyczne, platforma może wykryć anomalie sugerujące ewentualne cyberzagrożenia.
  - **Wykrywanie sygnatur**. Wykrywanie sygnatur to bardziej tradycyjna, lecz wciąż podstawowa technika. Polega na skanowaniu przychodzących danych i wyszukiwaniu w nich sygnatur zagrożeń, które mogą obejmować cyfrowe odciski złośliwego oprogramowania i innych niebezpiecznych czynników. Ta metoda jest szczególnie skuteczna w wykrywaniu i eliminowaniu znanych zagrożeń.
- **Wysyłanie ostrzeżeń**. W przypadku wykrycia zagrożenia, takiego jak nowy wirus czy bieżący atak cybernetyczny, platformy natychmiast wysyłają ostrzeżenia. Pomaga to zespołom ds. cyberbezpieczeństwa szybko podjąć odpowiednie działania.
- **Synergia z innymi narzędziami**. Można powiedzieć, że te platformy to gracze zespołowi. Współpracują z innymi narzędziami z zakresu cyberbezpieczeństwa, takimi jak zapory sieciowe i oprogramowanie antywirusowe, aby wszystkie elementy sieci danej organizacji były chronione przed zagrożeniami.

Niektóre z dostępnych platform

Spójrzmy na listę cieszących się popularnością platform do analizy cyberzagrożeń.

- **Trellix** (wcześniej FireEye; *https://www.trellix.com/platform*). Ta platforma jest znana z namierzania złożonych cyberzagrożeń i radzenia sobie z nimi.
- **IBM X-Force Exchange** (*https://exchange.xforce.ibmcloud.com*). Funkcjonuje jako centrum społecznościowe, w ramach którego eksperci ds. cyberbezpieczeństwa z całego świata dzielą się informacjami na temat zagrożeń. W końcu dzielenie się informacjami jest wyrazem troski.
- **CrowdStrike Falcon X** (*https://www.crowdstrike.com/platform*). Ta platforma to połączenie automatyki i ludzkiej inteligencji. Do rozpoznawania zagrożeń wykorzystuje nie tylko technologię, lecz także opinie ekspertów.
- **Recorded Future** (*https://www.recordedfuture.com*). No dobrze, to mój osobisty faworyt! Ta platforma przepowiada przyszłość cyberbezpieczeństwa niczym zawodowy wróżbita. Przegląda tony danych i przewiduje przyszłe zagrożenia, pomagając organizacjom przygotować się na to, co nadchodzi. Dodatkowo udostępnia mnóstwo darmowych zasobów z zakresu analizy bezpieczeństwa.

OSINT odgrywa istotną rolę w ramach tych platform. Zbierane przez nie dane OSINT czynią ich narzędzia do analizy zagrożeń jeszcze potężniejszymi, zapewniając szerszy i dokładniejszy obraz potencjalnych cyberzagrożeń. Zaczynasz dostrzegać prawdziwą potęgę OSINT?

Wykorzystanie danych OSINT w procesach analizy zagrożeń

Biały wywiad odgrywa istotną rolę w ochronie organizacji przed nieustannie rozwijającymi się cyberzagrożeniami. Używając publicznie dostępnych danych, zespoły ds. bezpieczeństwa mogą zdobyć nieocenioną wiedzę, pozwalającą ulepszyć plany obrony. Integracja OSINT z istniejącymi systemami wymaga jednak dokładnego przemyślenia strategii, aby wyłowić istotne sygnały z morza szumu.

Co chwila słyszę pytanie: „Dale, jako cyfrowy kowboj, jak połączyłbyś OSINT z analizą zagrożeń?". Każda firma jest inna, ale z grubsza wyglądałoby to tak:

1. Najpierw określ cel! Zanim wskoczysz w siodło, zastanów się, gdzie chcesz dotrzeć. Będziesz walczyć z zagrożeniami branżowymi czy badać atak? Różni wrogowie oznaczają różne alianse. Mogą one obejmować frameworki do modelowania zagrożeń w celu ich identyfikowania z uwzględnieniem branży, wielkości organizacji i cyfrowego śladu. Takie narzędzia pomagają kategoryzować zagrożenia i uszeregować je w kolejności prawdopodobieństwa i potencjalnego wpływu.

2. Następnie zagoń do swojej zagrody parę faktów. Mogą pochodzić z publicznych forów, witryn poświęconych bezpieczeństwu oraz pułapek typu honeypot. Nie wszystkie źródła są sobie równe. Renoma też odgrywa rolę. Aby zebrać dane, możemy użyć crawlerów, które będą systematycznie przeglądać sieć i zbierać informacje. Narzędzia takie jak Shodan mogą skanować internet w poszukiwaniu podłączonych do niego urządzeń, a inne — pozyskiwać dane z publicznych forów i mediów społecznościowych. Użycie API różnych platform bezpieczeństwa może zautomatyzować zbieranie informacji.
3. Potem oczyścimy dane, aby się przygotować na rodeo. Eliminujemy duplikaty i zostawiamy tylko istotne dane, a w procesie normalizacji nadajemy im jednolity format dla ułatwienia analizy. Dodanie kontekstu może obejmować opatrzenie danych metadanymi, takimi jak wiarygodność źródła lub istotność dla danego modelu zagrożeń. Od razu lepiej!
4. Teraz weźmy byka za rogi! Postarajmy się odkryć powiązania i wzorce. Łączymy poszlaki, aby rozpoznać ataki, analizujemy trendy, aby zidentyfikować zagrożenia, a nawet staramy się określić autorów, aby bandyci stojący za atakami ponieśli zasłużoną karę. Modele uczenia maszynowego można wyszkolić do tego, aby wykrywały wartości odstające i podejrzane wzorce w danych. Takie odchylenia mogą wskazywać na zbliżające się zagrożenia. Narzędzia do analizy danych sieciowych mogą posłużyć do połączenia różnych fragmentów informacji, ujawniając atakujących lub ich metody. Dobra robota!
5. Zdobywszy nowe informacje, wracamy do hacjendy z trofeum. Spostrzeżeniami dzielimy się ze swoim klanem, aby wszyscy byli lepiej przygotowani na zagrożenie. Dzielenie się wiedzą z zespołem obejmuje wykorzystanie narzędzi do współpracy, a także wykorzystanie wyników pracy do dostosowania istniejących systemów bezpieczeństwa. Zbieranie informacji zwrotnych może mieć formę regularnych spotkań lub cyfrowych platform. Ten krok umożliwi stałe doskonalenie procesu zbierania wywiadu. Ja sam biorę sobie informacje zwrotne do serca i staram się stale usprawniać swój sposób działania.
6. Po wszystkim zdobyte informacje służą nam za psa pasterskiego. Na ich podstawie konfigurujemy zapory sieciowe, aby blokowały znane szkodliwe adresy IP, dostosowujemy filtry spamu, aby wyłapywać nowe ataki phishingowe, i aktualizujemy szkolenia dla pracowników o najnowsze trendy w zakresie cyberzagrożeń. W skrócie: staramy się zabezpieczyć przed drapieżnikami!
7. Regularnie przeglądamy i wykorzystujemy nowe narzędzia do automatyzacji powtarzalnych zadań. Staramy się też poznać nowe wybiegi przeciwników. Dodajmy do tego trochę współpracy ze społecznością i będziemy najlepszymi kowbojami na Dzikim Zachodzie!
8. Na koń, szeryfie! Razem ochronimy to przedsięwzięcie przed wszelkiego rodzaju cyberszumowinami — a to wszystko dzięki lśniącemu koltowi analizy zagrożeń. Ruszajmy!

Dzielenie się informacjami OSINT przypomina informowanie sąsiadów o podejrzanym samochodzie zaparkowanym za rogiem. Dzięki temu wszyscy możemy być czujniejsi

i bezpieczniejsi. W cyberświecie, jeżeli dowiemy się o zagrożeniu lub nowej sztuczce hakerskiej i powiemy o tym innym, będą mieli większą szansę się przed tym zagrożeniem uchronić.

Dzielenie się informacjami pochodzącymi z OSINT z innymi platformami i zespołami

Ważne jest przemyśleć, w jaki sposób i z kim chcemy się podzielić informacjami.

Zacznijmy od tego, kogo wtajemniczyć:

- **Zespoły wewnętrzne**. To osoby w obrębie naszej organizacji, które zajmują się systemami informatycznymi i bezpieczeństwem. Potrzebują szczegółowych, technicznych informacji, aby skutecznie reagować na zagrożenia. Ta grupa osób zazwyczaj ceni konkrety. Określ rodzaj złośliwego oprogramowania, metody ataku oraz wskaźniki zagrożenia. Wnikliwa analiza zagrożeń pomoże im opracować precyzyjne mechanizmy obronne.
- **Inne działy**. Nie wszyscy w firmie rozumieją techniczne detale zagrożenia i nie wszyscy powinni mieć do nich dostęp. Na przykład działy marketingu i sprzedaży należy poinformować o zagrożeniu, ale w sposób prosty i przejrzysty. Możemy ogłosić: „Oszuści wysyłają maile phishingowe, podając się za klienta. Uważajcie na wszelkie nietypowe zapytania i żądania płatności".
- **Platformy zewnętrzne**. To specjalistyczne fora i przestrzenie cyfrowe, gdzie specjaliści ds. cyberbezpieczeństwa z różnych organizacji dzielą się informacjami. Platformy takie jak ThreatConnect (*https://threatconnect.com*) czy IBM X-Force Exchange, o których wspominaliśmy wcześniej, to doskonałe przykłady. Nie chodzi tylko o to, żeby samemu zdobyć informacje. Dobrze jest też dołożyć swoją cegiełkę do wspólnej ochrony przed cyberzagrożeniami. Korzystając z tych platform, trzeba uważać, aby ujawnić na tyle dużo, aby to było pomocne, ale na tyle mało, żeby nie stworzyć dodatkowych podatności.

Dostosowanie komunikatu też jest ważne:

- **Do zespołów technicznych**. Ta grupa potrzebuje pełnego obrazu sytuacji, w tym danych technicznych, takich jak podejrzane adresy IP, nazwy domen i hasze plików. Ten poziom szczegółowości pozwala odpowiednio dostosować zabezpieczenia, takie jak zapory sieciowe i oprogramowanie antywirusowe, aby rozpoznawały nowe zagrożenia.
- **Dla osób nietechnicznych**. Uprość przekaz. Celem jest uświadomienie zagrożenia bez przytłaczania żargonem. Na przykład jeżeli istnieje ryzyko ataku za pomocą wiadomości e-mailowych, trzeba tej grupie osób w prosty sposób doradzić, czego powinny się wystrzegać: „Uważajcie na maile, w których ktoś prosi o podanie wrażliwych danych, i nie klikajcie linków z nieznanych źródeł".

