Spis treści

SŁOWO WSTĘPNE **17**

PODZIĘKOWANIA **21**

WPROWADZENIE **23**
Kilka słów podziękowania 24
Kilka słów o książce 25
Część I. Podstawy 25
Część II. Przygotowania 26
Część III. Ataki 26
Część IV. Tworzenie exploitów 27
Część V. Ataki na urządzenia mobilne 28

0
ELEMENTARZ TESTÓW PENETRACYJNYCH **29**
Etapy testów penetracyjnych 30
Faza wstępna 31
Zbieranie informacji 32
Mapowanie zagrożeń 33
Wykrywanie i analiza podatności 33

Atak ... 33
Powłamaniowa eksploracja skompromitowanego systemu ... 33
Raportowanie ... 34
Podsumowanie ... 36

I Podstawy

1 TWORZENIE WIRTUALNEGO ŚRODOWISKA TESTOWEGO ... 39
Instalowanie pakietu VMware ... 39
Instalacja i konfiguracja systemu Kali Linux ... 40
Konfiguracja połączeń sieciowych maszyny wirtualnej ... 44
Instalowanie pakietu Nessus ... 48
Instalowanie dodatkowych pakietów oprogramowania ... 52
Instalowanie emulatorów systemu Android ... 54
SPF — Smartphone Pentest Framework ... 60
Instalacja wirtualnych celów ataku ... 61
Tworzenie maszyny-celu z systemem Windows XP ... 62
VMware Player w systemie Microsoft Windows ... 62
VMware Fusion w systemie Mac OS ... 65
Instalowanie i aktywacja systemu Windows ... 65
Instalowanie pakietu VMware Tools ... 68
Wyłączanie zapory sieciowej systemu Windows XP ... 70
Ustawianie haseł dla kont użytkowników ... 70
Ustawianie statycznego adresu IP ... 71
Konfiguracja systemu Windows XP do pracy jak w domenie ... 73
Instalowanie oprogramowania podatnego na ataki ... 75
Instalowanie pakietów Immunity Debugger oraz Mona ... 81
Tworzenie maszyny-celu z systemem Ubuntu 8.10 ... 82
Tworzenie maszyny-celu z systemem Windows 7 ... 83
Tworzenie konta użytkownika ... 83
Wyłączanie automatycznego instalowania aktualizacji ... 85
Ustawianie statycznego adresu IP ... 85
Dodawanie kolejnego interfejsu sieciowego ... 87
Instalowanie dodatkowego oprogramowania ... 88
Podsumowanie ... 90

2 PRACA Z SYSTEMEM KALI LINUX ... 91
Wiersz poleceń systemu Linux ... 92
System plików w Linuksie ... 92
Zmiana katalogów ... 92

Dokumentacja poleceń — strony podręcznika man ... 93
Uprawnienia użytkowników ... 94
Dodawanie kont użytkowników ... 95
Dodawanie konta użytkownika do pliku sudoers ... 96
Przełączanie kont użytkowników i korzystanie z polecenia sudo ... 96
Tworzenie nowych plików i katalogów ... 97
Kopiowanie, przenoszenie i usuwanie plików ... 97
Dodawanie tekstu do pliku ... 98
Dołączanie tekstu do pliku ... 99
Prawa dostępu do plików ... 99
Edytowanie plików ... 100
Wyszukiwanie tekstu ... 101
Edytowanie plików przy użyciu edytora vi ... 101
Przetwarzanie danych ... 102
Zastosowanie polecenia grep ... 103
Zastosowanie polecenia sed ... 104
Dopasowywanie wzorców za pomocą polecenia awk ... 104
Zarządzanie zainstalowanymi pakietami oprogramowania ... 105
Procesy i usługi ... 106
Zarządzanie połączeniami sieciowymi ... 106
Ustawianie statycznego adresu IP ... 107
Przeglądanie połączeń sieciowych ... 108
Netcat — uniwersalne narzędzie do połączeń TCP/IP ... 108
Sprawdzanie, czy system zdalny nasłuchuje na danym porcie ... 109
Proces nasłuchujący poleceń powłoki ... 110
„Wypychanie" powłoki do procesu nasłuchującego ... 111
Automatyzacja zadań za pomocą procesu cron ... 112
Podsumowanie ... 113

