

Słowo wstępne (11)

Przedmowa (13)

Wprowadzenie (19)

Rozdział 1. Włamania do systemów - stan na dzień dzisiejszy (23)

Rozdział 2. Określenie hakera (29)

- 2.1. Poziomy umiejętności hakerów (30)
 - o 2.1.1[msj1]. Hakerzy pierwszorzędni (30)
 - o 2.1.2. Hakerzy drugorzędni (30)
 - o 2.1.3. Hakerzy trzeciorzędni (31)
- 2.2. Konsultanci do spraw zabezpieczeń (32)
- 2.3. Mity o hakerach (33)
- 2.4. Mity o zabezpieczaniu informacji (34)

Rozdział 3. Penetracja na zamówienie (37)

- 3.1. Konsekwencje testów penetracyjnych (38)
- 3.2. Wymagania stawiane niezależnemu konsultantowi (39)
 - o 3.2.1. Umiejętności (39)
 - o 3.2.2. Wiedza (39)
 - o 3.2.3. Zestaw narzędzi (40)
 - o 3.2.4. Sprzęt (40)
 - o 3.2.5. Rejestrowanie działań (41)
 - o 3.2.6. Etyka (41)
- 3.3. Zapowiedziane i niezapowiedziane testy penetracyjne (42)
 - o 3.3.1. Definicje (42)
 - o 3.3.2. Wady i zalety obu rodzajów testów penetracyjnych (43)
 - o 3.3.3. Dokumentowanie możliwości ataku (44)

Rozdział 4. Niebezpieczne miejsca (45)

- 4.1. Luki w zabezpieczeniach aplikacji (47)
- 4.2. Implementacje BIND (Berkeley Internet Name Domain) (48)
- 4.3. Interfejs CGI (Common Gateway Interface) (48)
- 4.4. Usługi tekstu otwartego (49)
- 4.5. Konta domyślne (49)
- 4.6. Usługa DNS (49)
- 4.7. Uprawnienia do pliku (50)
- 4.8. Protokół FTP i telnet (50)
- 4.9. ICMP (51)
- 4.10. IMAP i POP (51)
- 4.11. Modemy (52)
- 4.12. Brak monitoringu i wykrywania ataków (52)
- 4.13. Architektura sieci (53)
- 4.14. System plików NFS (Network File System) (54)
- 4.15. Porty systemu NT 135 - 139 (54)
- 4.16. Połączenie null connection w systemie NT (55)
- 4.17. Słabe hasło i identyfikator użytkownika (55)
- 4.18. Usługi zdalnego administrowania (56)
- 4.19. Zdalne wywołanie procedury (RPC) (57)

- 4.20. Usługa sendmail (57)
- 4.21. Usługi uruchamiane domyślnie (58)
- 4.22. Protokół SMTP (Simple Mail Transport Protocol) (58)
- 4.23. Łańcuch kontrolny protokołu SNMP (Simple Network Management Protocol) (59)
- 4.24. Wirusy i ukryte kody (59)
- 4.25. Przykładowe pliki serwera WWW (60)
- 4.26. Ogólna podatność serwera WWW na atak (61)
- 4.27. Monitorowanie luk w zabezpieczeniach (61)

Rozdział 5. Penetracja przez internet (65)

- 5.1. Tworzenie wykazu urządzeń w sieci (66)
 - o 5.1.1. Polecenie Whois (66)
 - o 5.1.2. Przesłanie informacji o strefie (68)
 - o 5.1.3. Polecenie PING (69)
 - o 5.1.4. Śledzenie trasy (70)
- 5.2. Analiza podatności na atak (71)
 - o 5.2.1. Rozpoznawanie systemów operacyjnych (72)
 - o 5.2.2. Skanowanie portów (72)
 - o 5.2.3. Wykaz aplikacji (74)
 - o 5.2.4. Przeszukiwanie internetu (75)
- 5.3. Wykorzystywanie słabych punktów (75)
- Studium przypadku: Komputery dołączone jednocześnie do dwóch sieci (77)

Rozdział 6. Penetracja przez połączenie telefoniczne (81)

