O Autorze (19)
Przedmowa (21)
Rozdział 1. Wprowadzenie (23)

- 1.1. Kto powinien przeczytać tę książkę? (23)
- 1.2. Sposób organizacji książki (24)
  - 1.2.1. Konwencje zastosowane w książce (27)
  - 1.2.2. Podstawy (28)
- 1.3. Przed czym się bronimy? (30)
- 1.4. Kim są wrogowie? (31)
- 1.5. Cele działania (34)
- 1.6. Koszty: Ochrona kontra włamania (35)
- 1.7. Zabezpieczanie sprzętu (35)
- 1.8. Zabezpieczanie sieci oraz dostępu modemowego (35)
- 1.9. Zabezpieczanie dostępu do systemu (36)
- 1.10. Zabezpieczanie plików (37)
- 1.11. Przygotowanie do wykrywania włamania (37)
- 1.12. Przywracanie działania systemu po włamaniu (38)

Część I Zabezpieczanie systemu (39)
Rozdział 2. Szybkie rozwiązania najczęstszych problemów (43)

- 2.1. Podstawy zabezpieczeń systemu Linux (44)
  - 2.1.1. Labirynt krętych korytarzy (44)
  - 2.1.2 Drogi przeprowadzania ataku (49)
  - 2.1.3. Pierścienie zabezpieczeń (52)
- 2.2. Siedem grzechów głównych (54)
  - 2.2.1. Słabe oraz domyślne hasła (grzech 1) (54)
  - 2.2.2. Otwarte porty sieciowe (grzech 2) (56)
  - 2.2.3. Stare wersje oprogramowania (grzech 3) (59)
  - 2.2.4. Niebezpieczne oraz źle skonfigurowane programy (grzech 4) (60)
  - 2.2.5. Niewystarczające zasoby oraz niewłaściwie zdefiniowane priorytety (grzech 5) (67)
  - 2.2.6. Przedawnione oraz niepotrzebne konta (grzech 6) (70)
  - 2.2.7. Zwłoka w działaniu (grzech 7) (71)
- 2.3. Hasła - kluczowa kwestia dobrego zabezpieczenia (71)
  - 2.3.1. Zapobieganie słabym i domyślnym hasłom (72)
- 2.4. Zaawansowane techniki dotyczące haseł (77)
  - 2.4.1. Ukrywanie haseł przy użyciu pliku shadow w celu zapewnienia odpowiednich zabezpieczeń (78)
  - 2.4.2. Prośba o ponowne wprowadzenie hasła (79)
  - 2.4.3. Czy hasła powinny mieć określony okres ważności? (81)
  - 2.4.4. Nazwy kont (82)
- 2.5. Zabezpieczanie systemu przed pomyłkami użytkowników (83)
  - 2.5.1. Zagrożenia spowodowane przez oprogramowanie importowane (87)
  - 2.5.2. Edukacja użytkowników (88)
- 2.6. Przebaczenie jest lepsze niż zezwolenie (89)
  - 2.6.1. Katalogi oraz sticky bit (91)
  - 2.6.2. Wyszukiwanie problemów z prawami dostępu (92)
  - 2.6.3. Wykorzystanie umask w skryptach startowych (97)

- 2.7. Zagrożenia oraz środki zaradcze podczas początkowej konfiguracji systemu (98)
  - 2.7.1. Sprawdzanie zabezpieczeń systemu Red Hat 7.3 (100)
- 2.8. Ograniczanie nierozsądnego dostępu (104)
  - 2.8.1. Ograniczenie terminali, z których mogą pochodzić nadchodzące połączenia (104)
  - 2.8.2. Dzwonienie z zewnątrz (wardialing) (106)
  - 2.8.3. Zabezpieczanie niekontrolowanego dostępu do danych (107)
  - 2.8.4. Ograniczanie interfejsów serwera (108)
- 2.9. Zapory sieciowe oraz zabezpieczenia korporacyjne (108)
  - 2.9.1. Zabezpieczanie obejść zapór sieciowych (109)
  - 2.9.2. Tunelowanie poprzez zapory sieciowe (113)
  - 2.9.3. Opcje jądra dotyczące protokołów (116)
  - 2.9.4. Filtrowanie pakietów wychodzących (117)
  - 2.9.5. Pułapki w lokalnej sieci komputerowej (118)
  - 2.9.6. Wewnątrzfirmowe zapory sieciowe powstrzymujące atak (121)
- 2.10. Wyłączanie niepotrzebnych usług (125)
- 2.11. Silne zabezpieczenia wymagają minimalnej ilości usług (132)
- 2.12. Zamurowywanie luk w systemie (133)
  - 2.12.1. Nie używaj programu finger (133)
  - 2.12.2. Wyłączanie usługi rwhod (135)
  - 2.12.3. Wyłączanie usługi rwalld (136)
  - 2.12.4. Wyłączanie usługi SNMP (136)
  - 2.15.5. Wyłączanie usług NFS, mountd oraz portmap (138)
  - 2.12.6. Przełączanie usługi NFS na używanie protokołu TCP (139)
  - 2.12.7. Wyłączanie usług rsh, rcp, rlogin oraz rexec (140)
  - 2.12.8. Wyłączanie usług echo oraz chargen (141)
  - 2.12.9. Wyłączanie usług talk oraz ntalk (142)
  - 2.12.10. Wyłączanie usługi TFTP (142)
  - 2.12.11. Wyłączanie usług systat oraz netstat (142)
  - 2.12.12. Wyłączanie wewnętrznych usług xinetd (143)
- 2.13. Nowe lampy zamiast starych (143)
  - 2.13.1. Uaktualnianie jądra w wersji 2.4 (147)
  - 2.13.2. Uaktualnianie jądra w wersji 2.2 (148)
  - 2.13.3. Uaktualnianie programu sendmail (148)
  - 2.13.4. Wzmacnianie programu sendmail w celu odparcia ataków DoS (151)
  - 2.13.5. Uaktualnianie programu SSH (154)
  - 2.13.6. Uaktualnianie usługi WU-FTPD (154)
  - 2.13.7. Uaktualnianie programu Netscape (155)
  - 2.13.8. Blokowanie reklam internetowych (156)
- 2.14. Zjednoczeni zginiemy, podzieleni przetrwamy (157)

