

Spis treści

Słowo wstępne — Adrian Kapczyński	13
Słowo wstępne — Dagmara Modrzejewska	15
Przedmowa	17
CZĘŚĆ I Tworzenie własnego laboratorium do testów	
ROZDZIAŁ 1. Co będzie potrzebne, aby wykorzystać w pełni informacje zawarte w książce?	21
ROZDZIAŁ 2. VirtualBox — instalacja i konfiguracja	24
2.1. Czym jest i do czego służy VirtualBox?	24
2.2. Pobieranie VirtualBoxa	25
2.3. Instalacja VirtualBoxa	26
2.4. Instalacja opcjonalnych funkcji VirtualBoxa	31
2.5. Co dalej?	32
2.6. Kali Linux a Parrot OS	33
2.7. Pobieranie plików instalacyjnych	34
2.8. Przydzielenie przestrzeni dyskowej dla dystrybucji Linux w VirtualBoksie	35
2.9. Konfiguracja maszyn wirtualnych i sieci w VirtualBoksie	40
2.9.1. Tworzenie sieci	40
2.10. Maszyny wirtualne	44
2.10.1. Przydzielanie zasobów sprzętowych maszynom wirtualnym	45
2.10.2. Pamięć w VirtualBoksie	50
2.11. Podsumowanie	51
ROZDZIAŁ 3. Instalacja Kali Linux i Parrot OS	52
3.1. Instalacja Kali Linux	52
3.2. Instalacja Parrot OS	65
3.3. Migawki	73
3.4. Współdzielony katalog	77
3.5. Czy to bezpieczne?	81
3.6. Instalacja a gotowe obrazy	82
3.7. Podsumowanie	82
ROZDZIAŁ 4. Obsługa dystrybucji Linux — podstawy, które musisz znać, aby swobodnie pracować w Linuksie	83
4.1. Graficzny interfejs	83
4.2. Konsola	84
4.2.1. Polecenie pwd	84
4.2.2. Polecenie ls	85
4.2.3. Polecenie cd	86
4.2.4. Powtórka z poznanych poleceń	87
4.2.5. Ścieżka w Linuksie	88
4.2.6. Ścieżki względne i bezwzględne	88
4.2.7. Magiczny Tab	89
4.2.8. Aktualizacja	89
4.2.9. Rodzaje aktualizacji	93
4.2.10. Wersja dystrybucji	93
4.2.11. Podział konsoli	94
4.2.12. Konto root	95
4.2.13. Inne przydatne polecenia	95
4.3. Podsumowanie	96
ROZDZIAŁ 5. Do czego adapter sieciowy?	97
5.1. Czym różni się Wi-Fi od WLAN?	97

5.1.1. Technologie Wi-Fi	97
5.2. Jakie opcje powinien mieć adapter, aby w pełni wykorzystać możliwości opisane w książce?	98
5.3. Lista adapterów kompatybilnych z Kali Linux	99
5.4. Adaptery, z których ja korzystam	100
5.5. Instalacja sterowników	101
5.5.1. Dodanie adapterów do maszyn wirtualnych	101
5.5.2. Kali Linux	103
5.5.3. Parrot OS	109
5.6. Adapter podłączony do huba	109
5.7. Podsumowanie	110
ROZDZIAŁ 6. Maszyny wirtualne, które przydadzą się do testów	111
6.1. Microsoft Windows 11	111
6.2. Instalacja Ubuntu 24.04.1 LTS	125
6.3. Podsumowanie	134
ROZDZIAŁ 7. Na zakończenie — etyka	135
CZĘŚĆ II Łamanie zabezpieczeń sieci WLAN	
ROZDZIAŁ 8. Niezbędna wiedza związana z sieciami	141
8.1. Jak powstaje sieć?	141
8.2. Komunikacja w sieci	145
8.3. Po co adres IP?	147
8.4. Adresacja IP	148
8.4.1. DHCP	148
8.4.2. Adresacja statyczna	148
8.5. Z czego składa się adres IP?	148
8.6. Zewnętrzny a lokalny adres IP	149
8.7. Podsumowanie	149
ROZDZIAŁ 9. Informacje wokół nas	150
9.1. Sieci w naszym otoczeniu	150
9.2. Tryby adaptera bezprzewodowego	151
9.3. Adapter działający w trybie monitor	152
9.3.1. Zmiana trybu adaptera manualnie	152
9.3.2. Zmiana trybu adaptera za pomocą jednego polecenia	154
9.3.3. Odłączenie zbędnych procesów	155
9.4. Wyłapywanie pakietów	155
9.5. Wyłapywanie i przechwytywanie pakietów na określonych częstotliwościach	157
9.6. Kanały i częstotliwości	158
9.7. Różnica pomiędzy 2,4, 5 i 6 GHz	161
9.8. Sieci i pakiety z konkretnego kanału	161
9.9. Podsumowanie	162
ROZDZIAŁ 10. Sieci ukryte i filtrowanie adresów MAC	163
10.1. Ustawienie routera — tworzenie ukrytej sieci	163
10.1.1. TP-Link Archer AX12	163
10.1.2. Tenda N300	167
10.2. Odkrywamy ESSID sieci	169
10.3. Ustawienie filtracji adresów MAC	172
10.3.1. Ustawienia routera TP-Link	172
10.3.2. Ustawienia routera Tenda	174
10.4. Zamiana adresu MAC	175
10.4.1. Co zrobić, gdy adres MAC nadal wraca do swojej pierwotnej formy?	176
10.4.2. Unikatowość adresu MAC	176
10.4.3. Po co zmieniać adres MAC?	177