- 6.1. Atak war dialing (81)
- 6.2. Metoda war dialing (82)
 - o 6.2.1. Wybieranie numeru (82)
 - o 6.2.2. Rejestrowanie się (82)
 - o 6.2.3. Ekrany logowania (83)
- 6.3. Poszukiwanie numerów (84)
- 6.4. Metody zapobiegawcze (85)
- 6.5. Narzędzia do ataku war dialing (86)
 - o 6.5.1. ToneLoc (86)
 - o 6.5.2. THC-Scan (88)
 - o 6.5.3. TeleSweep (91)
 - o 6.5.4. PhoneSweep (92)
- Studium przypadku: War Dialing (92)

Rozdział 7. Wewnętrzne testy penetracyjne (95)

- 7.1. Scenariusze (96)
- 7.2. Zbieranie informacji o sieci (97)
- 7.3. Informacje o systemie NT (101)
- 7.4. Unix (104)
- 7.5. Poszukiwanie narzędzi ataku (105)
- 7.6. Analiza ruchu w sieci (106)
- 7.7. Zdalne instalowanie zestawu narzędzi (108)

- 7.8. Skanowanie w poszukiwaniu słabych punktów (109)
- Studium przypadku: Sprawdzanie komputera stacjonarnego (109)

Rozdział 8. Socjotechnika (111)

- 8.1. Telefon (111)
 - o 8.1.1. Obsługa techniczna (112)
 - o 8.1.2. Niezadowolony klient (113)
 - o 8.1.3. Prośba o pomoc w logowaniu (115)
 - o 8.1.4. Metody dodatkowe (116)
- 8.2. Grzebanie w śmieciach (116)
- 8.3. Informacje z biurka (117)
- 8.4. Typowe środki zaradcze (118)

Rozdział 9. Metody uniksowe (121)

- 9.1. Usługi w systemie Unix (122)
 - o 9.1.1. Usługi inetd (123)
 - o 9.1.2. Usługi zdalne (127)
 - o 9.1.3. Usługi zdalnego wywołania procedury (RPC) (128)
- 9.2. Ataki powodujące przepełnienie bufora (129)
- 9.3. Zezwolenia do plików (130)
- 9.4. Aplikacje (132)
 - o 9.4.1. Serwery pocztowe (133)
 - o 9.4.2. Serwery WWW (134)
 - o 9.4.3. X Windows (135)
 - o 9.4.4. Serwery DNS (136)
- 9.5. Błędy w konfiguracji (137)
- 9.6. Narzędzia uniksowe (138)
 - o 9.6.1. Datapipe.c (138)
 - o 9.6.2. QueSO (139)
 - o 9.6.3. Cheops (139)
 - o 9.6.4. NFSSHELL (142)
 - o 9.6.5. XSCAN (143)
- Studium przypadku: Penetracja systemu Unix (144)

Rozdział 10. Zestaw narzędzi (147)

- 10.1. Sprzęt (147)
- 10.2. Oprogramowanie (148)
 - o 10.2.1. Stacja robocza Windows NT (149)
 - o 10.2.2. Linux (149)
- 10.3. VMware (150)

Rozdział 11. Zautomatyzowane skanery luk (153)

- 11.1. Definicja (153)
- 11.2. Zastosowanie (154)
- 11.3. Wady (154)

- 11.4. Skanery zbierające dane z sieci i skanery monitorujące działalność komputera (155)
- 11.5. Narzędzia (157)
- 11.6. Skanery zbierające dane z sieci (158)
 - o 11.6.1. Skaner Network Associates CyberCop (158)
 - o 11.6.2. ISS Internet Scanner (161)
 - o 11.6.3. Nessus (163)
 - o 11.6.4. Symantec (uprzednio Axent Technologies) NetRecon (165)
 - o 11.6.5. Bindview HackerShield (bv-control for Internet Security) (165)
- 11.7. Skanery monitorujące działalność komputera (166)
 - o 11.7.1. Symantec (uprzednio Axent Technologies) Enterprise Security Manager (ESM) (166)
- 11.8. Pentasafe VigilEnt (168)
- 11.9. Wnioski (169)

Rozdział 12. Narzędzia do pozyskiwania informacji (171)

- 12.1. WS_Ping ProPack (171)
- 12.2. NetScanTools (180)
- 12.3. Sam Spade (188)
- 12.4. Rhino9 Pinger (201)
- 12.5. VisualRoute (202)
- 12.6. Nmap (205)
- 12.7. What's running (207)

Rozdział 13. Skanery portów (209)

- 13.1. Nmap (209)
- 13.2. 7th Sphere Port Scanner (215)
- 13.3. Strobe (216)
- 13.4. SuperScan (217)

Rozdział 14. Programy do analizy ruchu w sieci (221)

- 14.1. Dsniff (222)
- 14.2. Linsniff (224)
- 14.3. Tcpdump (224)
- 14.4. BUTTSniffer (225)
- 14.5. SessionWall-3 (obecnie eTrust Intrusion Detection) (227)
- 14.6. AntiSniff (228)

Rozdział 15. Łamacze haseł (233)

- 15.1. L0phtCrack (233)
- 15.2. pwdump2 (239)
- 15.3. John the Ripper (240)
- 15.4. Cain (242)
- 15.5. ShowPass (243)

Rozdział 16. Narzędzia dla Windows NT (245)

- 16.1. NET USE (245)
- 16.2. Połączenie zerowe (246)
- 16.3. NET VIEW (247)
- 16.4. NLTEST (249)
- 16.5. NBTSTAT (250)
- 16.6. EPDUMP (251)
- 16.7. NETDOM (252)
- 16.8. Getmac (253)
- 16.9. Local administrators (253)
- 16.10. Global (254)
- 16.11. Ustat (255)
- 16.12. DumpSec (256)
- 16.13. User2sid i sid2user (259)
- 16.14. NetBIOS Auditing Tool (NAT) (260)
- 16.15. SMBGrind (263)
- 16.16. SRVCHECK (264)
- 16.17. SRVINFO (265)
- 16.18. AuditPol (266)
- 16.19. REGDMP (267)
- 16.20. Somarsoft DumpReg (268)
- 16.21. Remote (270)
- 16.22. Netcat (271)
- 16.23. SC (273)
- 16.24. AT (274)
- 16.25. FPIPE (275)
- Studium przypadku: Słabe hasła (276)
- Studium przypadku: Wewnętrzna penetracja systemu Windows (281)

Rozdział 17. Narzędzia penetracji WWW (285)

- 17.1. Whisker (286)
- 17.2. SiteScan (288)
- 17.3. THC Happy Browser (289)
- 17.4. wwwhack (290)
- 17.5. Web Cracker (292)
- 17.6. Brutus (293)
- Studium przypadku: Luka w oprogramowaniu Compaq Insight Manager (295)

Rozdział 18. Zdalne sterowanie systemem (299)

- 18.1. PcAnywhere (300)
- 18.2. Virtual Network Computing (304)
- 18.3. NetBus (307)
- 18.4. Back Orifice 2000 (311)

Rozdział 19. Systemy wykrywania włamań (315)

- 19.1. Definicja systemu wykrywania włamań (315)
- 19.2. Unikanie wykrycia (317)
 - o 19.2.1. Utażone skanowanie portów (320)

- o 19.2.2. Techniki agresywne (322)
- 19.3. Pułapki (323)
- 19.4. Cechy skutecznego systemu wykrywania włamań (323)
- 19.5. Wybór systemu wykrywania włamań (329)
 - o 19.5.1. RealSecure (329)
 - o 19.5.2. NetProwler (330)
 - o 19.5.3. Secure Intrusion Detection (330)
 - o 19.5.4. eTrust Intrusion Detection (331)
 - o 19.5.5. Network Flight Recorder (332)
 - o 19.5.6. Dragon (332)
 - o 19.5.7. Snort (333)

Rozdział 20. Zapory sieciowe (335)