Rozdział 3. Szybkie oraz proste sposoby włamania. Sposoby ich unikania (159)

- 3.1. X oznacza lukę w zabezpieczeniach (160)
- 3.2. Prawo dżungli - zabezpieczenia fizyczne (164)
- 3.3. Działania fizyczne (169)
  - 3.3.1. Uruchamianie systemu przy użyciu dyskietki lub płyty CD włamywacza (170)
  - 3.3.2. Ponowna konfiguracja pamięci CMOS (171)
  - 3.3.3. Dodawanie hasła CMOS (172)

    - 3.3.4. Obrona przed trybem pojedynczego użytkownika (173)
    - 3.3.5. Obrona przed kradzieżą przy użyciu dyskietki (175)
    - 3.3.6. Zapobieganie atakom przy użyciu kombinacji Ctrl-Alt-Del (175)
- 3.4. Wybrane krótkie zagadnienia (176)
    - 3.4.1. Modemy kablowe (176)
    - 3.4.2. $PATH: Katalog . grozi nieszczęściem (177)
    - 3.4.3. Blokowanie routingu źródłowego w IP (178)
    - 3.4.4. Blokowanie fałszowania adresów IP (180)
    - 3.4.5. Automatyczne blokowanie ekranu (181)
    - 3.4.6. /etc/mailcap (182)
    - 3.4.7. Program chattr oraz bit niezmienności (183)
    - 3.4.8. Bezpieczne usuwanie danych (184)
    - 3.4.9. Synchroniczne operacje wejścia-wyjścia (185)
    - 3.4.10. Znaczniki montowania służące do zwiększenia zabezpieczeń (186)
    - 3.4.11. Ukrywanie UDP w TCP oraz SSH (187)
    - 3.4.12. Problem z programem man (188)
    - 3.4.13. Ustawianie ograniczeń przy użyciu poleceń *limit (190)
    - 3.4.14. Dostępna publicznie historia poleceń powłoki (191)
    - 3.4.15. Podstawy protokołu rozwiązywania adresów (ARP) (192)
    - 3.4.16. Zapobieganie modyfikacjom pamięci podręcznej ARP (193)
    - 3.4.17. Atakowanie przełączników (195)
    - 3.4.18. Odpieranie ataków ARP na systemy oraz przełączniki (198)
    - 3.4.19. Technologia WEP (200)
    - 3.4.20. Przechwytywanie danych z diod LED (203)
    - 3.4.21. Powrót do powłoki (204)
    - 3.4.22. Zabezpieczenia dostawcy ISP (205)
    - 3.4.23. Podsłuchiwanie terminali (ttysnoop) (208)
    - 3.4.24. Program Star Office (208)
    - 3.4.25. Programy VMware, Wine, DOSemu oraz podobne (209)
- 3.5. Ataki za pomocą urządzeń terminalowych (209)
    - 3.5.1. Przechwytywanie klawisza funkcyjnego (210)
    - 3.5.2. Podatność na przeprogramowanie klawiszy złożonych (211)
    - 3.5.3. Zmiana pliku z logiem w programie xterm (211)
- 3.6. Podglądanie zawartości dysku (212)
    - 3.6.1. Prawdziwe usuwanie plików (213)
    - 3.6.2. Usuwania starych poufnych danych umieszczonych w wolnych blokach (216)
    - 3.6.3. Usuwanie całej zawartości dysku (219)
    - 3.6.4. Zniszczenie twardego dysku (220)

Rozdział 4. Powszechne włamania przy wykorzystaniu podsystemów (221)

- 4.1. Usługi NFS, mountd oraz portmap (222)
- 4.2. Program Sendmail (224)
    - 4.2.1. Wykorzystywanie oddzielnych lub wielu serwerów pocztowych w celu dodatkowego zabezpieczenia (226)
    - 4.2.2. Podstawowe zabezpieczenia programu Sendmail (227)
    - 4.2.3. Opcje bezpieczeństwa programu Sendmail (230)
    - 4.2.4. Fałszowanie adresu nadawcy wiadomości pocztowych (234)
    - 4.2.5. Skąd pochodzą te wszystkie niechciane wiadomości? (234)

    - 4.2.6. Wyłączanie przesyłania niechcianych wiadomości (237)
    - 4.2.7. Blokowanie niechcianych wiadomości (237)
    - 4.2.8. Oszukiwanie robotów poszukujących adresów (238)
    - 4.2.9. Umożliwianie ograniczonego zaufania (238)
    - 4.2.10. Zezwalanie klientom POP oraz IMAP na wysyłanie poczty (240)
    - 4.2.11. Uniemożliwianie użycia otwartych list dystrybucyjnych (241)
    - 4.2.12. Atak DoS na program Sendmail, polegający na zapełnieniu dysku (241)
- 4.3. Program Telnet (242)
- 4.4. Usługa FTP (243)
    - 4.4.1. Konfiguracja anonimowej usługi FTP (246)
    - 4.4.2. Zagrożenia spowodowane przez serwery pośredniczące FTP (252)
- 4.5. Usługi rsh, rcp, rexec oraz rlogin (253)
    - 4.5.1. Bezpieczeństwo programów R* (254)
    - 4.5.2. Niebezpieczeństwo programów R* (255)
- 4.6. Usługa DNS (named) (256)
    - 4.6.1. Ograniczanie konsekwencji nadużycia usługi named (257)
    - 4.6.2. Służyć człowiekowi (258)
- 4.7. Serwery POP oraz IMAP (260)
    - 4.7.1. Hasła w wierszu poleceń (262)
- 4.8. Konfiguracja Samby (264)
    - 4.8.1. Czym jest Samba? (265)
    - 4.8.2. Wersje (265)
    - 4.8.3. Czy Samba jest zainstalowana? (265)
    - 4.8.4. Jaką wersję Samby posiadam? (266)
    - 4.8.5. Plik smb.conf (266)
    - 4.8.6. Plik smbpasswd (268)
    - 4.8.7. Plik odwzorowań użytkowników (269)
    - 4.8.8. Pliki z logami (270)
    - 4.8.9. Dynamiczne pliki danych (271)
    - 4.8.10. Bezpieczna konfiguracja Samby (271)
    - 4.8.11. Bezpieczeństwo sieciowe usługi Samba (272)
    - 4.8.12. Bezpieczeństwo plików Samby (275)
    - 4.8.13. Bezpieczeństwo użytkownika (280)
    - 4.8.14. Bezpieczeństwo zarządzania Sambą (284)
    - 4.8.15. Wykorzystywanie SSL z Sambą (286)
- 4.9. Blokowanie odwołań do programu Squid (286)
- 4.10. Usługa syslogd (290)
- 4.11. Usługa print (lpd) (291)
- 4.12. Usługa ident (292)
- 4.13. Usługi INND oraz News (293)
- 4.14. Bezpieczeństwo twoich danych w firmie rejstrującej domeny (294)

Rozdział 5. Ataki powszechnie stosowane przez włamywaczy (297)

- 5.1. Ataki przypuszczane przy użyciu predefiniowanych narzędzi (298)
- 5.2. Fałszowanie pakietów (299)
    - 5.2.1. Dlaczego udaje się fałszowanie pakietów UDP (302)
    - 5.2.2. Fałszowanie sekwencji TCP (304)
    - 5.2.3. Przechwytywanie sesji TCP (305)
- 5.3. Ataki typu SYN Flood (306)

- 5.4. Obrona przed atakami typu SYN Flood (307)
- 5.5. Zapobieganie fałszowaniu sekwencji TCP (307)
- 5.6. Sztormy pakietów, ataki smurfów oraz fraglesi (308)
    - 5.6.1. Zapobieganie wykorzystaniu systemu w charakterze wzmacniacza (310)
    - 5.6.2. Obrona przed atakiem używającym sztormu pakietów (312)
    - 5.6.3. Routery Cisco (313)
    - 5.6.4. Ataki DDoS: zasoby sieciowe z narzędziami do przeciwdziałania (314)
- 5.7. Przepełnianie buforów oraz niszczenie zawartości pamięci (314)
- 5.8. Techniki fałszowania (315)
    - 5.8.1. Fałszowanie wiadomości pocztowych (316)
    - 5.8.2. Atak realizowany przy użyciu adresu MAC (317)
    - 5.8.3. Zmiana pamięci podręcznej ARP (318)
    - 5.8.4. Zmiana pamięci podręcznej DNS (319)
- 5.9. Atak typu Man-in-the-Middle (319)

Rozdział 6. Zaawansowane problemy bezpieczeństwa (323)