Szybkie dzielenie się istotnymi informacjami

Cyberbezpieczeństwo to obszar, który podlega szybkim zmianom — tak jak zagrożenia. Szybkie dzielenie się informacjami pomaga zespołowi podjąć działania, zanim zagrożenie lub zmiany wymkną się spod kontroli.

Upewnij się, że to, czym się dzielimy, jest istotne dla odbiorców. Jeżeli informacje nie mają bezpośredniego odniesienia i nie przydadzą się danej osobie, może lepiej je pominąć. Przeładowanie nieistotnymi szczegółami lub informacjami może prowadzić do przegapienia tego, co istotne.

Gdy dzielimy się informacjami, zwłaszcza na platformach zewnętrznych, musimy uważać na wrażliwe dane. Zawsze miej na uwadze równowagę między użytecznością informacji a ochroną wrażliwych danych. Na przykład stwierdzenie, że dany rodzaj ataku jest coraz częstszy, jest przydatne. Dzielenie się szczegółami na temat podatności w obrębie firmy — nie.

Zachęcaj do dwukierunkowej wymiany. Gdy dzielisz się informacją, poproś o informacje zwrotne i dodatkowe uwagi. Dzięki temu możemy uzyskać świeże spojrzenie i lepiej zrozumieć zagrożenie. To jak praca nad projektem grupowym, gdzie każdy może przyczynić się do tego, że końcowy rezultat będzie lepszy.

Dzieląc się tym, co wiemy o cyberzagrożeniach, nie tylko pomagamy swojemu zespołowi lub swojej firmie, lecz zaczynamy być również częścią większego zespołu, który dba o bezpieczeństwo internetu. Pamiętaj: w dziedzinie cyberbezpieczeństwa dzielenie się wiedzą sprawia, że wszyscy stajemy się silniejsi.

Tworzenie strategii analizy zagrożeń opartej na OSINT

W tej części naszej podróży po tajnikach OSINT zagłębimy się w kolejny kluczowy aspekt, a mianowicie w tworzenie strategii **analizy cyberzagrożeń** opartej na białym wywiadzie. Z początku możesz poczuć się jak w powieści szpiegowskiej, lecz w istocie to dość proste. Przede wszystkim musimy zrozumieć wymagania.

Jakich informacji wywiadowczych potrzebujemy?

Te wymagania mają kluczowe znaczenie w dziedzinie cyberbezpieczeństwa. Chodzi o maksymalne skoncentrowanie się na tym, co jest najbardziej użyteczne z punktu widzenia bezpieczeństwa danej organizacji. Powiedzmy, że stoimy na czele działu ds. cyberbezpieczeństwa firmy. Nasze pierwsze pytanie brzmi: jakich informacji potrzebujemy, aby się bronić? Odpowiedź na to pytanie to nasze wymagania dotyczące informacji wywiadowczych. Dla specjalistów ds. cyberbezpieczeństwa oznacza to możliwość rozpoznania najpilniejszych zagrożeń i zareagowania na nie.

Określenie najważniejszych potrzeb informacyjnych

Kolejne ważne pytanie brzmi: jak dowiedzieć się, jakich informacji potrzebujemy? Odpowiedź na to pytanie jest odmienna dla każdej organizacji. Dla producenta gier najważniejsza może być ochrona serwerów i danych graczy. W sklepie internetowym nacisk może paść na zabezpieczenie transakcji.

Wysoka specyficzność jest istotna. Nie wystarczy powiedzieć: „Chcemy, aby nasza sieć była bezpieczna". Trzeba być dokładnym. Jakie aspekty sieci? Na które ataki jesteśmy najbardziej narażeni? Im dokładniejszy opis, tym lepiej możemy dostosować swoje wysiłki.

Ponadto wymagania dotyczące danych wywiadowczych muszą się pokrywać z ogólnymi dążeniami firmy. Na przykład jeżeli firma najbardziej obawia się naruszeń danych, wysiłki zespołu powinny skupiać się głównie na zapobieganiu takiemu zagrożeniu.

Rola OSINT

OSINT jest jak mocne szkło powiększające, które pozwala skupić się na istotnych szczegółach w morzu informacji. Specjaliści ds. cyberbezpieczeństwa wykorzystują OSINT do monitorowania publicznie dostępnych źródeł, takich jak media społecznościowe, fora, blogi i witryny informacyjne, aby gromadzić wiedzę na temat ewentualnych zagrożeń. Informacje te mogą obejmować najświeższe trendy w obszarze złośliwego oprogramowania omawiane na forum hakerskim czy informacje na temat naruszeń podane w wiadomościach. Wykorzystując OSINT, specjaliści ds. cyberbezpieczeństwa mogą uzyskać przewagę nad zagrożeniami i podjąć zapobiegawcze działania chroniące organizację. „W jaki sposób?" — zapytasz. Podzielmy to na mniejsze kawałki.

Dojrzałość ma znaczenie

Wykorzystanie białego wywiadu różni się znacznie w zależności od poziomu dojrzałości organizacji. Dla nowych podmiotów OSINT może po prostu oznaczać zdobywanie informacji na temat trendów i nowości w branży. W miarę rozwoju podejście organizacji do OSINT staje się bardziej ustrukturyzowane i powiązane z ogólnym systemem zabezpieczeń. Dojrzałe organizacje zazwyczaj będą dysponowały specjalnymi zespołami i zaawansowanymi narzędziami do zarządzania danymi z otwartych źródeł i ich analizy. Te zespoły wykorzystują OSINT nie tylko po to, aby się zorientować w sytuacji, lecz również do analiz prognostycznych, analizy trendów, a nawet przewidywania prawdopodobnych zagrożeń.

Łączenie danych wewnętrznych i zewnętrznych

Kluczowa jest integracja wyników badań OSINT z wewnętrznymi źródłami danych. Mogą to być logi bezpieczeństwa, sprawozdania na temat incydentów oraz informacje zwrotne od pracowników. Powiązanie tych źródeł danych zapewnia kompleksowy obraz warunków w dziedzinie cyberbezpieczeństwa.

Program analizy cyberzagrożeń powinien obejmować nieustanne monitorowanie zarówno wewnętrznych, jak i zewnętrznych źródeł. Konieczne jest również śledzenie najnowszych wydarzeń w cyfrowym świecie i regularne aktualizowanie baz danych z informacjami, aby upewnić się, że są aktualne i istotne.

Tworzenie zróżnicowanego i wykwalifikowanego zespołu

Zespół do analizy cyberzagrożeń to podstawa naszej strategii. Powinien składać się z osób o różnych umiejętnościach i wywodzących się z różnych środowisk. Potrzebujesz ekspertów ds. cyberbezpieczeństwa, analityków danych, badaczy, a nawet osób zainteresowanych psychologią, aby zrozumieć motywy działań hakerów. Przy tworzeniu zespołu weź pod uwagę następujące kwestie:

- Dbaj o to, aby umiejętności zespołu były aktualne oraz aby nieustannie się rozwijały. Zachęcaj do ustawicznego uczenia się i rozwoju zawodowego poprzez uczestnictwo w konferencjach oraz organizowanie regularnych sesji szkoleniowych i warsztatów. Dzięki temu zespół nie zostanie w tyle i zawsze będzie dobrze poinformowany.
- Stwórz warunki sprzyjające współpracy. Członkowie zespołu powinni móc dzielić się swoimi pomysłami i spostrzeżeniami. Dbaj o ducha innowacyjności, aby zachęcać członków zespołu do wychodzenia poza schematy i opracowywania nowych metod gromadzenia i analizowania danych.
- Wzmacniaj program analizy cyberzagrożeń, zapewniając mu odpowiednie narzędzia. Obejmuje to oprogramowanie do gromadzenia i analizy danych, dostęp do platform analizy zagrożeń oraz narzędzia do monitorowania cyberbezpieczeństwa. Wybierz narzędzia, które są skalowalne, wygodne w użyciu i mają szeroki wachlarz funkcjonalności odpowiadających wyznaczonym celom.
- Czasami gotowe narzędzia mogą nie spełniać wszystkich potrzeb i dlatego konieczne jest opracowanie własnego rozwiązania. Może to obejmować utworzenie szytego na miarę oprogramowania do analizy danych lub unikatowego algorytmu do wykrywania zagrożeń.

Przy opracowywaniu strategii analizy cyberzagrożeń opartej na OSINT pamiętajmy o tym, aby zorientować się, jakie konkretne informacje są potrzebne do celów cyberbezpieczeństwa.

To kwintesencja integracji danych z otwartych źródeł i analizy zagrożeń. Chodzi o sprytne połączenie istotnych dla bezpieczeństwa danych z publicznych źródeł, wybranie właściwych narzędzi oraz gotowość do nieustannego uczenia się i dostosowywania. Pamiętaj, że bezpieczeństwo w internecie polega na dysponowaniu odpowiednią wiedzą i na współpracy.

Studium przypadku, czyli rola OSINT w prawdziwych incydentach z zakresu cyberbezpieczeństwa

W lipcu 2020 r. portal Twitter (obecnie X) padł ofiarą istotnego naruszenia bezpieczeństwa. Konta wpływowych osób i organizacji, takich jak Barack Obama, Elon Musk, Jeff Bezos oraz Apple, przejęto i użyto do wyłudzania bitcoinów (*https://www.theverge.com/22163643/twitter-hack-bitcoin-scamjuly-2020-elon-musk*).

Atak rozpoczął się od akcji phishingowej skierowanej przeciwko pracownikom Twittera. Przeprowadzona telefonicznie operacja spear phishingowa miała na celu uzyskanie dostępu do kont z dostępem do narzędzi wewnętrznych.

Atakujący udawali przedstawicieli działu IT Twittera i zdołali przekonać pracowników, by podali swoje dane do do logowania. Dzięki skutecznej sztuczce socjotechnicznej napastnikom udało się uzyskać dostęp do wewnętrznych systemów firmy.

Po ataku OSINT odegrał kluczową rolę w zrozumieniu charakteru naruszenia. Badacze i specjaliści ds. cyberbezpieczeństwa wykorzystali publicznie dostępne informacje, takie jak dane rejestracyjne domen i analiza IP, do wykrycia źródła incydentu.

Analiza adresów do portfeli kryptowalutowych podanych w fałszywych tweetach oraz weryfikacja w różnych źródłach publicznie dostępnych danych na temat transakcji blockchain pomogły opracować schemat przepływu wyłudzonych funduszy. Do monitorowania rozprzestrzeniania się i wpływu incydentu w mediach społecznościowych użyto narzędzi OSINT. Pomogło to szybko zrozumieć zasięg ataku. Odpowiedź Twittera obejmowała zablokowanie zainfekowanych kont, usunięcie oszukańczych tweetów, a także tymczasowe ograniczenie możliwości publikowania tweetów przez zweryfikowane konta.

