

Spis treści

Wskazówki prawne i zalecenia	11
Art. 267.	11
Art. 268.	12
Art. 268a.	12
Art. 269.	12
Art. 269a.	13
Art. 269b.	13
Zalecenia dotyczące prowadzenia własnych testów	13
Ważna uwaga dotycząca aplikacji antywirusowych	14
Moduł 1. Wstęp	15
Słowem wstępu	15
Czym są rootkity	15
Schemat budowy rootkita	16
Przykłady rootkitów	16
Co trzeba wiedzieć na początek	17
Kompatybilność i aktualna wersja kodu źródłowego	17
Literatura uzupełniająca	18
Praktyka – zapis modułu video	18
Moduł 2. Podstawy	31
Szybki kurs assemblera	31
Podział rejestrów	31
Format zapisu instrukcji	33
Tworzenie shellcodu	35
Oczym musimy pamiętać pisząc shellcode?	36
Wyjaśnienie potrzebnych pojęć	36
Technika code injection	37
Wywołania systemowe w systemach 64-bitowych	37
Praktyka – zapis modułu video	37

Moduł 3. Ukrywanie obecności w systemie	47
Wstęp	47
Teoria	47
Piszemy kod rootkita	49
Ukrywamy proces	56
Praktyka – zapis modułu video – cz. 1	64
Ukrywamy pliki	77
Praktyka – zapis modułu video – cz. 2	83
Ukrywamy wpis w rejestrze	94
Praktyka – zapis modułu video – cz. 3	96
Uwagi odnośnie trybu 64-bitowego	102
Moduł 4. Tworzenie backdoora	107
Tworzymy backdoora, czyli tylne drzwi do systemu	107
Keylogger	108
Wykonujemy zrzut ekranu	118
Wysyłanie logów	119
Autorun	121
Praktyka – zapis modułu video – cz. 1	122
Zdalna konsola	134
Praktyka – zapis modułu video – cz. 2	140
Moduł 5. Środki ochrony systemów Windows	151
Jakie mechanizmy obronne posiadają systemy Windows?	151
Praktyka – zapis modułu video	154
Moduł 6. Tworzenie niewykrywalnych aplikacji	161
Jak antywirusy wykrywają zagrożenia?	161
Sygnatury	161
Praktyka – zapis modułu video – cz. 1	163
Heurystyka	168
Praktyka – zapis modułu video – cz. 2	169
Emulacja	172
Opis algorytmu RC4	173
Wywołania systemowe a architektura 64-bitowa	175
Praktyka – zapis modułu video – cz. 3	178

Moduł 7. Omijanie firewalla	183
Omijamy firewall	183
Modyfikacja zdalnej konsoli	191
Praktyka – zapis modułu video	192
Moduł 8. Utrzymanie programu przy życiu	201
Miejsca ukrycia programu	201
Uruchomienie programu jako usługi systemowej	207
Dll spoofing	207
Praktyka – zapis modułu video	210
Moduł 9. Obrona	221
Programy do wykrywania rootkitów	221
Praktyka – zapis modułu video	229
Moduł 10. Rozwój rootkita	241
Rozwój biblioteki dll i zdalnej konsoli	241
Omówienie kodu	242
Podsumowanie	252