

Przedmowa (21)

Rozdział 1. Wprowadzenie do bezpieczeństwa systemów otwartych (25)

- Wstęp (25)
 - Narzędzia zastosowane w tej książce (27)
- Korzystanie z oprogramowania na podstawie licencji GNU (27)
 - Płatne oprogramowanie GPL (28)
 - Czy mogę używać oprogramowania GPL w mojej firmie? (29)
- Umiejętności obsługi oprogramowania: osobliwości systemów otwartych i sposoby radzenia sobie z nimi (29)
 - Ogólny brak wsparcia podczas instalacji i konfiguracji oprogramowania (30)
 - Nieczęste i nieregularne harmonogramy uaktualnień (30)
 - Dominacja poleceń z linii (30)
 - Brak kompatybilności wstecz i standardowej dystrybucji (30)
 - Niewygodne ścieżki uaktualnień (31)
 - Konflikty obsługi bibliotek i wsparcie limitowanej liczby platform (31)
 - Zmiany interfejsów (31)
 - Częściowo opracowane rozwiązania (32)
- Z jakich archiwów powinienem korzystać: RPM czy Tar? (33)
 - Archiwa typu Tar (33)
 - Red Hat Package Manager (34)
 - Debian (35)
- Pozyskiwanie oprogramowania typu open source (35)
 - SourceForge (35)
 - Freshmeat (36)
 - Packetstorm (37)
 - SecurityFocus (38)
 - Czy pobieranie danych jest bezpieczne? (38)
- Krótki przegląd metod szyfrujących (39)
 - Szyfrowanie za pomocą klucza symetrycznego (40)
 - Szyfrowanie przy użyciu klucza asymetrycznego (41)
- Klucz publiczny i relacje zaufania (42)
 - Szyfrowanie jednostronne (43)
 - GNU Privacy Guard (43)
 - Instalacja GNU Privacy Guard (44)
 - Pomijanie weryfikacji klucza publicznego (50)
 - Zastosowanie GPG do sprawdzania podpisów w archiwach tar (50)
 - Polecenie md5sum (51)
- Procedury inspekcji (51)
 - Ochrona stacji sieciowych (52)
 - Zabezpieczanie danych przesyłanych w sieci (52)
 - Zabezpieczanie obrębu sieci (53)
- Podsumowanie (54)
- Szybki przegląd rozwiązań (55)
 - Korzystanie z oprogramowania na podstawie licencji GNU (55)
 - Umiejętności obsługi oprogramowania: osobliwości systemów otwartych i sposoby radzenia sobie z nimi (55)
 - Z jakich archiwów powinienem korzystać: RPM czy Tar? (55)
 - Pozyskiwanie oprogramowania typu open source (56)
 - Krótki przegląd metod szyfrujących (56)

- o Klucz publiczny i relacje zaufania (57)
 - o Procedury inspekcji (57)
- Najczęściej zadawane pytania (57)

Rozdział 2. Wzmacnianie systemu operacyjnego (59)

- Wstęp (59)
- Aktualizacja systemu operacyjnego (60)
 - o Poprawki i uaktualnienia systemu Red Hat Linux (60)
- Radzenie sobie z obsługą systemu (61)
 - o Poprawki systemu Red Hat Linux: korekty i zalecenia (61)
 - Studium przypadku: poprawianie błędów (63)
- Ręczne blokowanie niepotrzebnych usług i portów (64)
 - o Blokowanie usług (65)
 - Plik xinetd.conf (65)
- Blokowanie portów (67)
 - o Dobrze znane i zarejestrowane porty (67)
 - o Określanie portów do zablokowania (68)
 - o Blokowanie portów (70)
 - Usługi xinetd (70)
 - Samodzielne usługi (70)
- Wzmacnianie systemu za pomocą programu Bastille (71)
 - o Funkcje programu Bastille (72)
 - o Wersje programu Bastille (79)
 - o Instalacja i wdrożenie programu Bastille (79)
 - o Cofanie zmian dokonanych za pomocą programu Bastille (87)
- Kontrola dostępu na poziomie administracyjnym za pomocą Sudo (90)
 - o Wymagania systemowe (91)
 - o Polecenie sudo (92)
 - o Pobieranie programu sudo (93)
 - o Instalacja sudo (94)
 - o Konfiguracja sudo (97)
 - o Korzystanie z sudo (100)
 - o No Password (102)
 - o Rejestracja poleceń sudo (102)
- Zarządzanie plikami rejestracyjnymi (105)
- Stosowanie programów wspomagających rejestrowanie (106)
 - o SWATCH (107)
 - o Scanlogd (109)
 - o Syslogd-ng (109)
- Podsumowanie (111)
- Szybki przegląd rozwiązań (112)
 - o Aktualizacja systemów operacyjnych (112)
 - o Radzenie sobie z obsługą systemu (113)
 - o Ręczne blokowanie niepotrzebnych usług i portów (113)
 - o Blokowanie portów (113)
 - o Wzmacnianie systemu za pomocą programu Bastille (114)
 - o Kontrola dostępu na poziomie administracyjnym za pomocą Sudo (114)
 - o Zarządzanie plikami rejestracyjnymi (114)
 - o Stosowanie programów wspomagających rejestrowanie (115)