OSINT odgrywał również rolę w analizie powypadkowej, pomagając zrozumieć taktykę atakujących i zapobiec podobnym oszustwom w przyszłości. Incydent podkreślił znaczenie szkolenia pracowników w radzeniu sobie z socjotechniką oraz potrzebę tworzenia solidnych zabezpieczeń wewnętrznych. Udowodnił też wartość OSINT w reagowaniu na bieżące zagrożenia i w analizie powypadkowej.

Atak na Twittera z 2020 r. służy jako wybitny przykład tego, w jaki sposób zaawansowany atak phishingowy połączony z socjotechniką może prowadzić do istotnych naruszeń bezpieczeństwa. Pokazuje również kluczową rolę OSINT w szybkiej identyfikacji cyberzagrożeń, reagowaniu na nie i wyciąganiu wniosków. Incydent wskazuje również na potrzebę zachowania stałej czujności i udoskonalania praktyk z zakresu cyberbezpieczeństwa. Mam nadzieję, że teraz w pełni rozumiesz, w jaki sposób OSINT może pomóc w analizie cyberzagrożeń.

Podsumowanie

W tym rozdziale przeszliśmy od teoretycznych rozmów na temat OSINT do jego praktycznego zastosowania w obszarze cyberbezpieczeństwa. Odnosząc się do prawdziwych sytuacji, omówiłem integrację analizy zagrożeń z OSINT, rolę OSINT w wykrywaniu cyberzagrożeń oraz wkład OSINT w zwiększanie cyberbezpieczeństwa. Dzięki temu masz teraz praktyczną wiedzę na temat tego, jak skutecznie korzystać z OSINT. Nowo nabyte zrozumienie umożliwia nam wykrywanie potencjalnych zagrożeń dzięki połączeniu wiedzy i krytycznego spojrzenia, a także wykorzystanie tych umiejętności do szerokiego spektrum zagadnień z zakresu cyberbezpieczeństwa, gdzie ludzkie interakcje mają kluczowe znaczenie.

W następnym rozdziale przyjrzymy się, w jaki sposób możemy chronić swoje prywatne i firmowe informacje przed cyberzagrożeniami.

Rozdział 7

Ochrona własnej tożsamości i organizacji przed cyberzagrożeniami

W świecie, w którym nasze życie w coraz większym stopniu toczy się online, zabezpieczenie własnej tożsamości i organizacji przed cyberzagrożeniami jest ważniejsze niż kiedykolwiek wcześniej. W tym rozdziale nauczysz się przede wszystkim chronić samego siebie. Dowiesz się, jak publicznie dostępne informacje mogą stać się potężnym narzędziem w tej walce. Pamiętaj jednak o tym, że jest to miecz obusieczny, zdolny zarówno zagrozić naszej cyfrowej tożsamości i zasobom firmy, jak i je chronić. Dzięki tej podróży udoskonalisz umiejętności korzystania z **białego wywiadu** (**OSINT**) — nie tylko jako teoretycznego podejścia, lecz również jako praktycznego narzędzia w arsenale cyberzabezpieczeń.

W tym rozdziale zajmiemy się przede wszystkim następującymi tematami:

- zrozumienie roli OSINT w ochronie tożsamości osób i zasobów organizacji;
- osobista higiena cyfrowa a OSINT;
- ocena i wzmacnianie bezpieczeństwa organizacji dzięki OSINT;
- wykrywanie cyberzagrożeń i reagowanie na nie;
- prowadzenie dochodzeń w sprawie incydentów i naruszeń cyberbezpieczeństwa;
- tworzenie solidnych cyberzabezpieczeń dzięki OSINT.

W tym rozdziale naprawdę zagłębimy się w te tematy, ale ci, którzy nie pominęli żadnego rozdziału, nie powinni mieć problemów. Do dzieła!

Zrozumienie roli OSINT w ochronie tożsamości osób i zasobów organizacji

Witaj w ostatnim rozdziale tej książki. Jest on w pełni poświęcony zabezpieczeniu Ciebie i Twojej organizacji przed internetowymi zagrożeniami. OSINT stanowi kluczowe narzędzie w tej nieustającej walce, gdyż umożliwia zbieranie i analizowanie publicznie dostępnych danych, przekształca je w informacje wywiadowcze oraz pomaga w podejmowaniu decyzji. Dane mogą pochodzić z najróżniejszych źródeł, w tym z wiadomości, rejestrów publicznych i mediów społecznościowych.

Rola OSINT w obszarze cyberbezpieczeństwa jest złożona. Osobom prywatnym OSINT może pomóc w ochronie ich internetowej tożsamości. W czasach gdy nasz cyfrowy ślad jest rozległy i często publicznie dostępny, musimy być świadomi tego, jakie informacje o nas można pozyskać w sieci. Techniki OSINT mogą pomóc zidentyfikować podatności dotyczące naszej cyfrowej obecności, takie jak niezabezpieczone dane osobowe, a także pokazać nam, jakie kroki należy podjąć, aby je zabezpieczyć.

W przypadku organizacji OSINT ma istotne znaczenie w ochronie przed różnego rodzaju cyberzagrożeniami. Pomaga określić podatności w cyfrowej infrastrukturze, zrozumieć sposób działania potencjalnych napastników oraz przygotować się na nadchodzące zagrożenia. Dzięki OSINT jesteśmy również w stanie monitorować wzmianki na temat cyfrowej obecności firmy, by uzyskać wgląd w potencjalne ryzyko dla reputacji oraz możliwość podjęcia działań.

Rola OSINT w zapobieganiu cyberzagrożeniom

Zapobiegawcze działania OSINT zapewniają kilka korzyści w obszarze cyberbezpieczeństwa. Przede wszystkim umożliwiają wczesną identyfikację zagrożeń. Dzięki stałemu monitorowaniu różnych ogólnodostępnych źródeł organizacje mogą wykryć potencjalne zagrożenia, zanim przybiorą formę prawdziwego ataku. To wczesne wykrywanie stanowi podstawę do wdrożenia środków zaradczych na czas.

Kolejna zaleta proaktywnego prowadzenia badań OSINT jest związana z analizą zagrożeń. OSINT pomaga organizacjom poznać szerszy kontekst, w tym motywy i sposoby działania sprawców. Zrozumienie tych aspektów ma decydujący wpływ na skuteczność strategii obrony.

Proaktywny biały wywiad wspiera również zarządzanie ryzykiem. Dzięki stałej ocenie zagrożeń organizacje mogą dostosować swoje strategie z zakresu cyberbezpieczeństwa do ewoluujących zagrożeń. Aktywne podejście do cyberbezpieczeństwa gwarantuje, że zabezpieczenia pozostają aktualne i niezawodne.

Ponadto w każdym aspekcie cyberbezpieczeństwa aktywna postawa jest dużo lepszym rozwiązaniem niż ograniczenie się do reagowania. Jest to dla nas w pewnym sensie *gwarancja stałego zatrudnienia*.

Osobista higiena cyfrowa a OSINT

Nasz cyfrowy ślad to dane, które zostawiamy w internecie. Obejmuje to aktywność w mediach społecznościowych, posty na forach, transakcje cyfrowe i wszelkie inne dane online. Zostawiasz ten ślad nie tylko wtedy, gdy korzystasz z komputera. Pomyśl tylko o danych, które ujawniasz za pomocą swojego telefonu!

Narzędzia takie jak agregatory danych, wyszukiwarki oraz inne wyspecjalizowane programy przeczesują internet i kompilują szczegółowy obraz naszego śladu cyfrowego. Badanie tych danych pomaga określić, które zachowania i udostępnienia danych wiążą się z ryzykiem. Na przykład dzielenie się zbyt dużą ilością informacji w mediach społecznościowych może uczynić z nas łatwy cel kradzieży tożsamości lub ataków socjotechnicznych. Dzięki regularnemu sprawdzaniu swojego cyfrowego śladu możemy podejmować świadome decyzje na temat swoich działań online i zmniejszyć podatność na cyberzagrożenia.

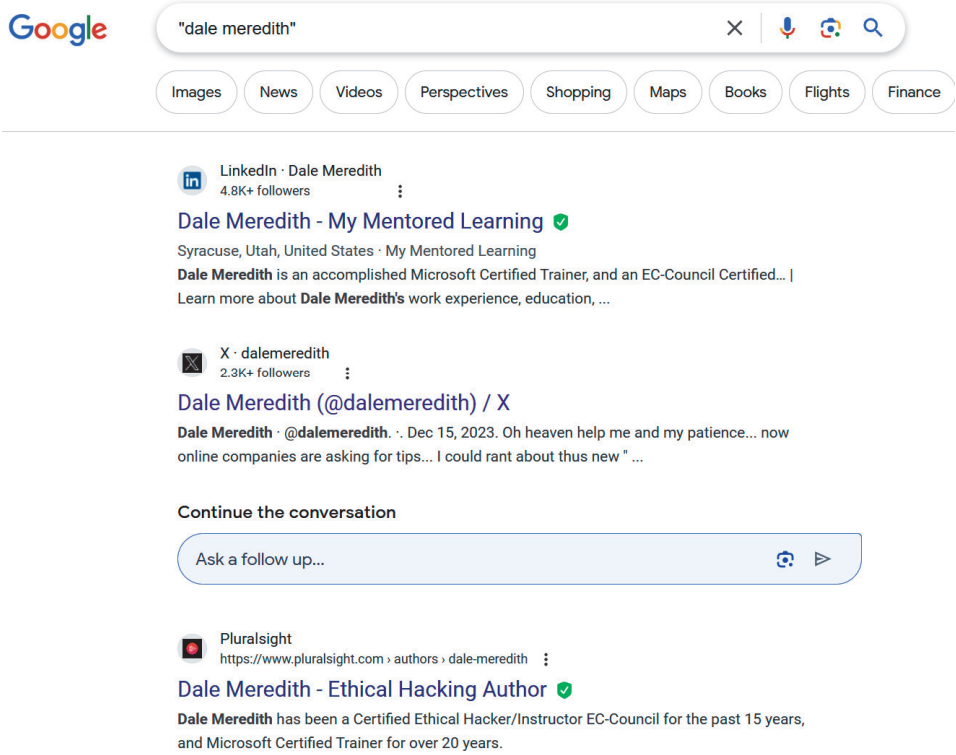
Identyfikowanie i ograniczanie ryzyka wynikającego z cyfrowego śladu

Po uzyskaniu jasnego obrazu cyfrowego śladu następnym krokiem jest ograniczenie związanego z nim ryzyka. Obejmuje to użycie bardziej rygorystycznych ustawień prywatności w mediach społecznościowych, zachowanie ostrożności podczas dzielenia się informacjami online, a także regularne sprawdzanie kont internetowych pod kątem śladów nieuprawnionego dostępu lub nietypowej aktywności.