- 6.1. Konfigurowanie zabezpieczeń w przeglądarce Netscape (324)
    - 6.1.1. Ważne preferencje przeglądarki Netscape (324)
    - 6.1.2. Przeglądanie własnych cookies (328)
    - 6.1.3. Preferencje użytkowników w przeglądarce Netscape (328)
    - 6.1.4. Narzędzie Netscape Personal Security Manager (329)
    - 6.1.5. Bezpieczeństwo skryptów Java w przeglądarce Netscape (329)
- 6.2. Blokowanie dostępu do urządzeń wejścia-wyjścia (331)
    - 6.2.1. Dlaczego urządzenie /dev/tty ma tryb 666? (337)
    - 6.2.2. Bezpieczeństwo bufora konsoli wirtualnej (337)
    - 6.2.3. Szyfrujący sterownik dysku (337)
- 6.3. Usuwanie problemów z serwerem Apache (httpd) (338)
    - 6.3.1. Prawa własności i uprawnienia serwera Apache (339)
    - 6.3.2. Server Side Includes (SSI) (340)
    - 6.3.3. Dyrektywa ScriptAlias (341)
    - 6.3.4. Zapobieganie zmianom ustawień ogólnosystemowych (341)
    - 6.3.5. Kontrolowanie katalogów dostępnych dla Apache (342)
    - 6.3.6. Kontrolowanie rozszerzeń plików dostępnych dla Apache (342)
    - 6.3.7. Inne ustawienia (343)
    - 6.3.8. Opróżnianie bazy danych (344)
    - 6.3.9. Blokowanie niepożądanych osób (347)
    - 6.3.10. Odsyłacze do witryny (347)
- 6.4. Specjalne techniki dla serwerów WWW (348)
    - 6.4.1. Zbuduj niezależne twierdze (349)
    - 6.4.2. Nie ufaj skryptom CGI (349)
    - 6.4.3. Ukryte zmienne formularzy i zatrute cookies (350)
    - 6.4.4. Proszę, weź sobie naszych pracowników (350)
    - 6.4.5. Blokowanie robota przeszukującego strony internetowe (351)
    - 6.4.6. Niebezpieczne programy CGI (352)
    - 6.4.7. Dziura w programie CGI query (353)
    - 6.4.8. Odszyfrowanie zakodowanych adresów URL (354)
    - 6.4.9. Dziura w programie CGI counterfiglet (356)
    - 6.4.10. Dziura w programie CGI phf (356)
    - 6.4.11. Skrypty i programy CGI (356)

    - 6.4.12. Wymuszenie blokowania adresów URL (363)
    - 6.4.13. Wykrywanie zmodyfikowanych stron internetowych (365)
- 6.5. Jednokierunkowa ścieżka danych karty kredytowej (366)
- 6.6. Zapewnianie najwyższego poziomu bezpieczeństwa (370)
- 6.7. Ograniczanie miejsca i czasu logowania (379)
- 6.8. Nietypowe, ale niebezpieczne problemy (381)
    - 6.8.1. Zabezpieczanie przed atakami przepełnienia bufora (381)
    - 6.8.2. Usuwanie zagrożenia chroot() (383)
    - 6.8.3. Atak Symlink (385)
    - 6.8.4. Problem z katalogami lost+found (388)
    - 6.8.5. Wyścig rm -r (389)
- 6.9. Usuwanie symulatorów logowania (390)
    - 6.9.1. Aktualizacja pliku /etc/issue (392)
    - 6.9.2. Dostosowanie programu /bin/login (394)
    - 6.9.3. Obsługa Secure Attention Key w jądrze (394)
- 6.10. Ochrona przed przepełnieniem bufora za pomocą Libsafe (397)

Rozdział 7. Ustanawianie zasad zabezpieczeń (399)

- 7.1. Ogólne zasady (400)
- 7.2. Zasady użytkowania komputerów (401)
- 7.3. Zasady dotyczące kont użytkowników (403)
- 7.4. Zasady dotyczące poczty elektronicznej (404)
- 7.5. Zasady dotyczące komunikacji za pomocą wiadomości błyskawicznych (Instant Messaging) (406)
- 7.6. Zasady dotyczące serwera WWW (407)
- 7.7. Zasady dotyczące serwera plików i baz danych (408)
- 7.8. Zasady dotyczące zapory sieciowej (409)
- 7.9. Zasady dotyczące komputerów biurkowych (409)
- 7.10. Zasady dotyczące komputerów przenośnych (410)
- 7.11. Zasady usuwania komputerów i nośników (414)
- 7.12. Zasady dotyczące topologii sieci (414)
    - 7.12.1. Zasady dotyczące topologii sieci wewnętrznej (415)
- 7.13. Zasady zgłaszania problemów (418)
- 7.14. Zasady własności (418)
- 7.15. Zasady dotyczące zasad (419)

Rozdział 8. "Zaufanie" do innych komputerów (421)

- 8.1. Bezpieczne i niebezpieczne systemy (422)
- 8.2. Nie ufaj nikomu - najwyższy poziom bezpieczeństwa (423)
- 8.3. Systemy Linux i UNIX pod kontrolą (424)
- 8.4. Systemy mainframe pod kontrolą (426)
- 8.5. Jedno okno jest warte tysiąca dziur (426)
- 8.6. Słabe punkty w zaporze sieciowej (428)
- 8.7. Wirtualne sieci prywatne (432)
- 8.8. Linux i wirusy (433)

Rozdział 9. Nietypowe metody włamania (435)

- 9.1. Techniki rodem z filmu Mission Impossible (435)
- 9.2. Szpiedzy (438)
    - 9.2.1. Szpiegostwo przemysłowe (439)
- 9.3. Fanatycy i ataki samobójcze (439)

Rozdział 10. Analiza przypadków (441)