3
PROGRAMOWANIE ... 115
Skrypty powłoki bash ... 115
Polecenie ping ... 115
Prosty skrypt powłoki bash ... 116
Uruchamianie skryptu ... 117
Dodawanie nowych możliwości za pomocą polecenia if ... 117
Pętla for ... 118
Zwiększanie przejrzystości wyników działania ... 120
Skrypty w języku Python ... 123
Łączenie z wybranym portem sieciowym ... 124
Instrukcja if w języku Python ... 124
Pisanie i kompilowanie programów w języku C ... 125
Podsumowanie ... 127

4
PAKIET METASPLOIT FRAMEWORK 129
Uruchamianie pakietu Metasploit 131
Wyszukiwanie modułów pakietu Metasploit 132
Baza modułów pakietu Metasploit 133
Wbudowane polecenie search 134
Ustawianie opcji modułu exploita 137
Opcja RHOST 138
Opcja RPORT 138
Opcja SMBPIPE 138
Opcja Exploit Target 139
Ładunki (kod powłoki) 140
Wyszukiwanie kompatybilnych ładunków 140
Przebieg testowy 141
Rodzaje powłok 142
Bind shell 142
Reverse shell 143
Ręczne wybieranie ładunku 143
Interfejs wiersza poleceń Msfcli 145
Uzyskiwanie pomocy 146
Wyświetlanie opcji 146
Ładunki 147
Tworzenie samodzielnych ładunków za pomocą narzędzia Msfvenom 148
Wybieranie ładunku 149
Ustawianie opcji 149
Wybieranie formatu ładunku 150
Dostarczanie ładunków 151
Zastosowanie modułu multi/handler 151
Zastosowanie dodatkowych modułów 153
Podsumowanie 155

II
Przygotowania

5
ZBIERANIE INFORMACJI 159
OSINT — biały wywiad 160
Netcraft 160
Zapytania whois 161
Zapytania DNS 162
Poszukiwanie adresów poczty elektronicznej 165
Maltego 166

Skanowanie portów ... 170
Ręczne skanowanie portów ... 170
Skanowanie portów przy użyciu programu Nmap ... 172
Podsumowanie ... 180

6
WYSZUKIWANIE PODATNOŚCI I LUK W ZABEZPIECZENIACH ... 181
Od skanu z detekcją wersji do wykrycia potencjalnej luki w zabezpieczeniach ... 182
Nessus ... 182
Karta Policies — tworzenie polityki skanowania Nessusa ... 183
Skanowanie za pomocą Nessusa ... 186
Kilka słów na temat rankingu podatności i luk w zabezpieczeniach ... 189
Dlaczego powinieneś używać skanerów podatności? ... 189
Eksportowanie wyników skanowania ... 190
Odkrywanie podatności i luk w zabezpieczeniach ... 191
NSE — Nmap Scripting Engine ... 191
Uruchamianie wybranego skryptu NSE ... 194
Moduły skanerów pakietu Metasploit ... 196
Sprawdzanie podatności na exploity za pomocą polecenia check pakietu Metasploit ... 197
Skanowanie aplikacji internetowych ... 199
Pakiet Nikto ... 199
Ataki na pakiet XAMPP ... 200
Poświadczenia domyślne ... 201
Samodzielna analiza podatności ... 202
Eksploracja nietypowych portów ... 202
Wyszukiwanie nazw kont użytkowników ... 204
Podsumowanie ... 205

7
PRZECHWYTYWANIE RUCHU SIECIOWEGO ... 207
Przechwytywanie ruchu w sieci ... 208
Zastosowanie programu Wireshark ... 208
Przechwytywanie ruchu sieciowego ... 209
Filtrowanie ruchu sieciowego ... 210
Rekonstruowanie sesji TCP ... 211
Analiza zawartości pakietów ... 212
Ataki typu ARP Cache Poisoning ... 213
Podstawy protokołu ARP ... 214
Przekazywanie pakietów IP ... 216
Zatruwanie tablicy ARP przy użyciu polecenia arpspoof ... 217
Zastosowanie zatruwania tablic ARP do podszywania się pod domyślną bramę sieciową ... 219
Ataki typu DNS Cache Poisoning ... 220
Zatruwanie DNS — podstawy ... 222
Zatruwanie DNS przy użyciu polecenia dnsspoof ... 222