Oto kilka najlepszych praktyk w zakresie ograniczania ryzyka:

- **Kontroluj swoją cyfrową obecność**. Regularnie przeprowadzaj swoisty audyt swoich kont internetowych i profilów w mediach społecznościowych. Sprawdzaj wcześniej udostępnione informacje i oceniaj ich wrażliwość. Czy te informacje mogą zostać użyte przeciwko Tobie (np. do kradzieży tożsamości, ataków socjotechnicznych itp.)? Organizacje mogą w tym celu skorzystać z narzędzi takich jak:
  - **Sprout Social** (*https://www.sproutsocial.com*) — kompleksowe narzędzie do zarządzania mediami społecznościowymi, umożliwiające prowadzenie audytów i analiz;
  - **Hootsuite** (*https://www.hootsuite.com*) — narzędzie do zarządzania wieloma kontami w mediach społecznościowych oraz śledzenia ich wpływu;
  - **Google Analytics** (*https://analytics.google.com*) — podstawowe narzędzie do monitorowania ruchu na stronach internetowych i analizowania efektywności witryn.
- **Podnieś poziom ustawień prywatności**. W mediach społecznościowych, takich jak Facebook, X, Instagram czy LinkedIn, przejrzyj i dostosuj swoje ustawienia dotyczące prywatności, aby ograniczyć, grono osób, które mogą zobaczyć Twoje posty, dane kontaktowe i szczegółowy profil.

- **Wygoogluj się**. Użyj wyszukiwarki, aby sprawdzić, jakie informacje na Twój temat są publicznie dostępne (rysunek 7.1).



Rysunek 7.1. Wyszukaj siebie lub swoją firmę w wyszukiwarce Google

Sprawdź swoje imię i nazwisko, adresy e-mailowe oraz numery telefonów. Dowiesz się, jakie dane mogą znaleźć ewentualni napastnicy.

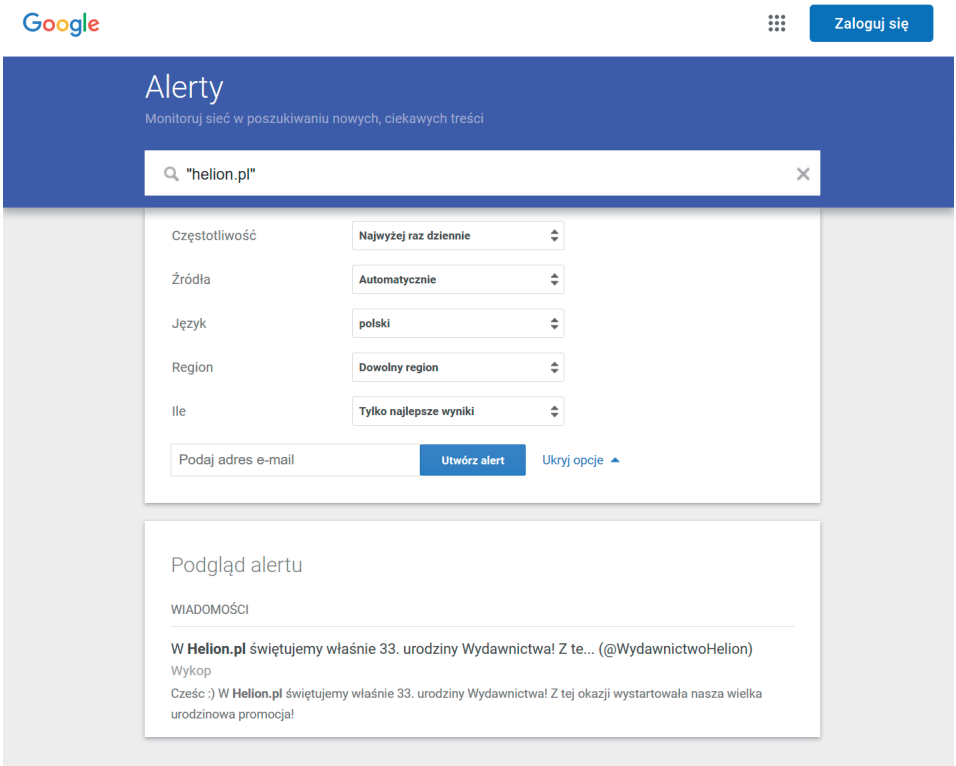
- **Przejrzyj i usuń niepotrzebne informacje**. Jeżeli znajdziesz wrażliwe informacje na swój temat w internecie (np. na starych blogach i forach lub w mediach społecznościowych), podejmij odpowiednie kroki, aby je usunąć. Skontaktuj się z administratorami witryn, jeżeli to potrzebne.

Następujące narzędzia mogą nam pomóc w zarządzaniu cyfrową obecnością:

- **Alerty Google** (*https://www.google.com/alerts*). Ustaw powiadomienia na swoje imię i nazwisko oraz inne cyfrowe identyfikatory (rysunek 7.2).

  Ta usługa zawiadamia nas, gdy w internecie pojawiają się nowe informacje zawierające dany identyfikator. Monitoruję w ten sposób swoje imię i nazwisko. Kilka razy uratowało mi to skórę.

- **Have I Been Pwned?** (*https://haveibeenpwned.com*). Tę witrynę prowadzi mój przyjaciel Troy Hunt. Możemy tutaj sprawdzić, czy nasz adres e-mailowy

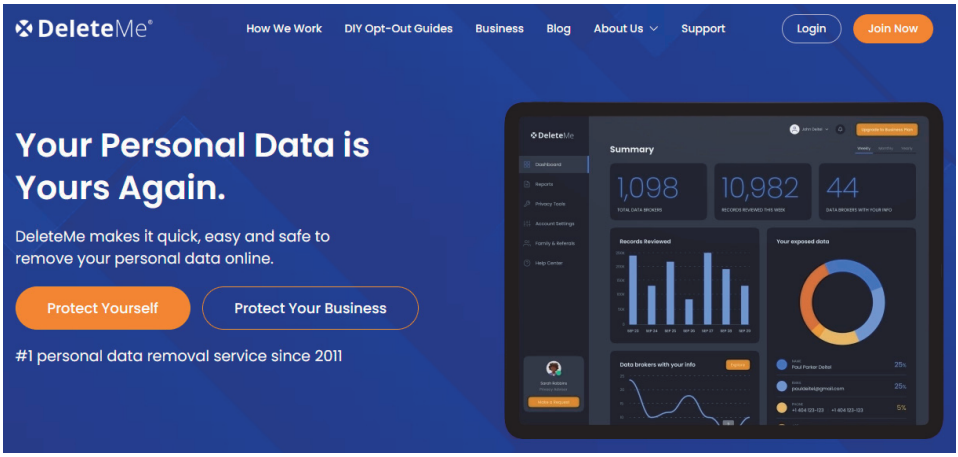


Rysunek 7.2. Alerty Google powiadamiają o nowych wynikach wyszukiwania

padł ofiarą wycieku danych. Pomaga to zrozumieć potencjalne zagrożenie i podjąć kroki, takie jak zmiana hasła lub zastosowanie bezpieczniejszych ustawień. Pamiętaj kliknąć przycisk *Notify me* (powiadom mnie). Dzięki temu natychmiast otrzymasz powiadomienie, jeżeli pojawi się wyciek obejmujący Twój adres e-mailowy.

- **Ustawienia i narzędzia chroniące prywatność w mediach społecznościowych**. Większość portali społecznościowych oferuje narzędzia i ustawienia do kontroli prywatności. Poznaj te opcje i naucz się z nich korzystać, aby zarządzać swoją widocznością w sieci. Zauważ, że portale stale zmieniają dostępne funkcjonalności, więc bądź na bieżąco z publikowanymi przez nie komunikatami.
- **Usługi usuwania danych**. Aby pozbyć się danych, których nie jesteś w stanie usunąć ręcznie, skorzystaj z usług takich jak DeleteMe (*https://joindeleteme.com*), a usługodawca skontaktuje się w Twoim imieniu z brokerami danych i witrynami (rysunek 7.3).

  DeleteMe to naprawdę świetna usługa i narzędzie, przy czym jest to dość kosztowne rozwiązanie. Czy można jednak wycenić naszą prywatność?



Rysunek 7.3. DeleteMe pomaga zarządzać danymi osobowymi online

- **Bądź na bieżąco**. Śledź najnowsze trendy w obszarze prywatności i bezpieczeństwa online. Dowiaduj się o nowych metodach wykorzystywanych przez cyberprzestępców, a także poznawaj nowe narzędzia i usługi, które chronią Twoją cyfrową tożsamość.
- **Dowiedz się więcej na temat phishingu i socjotechniki**. Naucz się wykrywać ataki phishingowe i metody socjotechniczne. Dzięki tej wiedzy nie staniesz się ofiarą oszustwa zagrażającego Twoim danym osobowym. Najlepszym sposobem, aby zapoznać się z tematem phishingu i socjotechniki, jest wspaniały filmik z konferencji DEF CON, który prezentuje odczyt innowacyjnego pentestera Chrisa Pritcharda. Możesz się zapoznać z tym materiałem pod adresem *https://www.youtube.com/watch?v=jfXwdH-fkLE*.

Podejmując te kroki i wykorzystując dostępne narzędzia, każdy z nas może znacznie ograniczyć ryzyko powiązane ze swoją cyfrową obecnością. Aktywne podejście do cyfrowej higieny nie tylko chroni nasze prywatne dane, lecz również ogranicza naszą ogólną podatność na cyberzagrożenia.

Wyższy poziom prywatności i bezpieczeństwa

Oprócz monitorowania i ograniczania ryzyka istotne jest również zwiększanie naszego ogólnego poziomu prywatności i bezpieczeństwa online. Obejmuje to silne, unikatowe hasła do różnych kont, składające się z kombinacji liter, cyfr i znaków specjalnych. Hasła nie powinny być łatwe do zgadnięcia z użyciem technik OSINT — unikaj imion, nazwisk, dat urodzenia, hobby czy nazw drużyn sportowych. Chcemy również pamiętać o złotej zasadzie tworzenia haseł: *im dłuższe, tym lepsze*. Nie używaj wielokrotnie tego samego hasła. Gorąco polecam korzystanie z menedżera haseł, który w tym pomaga. Tam, gdzie to możliwe, ustaw uwierzytelnienie dwuskładnikowe (ang. *two-factor authentication*). Bądź też na bieżąco z informacjami na temat najnowszych ataków phishingowych i socjotechnicznych.

Narzędzia OSINT mogą pomóc wykryć ewentualne podatności w naszych zachowaniach i cyfrowych zasobach. Mogą na przykład pokazać, czy nasze dane osobowe nie znajdują się w bazach danych wycieków lub czy nasz adres e-mailowy nie jest wykorzystywany do spamowania.