- 10.1. Wyznania kreta w systemie Berkeley (442)
- 10.2. Błędni rycerze (445)
- 10.3. Ken Thompson włamuje się do marynarki (447)
- 10.4. Koń trojański w maszynie wirtualnej (448)
- 10.5. Wpadka ze zmianą wpisów DNS firmy AOL (449)
- 10.6. Ja naprawdę jestem niewinny, przysięgam! (451)
- 10.7. Włamania realizowane z wykorzystaniem laptopa i budki telefonicznej (452)
- 10.8. Kilka centów z każdego dolara (453)
- 10.9. Organizacja non-profit ma pecha (454)
- 10.10. Upór czasami się opłaca (455)
- 10.11. Pakiet .Net z wirusem Nimda (456)

Rozdział 11. Ostatnio zaobserwowane metody włamań (459)

- 11.1. Ataki fragmentacji (460)
- 11.2. Niepowodzenie maskarady IP dla ICMP (461)
- 11.3. Atak Ping of Death zatapia holenderskiego spedytora (462)
- 11.4. Kapitanie, ktoś nas skanuje! (ukryte skanowanie) (463)
- 11.5. Modemy kablowe - marzenie krakera (464)
- 11.6. Użycie programu sendmail do blokowania ataków e-mailowych (464)
- 11.7. Odgadywanie adresów kont za pomocą programu sendmail (465)
- 11.8. Tajemnicza blokada bazy danych Ingres (466)
- 11.9. Śledzenie użytkowników (466)
    - 11.9.1. Numer seryjny Pentium III (467)
    - 11.9.2. Szpiegowanie poprzez identyfikator GUID (467)
- 11.10. Koordynowane ataki DDoS (468)
- 11.11. Ukryte konie trojańskie (472)
    - 11.11.1. Do czego potrzebne są pakiety zwrotne echa ICMP? (473)
    - 11.11.2. Przyszłe kierunki rozwoju koni trojańskich (474)
    - 11.11.3. Tryb promiscuous w komunikatach jądra (475)
- 11.12. Narzędzie Linuxconf i port TCP 98 (476)
- 11.13. Złośliwe znaczniki i skrypty HTML (476)
- 11.14. Problemy z formatowaniem i procedura syslog() (477)

Część II Przygotowanie do ataku (479)
Rozdział 12. Zwiększanie bezpieczeństwa systemu (481)

- 12.1. Zabezpieczanie sesji użytkownika za pomocą SSH (481)
    - 12.1.1. Kompilacja SSH2 (484)
    - 12.1.2. Konfiguracja SSH (486)
    - 12.1.3. Wykorzystanie SSH (489)
    - 12.1.4. Przekazywanie poleceń sesji X za pomocą SSH (491)
    - 12.1.5. Wykorzystanie sftp (491)

    - 12.1.6. Wykorzystanie scp (492)
    - 12.1.7. Obsługa innych serwisów TCP za pomocą SSH (493)
    - 12.1.8. Zagrożenia, przed którymi SSH nie uchroni (495)
- 12.2. Virtual Private Networks (VPN) (496)
    - 12.2.1. Zagrożenia w sieciach VPN (496)
    - 12.2.2. VPN z użyciem SSH, PPP oraz Perla (500)
    - 12.2.3. CIPE (Crypto IP Encapsulation) (502)
    - 12.2.4. VPN z wykorzystaniem FreeS/WAN IPSec (502)
    - 12.2.5. PPTP (Point-to-Point Tunneling Protocol) (503)
    - 12.2.6. Zebedee (503)
    - 12.2.7. Pomiary wydajności sieci VPN (503)
- 12.3. Pretty Good Privacy (PGP) (504)
- 12.4. Wykorzystanie GPG do łatwego szyfrowania plików (505)
    - 12.4.1. Pobieranie GPG (507)
    - 12.4.2. Kompilacja (507)
    - 12.4.3. Wykorzystanie GPG (508)
    - 12.4.4. Generowanie i zarządzanie własnym kluczem (510)
    - 12.4.5. Wymiana kluczy (512)
    - 12.4.6. Rozpowszechnianie własnego klucza publicznego (515)
    - 12.4.7. Pliki podpisów (516)
    - 12.4.8. Szyfrowanie i podpisywanie listów e-mail (518)
    - 12.4.9. Szyfrowanie kopii zapasowych oraz inne wykorzystania gpg (519)
    - 12.4.10. Bezpieczeństwo GPG na bardzo wysokim poziomie (520)
- 12.5. Zapory sieciowe oraz DMZ z wykorzystaniem IP Tables (522)
    - 12.5.1. Teoria w praktyce: zabezpieczanie niewielkiej sieci (522)
    - 12.5.2. Zalety IP Tables w stosunku do IP Chains (538)
    - 12.5.3. Wady IP Tables w stosunku do IP Chains (539)
    - 12.5.4. Śledzenie połączeń w IP Tables - fakty i mity (543)
    - 12.5.5. Zwalczanie przejęć połączeń oraz ataków ICMP (545)
    - 12.5.6. Konfiguracja zapory sieciowej w dystrybucji Red Hat (547)
    - 12.5.7. Konfiguracja zapory sieciowej w dystrybucji SuSE Linux (549)
    - 12.5.8. Sztuczki i techniki związane z zaporami sieciowymi (551)
    - 12.5.9. Tworzenie zapory sieciowej oraz DMZ za pomocą IP Tables (570)
    - 12.5.10. Czego nie można zrealizować za pomocą IP Tables (571)
    - 12.5.11. Maskarada IP (NAT) - szczegóły (573)
    - 12.5.12. Funkcje IP Tables (578)
    - 12.5.13. Uruchamianie skryptu konfigurującego zaporę (580)
    - 12.5.14. Budowanie DMZ (583)
    - 12.5.15. Sekrety routowania (588)
    - 12.5.16. Mniej popularne funkcje IP Tables (590)
    - 12.5.17. Zapory sieciowe z kontrolą stanu (591)
    - 12.5.18. Zagrożenia SSH (592)
    - 12.5.19. Dostęp do poczty za pomocą połączeń szyfrowanych (594)
- 12.6. Zapora sieciowa oraz DMZ za pomocą IP Chains (595)
    - 12.6.1. Czego nie można zrealizować za pomocą IP Chains (597)
    - 12.6.2. Maskarada IP (NAT) w wersji IP Chains (599)
    - 12.6.3. Polecenia IP Chains (604)
    - 12.6.4. Uruchamianie skryptu konfigurującego zaporę (606)
    - 12.6.5. Podstawowe wykorzystanie zapory sieciowej zbudowanej za pomocą IP Chains (610)

    - 12.6.6. Blokowanie zagrożeń z zewnątrz (611)
    - 12.6.7. Maskarada IP (619)
    - 12.6.8. Konfiguracja DMZ (621)
    - 12.6.9. Zapory sieciowe z kontrolą stanu (623)
    - 12.6.10. Zagrożenia SSH (625)
    - 12.6.11. Dostęp do poczty za pomocą połączeń szyfrowanych (627)

Rozdział 13. Przygotowanie sprzętu (629)

- 13.1. Wyczucie czasu (629)
- 13.2. Zaawansowane przygotowania (632)
- 13.3. Przełączanie na system zapasowy (634)
    - 13.3.1. Wybór systemów wymagających przygotowania systemu zapasowego (634)
    - 13.3.2. Dwa typy systemów zapasowych (635)
    - 13.3.3. Projektowanie zapasowego systemu bezpieczeństwa (635)
    - 13.3.4. Utrzymanie systemu zapasowego w pogotowiu (637)
    - 13.3.5. Sprawdzanie pamięci podręcznej (639)
    - 13.3.6. Dysk zapasowy (640)

Rozdział 14. Przygotowanie konfiguracji (641)

- 14.1. TCP Wrappers (641)
    - 14.1.1. Wykorzystanie TCP Wrappers (643)
    - 14.1.2. Zaawansowane wykorzystanie TCP Wrappers (644)
- 14.2. Adaptacyjne zapory sieciowe: zakładanie pułapek na włamywaczy za pomocą Cracker Trap (646)
    - 14.2.1. Konfiguracja (654)
    - 14.2.2. Plik /etc/services (655)
    - 14.2.3. Pliki /etc/xinetd.d/* (657)
    - 14.2.4. Plik /etc/inetd.conf (658)
    - 14.2.5. Plik /etc/hosts.allow (660)
    - 14.2.6. Plik /etc/hosts.deny (661)
    - 14.2.7. Przechwytywanie ataków za pomocą przekierowania portów (662)
    - 14.2.8. Wykorzystanie PortSentry w połączeniu z Cracker Trap (666)
- 14.3. Blokowanie serwisów włamywaczy za pomocą modyfikacji jądra Linuksa (666)
- 14.4. Ćwiczenia pożarowe (668)
    - 14.4.1. Lądowanie awaryjne (669)
    - 14.4.2. To tylko test (670)
    - 14.4.3. Zagrożenia i środki ostrożności (670)
    - 14.4.4. Planowanie materii do ćwiczeń (671)
    - 14.4.5. Systemy testowe (671)
    - 14.4.6. Bezpieczne konie trojańskie (672)
    - 14.4.7. Rozmiar ma znaczenie (673)
    - 14.4.8. Sprawiamy więcej kłopotu (674)
- 14.5. Włamania do własnego systemu przy pomocy brygad tygrysa (675)
    - 14.5.1. Testy penetracyjne (677)

Rozdział 15. Skanowanie własnego systemu (679)

- 15.1. Skaner zabezpieczeń Nessus (680)
- 15.2. Testery zabezpieczeń SARA i SAINT (680)
- 15.3. Maper sieci nmap (681)
- 15.4. Wykrywacz ataków Snort (686)
- 15.5. Skanowanie i analizowanie za pomocą programu SHADOW (687)
- 15.6. John the Ripper (687)
- 15.7. Zapisywanie sum kontrolnych bazy danych RPM (688)
    - 15.7.1. Niestandardowe dyskietki ratunkowe (689)

Część III Wykrywanie włamania (691)
Rozdział 16. Monitorowanie aktywności (693)

