

Spis treści |

O autorze	13
O korektorach merytorycznych	14
Wstęp	15

CZĘŚĆ 1. Podstawy działania zespołów Blue Team i Purple Team

ROZDZIAŁ 1.

Podstawy działania zespołów Red, Blue i Purple Team	23
Jak zacząłem pracę z systemem Kali Linux	24
Czym jest Kali Linux?	26
Dlaczego system Kali Linux jest tak popularny?	28
Zespół Red Team	30
Zespół Blue Team	31
Zespół Purple Team	35
Podsumowanie	38

ROZDZIAŁ 2.

Wprowadzenie do informatyki śledczej	39
Czym jest informatyka śledcza?	39
Dlaczego potrzebujemy zespołów Red i Purple Team?	41
Metodologia i procedury w informatyce śledczej	43
Normy i standardy z zakresu informatyki śledczej	46
Porównanie systemów operacyjnych dla informatyki śledczej	47
DEFT Linux	49
CAINE Linux	51
CSI Linux	57
Kali Linux	62

Dlaczego należy korzystać z wielu narzędzi w dochodzeniach cyfrowych	66
Komercyjne narzędzia śledcze	67
Techniki anti-forensics — zagrożenie dla informatyki śledczej	69
Podsumowanie	72

ROZDZIAŁ 3.

Instalowanie systemu Kali Linux	74
Wymagania techniczne	74
Pobieranie systemu Kali Linux	75
Pobieranie wymaganych narzędzi i obrazów	77
Pobieranie obrazu Kali Linux Everything	78
Instalowanie systemu Kali Linux na przenośnych nośnikach pamięci	80
Instalowanie systemu Kali Linux jako samodzielnego systemu operacyjnego	87
Instalowanie systemu Kali Linux w maszynie wirtualnej VirtualBox	88
Przygotowanie maszyny wirtualnej z systemem Kali Linux	89
Instalowanie systemu Kali Linux w maszynie wirtualnej	93
Instalowanie i konfigurowanie systemu Kali Linux	98
Podsumowanie	110

ROZDZIAŁ 4.

Instalowanie dodatkowych komponentów systemu Kali Linux

i zadania do wykonania po instalacji	111
Instalacja wstępnie skonfigurowanej wersji Kali Linux w maszynie wirtualnej VirtualBox	112
Instalowanie systemu Kali Linux na platformie Raspberry Pi 4	115
Aktualizacja systemu Kali Linux	120
Włączanie konta użytkownika root w systemie Kali Linux	123
Instalowanie metapakietu kali-tools-forensics	127
Podsumowanie	128

ROZDZIAŁ 5.

Instalowanie pakietu Wine w systemie Kali Linux	129
Pakiet Wine i jego zalety w systemie Kali Linux	129
Instalowanie pakietu Wine	130
Konfigurowanie pakietu Wine	135
Testowanie pakietu Wine	138
Podsumowanie	143

CZĘŚĆ 2.

Podstawowe zagadnienia oraz najlepsze praktyki informatyki śledczej i reagowania na incydenty

ROZDZIAŁ 6.

Systemy plików i nośniki pamięci masowej	147
Historia i rodzaje nośników danych	148
Firma IBM i historia nośników pamięci	148
Wymienne nośniki danych	149
Napędy z taśmą magnetyczną	149
Dyskietki	150
Optyczne nośniki danych	151
Płyty Blu-ray	153
Pamięci flash	153
Pamięci flash z portem USB	155
Karty pamięci flash	156
Dyski twarde	159
Dyski twarde IDE	160
Dyski twarde SATA	161
Dyski SSD	163
Systemy plików i systemy operacyjne	165
Microsoft Windows	166
Macintosh (macOS)	167
Linux	167
Typy i stany danych	168
Metadane	168
Slack space	168
Dane ulotne i nieulotne oraz kolejność gromadzenia dowodów cyfrowych	169
Znaczenie pamięci RAM oraz pliku stronicowania i pamięci podręcznej w dochodzeniach DFIR	172
Podsumowanie	173

ROZDZIAŁ 7.

Reagowanie na incydenty, pozyskiwanie cyfrowego materiału dowodowego oraz normy i standardy z zakresu informatyki śledczej	174
Procedury pozyskiwania dowodów cyfrowych	175
Reagowanie na incydenty i osoby reagujące w pierwszej kolejności	176

Zbieranie i dokumentowanie dowodów cyfrowych	178
Narzędzia do fizycznego pozyskiwania danych	179
Pozyskiwanie danych z komputerów włączonych i wyłączonych	183
Kolejność pozyskiwania danych ulotnych	183
Pozyskiwanie danych z urządzeń włączonych i wyłączonych	183
Formularz kontroli łańcucha dowodowego	185
Znaczenie urządzeń blokujących zapis na nośnikach danych	186
Tworzenie binarnych obrazów danych i zachowywanie integralności dowodów cyfrowych	188
Skrót MD5 (Message Digest)	188
Skrót SHA (Secure Hashing Algorithm)	190
Najlepsze praktyki pozyskiwania danych i standardy DFIR	191
Normy i standardy w informatyce śledczej	192
Podsumowanie	193

CZĘŚĆ 3.

Dochodzenia cyfrowe i reagowanie na incydenty z użyciem narzędzi dostępnych w systemie Kali Linux

ROZDZIAŁ 8.

Narzędzia do gromadzenia dowodów cyfrowych	197
Zastosowanie polecenia fdisk do rozpoznawania partycji	198
Identyfikacja urządzenia za pomocą polecenia fdisk	200
Zastosowanie silnych algorytmów funkcji skrótu do zapewnienia integralności dowodów cyfrowych	202
Tworzenie obrazów binarnych nośników pamięci za pomocą programu DC3DD	204
Weryfikacja wartości skrótu kryptograficznego obrazów binarnych	209
Wymazywanie dysku za pomocą programu DC3DD	210
Tworzenie obrazów binarnych nośników pamięci za pomocą programu DD	212
Tworzenie obrazów dysków za pomocą programu Guymager	214
Uruchamianie programu Guymager	215
Tworzenie binarnych obrazów nośników danych za pomocą programu Guymager	216

Tworzenie obrazów nośników danych i pamięci operacyjnej za pomocą programu FTK Imager uruchamianego za pośrednictwem pakietu Wine	221
Instalowanie programu FTK Imager	222
Tworzenie obrazów zawartości pamięci RAM za pomocą programu FTK Imager	229
Tworzenie obrazów pamięci RAM i plików stronicowania za pomocą programu Belkasoft RAM Capturer	231
Podsumowanie	232

ROZDZIAŁ 9.

Odzyskiwanie skasowanych plików i narzędzia do odtwarzania danych234

Podstawy działania plików	235
Pobieranie plików do ćwiczeń	236
Odzyskiwanie plików i carving danych za pomocą programu Foremost	237
Odzyskiwanie plików graficznych za pomocą programu Magic Rescue	241
Odzyskiwanie danych za pomocą programu Scalpel	246
Odzyskiwanie danych za pomocą programu bulk_extractor	250
Odzyskiwanie NTFS za pomocą programu scrounge-ntfs	254
Odzyskiwanie obrazów za pomocą programu Recoverjpeg	258
Podsumowanie	262

ROZDZIAŁ 10.

Analiza śledcza zawartości pamięci przy użyciu pakietu Volatility 3264

Co nowego w pakiecie Volatility 3 Framework	265
Pobieranie przykładowych plików zrzutu pamięci	266
Instalacja pakietu Volatility 3 w systemie Kali Linux	267
Analiza śledcza pliku obrazu pamięci przy użyciu pakietu Volatility 3	273
Weryfikacja obrazu i systemu operacyjnego	273
Identyfikacja i analiza uruchomionych procesów	275
Podsumowanie	284

ROZDZIAŁ 11.

Analiza artefaktów systemowych, malware i oprogramowania

ransomware285

Identyfikacja urządzeń i systemów operacyjnych za pomocą programu p0f	286
swap_digger — narzędzie do analizy pliku wymiany systemu Linux	290
Instalowanie i sposób użycia programu swap_digger	290
Wyodrębnianie haseł za pomocą programu MimiPenguin	292
Analiza złośliwych plików PDF	293

Automatyczna analiza złośliwych plików w serwisie Hybrid Analysis	297
Analiza oprogramowania ransomware przy użyciu pakietu Volatility 3	299
Wtyczka pslist	301
Podsumowanie	307

CZĘŚĆ 4.

Zautomatyzowane narzędzia DFIR

ROZDZIAŁ 12.

Pakiet Autopsy Forensic Browser	311
Wprowadzenie do pakietów Autopsy i The Sleuth Kit	312
Pobieranie przykładowych plików do użycia i tworzenie nowego dochodzenia za pomocą nakładki Autopsy Forensic Browser	313
Uruchamianie nakładki Autopsy Forensic Browser	314
Tworzenie nowego dochodzenia w nakładce Autopsy Forensic Browser	317
Analiza dowodów przy użyciu nakładki Autopsy Forensic Browser	323
Podsumowanie	328

ROZDZIAŁ 13.

Przeprowadzanie dochodzeń cyfrowych przy użyciu pakietu Autopsy 4	329
Funkcje interfejsu użytkownika pakietu Autopsy 4	330
Instalowanie pakietu Autopsy 4 w systemie Kali Linux za pomocą pakietu Wine	331
Pobieranie przykładowych plików obrazów do analizy	335
Tworzenie nowych dochodzeń i wprowadzenie do interfejsu pakietu Autopsy 4	336
Analizowanie katalogów i odzyskiwanie usuniętych plików i artefaktów za pomocą Autopsy 4	343
Podsumowanie	347

CZĘŚĆ 5.

Narzędzia do analizy śledczej połączeń sieciowych

ROZDZIAŁ 14.

Narzędzia do wykrywania i eksplorowania sieci	351
Zastosowanie programu netdiscover do wykrywania i identyfikowania urządzeń w sieci	352

Zastosowanie skanera Nmap do wykrywania i identyfikowania urządzeń w sieci	355
Zastosowanie skanera Nmap do wykrywania otwartych portów i usług	357
Zastosowanie wyszukiwarki Shodan.io do wyszukiwania urządzeń IoT, zapór sieciowych, systemów CCTV i serwerów	360
Zastosowanie filtrów Shodan do wyszukiwania urządzeń IoT	362
Podsumowanie	365

ROZDZIAŁ 15.

Analiza pakietów sieciowych za pomocą programu Xplico	367
Instalowanie pakietu Xplico w systemie Kali Linux	368
Instalowanie systemu DEFT Linux 8.1 w maszynie wirtualnej VirtualBox	369
Pobieranie przykładowych plików do analizy	374
Uruchamianie pakietu Xplico w systemie DEFT Linux	375
Zastosowanie pakietu Xplico do automatycznej analizy ruchu sieciowego, poczty elektronicznej i połączeń głosowych	378
Zautomatyzowana analiza ruchu http	380
Zautomatyzowana analiza ruchu SMTP	384
Zautomatyzowana analiza ruchu VoIP	385
Podsumowanie	387

ROZDZIAŁ 16.

Narzędzia do analizy ruchu sieciowego	388
Przechwytywanie pakietów za pomocą programu Wireshark	389
Analiza pakietów sieciowych za pomocą programu NetworkMiner	396
Analiza pakietów sieciowych za pomocą programu PcapXray	402
Analiza online plików PCAP w witrynie packettotal.com	407
Analiza online plików PCAP w witrynie apackets.com	411
Tworzenie raportów i prezentacja wyników	415
Podsumowanie	416