Konieczne jest też wdrożenie najlepszych praktyk z zakresu higieny cyfrowej. Obejmuje to regularne aktualizowanie oprogramowania, aby załatać luki w bezpieczeństwie, zachowywanie ostrożności w wyborze usług i aplikacji, a także nieustanne poszerzanie swojej wiedzy na temat cyberzagrożeń i ich unikania. Osobiście przeraża mnie rozwój **sztucznej inteligencji (SI)**. Technologie takie jak deepfake i generatywna sztuczna inteligencja (GenAI) zmieniają nasz świat. Jak zawsze w takich przypadkach hakerzy znajdą sposób, aby je wykorzystać przeciwko nam. Dodaj więc sztuczną inteligencję do tematów, z którymi trzeba się zapoznać.

Ocena i wzmacnianie bezpieczeństwa organizacji dzięki OSINT

Bezpieczeństwo organizacji zależy od najsłabszego ogniwa. Infrastruktura zewnętrzna, która obejmuje zasoby dostępne w sieci, takie jak strony internetowe, serwery poczty elektronicznej czy usługi chmurowe, często jest otwarta na wiele wektorów ataków. Zrozumienie i zabezpieczenie tych aspektów cyfrowej obecności organizacji odgrywa *kluczową rolę*, a OSINT ma decydujący wpływ na sukces tych starań, gdyż uzupełnia analizę podatności i wektorów zagrożeń.

Proces oceny i wzmacniania zabezpieczeń sieci obejmuje wykrywanie podatności w aplikacjach webowych, serwerach poczty elektronicznej, konfiguracjach DNS i innych publicznie dostępnych zasobach, a następnie wdrażanie środków zapobiegawczych.

Wykrywanie ewentualnych podatności

Oto krótka lista zagadnień, na które należy zwrócić uwagę, oraz powiązanych narzędzi, których można użyć do wykrywania podatności w infrastrukturze firmy:

- **Aplikacje i witryny internetowe**. Aplikacje dostępne w sieci są często punktem wyjścia do ataku. Narzędzia takie jak Nikto2 (*https://cirt.net/Nikto2*) mogą przeskanować aplikacje webowe pod kątem ponad 7000 podatności, nie pomijając złożonych, wielopoziomowych formularzy i obszarów zabezpieczonych hasłem (rysunek 7.4).

  Możliwość przeprowadzenia pełnego lub inkrementalnego skanu zapewnia szeroki zakres ochrony.

- **Serwery poczty elektronicznej**. Systemy poczty elektronicznej są częstym celem ataków phishingowych i rozsyłania złośliwego oprogramowania. Narzędzia takie jak Vipre (*https://vipre.com*) zapewniają kompleksowe

```
┌──(kali㉿kali)-[~]
└─$ nikto -h scanme.nmap.org
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2024-02-12 18:27:28 (GMT-7)
---------------------------------------------------------------------------
```

Rysunek 7.4. Skanowanie domeny scanme.nmap.org narzędziem Nikto

zabezpieczenia poczty elektronicznej, chronią przed wirusami, oprogramowaniem wymuszającym okup oraz kradzieżą tożsamości, a także oferują bieżącą analizę zagrożeń dla przedsiębiorstw.

- **Bezpieczeństwo sieci**. Zabezpieczenie infrastruktury sieciowej to podstawa. Otwartoźródłowe narzędzie monitorujące Zeek (*https://zeek.org*) działa w sposób pasywny. Obserwuje ruch sieciowy bez podejmowania działań, generuje szczegółowe logi na temat transakcji i treści plików, a następnie udostępnia je do analizy bezpieczeństwa (rysunek 7.5).

```
root@debian12:/opt/zeek/logs/current# cat dns.log | zeek-cut id.orig_h query answers
10.0.2.15       -       -
10.0.2.15       httpredir.debian.org    debian.map.fastlydns.net,199.232.46.132
10.0.2.15       httpredir.debian.org    debian.map.fastlydns.net,2a04:4e42:48::644
10.0.2.15       _http._tcp.security.debian.org  debian.map.fastlydns.net
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15       httpredir.debian.org    debian.map.fastlydns.net,199.232.46.132
10.0.2.15       httpredir.debian.org    debian.map.fastlydns.net,2a04:4e42:48::644
10.0.2.15       download.opensuse.org   195.135.221.134
10.0.2.15       download.opensuse.org   2001:67c:2178:8::13
root@debian12:/opt/zeek/logs/current#
```

Rysunek 7.5. Zeek pozwala pasywnie przeglądać żądania napływające do sieci

Jeżeli zajmujesz się cyberbezpieczeństwem od kilku lat, możesz pamiętać produkt o nazwie **Bro**. Zeek jest próbą jego odtworzenia. Dostarcza ponad 60 plików logów i śledzi ponad 3000 wydarzeń sieciowych. Pobrano go ponad 10 000 razy. Integracja z DNS pozwala zapobiegać atakom przekierowania i przejęcia ruchu. Regularna analiza rekordów DNS może pomóc w wykryciu nieprawidłowej konfiguracji lub nieupoważnionych zmian. Zaufaj mi, to użyteczne narzędzie.

- **Regularne skany pod kątem podatności**. Stałe monitorowanie cyfrowych zasobów z użyciem narzędzi takich jak SanerNow firmy SecPod (*https://www.secpod.com*) może wykryć podatności i błędną konfigurację. Funkcjonalności instalowania aktualizacji i zarządzania podatnościami w czasie rzeczywistym zapewniają natychmiastowe i skuteczne usuwanie wykrytych zagrożeń.

- **Bezpieczeństwo punktów końcowych**. Ochrona punktów końcowych przed złośliwym oprogramowaniem i innymi zagrożeniami to decydujący czynnik. Malwarebytes (*https://www.malwarebytes.com*) i wiele innych firm oferują funkcjonalności z zakresu ochrony punktów końcowych oraz reagowania na incydenty, takie jak wykrywanie anomalii, analiza wzorców zachowań i zapobieganie zagrożeniom w czasie rzeczywistym.

Prywatność a korzystanie z narzędzi internetowych

Narzędzia takie jak Nikto2, Vipre, Zeek, SanerNow czy Malwarebytes wykorzystywane w prawidłowy sposób i z odpowiednią ostrożnością, mogą dostarczyć cennych informacji na temat stanu zabezpieczeń bez poświęcania prywatności. Przy wyborze narzędzi do wykrywania podatności należy kierować się ostrożną oceną bezpieczeństwa, standardów prywatności oraz wymagań dotyczących zgodności specyficznych dla danej organizacji.

Cyfrowy świat szybko się zmienia, podobnie jak sposoby działania hakerów. Aby zadbać o bezpieczeństwo swojego cyfrowego domu, musimy być na bieżąco z nowymi narzędziami i rozwiązaniami. Tak jak aktualizujemy urządzenia i oprogramowanie, tak musimy też aktualizować swoją wiedzę.

Wykrywanie cyberzagrożeń takich jak oprogramowanie wymuszające okup i reagowanie na nie

W dzisiejszej cyfrowej rzeczywistości zagrożenia nieustannie ewoluują, a oprogramowanie wymuszające okup stanowi niezwykle podstępną formę ataku. Oprogramowanie wymuszające okup (ang. *ransomware*) to rodzaj złośliwego oprogramowania, które blokuje dostęp do komputera lub danych, zazwyczaj poprzez szyfrowanie, w celu uzyskania okupu. Ten rodzaj cyberataków zyskał złą sławę ze względu na paraliżujący wpływ na osoby prywatne, firmy i infrastrukturę publiczną.

- **Najważniejsze cechy**. Większość programów wymuszających okup szyfruje pliki na urządzeniu ofiary, blokując do nich dostęp. Atakujący żądają pieniędzy w zamian za udostępnienie klucza odszyfrowywania. Płatność zazwyczaj ma być uiszczona w kryptowalutach takich jak bitcoin, co sprawia, że trudniej wyśledzić sprawców.

  Dawniej te ataki nie miały sprecyzowanego celu, ale najnowsze trendy pokazują zwiększającą się liczbę ataków przeciwko konkretnym organizacjom, firmom czy usługom, które są w stanie zapłacić wyższy okup. Podobnie jak inne cyberzagrożenia ransomware często uzyskuje dostęp do systemów dzięki e-mailom phishingowym, które skłaniają użytkowników do pobrania złośliwego oprogramowania.

- **Wpływ**. Oprócz konieczności zapłacenia okupu ofiary często ponoszą straty finansowe ze względu na zakłócenia w działaniu, utratę danych i szkody dla reputacji. Ransomware może sparaliżować całe systemy, stwarzając istotne wyzwania operacyjne, zwłaszcza we wrażliwych sektorach, takich jak ochrona zdrowia i organy administracji publicznej. Nawet w przypadku zapłaty okupu nie ma gwarancji, że dane uda się w pełni odzyskać i że atakujący nie wykorzystali ich do innych celów.
- **Eliminowanie i ograniczanie ryzyka**. Aby zabezpieczyć się przed oprogramowaniem wymuszającym okup, należy regularnie wykonywać kopie zapasowe, szkolić pracowników z zakresu ochrony przed phishingiem oraz dbać o aktualność środków bezpieczeństwa. Regularne kopie zapasowe umożliwiają odzyskanie danych w przypadku ataku, a szkolenia pracowników zapobiegają początkowej infekcji złośliwym oprogramowaniem. Instalowanie najnowszych poprawek bezpieczeństwa może uniemożliwić atakującym wykorzystanie znanych podatności. Także solidny plan reagowania na incydenty może istotnie ograniczyć wpływ ataku z wymuszeniem okupu.
- **Aktualne trendy**. Analizy pokazują, że ataki są coraz bardziej zaawansowane, a napastnicy przeprowadzają szeroko zakrojone rozpoznanie, aby skuteczniej zaatakować daną organizację czy branżę. Niepokojącym trendem jest również wzrost taktyki podwójnego wymuszenia. Atakujący bowiem nie tylko szyfrują dane ofiary, lecz także grożą opublikowaniem poufnych informacji w przypadku odmowy zapłaty.

Wykrywanie ataków phishingowych i socjotechnicznych

Aby wykryć złośliwe oprogramowanie z użyciem OSINT, potrzebne jest bardzo aktywne podejście do cyberbezpieczeństwa. Dzięki monitorowaniu forów hakerskich i aukcji w dark webie specjaliści uzyskują wczesne sygnały ostrzegawcze na temat nowych wariantów złośliwego oprogramowania i ataków. Analiza zagrożeń odgrywa kluczową rolę, gdyż powiadamia o nadciągających zagrożeniach w czasie rzeczywistym. Analiza e-maili phishingowych, które często służą do rozpowszechniania złośliwego oprogramowania, umożliwia zidentyfikowanie wektorów ataków. Dodatkowo sprawdzenie haszy plików, adresów IP czy adresów URL w publicznych bazach danych pomaga w rozpoznaniu wskaźników związanych z atakami. Metodologia OSINT wspiera zespoły ds. cyberbezpieczeństwa w przewidywaniu zagrożeń, ograniczaniu ich wpływu i skutecznej ochronie cyfrowych zasobów.