- 20.1. Definicja (335)
- 20.2. Monitorowanie (336)
- 20.3. Konfiguracja (337)
- 20.4. Nadzorowanie zmian (338)
- 20.5. Rodzaje zapór sieciowych (338)
 - o 20.5.1. Zapory sieciowe z filtrowaniem pakietów (339)
 - o 20.5.2. Zapory sieciowe z kontrolą ładunku (340)
 - o 20.5.3. Zapory sieciowe z serwerem pośredniczącym (340)
- 20.6. Translacja adresów sieci wewnętrznej (341)
- 20.7. Omijanie zapór sieciowych (341)
- 20.8. Zapory sieciowe a wirtualne sieci prywatne (344)
- Studium przypadku: Atak na serwer IIS: MDAC (345)

Rozdział 21. Ataki odmowy obsługi (349)

- 21.1. Ataki wyczerpania zasobów (351)
 - o 21.1.1. Papasmurf (351)
 - o 21.1.2. Trash2 (353)
 - o 21.1.3. Igmpofdeath.c (353)
 - o 21.1.4. Fawx (354)
 - o 21.1.5. OBSD_fun (354)
- 21.2. Zatykanie portów (355)
 - o 21.2.1. Multilate (355)
 - o 21.2.2. Pepsi5 (356)
- 21.3. Zalewanie pakietami SYN (356)
 - o 21.3.1. Synful (357)
 - o 21.3.2. Synk4 (357)
 - o 21.3.3. Naptha (358)
- 21.4. Fragmentacja pakietów IP (358)
 - o 21.4.1. Jolt2 (359)
 - o 21.4.2. Teardrop (360)
 - o 21.4.3. Syndrop (360)
 - o 21.4.4. Newtear (361)
- 21.5. Rozproszone ataki odmowy obsługi (361)
 - o 21.5.1. Tribe Flood Network 2000 (363)
 - o 21.5.2. Trin00 (365)

- o 21.5.3. Stacheldraht (366)
 - o 21.5.4. Obsługa sieci DDoS (368)
- 21.6. Ataki odmowy obsługi wymierzone w aplikacje (369)
 - o 21.6.1. Up Yours (370)
 - o 21.6.2. Wingatecrash (372)
 - o 21.6.3. WinNuke (372)
 - o 21.6.4. BitchSlap (373)
 - o 21.6.5. DOSNuke (373)
 - o 21.6.6. Shutup (374)
 - o 21.6.7. Ataki odmowy obsługi wymierzone w serwery WWW (374)
- 21.7. Zbiorcze narzędzia ataków odmowy obsługi (375)
 - o 21.7.1. CyberCop (376)
 - o 21.7.2. ISS Internet Scanner (376)
 - o 21.7.3. Toast (378)
 - o 21.7.4. Spike.sh5.3 (379)
- 21.8. Podsumowanie (380)

Rozdział 22. Podsumowanie (381)

- 22.1. Profilaktyka (381)
- 22.2. Aktualizacja (385)
 - o 22.2.1. Witryny WWW (385)
 - o 22.2.2. Listy dystrybucyjne poczty elektronicznej (386)

Rozdział 23. Trendy i mody (393)

- 23.1. Uwierzytelnianie (393)
 - o 23.1.1. Uwierzytelnianie wieloelementowe (394)
 - o 23.1.2. Metody biometryczne (394)
 - o 23.1.3. Uwierzytelnianie z wykorzystaniem żetonów (395)
 - o 23.1.4. Usługi katalogowe (396)
- 23.2. Szyfrowanie (396)
- 23.3. Infrastruktura klucza publicznego (397)
- 23.4. Systemy rozproszone (398)
- 23.5. Dochodzenia komputerowe (398)
- 23.6. Regulacje prawne (399)
- 23.7. Techniki włamań (400)
- 23.8. Profilaktyka (401)
- 23.9. Ubezpieczenia od skutków przestępstw komputerowych (401)

Dodatek A Zawartość płyt CD-ROM (403)

Dodatek B Dwadzieścia najgroźniejszych dla bezpieczeństwa internetu luk w oprogramowaniu (407)

Skorowidz (449)