Ataki SSL ... 224
SSL — podstawy ... 224
Zastosowanie programu Ettercap do przeprowadzania ataków SSL MiTM ... 224
Ataki typu SSL Stripping ... 226
Zastosowanie programu SSLstrip ... 228
Podsumowanie ... 230

III
Ataki

8
EKSPLORACJA ŚRODOWISKA CELU ... 233
Powracamy do luki MS08-067 ... 234
Ładunki Metasploita ... 234
Meterpreter ... 236
Wykorzystywanie domyślnych poświadczeń logowania w dodatku WebDAV ... 237
Uruchamianie skryptów na atakowanym serwerze WWW ... 238
Kopiowanie ładunku przygotowanego za pomocą programu Msfvenom ... 239
Wykorzystywanie otwartej konsoli phpMyAdmin ... 241
Pobieranie plików za pomocą TFTP ... 243
Pobieranie wrażliwych plików ... 244
Pobieranie pliku konfiguracyjnego ... 244
Pobieranie pliku Windows SAM ... 245
Wykorzystywanie błędów przepełnienia bufora w innych aplikacjach ... 246
Wykorzystywanie luk w zabezpieczeniach innych aplikacji internetowych ... 248
Wykorzystywanie luk w zabezpieczeniach usług ... 250
Wykorzystywanie otwartych udziałów NFS ... 251
Podsumowanie ... 253

9
ATAKI NA HASŁA ... 255
Zarządzanie hasłami ... 255
Ataki typu online ... 256
Listy haseł ... 257
Odnajdowanie nazw kont użytkowników i haseł przy użyciu programu Hydra ... 261
Ataki typu offline ... 263
Odzyskiwanie haszy haseł systemu Windows z pliku SAM ... 264
Pozyskiwanie zahaszowanych haseł
z wykorzystaniem fizycznego dostępu do systemu ... 266
Algorytm LM kontra NTLM ... 269
Problem z haszami haseł w formacie LM ... 270
John the Ripper ... 271

Łamanie haseł systemu Linux ... 272
Łamanie haseł przechowywanych w plikach konfiguracyjnych ... 274
Tęczowe tablice ... 275
Usługi łamania haseł dostępne w sieci ... 275
Pozyskiwanie haseł z pamięci operacyjnej za pomocą programu Windows Credentials Editor ... 276
Podsumowanie ... 277

10
WYKORZYSTYWANIE LUK W ZABEZPIECZENIACH PO STRONIE KLIENTA ... 279
Omijanie filtrowania za pomocą ładunków pakietu Metasploit ... 280
Ładunek AllPorts ... 280
Ładunki HTTP i HTTPS ... 282
Ataki po stronie klienta ... 283
Luki w zabezpieczeniach przeglądarek sieciowych ... 284
Exploity dla plików PDF ... 292
Luki w zabezpieczeniach środowiska Java ... 298
Moduł browser_autopwn ... 304
Winamp ... 307
Podsumowanie ... 309

11
ATAKI SOCJOTECHNICZNE ... 311
Pakiet SET — Social-Engineer Toolkit ... 313
Ukierunkowane ataki phishingowe ... 314
Wybieranie ładunku ... 315
Ustawianie opcji ... 315
Wybieranie nazwy generowanego pliku ... 316
Jeden czy wielu adresatów? ... 316
Tworzenie szablonu wiadomości e-mail ... 316
Definiowanie celu ataku ... 317
Tworzenie procesu nasłuchującego ... 318
Ataki z wykorzystaniem stron internetowych ... 319
Masowe ataki e-mailowe ... 322
Ataki wielopłaszczyznowe ... 325
Podsumowanie ... 326

12
OMIJANIE PROGRAMÓW ANTYWIRUSOWYCH ... 327
Trojany ... 328
Msfvenom ... 328
Jak działają aplikacje antywirusowe? ... 331
Microsoft Security Essentials ... 332