Sprawdzenie podejrzanych adresów URL z użyciem technik OSINT może zapewnić cenne informacje na temat rejestracji domeny, reputacji i ewentualnej powiązanej działalności przestępczej. W ramach tej procedury decydujący wpływ mają zasoby takie jak zapytania WHOIS, ponieważ dostarczają informacji o właścicielach domen i ewentualnych problemach z autentycznością ich witryn.

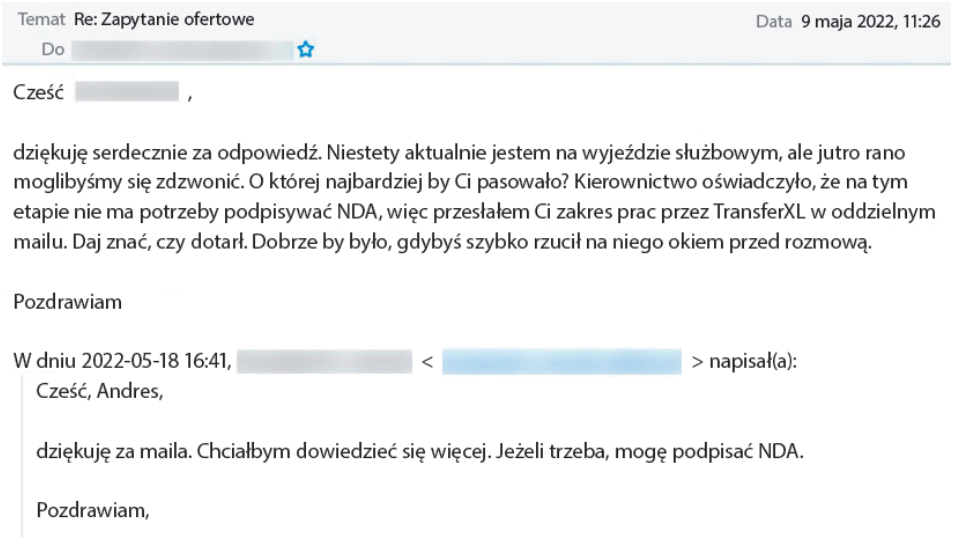
Analiza nagłówków e-maili to kolejny istotny aspekt. Aby wykryć nieprawidłowości lub oznaki podszywania się (ang. *email spoofing*), konieczne jest uważne przyglądanie się nagłówkom e-maili. Pola nagłówka, takie jak *Received: from* (otrzymano od), mogą dostarczyć ważnych informacji na temat pochodzenia e-maila, w tym o ukrytych zamiarach autorów.

Analiza mediów społecznościowych odgrywa zasadniczą rolę w wykrywaniu zagrożeń socjotechnicznych. Badając profile i posty, można zebrać informacje na temat danej osoby, jej zainteresowań i powiązań, które mogą zostać wykorzystane w ramach ukierunkowanego ataku. Regularne monitorowanie platform online pod kątem publicznie dostępnych informacji na temat pracowników ma kluczowe znaczenie dla firm w zapobieganiu atakom socjotechnicznym.

Czas na historię o egzotycznej lilii

Wspaniałym przykładem tego, w jaki sposób cyberprzestępcy mogą wykorzystywać techniki OSINT do prowadzenia ataków spear phishingowych, jest grupa hakerska Exotic Lily („egzotyczna lilia").

To prawdziwi mistrzowie spear phishingu. Ten rodzaj phishingu przypomina łowienie ryb w jeziorze — nie polujemy jednak na wszystkie ryby, lecz na jedną konkretną, i to z harpunem w ręku. Cyberprzestępcy tacy jak grupa Exotic Lily nie wysyłają e-maili na chybił trafił do tysięcy osób. Wybierają jedną konkretną osobę lub firmę, a potem tworzą wiadomość przeznaczoną specjalnie dla niej. Te e-maile wyglądają na prawdziwe i godne zaufania. Pochodzą od kolegi, szefa lub znanego kontrahenta (rysunek 7.6).


Temat Re: Zapytanie ofertowe
Data 9 maja 2022, 11:26
Do

Cześć ,

dziękuję serdecznie za odpowiedź. Niestety aktualnie jestem na wyjeździe służbowym, ale jutro rano moglibyśmy się zdzwonić. O której najbardziej by Ci pasowało? Kierownictwo oświadczyło, że na tym etapie nie ma potrzeby podpisywać NDA, więc przesłałem Ci zakres prac przez TransferXL w oddzielnym mailu. Daj znać, czy dotarł. Dobrze by było, gdybyś szybko rzucił na niego okiem przed rozmową.

Pozdrawiam

W dniu 2022-05-18 16:41, < > napisał(a):

Cześć, Andres,

dziękuję za maila. Chciałbym dowiedzieć się więcej. Jeżeli trzeba, mogę podpisać NDA.

Pozdrawiam,

Rysunek 7.6. Przykład jednej z wiadomości e-mailowych grupy Exotic Lily

Jak im się to udaje? Przede wszystkim odrabiają pracę domową i zdobywają szczegółowe informacje o docelowym środowisku. Przeszukują media społecznościowe, witryny firmowe i inne publiczne zasoby, aby zdobyć informacje o osobie lub firmie, którą chcą zaatakować. Dzięki temu fałszywe wiadomości brzmią przekonująco.

Przyjrzyjmy się przykładowi. Powiedzmy, że grupa Exotic Lily dowiedziała się, że uczestniczyłeś w konferencji na temat cyberbezpieczeństwa. Mogłaby wysłać e-maila wyglądającego tak, jakby pochodził od organizatorów konferencji. Mógłby informować o zmianie w harmonogramie i odsyłać do linka po więcej szczegółów. Gdy klikniesz link, nieświadomie instalujesz na swoim urządzeniu złośliwe oprogramowanie, które może wyrządzić dużo szkód. Może na przykład zaszyfrować pliki i zażądać pieniędzy za ich odszyfrowanie lub potajemnie obserwować wszystko, co robisz na komputerze, i przesyłać informacje atakującemu.

Spear phishing w wykonaniu grupy Exotic Lily to istny majstersztyk. Używa ona prawdziwych nazwisk, odpowiednich logotypów, a nawet pasującego żargonu, aby przekonać o autentyczności e-maila. Może posłużyć się szczegółami z Twojego życia prywatnego lub pracy, o których myślisz, że nikt inny o nich nie wie. To właśnie czyni te ataki tak niebezpiecznymi i trudnymi do wykrycia.

Zrozumienie, jak działa grupa Exotic Lily, zwiększa szansę na uchronienie się przed zagrożeniem. Pamiętajmy, że w cyfrowym świecie nie wszystko jest tym, na co wygląda. Bądźmy ostrożni, zwłaszcza w przypadku e-maili, które skłaniają nas do kliknięcia linku lub pobrania załączników. To nasza pierwsza linia obrony. W następnym podrozdziale wyjaśnię, jak ochronić się przed tymi atakami i zapewnić bezpieczeństwo swoich danych.

Grupa Cobalt Dickens i jej sprytne ataki spear phishingowe

Czy nazwa Cobalt Dickens brzmi znajomo? To grupa, która specjalizuje się w wysyłaniu perfekcyjnie spreparowanych e-maili do środowisk uniwersyteckich. Wyobraź sobie, że dostajesz wiadomość, która wygląda dokładnie tak, jakby przyszła z działu IT Twojej uczelni (rysunek 7.7). Proszą Cię o zaktualizowanie hasła. Wygląda wiarygodnie. I na to właśnie liczą!

Drogi Czytelniku,
informujemy, że Twój dostęp do bazy danych Biblioteki wkrótce wygaśnie. Pełny dostęp do zasobów jest ograniczony do pracowników Biblioteki, pracowników Uczelni, w tym profesorów emerytowanych i profesorów wizytujących, aktualnie zarejestrowanych studentów oraz osób uczestniczących w kursach przygotowawczych organizowanych przy Uczelni. Aby uzyskać pełny dostęp, prosimy o zalogowanie się na konto biblioteczne z użyciem tego linku:

Rysunek 7.7. E-mail phishingowy w stylu grupy Cobalt Dickens

Na e-mailach się nie kończy. Grupa potrafi stworzyć całe witryny, które wyglądają dokładnie tak, jak witryna uczelni. Kiedy niczego nieświadomy student się loguje, myśli, że jest na prawdziwej stronie. Tymczasem przekazuje swoją nazwę użytkownika i login prosto w ręce wyłudzaczy.

Co jest najbardziej interesujące? Grupa wykorzystuje narzędzia OSINT, co sprawia, że trudniej złapać jej członków. Gdy wkradają się do systemów uczelni, wyciągają stamtąd mnóstwo ważnych informacji. Czatują na ciekawe badania naukowe i innowacyjne pomysły, nad którymi pracuje się na uczelniach. To jednak nie koniec. Zdobywają też dane osobowe studentów i wykładowców, co stanowi istotny problem.

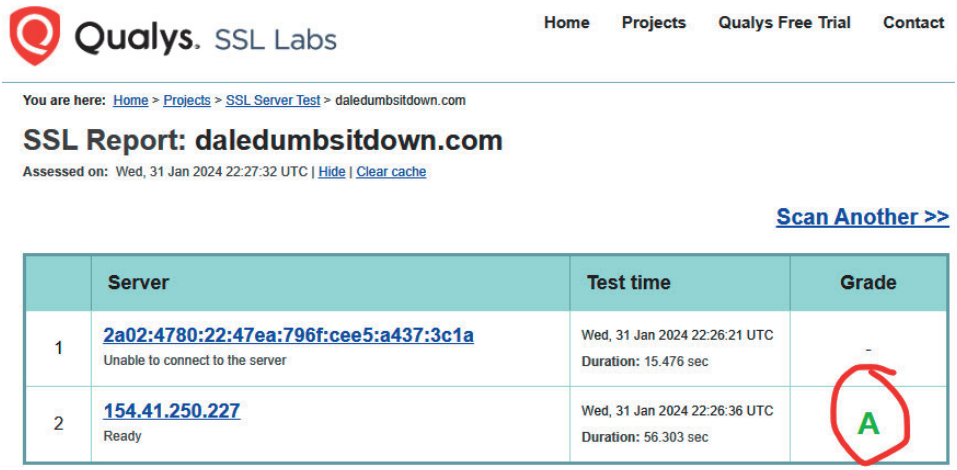
Zrozumienie, co robią takie grupy jak Cobalt Dickens czy Exotic Lily, pomaga przygotować się na zagrożenie. Musimy poznać sztuczki magika, żeby nie dać się im zwieść. Dzięki analizie tych podstępnych metod możemy lepiej się przygotować i chronić siebie samych oraz swoje organizacje przed tymi ludźmi. Uważajmy na e-maile i na to, gdzie się logujemy, jeżeli nie chcemy, aby sprytny lis wpadł do wirtualnego kurnika i narobił dużych szkód.