- 16.1. Pliki z logami (694)
- 16.2. Pliki z logami: sposoby i kontrsposoby (695)
- 16.3. Używanie programu Logcheck do sprawdzania logów, których nigdy nie sprawdzasz (696)
- 16.4. Używanie programu PortSentry do blokowania hakerów (702)
- 16.5. HostSentry (708)
- 16.6. Przywoływanie administratora systemu: włamanie w toku! (708)
- 16.7. Przykład automatycznego przywoływania (709)
- 16.8. Rozbudowywanie przykładu automatycznego przywoływania (711)
- 16.9. Informowanie o użyciu poleceń telnet i rsh (713)
- 16.10. Wykrywanie ataków ARP i MAC za pomocą programu Arpwatch (715)
- 16.11. Monitorowanie użycia portów (719)
- 16.12. Monitorowanie ataków za pomocą programu Ethereal (720)
    - 16.12.1. Budowanie programu Ethereal (720)
    - 16.12.2. Używanie programu Ethereal (721)
- 16.13. Monitorowanie sieci lokalnej za pomocą programu tcpdump (722)
    - 16.13.1. Budowanie programu tcpdump (722)
    - 16.13.2. Używanie programu tcpdump (723)
- 16.14. Monitorowanie skanerów za pomocą programu Deception Tool Kit (DTK) (726)
- 16.15. Monitorowanie procesów (729)
    - 16.15.1. Monitorowanie obciążenia (731)
- 16.16. Cron: śledzenie krakerów (732)
- 16.17. Identyfikacja dzwoniącego (732)

Rozdział 17. Wyszukiwanie w systemie anomalii (733)

- 17.1. Wyszukiwanie podejrzanych plików (733)
    - 17.1.1. Analiza podejrzanych plików (736)
    - 17.1.2. Rutynowe porównywanie zawartości plików (736)
- 17.2. Narzędzie Tripwire (738)
    - 17.2.1. Instalowanie programu Tripwire (739)
    - 17.2.2. Użycie programu Tripwire (740)
    - 17.2.3. Przed czym program Tripwire nie chroni? (742)
    - 17.2.4. Programy stanowiące alternatywę dla narzędzia Tripwire (743)
- 17.3. Wykrywanie usuniętych plików wykonywalnych (743)
- 17.4. Wykrywanie kart sieciowych działających w trybie promiscuous (745)
    - 17.4.1. L0pht AntiSniff (748)

- 17.5. Wyszukiwanie procesów działających w trybie promiscuous (749)
- 17.6. Automatyczne wykrywanie włamań na strony internetowe (750)

Część IV Przywracanie systemu po włamaniu (755)
Rozdział 18. Przywracanie kontroli nad systemem (759)

- 18.1. Wyszukiwanie aktywnych procesów uruchomionych przez włamywacza (760)
  - 18.1.1. Obsługa usuniętych plików wykonywalnych (761)
- 18.2. Obsługa aktywnych procesów uruchomionych przez włamywacza (762)
  - 18.2.1. Popularne konie trojańskie (768)
- 18.3. Odcięcie modemów, sieci, drukarek i systemów (770)

Rozdział 19. Wykrywanie i usuwanie uszkodzeń (773)

- 19.1. Sprawdzenie logów systemowych znajdujących się w katalogu /var/log (774)
- 19.2. Demony syslogd i klogd (774)
- 19.3. Zdalne logowanie (775)
- 19.4. Interpretowanie wpisów zawartych w logach systemowych (775)
  - 19.4.1. Program lastlog (776)
  - 19.4.2. Plik messages (777)
  - 19.4.3. Plik syslog (780)
  - 19.4.4. Plik kernlog (780)
  - 19.4.5. Plik cron (781)
  - 19.4.6. Plik xferlog (781)
  - 19.4.7. Plik daemon (782)
  - 19.4.8. Plik mail (782)
- 19.5. Kontrola innych logów (784)
- 19.6. Sprawdzanie odpowiedzi narzędzia TCP Wrappers (784)
- 19.7. Sposoby uszkadzania systemu plików (785)
- 19.8. Umieszczanie sfałszowanych danych (786)
- 19.9. Modyfikowanie programów monitorujących (786)
- 19.10. W domu pełnym luster (787)
- 19.11. Przywracanie kontroli (787)
- 19.12. Wyszukiwanie plików zmienionych przez włamywaczy (788)
  - 19.12.1. Interpretacja wyniku działania polecenia tar -d (791)
  - 19.12.2. Przyspieszenie operacji sprawdzania plików przy użyciu programu rpm (792)
  - 19.12.3. Naprawa pakietów RPM (793)
  - 19.12.4. Przywracanie baz danych (794)
  - 19.12.5. Uszkodzenie urządzeń peryferyjnych (795)
  - 19.12.6. Kradzież za pośrednictwem "diabelskich elektronów" (795)
  - 19.12.7. Metody uszkadzania jądra (796)
- 19.13. Metody identyfikacji włamywacza (796)
  - 19.13.1. Dowód modyfikacji danych (797)
- 19.14. Wyszukiwanie programów z ustawionym bitem set-UID (798)
- 19.15. Identyfikacja konia trojańskiego mstream (799)

Rozdział 20. Namierzanie komputera włamywacza (801)

- 20.1. Tłumaczenie liczbowego adresu IP za pomocą programu nslookup (802)

- 20.2. Tłumaczenie liczbowego adresu IP za pomocą programu dig (802)
- 20.3. Wyszukiwanie właścicieli domen .com (803)
- 20.4. Wyszukiwanie organizacji na podstawie adresu IP (804)
- 20.5. Sprawdzanie systemów .gov (804)
- 20.6. Korzystanie z programu ping (806)
- 20.7. Korzystanie z programu traceroute (807)
- 20.8. Wyniki z sąsiednich systemów (808)
- 20.9. Przykład międzynarodowego tropienia crakera (808)
- 20.10. Czy na pewno znalazłeś napastnika? (809)
- 20.11. Inni administratorzy: czy im zależy? (811)
    - 20.11.1. Przygotowanie dowodów na użytek administratora systemu (812)