10.4.4. Zmiana adresu MAC za pomocą narzędzia macchanger	178
10.5. Jak dostać się do sieci z filtrowaniem po adresie MAC?	178
10.6. Co zrobić w takiej sytuacji?	180
10.7. Podsumowanie	181
ROZDZIAŁ 11. Wired Equivalent Privacy — WEP	182
11.1. WEP?	182
11.2. Konfiguracja routera	183
11.3. Sposób na zdobycie hasła w sieci WEP	185
11.3.1. WEP z szyfrowaniem 64-bitowym	185
11.3.2. WEP z szyfrowaniem 128-bitowym	189
8 ETYCZNY HACKING I TESTY PENETRACYJNE	
11.4. Jak się zabezpieczyć?	190
11.5. Podsumowanie	191
ROZDZIAŁ 12. Wi-Fi Protected Access — WPA i WPA2	192
12.1. Różnice pomiędzy szyfrowaniem WPA a WPA2	192
12.2. WPS (Wi-Fi Protected Setup) — dziurawe uproszczenie podłączania urządzeń	193
12.2.1. TP-Link — włączanie WPS-a	194
12.2.2. Tenda — włączanie WPS-a	199
12.2.3. Inne sposoby na WPS	202
12.2.4. Mamy PIN — i co dalej?	203
12.3. Atak słownikowy na sieć WPA/WPA2	204
12.3.1. Handshake	204
12.3.2. Zdobywanie handshake'ów	205
12.3.3. Atak słownikowy	209
12.4. Co zrobić, by poczuć się bezpieczniej, korzystając z WPA2?	211
12.5. Podsumowanie	211
ROZDZIAŁ 13. Crunch — tworzenie własnych słowników	212
13.1. Tworzenie pierwszego słownika	212
13.2. Użycie wygenerowanego słownika	213
13.3. Tworzenie słownika, gdy znamy część hasła	213
13.4. Słownik ze wszystkimi możliwymi kombinacjami i jego obsługa	214
13.5. Wzorce	216
13.6. Podsumowanie	216
ROZDZIAŁ 14. Wi-Fi Protected Access 3 — WPA3	217
14.1. Porównanie WPA2 z WPA3	217
14.2. Konfiguracja routera	218
14.3. WPA3-Personal	219
14.4. WPA3-Personal + WPA2-PSK [AES]	220
14.5. Jak się zabezpieczyć?	221
14.6. Podsumowanie	222
ROZDZIAŁ 15. Sieci otwarte	223
15.1. Dlaczego sieci otwarte są niebezpieczne?	223
15.2. Prosty sposób, w jaki można zdobyć poufne dane	223
15.3. Bezpieczeństwo w sieci otwartej?	228
15.4. Podsumowanie	229
ROZDZIAŁ 16. Evil Twin — zły brat bliźniak!	230
16.1. Początkowe przygotowania	230
16.2. Pliki konfiguracyjne	231
16.2.1. Plik konfiguracyjny hostapd	231
16.2.2. Plik konfiguracyjny dnsmasq	232
16.2.3. Plik konfiguracyjny apache2	232
16.2.4. Strona logowania	233
16.3. Uruchomienie fałszywego punktu dostępowego	235

