

Przedmowa do wydania drugiego (13)

Przedmowa do wydania pierwszego (17)

Część I Zaczynamy! (21)

Rozdział 1. Wprowadzenie (23)

- 1.1. Truizmy bezpieczeństwa (23)
- 1.2. Wybieranie strategii bezpieczeństwa (27)
 - o 1.2.1. Pytania ważne podczas definiowania polityki bezpieczeństwa (28)
 - o 1.2.2. Stanowisko (30)
- 1.3. Bezpieczeństwo na podstawie systemu ochrony pojedynczego komputera (32)
- 1.4. Bezpieczeństwo "obwodowe" (33)
- 1.5. Strategie sieci bezpiecznych (34)
 - o 1.5.1. Bezpieczeństwo stacji roboczej (34)
 - o 1.5.2. Bramy i zapory sieciowe (36)
 - o 1.5.3. Strefa DMZ (38)
 - o 1.5.4. Szyfrowanie - bezpieczeństwo komunikacji (39)
- 1.6. Etyka w odniesieniu do bezpieczeństwa informatycznego (40)
- 1.7. OSTRZEŻENIE (42)

Rozdział 2. Omówienie bezpieczeństwa protokołów niższych warstw (43)

- 2.1. Podstawowe protokoły (43)
 - o 2.1.1. IP (44)
 - o 2.1.2. ARP (46)
 - o 2.1.3. TCP (47)
 - o 2.1.4. SCTP (51)
 - o 2.1.5. UDP (52)
 - o 2.1.6. ICMP (52)
- 2.2. Zarządzanie adresami i nazwami (53)
 - o 2.2.1. Routery i protokoły routingu (53)
 - o 2.2.2. System DNS (56)
 - o 2.2.3. BOOTP oraz DHCP (60)
- 2.3. IP w wersji 6. (61)
 - o 2.3.1. Format adresów IPv6 (62)
 - o 2.3.2. Neighbor Discovery (63)
 - o 2.3.3. DHCPv6 (64)
 - o 2.3.4. Filtrowanie IPv6 (64)
- 2.4. Urządzenia dokonujące translacji adresów (65)
- 2.5. Bezpieczeństwo sieci bezprzewodowych (66)
 - o 2.5.1. Umacnianie WEP (68)

Rozdział 3. Przegląd protokołów wyższych warstw (69)

- 3.1. Protokoły komunikacyjne (69)
 - o 3.1.1. SMTP (69)
 - o 3.1.2. MIME (72)
 - o 3.1.3. POP wersja 3 (73)
 - o 3.1.4. IMAP wersja 4 (74)
 - o 3.1.5. Instant Messaging (IM) (75)
- 3.2. Telefonía internetowa (76)

- o 3.2.1. H.323 (76)
 - o 3.2.2. SIP (76)
- 3.3. Protokoły oparte na RPC (77)
 - o 3.3.2. NIS (81)
 - o 3.3.3. NFS (81)
 - o 3.3.4. Andrew (83)
- 3.4. Protokoły przesyłania plików (84)
 - o 3.4.1. TFTP (84)
 - o 3.4.2. FTP (85)
 - o 3.4.3. Protokół SMB (90)
- 3.5. Zdalne logowanie (91)
 - o 3.5.1. Telnet (91)
 - o 3.5.2. Polecenia "r" (92)
 - o 3.5.3. Ssh (94)
- 3.6. Protokół SNMP (96)
- 3.7. Protokół NTP (97)
- 3.8. Usługi informacyjne (98)
 - o 3.8.1. Finger - poszukiwanie osób (99)
 - o 3.8.2. Whois - usługa przeszukiwania baz danych (99)
 - o 3.8.3. LDAP (99)
 - o 3.8.4. Usługi WWW (100)
 - o 3.8.5. Protokół NNTP (101)
 - o 3.8.6. Multicasting i Mbone (102)
- 3.9. Protokoły prawnie zastrzeżone (103)
 - o 3.9.1. RealAudio (104)
 - o 3.9.2. SQL*Net firmy Oracle (104)
 - o 3.9.3. Inne usługi firmowe (105)
- 3.10. Równorzędne sieci komputerowe (105)
- 3.11. X11 Window System (106)
 - o 3.11.1. xdm (107)
- 3.12. Small Services (108)