Dodatki (813)

Dodatek A Zasoby internetowe związane z najnowszymi sposobami włamań i ochrony (815)

- A.1. Listy wysyłkowe - obowiązkowe (816)
    - A.1.1. Centrum koordynacyjne CERT rządu Stanów Zjednoczonych (817)
    - A.1.2. Komitet doradczy CIAC rządu Stanów Zjednoczonych (817)
    - A.1.3. Bugtraq (817)
    - A.1.4. Lista X-Force firmy ISS (818)
    - A.1.5. Witryna mail-abuse.org (818)
- A.2. Listy wysyłkowe - opcjonalne (819)
    - A.2.1. Lista wysyłkowa SSH (819)
    - A.2.2. Lista wysyłkowa Network World Fusion (819)
- A.3. Grupy dyskusyjne (819)
- A.4. Adresy URL witryn poświęconych bezpieczeństwu (820)
    - A.4.1. Witryna Kurta Seifrieda (820)
    - A.4.2. Security Focus (820)
    - A.4.3. Analiza sądowa (820)
    - A.4.4. Witryna Hackerwhacker (821)
    - A.4.5. Numery portów używanych przez krakerów (821)
    - A.4.6. Opisy linuksowych wirusów (821)
    - A.4.7. Centrum NIPC agencji FBI (821)
    - A.4.8. FIRST (821)
    - A.4.9. Strona Linux Weekly News (822)
    - A.4.10. Linux Today (822)
    - A.4.11. Instytut SANS (822)
- A.5. Adresy URL witryn z narzędziami zabezpieczającymi (822)
    - A.5.1. Witryna autora książki (822)
    - A.5.2. Pobieranie programu Secure SHell (SSH) (824)
    - A.5.3. Pobieranie skryptu Bastille Linux (824)
    - A.5.4. Pobieranie skryptu wzmacniającego system SuSE (825)
    - A.5.5. Pobieranie programu Linux Intrusion Detection System (825)
    - A.5.6. Pretty Good Privacy (PGP) (825)
    - A.5.7. GNU Privacy Guard (GPG) (826)
    - A.5.8. Narzędzie tcpdump (826)
    - A.5.9. Ethereal - sniffer z interfejsem graficznym (826)
    - A.5.10. Narzędzie sniffit (827)
    - A.5.11. Pobieranie narzędzia Tripwire (827)

    - A.5.12. Zamienniki programu Tripwire (827)
    - A.5.13. Pobieranie skanera zabezpieczeń Nessus (828)
    - A.5.14. Pobieranie testera zabezpieczeń SARA (828)
    - A.5.15. Pobieranie programu nmap (828)
    - A.5.16. Pobieranie wykrywacza ataków Snort (829)
    - A.5.17. Pobieranie programu SHADOW (829)
    - A.5.18. Pobieranie testera zabezpieczeń SAINT (829)
    - A.5.19. Pobieranie narzędzia konfiguracyjnego IP Chains (829)
    - A.5.20. Pobieranie pakietu SSL (830)
    - A.5.21. Pobieranie programu sslwrap (830)
    - A.5.22. Witryna WWW programu CVS z obsługą SSH (830)
    - A.5.23. Pobieranie szyfrującego sterownika dysku (831)
    - A.5.24. Sendmail bez przywilejów roota (831)
    - A.5.25. Pobieranie programu postfix (831)
    - A.5.26. Libsafe (831)
    - A.5.27. Zaobserwowane ataki (832)
    - A.5.28. Analizowanie sieci napastnika z witryny Sam Spade (832)
- A.6. Adresy URL dokumentacji (832)
    - A.6.1. Dokumentacja Linuksa (832)
    - A.6.2. Pisanie bezpiecznych programów (833)
- A.7. Adresy URL narzędzi ogólnego zastosowania (833)
    - A.7.1. Debugger ddd (834)
    - A.7.2. Obliczanie czasu w różnych strefach czasowych (834)
- A.8. Adresy URL specyfikacji i definicji (834)
    - A.8.1. Pomarańczowa księga (834)
    - A.8.2. RFC 1813: NFS Version 3 (835)
    - A.8.3. Słownik NSA terminów związanych z bezpieczeństwem komputerowym (835)
- A.9. Aktualizacje dystrybucji Linuksa (835)
    - A.9.1. Red Hat (835)
    - A.9.2. Slackware (836)
    - A.9.3. SuSE (836)
    - A.9.4. Mandrake (836)
    - A.9.5. Caldera (836)
    - A.9.6. Debian (836)
    - A.9.7. Yellow Dog (837)
- A.10. Inne aktualizacje oprogramowania (837)
    - A.10.1. Pobieranie programu Sendmail (837)
    - A.10.2. Baza danych PostgreSQL (837)
    - A.10.3. Repozytoria oprogramowania Open Source (838)

Dodatek B Usługi i porty sieciowe (839)
Dodatek C Poziomy zagrożenia (845)
Dodatek D Skróty (857)
Skorowidz (863)