- Najczęściej zadawane pytania (115)

Rozdział 3. Skanowanie systemu i jego badanie (117)

- Wprowadzenie (117)
- Skanowanie w poszukiwaniu wirusów za pomocą aplikacji antywirusowych (118)
 - o Podstawy wirusów w systemie Linux (118)
 - o Używanie programu AntiVir (119)
 - Tryb z użyciem klucza oraz bez jego użycia (121)
 - Uzyskiwanie licencji programu AntiVir (122)
 - Ćwiczenie: uaktualnianie programu AntiVir (122)
 - o Używanie programu TkAntivir (124)
 - Wymagane biblioteki oraz ustawienia systemu (124)
 - Sprawdzanie obecności w systemie wirusów sektora rozruchowego oraz wirusów pocztowych (125)
 - Dodatkowe informacje (126)
 - Ćwiczenie: wykorzystanie programu TkAntivir (127)
- Skanowanie systemu w poszukiwaniu ataków typu DDoS za pomocą programu Zombie Zapper (129)
 - o W jaki sposób działają programy typu zombie i jak je powstrzymać? (130)
 - o Kiedy powinienem użyć programu typu zombie zapper? (131)
 - Jakiego programu Zombie Zapper powinienem użyć? (132)
 - Dlaczego program Zombie Zapper wymaga kompilacji? (132)
 - Ćwiczenie: używanie programu Zombie Zapper (133)
- Skanowanie portów systemowych za pomocą Gnome Service Scan Port Scanner (134)
 - o Wymagane biblioteki (136)
 - o W jakim celu mam używać programu sprawdzającego porty? (136)
 - Ćwiczenie: używanie programu Gnome Service Scanner (137)
- Używanie programu Nmap (138)
 - o Czy program Nmap nie jest tylko kolejnym skanerem portów? (138)
 - o Nabywanie oraz instalacja programu Nmap (140)
 - Powszechnie używane opcje programu Nmap (140)
 - o Zastosowane przykłady (142)
 - Sprawdzanie całych sieci lub podsieci (142)
 - Sprawdzanie selektywne (143)
 - Dalsze ukrywanie operacji sprawdzania (143)
 - Zapisywanie do pliku tekstowego i odczytywanie z niego (144)
 - Sprawdzanie zapór sieciowych oraz systemów IDS (145)
 - Ćwiczenie: fałszowanie adresu źródłowego (145)
 - Regulowanie szybkości sprawdzania (146)
 - Ćwiczenie: przeprowadzanie "paranoicznego" skanowania (146)
 - Ćwiczenie: używanie programu Nmap (147)
 - o Używanie programu Nmap w trybie interaktywnym (147)
 - Ćwiczenie: używanie programu Nmap w trybie interaktywnym (148)
- Wykorzystanie NmapFE jako graficznego interfejsu użytkownika (149)
 - Ćwiczenie: używanie programu NmapFE (150)
- Wykorzystanie Remote Nmap jako centralnego urządzenia skanującego (150)
 - Ćwiczenie: sprawdzanie systemów za pomocą programu Rnmap (151)
- Instalacja programu Cheops w celu monitorowania sieci komputerowej (154)
 - o W jaki sposób działa program Cheops? (155)