Rozdział 4. Globalna pajęczyna. Zagrożenie czy realne niebezpieczeństwo? (109)

- 4.1. Protokoły WWW (110)
 - o 4.1.1. HTTP (110)
 - o 4.1.2. SSL (114)
 - o 4.1.3. FTP (114)
 - o 4.1.4. Adresy URL (115)
- 4.2. Zagrożenia dla klientów (117)
 - o 4.2.1. ActiveX (118)
 - o 4.2.2. Java i applety (118)
 - o 4.2.3. JavaScript (121)
 - o 4.2.4. Przeglądarki internetowe (122)
- 4.3. Ryzyko dla serwera (124)
 - o 4.3.1. Kontrola dostępu (125)
 - o 4.3.2. Skrypty serwera (125)
 - o 4.3.3. Zabezpieczanie serwera (126)
 - o 4.3.4. Wybór serwera (127)
- 4.4. Serwery WWW versus zapory sieciowe (129)

- 4.5. Sieć i bazy danych (131)
- 4.6. Podsumowanie (132)

Część II Zagrożenia (133)

Rozdział 5. Klasy ataków (135)

- 5.1. Kradzieże haseł (135)
- 5.2. Socjotechnika (139)
- 5.3. Błędy i tylne wejścia (140)
- 5.4. Niepowodzenia uwierzytelniania (144)
 - o 5.4.1. Wyścigi do uwierzytelnienia (144)
- 5.5. Błędy protokołów (145)
- 5.6. Wypływanie informacji (146)
- 5.7. Ataki lawinowe - wirusy i robaki (147)
- 5.8. Ataki blokady usług (148)
 - o 5.8.1. Ataki na łącza sieciowe (149)
 - o 5.8.2. Atak na warstwę sieciową (150)
 - o 5.8.3. DDoS (152)
 - o 5.8.4. Co zrobić w przypadku rozproszonego ataku odmowy usług? (153)
 - o 5.8.5. Rozpraszenie wsteczne (159)
- 5.9. Roboty sieciowe (160)
- 5.10. Ataki aktywne (160)

Rozdział 6. Warsztat i inne środki bojowe hakera (163)

- 6.1. Wprowadzenie (163)
- 6.2. Cele hakerów (164)
- 6.3. Skanowanie sieci (165)
- 6.4. Włamanie do komputera (166)
- 6.5. Bitwa o komputer (167)
 - o 6.5.1. Programy o uprawnieniach setuid root (168)
 - o 6.5.2. Rootkit (171)
- 6.6. Zacieranie śladów (171)
 - o 6.6.1. Furtki (172)
- 6.7. Metastaza (173)
- 6.8. Narzędzia hakerów (173)
 - o 6.8.1. Crack - atak słownikowy na hasła uniksowe (175)
 - o 6.8.2. Dsniff - narzędzie do podsłuchiwanie haseł (175)
 - o 6.8.3. Nmap - wyszukiwanie i identyfikacja komputerów (175)
 - o 6.8.4. Nbaudit - zdobywanie informacji na temat udziałów NetBIOS (176)
 - o 6.8.5. Juggernaut - narzędzie do przechwytywania połączeń TCP (176)
 - o 6.8.6. Nessus - skanowanie portów (177)
 - o 6.8.7. Narzędzia do ataku DDoS (177)
 - o 6.8.8. Ping of Death - wysyłanie nieprawidłowych pakietów (177)
 - o 6.8.9. Zestawy do tworzenia wirusów (177)
 - o 6.8.10. Inne narzędzia (178)
- 6.9. Brygady tygrysa (179)

Część III Bezpieczniejsze narzędzia i usługi (181)

Rozdział 7. Uwierzytelnianie (183)

- 7.1. Zapamiętywanie haseł (184)
 - o 7.1.1. Rzucanie kostką (187)
 - o 7.1.2. Rzeczywisty koszt haseł (188)
- 7.2. Hasła jednorazowe - czasowe (189)
- 7.3. Hasła jednorazowe - wezwanie-odpowiedź (190)
- 7.4. Algorytm haseł jednorazowych Lamporta (192)
- 7.5. Karty mikroprocesorowe (193)
- 7.6. Techniki biometryczne (193)
- 7.7. RADIUS (195)
- 7.8. Szkielet uwierzytelniania SASL (195)
- 7.9. Uwierzytelnianie komputer-komputer (196)
 - o 7.9.1. Uwierzytelnianie za pośrednictwem sieci (196)
 - o 7.9.2. Techniki kryptograficzne (196)
- 7.10. PKI (197)

Rozdział 8. Stosowanie niektórych narzędzi i usług (199)

- 8.1. Inetd - usługi sieciowe (200)
- 8.2. Ssh - korzystanie z terminala i dostęp do plików (200)
 - o 8.2.1. Uwierzytelnianie jednoelementowe w ssh (201)
 - o 8.2.2. Uwierzytelnianie dwuelementowe w ssh (203)
 - o 8.2.3. Słabe strony uwierzytelniania (204)
 - o 8.2.4. Uwierzytelnianie serwera (204)
- 8.3. Syslog (204)
- 8.4. Narzędzia administrowania siecią (205)
 - o 8.4.1. Monitorowanie sieci (205)
 - o 8.4.2. Posługiwanie się programem tcpdump (206)
 - o 8.4.3. Ping, traceroute oraz dig (207)
- 8.5. Chroot - uwięzienie podejrzanego oprogramowania (208)
- 8.6. Uwięzienie serwera Apache Web Server (212)
 - o 8.6.1. Osłony skryptów CGI (214)
 - o 8.6.2. Bezpieczeństwo uwięzionego serwera WWW (215)
- 8.7. Aftpd - demon prostego anonimowego serwera FTP (215)
- 8.8. Agenty przesyłania poczty (216)
 - o 8.8.1. Postfix (216)
- 8.9. POP3 oraz IMAP (217)
- 8.10. Samba - implementacja protokołu SMB (217)
- 8.11. Poskramianie programu named (218)
- 8.12. Dodanie obsługi SSL za pomocą programu sslwrap (219)

Część IV Zapory sieciowe i sieci VPN (221)

Rozdział 9. Rodzaje zapór sieciowych (223)

- 9.1. Filtry pakietów (224)
 - o 9.1.1. Topologia sieci a fałszowanie adresów (227)
 - o 9.1.2. Filtry routingu (231)
 - o 9.1.3. Przykładowe konfiguracje (232)
 - o 9.1.4. Wydajność filtrowania pakietów (234)
- 9.2. Filtrowanie na poziomie aplikacji (235)
- 9.3. Bramy poziomu obwodów (236)

- 9.4. Dynamiczne filtry pakietów (238)
 - o 9.4.1. Sposoby implementacji (238)
 - o 9.4.2. Replikacja a topologia (241)
 - o 9.4.3. Bezpieczeństwo dynamicznych filtrów pakietów (243)
- 9.5. Zapory sieciowe rozproszone (244)
- 9.6. Czego zapory sieciowe nie potrafią (245)

Rozdział 10. Filtrowanie usług (247)