Prowadzenie dochodzeń w sprawie incydentów i naruszeń cyberbezpieczeństwa

Istotną częścią reagowania na cyberzagrożenia jest badanie pod kątem technicznym witryn, które padły ofiarą ataku. Siły szybkiego reagowania mogą znaleźć podatności na stronach, analizując ich techniczne własności narzędziami OSINT. Informacje na temat hostowania witryny czy certyfikatów SSL to tylko dwa z wielu technicznych aspektów, nad którymi można się pochylić. Na przykład znajdujesz witrynę firmową na współdzielonym serwerze, który ma podatności. Używając narzędzi takich jak zapytania WHOIS czy DomainTools, możesz określić dostawcę usług hostingowych i przeanalizować znane podatności powiązane z tym dostawcą. W podobny sposób możesz użyć narzędzi takich jak SSL Test firmy SSL Labs (*https://www.ssllabs.com/ssltest*) do sprawdzenia certyfikatów SSL witryny, ujawniając potencjale luki w bezpieczeństwie, takie jak przestarzałe algorytmy szyfrowania lub certyfikaty wydane przez niezaufane podmioty (rysunek 7.8).

Sprawdzenie starszych wersji witryny, np. dostępnych w archiwum Wayback Machine (*https://web.archive.org*), również może dostarczyć użytecznych informacji. Dane kontaktowe kierownictwa wyższego rzędu, często obecne w starszych wersjach witryn firmowych, mogą stanowić podstawę do określenia zakresu naruszenia.

Kolejnym ważnym elementem badania docelowej witryny jest znalezienie jej subdomen. Mogą tam być przechowywane prywatne informacje, takie jak portale VPN czy adresy serwerów. Na temat architektury docelowej sieci można się również wiele dowiedzieć, korzystając z zapytań w wyszukiwarce Google, w tym także do odnalezienia tych subdomen. Przydatne są też narzędzia Shodan i Censys.



Rysunek 7.8. SSL Labs sprawdza bezpieczeństwo certyfikatów

Ludzie często zapominają dokładnie przeanalizować dostępne zasoby, takie jak oferty pracy i CV. Mogą one ujawnić informacje dotyczące systemu operacyjnego, sprzętu sieciowego, ustawień zapory sieciowej serwera oraz innych aspektów systemów informatycznych organizacji.

Ponadto dzięki narzędziom OSINT można odnaleźć wrażliwe informacje na temat firmy, które przypadkowo ujawniono na publicznych serwerach. Analizując ich metadane, możemy poznać wcześniej nieznane szczegóły na temat tych plików, takie jak dane autora, program użyty do utworzenia lub edycji pliku albo system operacyjny na urządzeniu.

Ujawnianie źródeł, zakresów i wpływu cyberincydentów

Gdy reagujemy na cyberincydenty, użycie odpowiedniego zestawu narzędzi może nam bardzo pomóc w określeniu, co się właściwie stało. Chcąc zrozumieć istotę sprawy, analitycy korzystają z narzędzi OSINT, aby analizować wzorce ruchu sieciowego i określić, co odbiega od *normy*. Wszelkie odchylenia mogą sugerować, że dzieje się coś podejrzanego. Poszukiwanie powtarzających się wzorców może też pokazać, czy są one generowane przez mechanizmy automatyczne, takie jak złośliwe oprogramowanie.

Niezwykle użyteczne jest wykrywanie anomalii, które wymykają się oczekiwanym normom administracyjnym dla danego systemu. Dzięki uważnemu przeglądaniu zebranych danych prowadzący badanie wychwytują błędy i zachowania, które odstają od normy.

Gromadzenie i badanie śladów pozostawionych przez złośliwe oprogramowanie na urządzeniu gospodarzu (ang. *host artifacts*) stanowi kolejny element układanki. Obejmuje to uruchomione procesy, usługi, hasze plików wykonywalnych oraz działania na

kontach. Każdy taki ślad zapewnia informacje na temat nieupoważnionego dostępu lub zmian.

Aby dokonać bardziej szczegółowej analizy, możemy przyjrzeć się niezweryfikowanym połączeniom internetowym, poleceniom powłoki PowerShell (w przypadku podstępnych ataków bez użycia plików) oraz procesom na plikach, które mogą sygnalizować kradzież danych. Dziwne wzorce logowania także potencjalnie wskazują na nieupoważniony dostęp.

Równie ważne są ślady pozostawione w sieci. Zbierający dane powinni sprawdzić ruch DNS, protokoły zdalnego dostępu, logi dostępu do witryny oraz inne źródła pod kątem sygnałów wskazujących na nieuprawniony dostęp lub kradzież danych.

Gdy staramy się zrozumieć cyberatak, korzystamy z dwóch sposobów gromadzenia danych: kryminalistyki cyfrowej i OSINT. Kryminalistyka cyfrowa szczegółowo analizuje dowody znalezione na urządzeniach i w sieciach. Obejmuje to sprawdzenie listy działających programów, aktywności kont i wszelkich nietypowych połączeń z internetem. Celem jest znalezienie śladów nieuprawnionego dostępu lub kradzieży danych.

OSINT gromadzi informacje ze źródeł dostępnych dla wszystkich, takich jak wiadomości, witryny internetowe czy portale społecznościowe. Nie zajmuje się bezpośrednio zaatakowanymi komputerami i sieciami, lecz opiera się na źródłach zewnętrznych.

Obie te metody są niezwykle istotne. Podczas gdy kryminalistyka cyfrowa pomaga zrozumieć, co dokładnie zdarzyło się w ramach cyberataku, OSINT zapewnia szerszy kontekst i tło. Tych dwóch detektywów tworzy zgrany zespół: jeden ogląda miejsce zbrodni, a drugi rozmawia z ludźmi i szuka wskazówek w najróżniejszych miejscach. Wykorzystując obie te metody, możemy uzyskać pełny obraz cyberataku i wzmocnić zabezpieczenia na przyszłość.

Tworzenie solidnych cyberzabezpieczeń dzięki OSINT

Jeżeli chcemy określić, jakie ryzyka mogą mieć największy wpływ na firmę, OSINT to niezbędny element układanki. Monitorując różne platformy w dark webie i clear webie („czystej sieci"), organizacje mogą znaleźć informacje o cyberprzestępcach, którzy wzięli je na celownik, niezabezpieczone poufne dane, publicznie udostępnione repozytoria czy dane uwierzytelniające ujawnione w ramach wycieków. Dzięki użyciu OSINT firmy mogą poznać wektory zagrożenia i wykryć niezabezpieczone dane, co poprawi ich zrozumienie trendów w obszarze cyberbezpieczeństwa w ogóle.

Istnieją aktywne i pasywne formy OSINT:

- Aby zbierać dane wywiadowcze w sposób pasywny, można utworzyć alerty Google dotyczące trendów w obszarze cyberbezpieczeństwa dla danej branży.
- Z kolei aktywny OSINT wymaga bardziej gruntownego podejścia do zbierania danych. Może na przykład obejmować włamanie się na forum w dark webie, które wymaga specjalnego dostępu, aby uzyskać bardziej kompleksowy obraz ewentualnych zagrożeń.

Jak powiązać to z chronioną przez nas organizacją? Najważniejsze jest dostosowanie wniosków do niepowtarzalnego zestawu podatności naszej organizacji. Wiążemy rezultaty badań z profilem ryzyka firmy, gdyż to, co dla jednych będzie stanowić niewielkie zagrożenie, może być krytyczną podatnością dla innych. Ten proces nie jest statyczny. To niekończąca się pętla składająca się z etapów monitorowania, analizy i adaptacji. Przypomina rozgrywanie partii szachów: każdy ruch jest wykalkulowany, a każda figura ma kluczowe znaczenie dla obrony.

Współpraca ze społecznością zajmującą się cyberbezpieczeństwem

Kolejnym strategicznym elementem jest współpraca. Dzielenie się wnioskami pozyskanymi z OSINT z innymi organizacjami przypomina tworzenie sojuszy w walce ze wspólnym wrogiem. Chodzi o utworzenie jednego frontu, gdzie współdzielona wiedza to tarcza chroniąca wszystkich.

Aktywność na forach z zakresu cyberbezpieczeństwa i udział w wydarzeniach branżowych ma istotne znaczenie. Nie jesteśmy już tylko biernymi słuchaczami, lecz współautorami. Nasze wnioski pozyskane na bazie OSINT mogą dla kogoś innego stanowić brakujący element układanki. Wydarzenia branżowe to tygiel, w którym mieszają się pomysły, strategie i doświadczenia. Angażując się we współpracę, zyskujemy dostęp do szerszego zakresu wiedzy, co z kolei napędza nasze własne strategie z zakresu cyberbezpieczeństwa. To symbiotyczna relacja, w ramach której każda udostępniona innym informacja wzmacnia zbiorową odporność.

Adaptacja do zmieniającego się spektrum zagrożeń

Pierwszym krokiem w tej adaptacji jest być na bieżąco. Cyberzagrożenia ewoluują szybko. To, co wczoraj było przełomową strategią obrony, dzisiaj może być nieaktualne. Aktualizowanie wiedzy o najnowsze trendy i zmiany w obszarze cyberbezpieczeństwa ma zasadnicze znaczenie. Oprócz dołączenia do forów online regularnie uczestnicz w seminariach z zakresu bezpieczeństwa, czytaj czasopisma branżowe oraz obserwuj wpływowe osoby w dziedzinie cyberbezpieczeństwa w mediach społecznościowych.

- **Publikacje branżowe**. Regularnie odwiedzaj witryny takie jak The Hacker News (*https://thehackernews.com*) i Krebs on Security (*https://krebsonsecurity.com*) w poszukiwaniu najnowszych informacji (rysunek 7.9). Ja monitoruję te źródła prawie codziennie.
- **Webinaria i szkolenia online**. Platformy takie jak Pluralsight (*https://www.pluralsight.com*) oferują bogactwo materiałów do nauki, dzięki którym zadbamy o swój rozwój i zachowamy czujność. Znam naprawdę świetnego autora, który opublikował tam ponad 30 kursów (rysunek 7.10). Zdecydowanie go polecam!

