

Spis treści

Przedmowa	11
Część I Łamanie programów	17
Rozdział 1. Asembler	19
Rejestry	20
Rozkazy asemblera	23
Źródła dodatkowych informacji	24
Rozdział 2. Reinżynieria oprogramowania systemu Windows	25
Historia reinżynierii oprogramowania	27
Narzędzia reinżynierii oprogramowania	27
Przykłady reinżynierii oprogramowania	39
Źródła dodatkowych informacji	47
Rozdział 3. Reinżynieria oprogramowania systemu Linux	49
Podstawowe narzędzia i techniki	50
Dobra deasemblacja	71
Trudności	84
Pisanie nowych narzędzi	89
Źródła dodatkowych informacji	129
Rozdział 4. Reinżynieria oprogramowania systemu Windows CE	131
Architektura systemu Windows CE	132
Podstawy reinżynierii oprogramowania systemu Windows CE	137
Reinżynieria oprogramowania Windows CE w praktyce	145
Reinżynieria programu serial.exe	161
Źródła dodatkowych informacji	174

Rozdział 5. Ataki przepełnienia bufora	175
Przepełnienie bufora.....	175
Wyjaśnienie pojęcia bufora.....	177
Uderzenie w stos.....	179
Przepełnienie sterty	180
Zapobieganie przepełnieniom bufora	180
Przepełnienie bufora w praktyce.....	182
Źródła dodatkowych informacji	189
 Część II Polowanie w sieci	 191
Rozdział 6. Protokoły TCP/IP.....	193
Krótką historią TCP/IP	193
Enkapsulacja	194
Protokół TCP	195
Protokół IP	197
Protokół UDP	199
Protokół ICMP	199
Protokół ARP	200
Protokół RARP	200
Protokół BOOTP.....	201
Protokół DHCP	201
Uzgadnianie TCP/IP	201
Ukryte kanały	203
Protokół IPv6	203
Ethereal	205
Analiza pakietów	206
Fragmentacja	208
Źródła dodatkowych informacji	214
 Rozdział 7. Socjotechnika.....	 215
Podstawy	216
Prowadzenie ataków	218
Zaawansowana socjotechnika	226
Źródła dodatkowych informacji	228
 Rozdział 8. Rekonesans	 229
Rekonesans online	229
Wnioski	242
Źródła dodatkowych informacji	242

Rozdział 9. Rozpoznawanie systemów operacyjnych	243
Ustanowienie sesji telnet.....	243
Rozpoznawanie stosu TCP	244
Narzędzia specjalizowane	247
Pasywne rozpoznawanie systemów operacyjnych.....	247
Nieostre rozpoznawanie systemów operacyjnych.....	251
Rozpoznawanie systemu operacyjnego na podstawie wartości czasu oczekiwania TCP/IP	253
Źródła dodatkowych informacji	254
Rozdział 10. Zacieranie śladów	255
Przed kim należy się ukrywać?	255
Zacieranie śladów po ataku.....	256
Ukrywanie się przed środkami dochodzeniowymi.....	262
Utrzymanie dostępu	268
Źródła dodatkowych informacji	275
Część III Ataki na systemy	277
Rozdział 11. Obrona systemu Unix	279
Hasła	280
Dostęp do plików.....	284
Dzienniki systemowe	287
Sieciowy dostęp do systemów Unix	291
Wzmacnianie Uniksa.....	296
Obrona sieci uniksowej.....	313
Serwer Apache	319
Źródła dodatkowych informacji	328
Rozdział 12. Ataki na system Unix.....	331
Ataki lokalne.....	331
Ataki zdalne.....	340
Ataki blokady usług	357
Źródła dodatkowych informacji	365
Rozdział 13. Ataki na systemy klienckie Windows	367
Ataki blokady usług	367
Ataki zdalne.....	377
Zdalny pulpit i zdalna pomoc.....	380
Źródła dodatkowych informacji	385

Rozdział 14. Ataki na serwery Windows	387
Historia wersji	387
Ataki na mechanizm uwierzytelniania Kerberos	388
Omijanie ochrony przed przepełnieniem bufora	393
Słabości mechanizmu Active Directory	394
Łamanie zabezpieczeń PKI	396
Łamanie zabezpieczeń kart elektronicznych	397
Szyfrowany system plików	400
Zewnętrzne narzędzia szyfrujące	402
Źródła dodatkowych informacji	405
Rozdział 15. Bezpieczeństwo usług WWW opartych na protokole SOAP	407
Szyfrowanie XML	408
Podpisy cyfrowe XML	410
Źródła dodatkowych informacji	411
Rozdział 16. Ataki za pomocą wymuszeń kodu SQL	413
Wprowadzenie do języka SQL	413
Ataki wymuszeń kodu SQL	417
Obrona przed wymuszeniami kodu SQL	424
Przykłady PHP-Nuke	428
Źródła dodatkowych informacji	431
Rozdział 17. Bezpieczeństwo sieci bezprzewodowych	433
Redukcja rozproszenia sygnału	433
Problemy z WEP	435
Łamanie zabezpieczeń WEP	435
Łamanie zabezpieczeń WEP w praktyce	441
Sieci VPN	442
TKIP	443
SSL	444
Wirusy bezprzewodowe	444
Źródła dodatkowych informacji	449
Część IV Zaawansowane techniki obrony	451
Rozdział 18. Analiza śladów w systemie audytowania	453
Podstawy analizy dzienników	454
Przykłady dzienników	454
Stany rejestrowane w dziennikach	464

Kiedy zaglądać do dzienników?	465
Przepelnienie dzienników i ich agregacja	467
Wyzwania związane z analizą dzienników	468
Narzędzia do zarządzania informacjami bezpieczeństwa	469
Globalna agregacja dzienników	469
Źródła dodatkowych informacji	470
Rozdział 19. Systemy detekcji włamań	471
Przykłady systemów IDS	472
Zastosowanie analizy Bayesowskiej	478
Sposoby oszukiwania systemów IDS	484
Przyszłość systemów IDS	486
Przypadek systemu IDS Snort	489
Błędy związane z rozmieszczaniem systemów IDS	494
Źródła dodatkowych informacji	496
Rozdział 20. Słoiki miodu	497
Motywy	499
Budowanie infrastruktury	499
Przechwytywanie ataków	511
Źródła dodatkowych informacji	512
Rozdział 21. Reagowanie na incydenty	513
Przykład z życia: chaos z powodu robaka	513
Definicje	514
Podstawowy schemat reagowania na incydenty	517
Małe sieci	521
Sieci średnich rozmiarów	528
Duże sieci	530
Źródła dodatkowych informacji	535
Rozdział 22. Zbieranie i zacieranie śladów	537
Podstawowe informacje o komputerach	538
Odpadki informacji	540
Narzędzia do zbierania śladów	541
Narzędzia śledcze na rozruchowych dyskach CD-ROM	547
Evidence Eliminator	551
Przykład procedury zbierania dowodów: atak na serwer FTP	559
Źródła dodatkowych informacji	569