16.4. Jak łatwo dać się nabrać?	236
16.5. Captive Portal	241
16.6. Jak nie dać się nabrać?	242
16.7. Podsumowanie	242
ROZDZIAŁ 17. WPA Enterprise	243
17.1. Evil Twin	243
17.2. Instalacja niezbędnego oprogramowania	244
17.3. Konfiguracja	244
17.4. Windows i Ubuntu	245
17.5. Atak deautoryzacji	247
17.6. Otrzymane dane	247
17.7. Łamanie hasła	247
17.8. Co zrobić, by zapobiec najgorszemu?	248
17.9. Podsumowanie	248
ROZDZIAŁ 18. Dodatkowe oprogramowanie	249
18.1. Alternatywa dla aireplay-ng — mdk4	249
18.1.1. Atak deautoryzacyjny	249
18.1.2. Restart urządzenia	250
18.1.3. Beacon Flooding	250
18.1.4. Podsumowanie	250
18.2. Wykrywanie urządzeń w przeglądarce — Kismet	251
18.3. Alternatywa dla narzędzia reaver — bully	253
18.4. Alternatywna dla aircrack-ng — cowpatty	254
18.5. Niezwykłe narzędzie do łamania haseł — hashcat	255
18.5.1. Konwersja pliku handshake do formatu obsługiwanego przez hashcat	256
18.5.2. Pobranie i instalacja narzędzia hashcat	256
18.5.3. System Windows	256
18.5.4. Dystrybucja Linuxa	259
18.6. Wiele w jednym — airgeddon	260
18.7. Automatyczne narzędzie do audytu — wifite	264
18.8. Prostota ataku — fluxion	265
18.9. Podsumowanie	268
CZĘŚĆ III Zagrożenia w sieci LAN	
ROZDZIAŁ 19. Wykrywanie urządzeń w sieci za pomocą Nmap	271
19.1. Uruchomienie Nmap	271
19.1.1. Graficzny interfejs Nmap	271
19.1.2. Korzystanie z Nmap z poziomu wiersza poleceń	272
19.2. Podstawowe informacje o celu	272
19.3. Podstawowe informacje o celu — Windows 11	274
19.4. Podstawowe informacje o celu — Ubuntu	278
19.5. Wyświetlanie bardziej szczegółowych informacji	278
10 ETYCZNY HACKING I TESTY PENETRACYJNE	
19.6. Skanowanie określonego zakresu adresów	280
19.7. Skanowanie określonych adresów z pliku	280
19.8. Wbudowany sposób skanowania sieci	281
19.9. Drugi wbudowany sposób skanowania	282
19.10. Skanowanie portów UDP	282
19.10.1. Podstawowy sposób skanowania	283
19.10.2. Jednoczesne skanowanie UDP i TCP	283
19.10.3. Wersja oprogramowania	284
19.11. Wykrywanie systemu	284
19.11.1. Podstawowe polecenie do wykrycia systemu	285

19.11.2. Agresywny sposób wykrycia systemu	287
19.12. Podsumowanie	287
ROZDZIAŁ 20. Man in the Middle	288
20.1. Czym jest atak MITM?	288
20.2. Protokół ARP	289
20.3. Atak ARP	290
20.4. Sniffing	293
20.5. Podsumowanie	294
ROZDZIAŁ 21. Bettercap	295
21.1. Zaczynamy	295
21.2. Pierwsze uruchomienie	296
21.2.1. Dlaczego jest to tak ważne?	296
21.3. Konfiguracja Bettercapa	297
21.4. Ważne opcje Bettercapa	298
21.5. Moduły Bettercapa	298
21.5.1. Urządzenia w sieci	299
21.5.2. Man in the Middle	300
21.6. Co z tym Man in the Middle?	301
21.7. Czym różni się HTTP od HTTPS?	301
21.8. Pozyskiwanie danych od użytkownika	302
21.9. Man in the Middle — błąd połączenia	303
21.10. Sposób na HTTPS	303
21.11. Upraszczamy korzystanie z Bettercapa	306
21.12. Czym jest HSTS i jak go obejść?	307
21.13. Przekierowanie na własny serwer	309
21.14. Wstrzykiwanie kodu JavaScript	311
21.15. Podsumowanie	312
ROZDZIAŁ 22. Stary, ale jary Ettercap	313
22.1. Podstawowa konstrukcja polecenia	313
22.2. MITM na całą sieć	315
22.3. MITM w Linuksie	317
22.4. Atak na pojedynczy cel	317
22.5. Podszycie się pod serwer DNS	318
22.6. Próba obejścia zabezpieczeń routera przed atakami ARP	319
22.7. Filtry podczas uruchomienia polecenia	320
22.8. HTTPS i HSTS	320
22.9. Podsumowanie	322
ROZDZIAŁ 23. Mitmproxy — kontrolowanie przepływu informacji	323
23.1. Pobranie i instalacja	323
23.2. Opis dostępnych narzędzi	324
23.3. Jak to działa?	324
23.4. Mitmweb	325
23.5. Mitmdump	334
23.6. Dlaczego Mitmproxy nie działa z HTTPS i HSTS?	335
23.7. Podsumowanie	335
ROZDZIAŁ 24. Przykład przeprowadzenia ataku	336
24.1. Wyszukanie aktywnych urządzeń w sieci	336
24.2. Narzędzie BeEF	337
24.3. Przygotowanie strony błędu	340
24.4. Man in the Middle	342
24.5. Użycie BeEF-a	342
24.6. Atak z użyciem Mitmproxy	345
24.7. Podsumowanie	346
DODATEK A Tworzenie sieci z wybranym typem szyfrowania	347

A.1. Co będzie niezbędne do stworzenia własnej sieci?	347
A.2. Tworzenie własnej sieci — pierwszy sposób	348
A.2.1. Linux Mint	348
A.2.2. Tworzenie bootowalnego pendrive'a	348
A.2.3. Bootowanie pendrive'a	350
A.2.4. Pierwsze uruchomienie	350
A.2.5. Tworzenie własnej sieci	351
A.3. Tworzenie własnej sieci — drugi sposób	354
A.3.1. Linux	354
A.4. Podsumowanie	355
Zakończenie	356