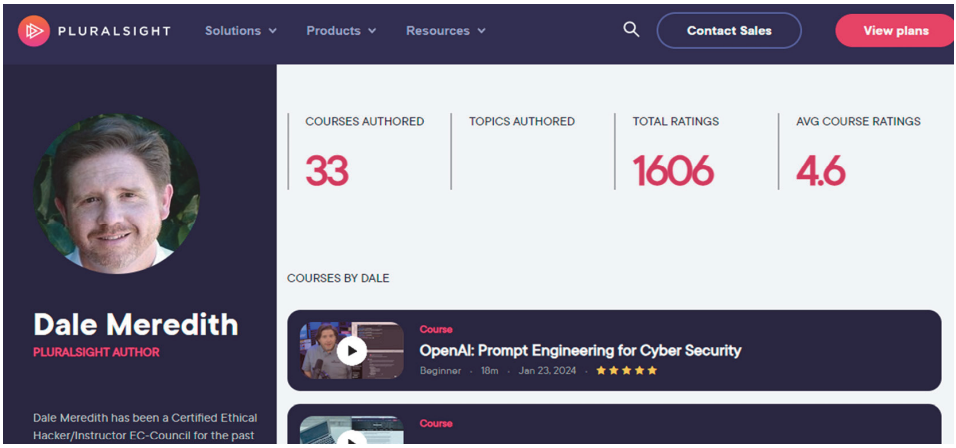


Rysunek 7.9. The Hacker News to wspaniałe źródło bieżących informacji

Istnieją też konferencje, w których powinniśmy uczestniczyć. Osobiście co roku biorę udział w konferencjach Black Hat i DEF CON w Las Vegas. Często znajdziecie mnie tam na warsztatach.

- **Media społecznościowe**. Obserwuj specjalistów ds. cyberbezpieczeństwa na portalach takich jak LinkedIn i X. Dzięki temu uzyskasz dostęp do bieżących aktualizacji i innych użytecznych zasobów. Tutaj również jest taki ktoś, kogo warto byłoby poobserwować! To *@dalemeredith*.

Pamiętaj, że w świecie cyberbezpieczeństwa informacja to nie tylko potęga. To także ochrona. Wykazuj się ciekawością, bądź na bieżąco, a nawet jeden krok przed innymi.



Rysunek 7.10. Profil mojego ulubionego autora kursów w serwisie Pluralsight

Aktualizowanie strategii cyberbezpieczeństwa opartej na OSINT

Strategia cyberbezpieczeństwa oparta na OSINT nie powinna być zapisana w kamieniu. Wymaga regularnych aktualizacji na podstawie najnowszych informacji i trendów. Oto kilka ważnych obszarów:

- **Ponowna ocena profilów ryzyka**. Podatności ewoluują wraz z organizacjami. Regularnie dokonuj przeglądów profilu ryzyka na podstawie najświeższych danych OSINT.
- **Ulepszanie zabezpieczeń**. Wnioski z wcześniejszych cyberincydentów mogą pomóc wzmocnić zabezpieczenia. Może to obejmować aktualizację zapory sieciowej, zwiększenie zabezpieczeń sieci czy przeszkolenie pracowników na temat nowej techniki phishingowej.
- **Wykorzystanie nowych narzędzi**. Wachlarz narzędzi OSINT jest coraz szerszy. Wypatruj nowych narzędzi i technologii, które mogą ułatwić gromadzenie i analizę danych wywiadowczych.

Nie zapomnij o narzędziach

Gdy chcemy stworzyć solidne zabezpieczenia z użyciem OSINT, istnieje kilka narzędzi i platform, które są niewiarygodnie skuteczne. W poprzednich rozdziałach przedstawiłem szereg narzędzi OSINT, które umożliwiają tworzenie silnych zabezpieczeń.

Uwaga

Większość tych narzędzi jest domyślnie zainstalowana w systemach Kali Linux, Parrot i Trace Labs, a wszystkie te dystrybucje to wspaniałe platformy dla entuzjastów OSINT.

Oto skrótowa lista niektórych użytecznych narzędzi OSINT wraz z informacjami o tym, gdzie można uzyskać do nich dostęp oraz jak z nich korzystać:

- **Shodan** (*https://www.shodan.io*). Ta „wyszukiwarka dla hakerów", jak ją czasem nazywają, zapewnia bieżące dane na temat urządzeń podłączonych do internetu. Wyobraź sobie, że starasz się wykryć niezabezpieczone bazy danych. Możesz rzucić okiem na Shodan i wyszukać konkretne rodzaje baz danych (np. MongoDB), które są publicznie dostępne. W odpowiedzi na zapytanie takie jak `product:MongoDB` Shodan wyświetli listę baz danych MongoDB dostępnych online. To zapytanie może wykryć bazy danych pozbawione odpowiednich zabezpieczeń. Realizując takie zapytania, zawsze działaj w sposób etyczny i legalny.
- **Google Hacking Database** (*https://www.exploit-db.com/google-hacking-database*). Korzystając z zapytań wymienionych w tej bazie danych, takich jak `intitle:index.of` plus wersja serwera lub konkretny rodzaj pliku, możemy wykryć publicznie dostępne katalogi zawierające poufne dane. Ta metoda pomaga zidentyfikować potencjalne wycieki danych albo obszary wymagające lepszego zabezpieczenia. Zawsze wykorzystujmy takie informacje w sposób odpowiedzialny i etyczny.
- **Maltego** (*https://www.maltego.com*). To wybitne narzędzie w zakresie wizualizacji powiązań. Pomaga mapować sieci i lepiej zrozumieć relacje między różnymi cyfrowymi encjami. Możemy zacząć od zbadania domeny, aby poznać jej cyfrowy ślad. Przy tworzeniu encji podaj nazwę domeny. Następnie zastosuj transformacje, aby poznać powiązane encje, takie jak e-maile, subdomeny czy konta w mediach społecznościowych. Narzędzie rozrysuje powiązania, zapewniając wgląd w infrastrukturę domeny i powiązany z nią podmiot.
- **theHarvester**. Narzędzie to można pobrać z GitHuba (*https://github.com/laramies/theHarvester*). Służy do znajdowania adresów e-mailowych, subdomen, osób lub stanowisk w ramach firmy oraz innych danych. Te informacje pomagają w analizie cyberbezpieczeństwa, dostarczając potencjalnych punktów wyjścia i powiązań do analizy celu.
- **Framework OSINT** (*https://osintframework.com*). Choć sam w sobie nie jest narzędziem, kategoryzuje narzędzia OSINT pod kątem poszukiwanych informacji, takich jak dane domenowe, wyszukiwanie osób czy analiza mediów społecznościowych. Ten framework pomaga użytkownikom znaleźć narzędzia odpowiednie do ich potrzeb badawczych, co ułatwia zbieranie danych wywiadowczych z publicznych źródeł. Witryna jest nieustannie aktualizowana o łącza do nowych narzędzi.
- **SpiderFoot** (*https://intel471.com/attack-surface-documentation*). Korzystanie z narzędzia SpiderFoot do celów OSINT należałoby zacząć od skanu konkretnego obiektu, takiego jak nazwa domeny czy adres IP. SpiderFoot automatyzuje proces zbierania różnorodnych informacji powiązanych z celem, włączając w to domeny, adresy e-mailowe i ewentualne podatności. Narzędzie usprawnia fazę rozpoznania w ramach oceny cyberbezpieczeństwa, ułatwiając wykrywanie zagrożeń.

- **Recon-ng** (*https://github.com/lanmaster53/recon-ng*). Korzystanie z narzędzia Recon-ng rozpoczęlibyśmy zazwyczaj od wybrania modułu odpowiedniego do rodzaju poszukiwanych danych, np. adresów e-mailowych powiązanych z domeną. Po konfiguracji modułu i niezbędnych parametrów Recon-ng wykona zadanie i zbierze dane z różnych publicznych źródeł. Narzędzie jest szczególnie użyteczne do budowania cyfrowych profili celów na podstawie publicznie dostępnych informacji.
- **TinEye** (*https://tineye.com*). To narzędzie do odwrotnego wyszukiwania grafiki przydaje się do weryfikowania prawdziwości obrazów i sprawdzania, czy pojawiły się w innych miejscach w sieci. Po prostu ładujemy zdjęcie lub wpisujemy adres URL, a TinEye przeszukuje swoją bazę danych pod kątem pasujących obrazów. W przypadku OSINT to narzędzie jest szczególnie przydatne w dochodzeniach dotyczących weryfikacji mediów cyfrowych.
- **X Pro** (wcześniej TweetDeck; *https://pro.twitter.com*). Służy do bieżącego monitorowania i analizy kanałów portalu X, w tym obserwowania hasztagów i wzmianek. Zapewnia cenny wgląd w trendy w mediach społecznościowych. Narzędzie jest szczególnie przydatne do celów OSINT, jeżeli chodzi o analizowanie nastrojów społecznych, określania trendów oraz bieżącego gromadzenia informacji z portalu X.
- **Creepy** (*https://github.com/ilektrojohn/creepy*). Jest to narzędzie OSINT do geolokalizacji. Creepy agreguje dane na temat lokalizacji z różnych portali społecznościowych i rozrysowuje ruch danej osoby na podstawie śladu cyfrowego. Jest szczególnie przydatne w dochodzeniach, które wymagają zrozumienia wzorców przemieszczania się danej osoby w czasie.

Chociaż te narzędzia mają ogromny potencjał gromadzenia danych OSINT, należy pamiętać, aby korzystać z nich rozsądnie i etycznie, z poszanowaniem obowiązującego prawa. W obszarze cyberbezpieczeństwa aktualna wiedza i rozeznanie odgrywają priorytetową rolę, gdyż dostępne technologie stale się zmieniają.

Podsumowanie

Ten rozdział pozwolił Ci zrozumieć, jak ważne w obszarze bezpieczeństwa jest nie zostać z tyłu. Korzystanie z takich źródeł jak The Hacker News czy Pluralsight może pomóc nam nie wypaść z obiegu. Aby radzić sobie z nowymi zagrożeniami, musimy nieustannie doskonalić swoje strategie cyberbezpieczeństwa. Udział w webinarach i obserwowanie ekspertów online to doskonały sposób, aby dowiedzieć się więcej. Pamiętaj, że w obszarze cyberbezpieczeństwa gotowość do nauki i zmian to klucz do cyfrowego bezpieczeństwa nas samych i naszych organizacji.

Mam nadzieję, że po przeczytaniu tej książki znaczenie OSINT jest dla Ciebie oczywiste. Zaczęliśmy od podstaw, poznaliśmy *szeroki wachlarz* narzędzi i technik, a potem rozmawialiśmy o bezpieczeństwie i anonimowości w sieci. Zobaczyliśmy, jak OSINT

pozwala wykryć nieoczywiste cyberzagrożenia, chroniąc nas i nasze organizacje. Dzięki białemu wywiadowi możemy być o krok przed hakerami i dbać o bezpieczeństwo swojego cyfrowego świata. OSINT to kluczowy element walki z cyfrowymi niebezpieczeństwami.


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion