



Spis treści

O autorze	15
O korektorze merytorycznym	16
Podziękowania	17
Wstęp	19
Rozdział 1. Pierwsze kroki	25
Dlaczego ta książka jest inna?	25
Co znajdziesz w tej książce, a czego nie	26
Poznaj moich kolegów ekspertów	26
Co musisz wiedzieć?	27
Płatne narzędzia i dane historyczne	27
A co z Maltego?	28
Wymagania	28
Ważne zasoby	29
OSINT	29
OSINT.link	30
Termbin	30
Hunchly	31
Listy słów i generatory	31
Serwery proxy	32
Wprowadzenie do kryptowalut	32
Jak funkcjonują kryptowaluty?	33
Eksploratory łańcuchów bloków	34
Podążając za pieniędzmi	36
Podsumowanie	39

Rozdział 2.	Śledztwa i hakerzy	40
	Droga śledczego	40
	Bądź wielki lub wracaj do domu	41
	Porada eksperta: Cat Murdock	41
	Włamanie, którego nie było	42
	Porada eksperta: Troy Hunt	43
	Dylematy moralne	44
	Porada eksperta: John Strand	44
	Różne ścieżki śledztwa	45
	Porada eksperta: Leslie Carhart	45
	Śledzenie cyberprzestępców	46
	The Dark Overlord	46
	Lista ofiar	47
	Krótkie wprowadzenie	48
	Struktura grupy i jej członkowie	49
	Podsumowanie	57
 Część I.	 Eksploracja sieci	 59
 Rozdział 3.	 Ręczna eksploracja sieci	 61
	Wykrywanie zasobów	62
	Przeszukiwanie bazy ARIN	62
	Zaawansowane wyszukiwanie	64
	DNSDumpster	65
	Hacker Target	67
	Shodan	68
	Censys	70
	Fierce	71
	Sublist3r	72
	Enumall	73
	Wyniki	74
	Zniekształcanie domen i porywanie adresów URL	75
	Podsumowanie	78
 Rozdział 4.	 Wykrywanie aktywności sieciowej (zaawansowane techniki skanowania)	 79
	Pierwsze kroki	79
	Uzyskanie listy aktywnych hostów	79
	Pełne skanowanie portów	80
	Omijanie zapory sieciowej i systemu IDS	82
	Analiza przyczyn odpowiedzi	82
	Omijanie zapory sieciowej	84

	Porada eksperta: William Martin	84
	Porównywanie wyników	89
	Formatowanie raportów	90
	Podsumowanie	91
Rozdział 5.	Zautomatyzowane narzędzia do rozpoznawania sieci	92
	Uwaga dotycząca jednego z celów testów	93
	SpiderFoot	93
	SpiderFoot HX (wersja premium)	99
	Intrigue	103
	Komentarz autora: Jonathan Cran	104
	Zakładka Entities	104
	Badanie domeny uberpeople.net	107
	Analiza wyników	111
	Eksportowanie wyników	112
	Recon-NG	114
	Wyszukiwanie modułów	117
	Korzystanie z modułów	117
	Wyszukiwanie portów za pomocą serwisu Shodan	120
	Podsumowanie	121
Część II.	Eksploracja internetu	123
Rozdział 6.	Pozyskiwanie informacji o witrynach internetowych	125
	BuiltWith	125
	Wyszukiwanie wspólnych witryn na podstawie identyfikatora Google Analytics	126
	Historia adresu IP i powiązane witryny	127
	WIG	128
	CMSMap	132
	Skanowanie pojedynczej witryny	133
	Skanowanie wielu witryn w trybie wsadowym	133
	Wykrywanie podatności na ataki	134
	WPScan	135
	Komunikat o braku systemu WordPress i omijanie zapory WAF	138
	Podsumowanie	142
Rozdział 7.	Przeszukiwanie katalogów	143
	Dirhunt	143
	Wfuzz	146
	Porada eksperta: Alex Heid	148

Photon	148
Przeszukiwanie witryny	149
Intrigue	152
Podsumowanie	154
Rozdział 8. Zaawansowane opcje wyszukiwarek	155
Porada eksperta: Alex Heid	155
Najważniejsze opcje	156
Znak odejmowania	156
Cudzysłów	156
Operator site:	156
Porada eksperta: Alex Heid	156
Operator intitle:	157
Operator allintitle:	157
Operator filetype:	158
Operator inurl:	158
Operator cache:	160
Operator allinurl:	160
Operator intext:	160
Potęga dorków	161
Nie zapominaj o Bing i Yahoo!	164
Zautomatyzowane narzędzia wyszukujące	164
Inurlbr	164
Podsumowanie	168
Rozdział 9. WHOIS	169
WHOIS	169
Zastosowania danych WHOIS	170
Dane historyczne	170
Whoisology	176
Zaawansowane wyszukiwanie domen	180
Warte pieniędzy? Oczywiście!	181
DomainTools	181
Wyszukiwanie domen	181
Wyszukiwanie wsadowe	182
Odwrotne wyszukiwanie adresów IP	182
Baza WHOIS na sterydach	183
Historia danych WHOIS	185
Siła widoków	185
Zgłębianie historycznych danych WHOIS	186
Odwrotna usługa WHOIS	188
Krzyżowa weryfikacja wszystkich informacji	190
Podsumowanie	191

Rozdział 10. Przejrzystość certyfikatów i internetowe archiwa	192
Przejrzystość certyfikatów	192
Co to wszystko ma wspólnego z cyberdochodzeniem?	193
Narzędzie CTFR	193
Serwis crt.sh	194
Przejrzystość w akcji: omijanie zabezpieczeń Cloudflare	195
Uwaga od Cloudflare	198
Skrypt CloudFlair i serwis Censys	200
Wayback Machine i archiwa wyszukiwarek	201
Przeszukiwanie buforów wyszukiwarek internetowych	202
CachedView.com	204
Przeszukiwanie serwisu Wayback Machine	204
Porada eksperta: Rob Fuller	204
Wyszukiwanie adresów URL	207
Podsumowanie	209
 Rozdział 11. Narzędzie Iris	 210
Podstawy narzędzia Iris	210
Wskazówki nawigacyjne	212
Konfiguracja narzędzia	212
Ustawienia wyników historycznych	213
Wskazówki	213
Odciski certyfikatów SSL	215
Historia WHOIS	218
Historia zrzutów ekranu	220
Historia hostingu	221
Wszystko razem	222
Uwaga: nie zatrzymuj się w tym miejscu	224
Najważniejsze odkrycie	227
Podsumowanie	228
 Część III. Poszukiwanie złota	 229
 Rozdział 12. Metadane dokumentów	 231
Exiftool	231
Metagoofil	233
Moduły narzędzia Recon-NG do analizy metadanych	235
Moduł metacrawler	235
Moduł interesting_files	237
Moduły geolokalizacyjne pushpin	238
Intrigue	242

FOCA	245
Utworzenie projektu	246
Wyodrębnianie metadanych	249
Podsumowanie	250
Rozdział 13. Ciekawe miejsca do poszukiwań	251
theHarvester	252
Skanowanie	253
Serwisy wklejkowe	256
psbdm.ws	256
Fora internetowe	256
Porada eksperta: Chris Roberts	257
Badanie historii forum (i grupy TDO)	257
Porada eksperta: Chris Roberts	258
Ustalenie tożsamości Cypera	259
Repozytoria kodów	261
SearchCode	262
Gitrob	265
Dzienniki zatwierdzeń	267
Strony wiki	268
Wikipedia	269
Podsumowanie	271
Rozdział 14. Publiczne magazyny danych	272
Porada eksperta: Bob Diachenko	272
Wyciek danych z Exactis i narzędzie Shodan	273
Atrybucja danych	273
Parametry narzędzia Shodan	274
CloudStorageFinder	276
Zasobniki AWS S3	277
Przestrzenie Digital Ocean	277
Bazy danych NoSQL	279
MongoDB	279
Porada eksperta: Bob Diachenko	279
Terminalowe narzędzia bazy MongoDB	283
Elasticsearch	285
NoScrape	288
MongoDB	289
Elasticsearch	290
Cassandra	294
AWS S3	295
Podsumowanie	296

