

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

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