VirusTotal ... 333
Omijanie programów antywirusowych ... 334
Kodowanie ... 335
Niestandardowe metody kompilowania ... 338
Szyfrowanie plików wykonywalnych przy użyciu programu Hyperion ... 341
Omijanie programów antywirusowych przy użyciu pakietu Veil-Evasion ... 343
Ukrywanie na widoku, czyli najciemniej jest pod latarnią ... 347
Podsumowanie ... 347

13
POWŁAMANIOWA EKSPLORACJA SKOMPROMITOWANEGO SYSTEMU ... 349
Meterpreter ... 350
Zastosowanie polecenia upload ... 351
Polecenie getuid ... 352
Inne polecenia Meterpretera ... 352
Skrypty Meterpretera ... 353
Moduły Metasploita wspomagające powłamaniową eksplorację systemu ... 354
Railgun ... 356
Lokalne podnoszenie uprawnień użytkownika ... 356
Polecenie getsystem w systemie Windows ... 357
Moduły typu Local Escalation dla systemu Windows ... 358
Omijanie mechanizmu UAC w systemie Windows ... 359
Podnoszenie uprawnień w systemie Linux ... 361
Wyszukiwanie informacji w skompromitowanym systemie ... 366
Wyszukiwanie plików ... 367
Przechwytywanie naciśniętych klawiszy (keylogging) ... 367
Gromadzenie poświadczeń logowania ... 368
Polecenie net ... 370
Inne sposoby ... 371
Sprawdzanie historii poleceń powłoki bash ... 372
Przechodzenie na kolejne systemy ... 372
PsExec ... 373
Uwierzytelnianie za pomocą skrótów — ataki typu pass the hash ... 374
SSHExec ... 376
Tokeny personifikacji ... 377
Incognito ... 378
Moduł SMB Capture ... 379
Pivoting ... 382
Dodawanie tras za pomocą polecenia route ... 384
Skanery portów w pakiecie Metasploit ... 384
Wykorzystywanie luk w zabezpieczeniach za pośrednictwem pivota ... 385
Moduł Socks4a i program ProxyChains ... 386

Utrzymywanie dostępu do skompromitowanego systemu ... 388
Tworzenie nowego konta użytkownika ... 388
Zapewnianie dostępu za pomocą Metasploita ... 389
Tworzenie zadań cron w systemie Linux ... 391
Podsumowanie ... 392

14
TESTOWANIE APLIKACJI INTERNETOWYCH ... 393
Burp Proxy ... 394
Wstrzykiwanie kodu SQL ... 399
Testowanie podatności na wstrzykiwanie kodu ... 400
Wykorzystywanie podatności na ataki typu SQL Injection ... 401
Zastosowanie programu SQLMap ... 402
Wstrzykiwanie kodu XPath ... 403
Ataki typu LFI — Local File Inclusion ... 405
Ataki typu RFI — Remote File Inclusion ... 408
Wykonywanie poleceń ... 409
Ataki typu XSS — Cross Site Scripting ... 411
Sprawdzanie podatności na ataki typu reflected XSS ... 412
Przeprowadzanie ataków typu XSS
za pomocą pakietu Browser Exploitation Framework (BeEF) ... 414
Ataki typu CSRF — Cross-Site Request Forgery ... 418
Skanowanie aplikacji internetowych za pomocą programu w3af ... 419
Podsumowanie ... 421

15
ATAKI NA SIECI BEZPRZEWODOWE ... 423
Przygotowania ... 423
Wyświetlanie listy dostępnych bezprzewodowych interfejsów sieciowych ... 425
Wyszukiwanie bezprzewodowych punktów dostępowych ... 425
Tryb monitora ... 426
Przechwytywanie pakietów ... 427
Sieci bezprzewodowe z otwartym dostępem ... 428
Protokół WEP ... 428
Słabości protokołu WEP ... 431
Łamanie kluczy szyfrowania WEP za pomocą pakietu Aircrack-ng ... 432
Protokół WPA — WiFi Protected Access ... 437
Protokół WPA2 ... 438
Podłączanie klientów w sieciach WPA/WPA2 Enterprise ... 438
Podłączanie klientów w sieciach WPA/WPA2 Personal ... 439
Czteroetapowa negocjacja uwierzytelniania ... 439
Łamanie kluczy szyfrowania WPA/WPA2 ... 440
Protokół WPS — WiFi Protected Setup ... 444
Problemy z protokołem WPS ... 445
Łamanie PIN-u protokołu WPS za pomocą programu Bully ... 445
Podsumowanie ... 445

IV
Tworzenie exploitów

16

PRZEPEŁNIENIE BUFORA NA STOSIE W SYSTEMIE LINUX 449

Kilka słów o pamięci 450
Przepełnienie bufora na stosie w systemie Linux 453
Program podatny na przepełnienie bufora na stosie 454
Wymuszanie awarii programu 456
Praca z debuggerem GDB 457
Wywoływanie awarii programu w debuggerze GDB 463
Kontrolowanie wskaźnika EIP 465
Przejmowanie kontroli nad działaniem programu 467
Kolejność (starszeństwo) bajtów 469
Podsumowanie 471

17

PRZEPEŁNIENIE BUFORA NA STOSIE W SYSTEMIE WINDOWS 473

Wyszukiwanie znanych podatności i luk w zabezpieczeniach serwera War-FTP 474
Wymuszanie awarii programu 476
Lokalizowanie rejestru EIP 479
Wyszukiwanie offsetu adresu powrotu za pomocą cyklicznego wzorca 480
Weryfikacja znalezionych offsetów 484
Przejmowanie kontroli nad działaniem programu 486
Uruchomienie powłoki 492
Podsumowanie 498

18

ZASTĘPOWANIE STRUKTURALNEJ OBSŁUGI WYJĄTKÓW 499

Exploity nadpisujące procedury SEH 500
Przekazywanie sterowania do procedur SEH 506
Wyszukiwanie ciągu znaków exploita w pamięci 506
POP POP RET 511
SafeSEH 512
Zastosowanie krótkich skoków 516
Wybieranie ładunku 517
Podsumowanie 520

19
FUZZING, PRZENOSZENIE KODU EXPLOITÓW I TWORZENIE MODUŁÓW METASPLOITA 521
Fuzzowanie programów 522
Wyszukiwanie błędów poprzez analizę kodu źródłowego 522
Fuzzowanie serwera TFTP 523
Próba wywołania awarii programu 525
Dostosowywanie kodu publicznie dostępnych exploitów do własnych potrzeb 529
Wyszukiwanie adresu powrotu 532
Zamiana kodu powłoki 533
Edytowanie kodu exploita 533
Tworzenie nowych modułów Metasploita 535
Tworzenie podobnego modułu exploita 538
Tworzenie kodu naszego exploita 538
Techniki zapobiegania atakom 543
Technika Stack Cookies 543
Mechanizm ASLR — randomizacja układu przestrzeni adresowej 544
Mechanizm DEP — zapobieganie wykonywaniu danych 545
Obowiązkowe cyfrowe podpisywanie kodu 545
Podsumowanie 546

V
Ataki na urządzenia mobilne

20
PAKIET SMARTPHONE PENTEST FRAMEWORK 549
Wektory ataków na urządzenia mobilne 550
Wiadomości tekstowe 550
Połączenia NFC 551
Kody QR 552
Pakiet Smartphone Pentest Framework 552
Konfiguracja pakietu SPF 552
Emulatory systemu Android 554
Dołączanie urządzeń mobilnych 555
Budowanie aplikacji SPF dla systemu Android 555
Instalowanie aplikacji SPF 556
Łączenie serwera SPF z aplikacją mobilną 557
Ataki zdalne 559
Domyślne poświadczenia logowania SSH na telefonach iPhone 559
Ataki po stronie klienta 561
Powłoka po stronie klienta 561
Zdalna kontrola nad urządzeniami mobilnymi za pomocą mechanizmu USSD 563

Złośliwe aplikacje ... 565
Tworzenie złośliwych agentów SPF ... 566
Powłamaniowa eksploracja urządzeń mobilnych ... 573
Zbieranie informacji ... 573
Zdalne sterowanie ... 575
Pivoting z wykorzystaniem urządzeń mobilnych ... 575
Podnoszenie uprawnień ... 582
Podsumowanie ... 583

MATERIAŁY DODATKOWE ... 585

SKOROWIDZ ... 591

POBIERANIE OPROGRAMOWANIA DLA ŚRODOWISKA TESTOWEGO ... 608