Część IV. Tropienie ludzi	297
Rozdział 15. Badanie ludzi, obrazów i lokalizacji	299
Porada eksperta: John Strand	299
PIPL	300
Porada eksperta: Cat Murdock	300
Wyszukiwanie ludzi	300
Publiczne rejestry i weryfikacja przeszłości	303
Ancestry.com	304
Przeszukiwanie rejestrów karnych	305
Wyszukiwanie obrazów	305
Porada eksperta: Cat Murdock	306
Grafika Google	306
TinEye	309
EagleEye	312
Narzędzie Cree.py i geolokalizacja	314
Pierwsze kroki	315
Śledzenie adresów IP	317
Porada eksperta: John Strand	318
Podsumowanie	318
Rozdział 16. Przeszukiwanie mediów społecznościowych	319
OSINT.rest	320
Inny obiekt badań	323
Twitter	326
Wtyczka SocialLinks do Maltego	328
Skiptracer	329
Wyszukiwanie	329
Userrecon	336
Reddit Investigator	338
Przełom w badaniu grupy TDO	340
Podsumowanie	341
Rozdział 17. Śledzenie profili i resetowanie haseł	342
Od czego zacząć (badanie TDO)?	342
Tworzenie tabeli śledztwa	343
Przeszukiwanie forów internetowych	344
Inżynieria społeczna	346
Porada eksperta: Chris Hadnagy	346
Hakerska inżynieria społeczna: historia Argona	347
Porada eksperta: John Strand	350
Koniec grupy TDO i forum KickAss	351

Wskazówki resetowania hasła	353
Wypełnienie arkusza Weryfikacje	354
Gmail	354
Facebook	356
PayPal	357
Twitter	360
Microsoft	362
Instagram	363
jQuery	364
ICQ	365
Podsumowanie	366
Rozdział 18. Hasła, rzuty i Data Viper	367
Hasła	368
Uzupełnienie profilu f3ttywap w tabeli śledztwa	368
Ważny zły zwrot	371
Pozyskiwanie danych	372
Jakość danych i kolekcje 1 – 5	372
Porada eksperta: Troy Hunt	374
Gdzie szukać wysokiej jakości danych?	375
Data Viper	375
Brakujące ogniwo: fora	375
Identyfikacja cr00ka	376
Skromne początki: Data Viper 1.0	384
Podsumowanie	384
Rozdział 19. Komunikacja z hakerami	386
Wyjście z cienia	386
Kto to był WhitePacket?	387
Kontakty Bev Robb	387
Stradinatras	388
Obfuscation i grupa TDO	389
Kim był Bill?	391
YoungBugsThug	392
Skąd wiedziałem, że to był Chris?	393
Czy ma to związek z botnetem Mirai?	394
Ustalenie przepływu informacji	397
Wykorzystanie hakerskich niesnasek	398
Powrót do TDO	400
Rozstrzygnięcie ostatniej kwestii	401
Podsumowanie	402

Rozdział 20. Zamieszanie wokół włamania za 10 milionów dolarów	403
GnosticPlayers	404
Zhakowane witryny	406
Wpisy GnosticPlayers	408
GnosticPlayers2	409
Tajemniczy trzeci członek grupy	411
Żarty się skończyły	412
Nawiązanie kontaktu	413
Gabriel/Bildstein vel Kuroi'sh	413
Odchwaszczanie dezinformacji	415
Zebranie wszystkiego w całość	416
Data Viper	418
Ufaj, ale sprawdzaj	419
Narzędzie Iris	421
Koniec historii	423
Co się naprawdę stało?	423
Outofreach	423
Kto zhakował GateHuba?	424
Wszystkie ścieżki poprowadziły znów do NSFW	426
Podsumowanie	427
 Epilog	 429