- 10.1. Usługi, które powinny być filtrowane (248)
 - o 10.1.1. DNS (248)
 - o 10.1.2. WWW (252)
 - o 10.1.3. FTP (253)
 - o 10.1.4. TCP (253)
 - o 10.1.5. NTP (254)
 - o 10.1.6. SMTP/Mail (254)
 - o 10.1.7. POP3/IMAP (255)
 - o 10.1.8. ssh (257)
- 10.2. Wykopywanie robaków (257)
- 10.3. Usługi, których nie lubimy (258)
 - o 10.3.1. UDP (258)
 - o 10.3.2. H.323 oraz SIP (260)
 - o 10.3.3. RealAudio (260)
 - o 10.3.4. SMB (260)
 - o 10.3.4. X Windows (260)
- 10.4. Inne usługi (261)
 - o 10.4.1. IPsec, GRE i IP w IP (261)
 - o 10.4.2. ICMP (261)
- 10.5. Coś nowego (262)

Rozdział 11. Inżynieria zapór sieciowych (263)

- 11.1. Zestawy reguł (264)
- 11.2. Proxy (267)
- 11.3. Budowa zapory sieciowej od podstaw (268)
 - o 11.3.1. Budowa prostej, osobistej zapory sieciowej (269)
 - o 11.3.2. Budowa zapory sieciowej dla firmy (273)
 - o 11.3.3. Filtrowanie bazujące na aplikacjach (279)
- 11.4. Problemy z zaporami sieciowymi (279)
 - o 11.4.1. Problemy nieumyślne (280)
 - o 11.4.2. Działalność wywrotowa (280)
 - o 11.4.3. Postępowanie z fragmentami IP (281)
 - o 11.4.4. Problem z FTP (282)
 - o 11.4.5. Kroczący ogień (282)
 - o 11.4.6. Administracja (283)
- 11.5. Testowanie zapór testowych (284)
 - o 11.5.1. Brygady tygrysa (284)
 - o 11.5.2. Zasady kontroli (285)

Rozdział 12. Tunelowanie i sieci VPN (287)

- 12.1. Tunele (288)
 - o 12.1.1. Tunele dobre i tunele złe (288)
- 12.2. Wirtualne sieci prywatne VPN (291)
 - o 12.2.1. Odległe oddziały (291)
 - o 12.2.2. Wspólne przedsięwzięcia (292)
 - o 12.2.3. Telepraca (293)
- 12.3. Oprogramowanie a sprzęt (298)
 - o 12.3.1. Sieci VPN realizowane przy użyciu oprogramowania (298)
 - o 12.3.2. Sieci VPN realizowane przy użyciu sprzętu (299)

Część V Ochrona organizacji (301)

Rozdział 13. Planowanie sieci (303)

- 13.1. Badania intranetu (305)
- 13.2. Sztuczki z routingiem w intranetach (306)
- 13.3. Ufamy komputerowi (309)
- 13.4. Pasek i szelki (311)
- 13.5. Klasy rozmieszczenia zapór sieciowych (312)

Rozdział 14. Bezpieczne komputery w nieprzyjaznym środowisku (315)

- 14.1. Co rozumiesz, mówiąc "bezpieczny"? (315)
- 14.2. Właściwości bezpiecznych komputerów (316)
 - o 14.2.1. Bezpieczne klienty (319)
 - o 14.2.2. Bezpieczne serwery (321)
 - o 14.2.3. Bezpieczne routery i inne urządzenia sieciowe (322)
- 14.3. Konfiguracja sprzętu (322)
- 14.4. Rozkładanie komputera (322)
- 14.5. Instalacja nowego oprogramowania (327)
- 14.6. Administrowanie bezpiecznym komputerem (328)
 - o 14.6.1. Dostęp (328)
 - o 14.6.2. Dostęp przy użyciu konsoli (329)
 - o 14.6.3. Zapisywanie zdarzeń w plikach raportów (329)
 - o 14.6.4. Archiwizacja (330)
 - o 14.6.5. Uaktualnianie oprogramowania (331)
 - o 14.6.6. Obserwowanie (334)
- 14.7. "Jazda bez trzymanki" - życie bez zapory sieciowej (334)

Rozdział 15. Detekcja włamań (337)

- 15.1. Gdzie monitorować? (338)
- 15.2. Rodzaje systemów IDS (339)
- 15.3. Administracja systemem IDS (340)
- 15.4. Narzędzia IDS (340)
 - o 15.4.1. Snort (341)

Część VI Otrzymane lekcje (343)

Rozdział 16. Wieczór z Berferdem (345)

- 16.1. Nieprzyjazne zachowanie (345)

- 16.2. Wieczór z Berferdem (347)
- 16.3. Na drugi dzień (352)
- 16.4. Więzienie (353)
- 16.5. Śledzenie Berferda (355)
- 16.6. Berferd wraca do domu (356)

Rozdział 17. Przejęcie Clarka (359)

- 17.1. Początki (359)
- 17.2. Clark (360)
- 17.3. Dochodzenie wstępne (361)
- 17.4. Badanie Clarka (362)
 - o 17.4.1. /usr/lib (363)
 - o 17.4.2. /usr/var/tmp (364)
- 17.5. Plik haseł (368)
- 17.6. Jak napastnikom udało się dostać? (368)
 - o 17.6.1. Jak zdobyli uprawnienia root? (369)
 - o 17.6.2. Co w ten sposób zyskali? (369)
- 17.7. Lepsze środki dochodzeniowe (369)
- 17.8. Otrzymane lekcje (370)

Rozdział 18. Bezpieczna komunikacja w niebezpiecznych sieciach (371)

- 18.1. System uwierzytelniania Kerberos (372)
 - o 18.1.1. Ograniczenia (375)
- 18.2. Szyfrowanie na poziomie łącza (376)
- 18.3. Szyfrowanie na poziomie warstwy sieciowej (377)
 - o 18.3.1. Protokoły ESP oraz AH (377)
 - o 18.3.2. Zarządzanie kluczami w IPsec (380)
- 18.4. Szyfrowanie na poziomie aplikacji (380)
 - o 18.4.1. Zdalne logowanie - ssh (381)
 - o 18.4.2. SSL (382)
 - o 18.4.3. Uwierzytelnianie w SNMP (385)
 - o 18.4.4. Bezpieczna poczta elektroniczna (385)
 - o 18.4.5. Bezpieczeństwo transmisji, a bezpieczeństwo obiektu (387)
 - o 18.4.6. GSS-API (387)

Rozdział 19. Co dalej? (389)

- 19.1. IPv6 (389)
- 19.2. DNSsec (390)
- 19.3. Microsoft i bezpieczeństwo (391)
- 19.4. Wszechobecność Internetu (391)
- 19.5. Bezpieczeństwo Internetu (391)
- 19.6. Zakończenie (392)

Dodatki (395)

Dodatek A Wprowadzenie do kryptografii (397)

- A.1. Symbolika (397)

- A.2. Kryptografia tajnego klucza (399)
- A.3. Tryby działania (401)
 - o A.3.1. Tryb elektronicznej książki kodowej (401)
 - o A.3.2. Tryb wiązania bloków szyfrogramu (401)
 - o A.3.3. Tryb sprzężenia zwrotnego z wyjścia (402)
 - o A.3.4. Tryb sprzężenia zwrotnego kryptogramu (403)
 - o A.3.5. Tryb licznikowy (403)
 - o A.3.6. Hasła jednorazowe (404)
 - o A.3.7. Klucze główne (404)
- A.4. Kryptografia klucza publicznego (405)
- A.5. Wymiana klucza wykładniczego (406)
- A.6. Podpisy cyfrowe (407)
- A.7. Bezpieczne funkcje mieszające (409)
- A.8. Znaczniki czasu (410)

Dodatek B Jak być na bieżąco? (413)

- B.1. Listy dyskusyjne (414)
- B.2. Zasoby w Internecie (415)
- B.3. Strony internetowe osób prywatnych (416)
- B.4. Strony producentów (417)
- B.5. Konferencje (418)

Lista bomb (421)

Lista akronimów (423)

Bibliografia (429)

Skorowidz (449)