- Uzyskiwanie programu Cheops (156)
 - Wymagane biblioteki (156)
- o Interfejs programu Cheops (157)
 - Tworzenie mapy związków pomiędzy komputerami (158)
 - Metody monitorowania przez program Cheops (158)
 - Kwestia połączenia (160)
 - Ćwiczenie: instalacja i konfiguracja programu Cheops (161)
- Instalacja programu Nessus w celu przetestowania zabezpieczeń demonów (165)
 - o Związki pomiędzy klientem a serwerem programu Nessus (167)
 - Klienci programu Nessus przeznaczone dla systemu Windows (168)
 - Wymagane biblioteki (169)
 - Kolejność instalacji (170)
 - o Konfiguracja modułów dodatkowych (172)
 - Tworzenie nowego użytkownika programu Nessus (172)
 - Baza danych reguł (173)
 - Ćwiczenie: instalacja programu Nessus oraz wykonanie sprawdzenia słabych punktów systemu (174)
 - o Uaktualnianie programu Nessus (177)
 - o Podstawy różnicowego, niezależnego oraz ciągłego sprawdzania (178)
 - Ćwiczenie: przeprowadzanie sprawdzania różnicowego oraz niezależnego za pomocą programu Nessus (180)
- Podsumowanie (181)
- Szybki przegląd rozwiązań (182)
 - o Skanowanie w poszukiwaniu wirusów za pomocą aplikacji antywirusowych (182)
 - o Skanowanie systemu w poszukiwaniu ataków typu DDoS za pomocą programu Zombie Zapper (183)
 - o Skanowanie portów systemowych za pomocą Gnome Service Scan Port Scanner (183)
 - o Wykorzystanie programu Nmap (183)
 - o Wykorzystanie NmapFE jako graficznego interfejsu użytkownika (184)
 - o Wykorzystanie Remote Nmap jako centralnego urządzenia skanującego (184)
 - o Instalacja programu Cheops w celu monitorowania sieci komputerowej (184)
 - o Instalacja programu Nessus w celu przetestowania zabezpieczeń demonów (185)
- Najczęściej zadawane pytania (FAQ) (185)

Rozdział 4. Instalacja Systemu Wykrywania Włamań (IDS) (187)

- Wprowadzenie (188)
- Podstawy strategii IDS i ich rodzaje (190)
 - o Rodzaje IDS (191)
 - Aplikacje IDS oparte na serwerze (191)
 - Aplikacje IDS oparte na sieci komputerowej (192)
 - Aplikacje IDS a odporność na uszkodzenia (193)
 - Co system IDS może zrobić dla mnie? (194)
 - Która strategia IDS jest najlepsza? (197)
 - o Aplikacje IDS oparte na sieci komputerowej a zapory sieciowe (198)
 - Aplikacje IDS (198)
- Instalacja programu Tripwire służącego do wykrywania zmian plików (200)

- o Zależności programu Tripwire (201)
 - o Dostępność (202)
 - o Instalacja programu Tripwire (202)
 - Pliki programu Tripwire (202)
 - o Kroki instalacji programu Tripwire (203)
 - Konfiguracja pliku założeń programu Tripwire (204)
 - Tworzenie pliku założeń programu Tripwire (205)
 - Tryb inicjalizacji bazy danych (205)
 - Sprawdzanie możliwości wysyłania wiadomości e-mail (206)
 - Tryb sprawdzania integralności (207)
 - Określanie innej bazy danych (207)
 - Odczytywanie raportów (208)
- Uaktualnianie aplikacji Tripwire w celu umożliwienia pojawiania się zmian w systemie operacyjnym (208)
 - o Uaktualnianie pliku założeń (209)
 - Co mam zrobić w przypadku wykrycia różnic? (209)
- Konfiguracja programu Tripwire w celu informowania o zmianach (209)
 - o Ćwiczenie: instalacja programu Tripwire (210)
 - o Ćwiczenie: zabezpieczanie bazy danych programu Tripwire (211)
 - o Ćwiczenie: wykorzystanie programu cron do automatycznego uruchamiania programu Tripwire (212)
- Instalacja programu PortSentry działającego jako system IDS na serwerze (212)
 - o Ważne pliki programu PortSentry (213)
 - o Instalacja programu PortSentry (214)
- Konfiguracja programu PortSentry w celu zablokowania użytkowników (214)
- Optymalizacja programu PortSentry w celu rozpoznawania rodzajów ataku (215)
 - o Ćwiczenie: instalacja i konfiguracja programu PortSentry (216)
 - o Ćwiczenie: czyszczenie reguł programu Ipchains (218)
 - o Ćwiczenie: uruchamianie zewnętrznych poleceń przy użyciu programu PortSentry (219)
- Instalacja i konfiguracja programu Snort (220)
 - o Dostępność (220)
 - Biblioteki dodatkowe (221)
 - o Podstawy reguł programu Snort (221)
 - o Zmienne programu Snort (222)
 - o Pliki i katalogi programu Snort (222)
 - o Moduły dodatkowe programu Snort (223)
 - o Uruchamianie programu Snort (224)
 - Rejestracja danych przechwyconych przez program Snort (225)
- Uruchamianie programu Snort w charakterze aplikacji IDS działającej w sieci komputerowej (227)
 - o Pomijanie serwerów (227)
 - Dodatkowe opcje dotyczące rejestracji: pliki tekstowe, Tcpdump oraz bazy danych (228)
- Konfiguracja programu Snort w celu rejestrowania do bazy danych (229)
 - o Kontrolowanie rejestrowania oraz komunikatów alarmowych (230)
 - o Uzyskiwanie informacji (230)
 - Ćwiczenie: instalacja programu Snort (231)
 - Ćwiczenie: wykorzystanie programu Snort w charakterze aplikacji IDS (232)

- Ćwiczenie: konfiguracja programu Snort w celu rejestrowania danych w bazie danych (233)
 - Ćwiczenie: wykonanie zapytań ze zdalnego serwera do bazy danych programu Snort (239)
- Moduły dodatkowe programu Snort (240)
 - o SnortSnarf (240)
 - Ćwiczenie: wykorzystanie programu SnortSnarf do czytania plików dziennika programu Snort (240)
 - o Konsola analiz dla baz danych zawierających informacje o włamaniach (241)
- Podsumowanie (242)
- Szybki przegląd rozwiązań (242)
 - o Podstawy strategii IDS i ich rodzaje (242)
 - o Instalacja programu Tripwire służącego do wykrywania zmian plików (243)
 - o Uaktualnianie aplikacji Tripwire w celu umożliwienia pojawiania się zmian w systemie operacyjnym (243)
 - o Konfiguracja programu Tripwire w celu informowania o zmianach (244)
 - o Instalacja programu PortSentry działającego jako system IDS na serwerze (244)
 - o Konfiguracja programu PortSentry w celu zablokowania użytkowników (244)
 - o Optymalizacja programu PortSentry w celu rozpoznawania rodzajów ataku (244)
 - o Instalacja i konfiguracja programu Snort (245)
 - o Uruchamianie programu Snort w charakterze aplikacji IDS działającej w sieci komputerowej (245)
 - o Konfiguracja programu Snort w celu rejestrowania do bazy danych (245)
 - o Moduły dodatkowe programu Snort (245)
- Najczęściej zadawane pytania (FAQ) (246)

Rozdział 5. Rozwiązywanie problemów z siecią komputerową za pomocą programów podsłuchujących (247)

- Wprowadzenie (247)
- Podstawy analizy pakietów oraz wymiany potwierdzeń protokołu TCP (250)
 - o Uzgadnianie połączenia TCP (251)
 - Ustanawianie połączenia TCP (251)
 - Kończenie połączenia TCP (252)
- Tworzenie filtrów za pomocą Tcpdump (252)
 - o Opcje programu Tcpdump (254)
 - Wyrażenia programu Tcpdump (256)
 - Operatory logiczne (259)
 - Instalacja i używanie programu Tcpdump (261)
- Konfiguracja programu Ethereal do przechwytywania pakietów w sieci (263)
 - o Opcje programu Ethereal (265)
 - o Filtry programu Ethereal (266)
 - o Konfiguracja programu Ethereal i przechwytywanie pakietów (267)
- Przeglądanie ruchu w sieci komputerowej pomiędzy serwerami za pomocą EtherApe (271)
 - o Konfiguracja programu EtherApe i przeglądanie ruchu w sieci komputerowej (273)
- Podsumowanie (275)

- Szybki przegląd rozwiązań (276)
 - o Podstawy analizy pakietów oraz wymiany potwierdzeń protokołu TCP (276)
 - o Tworzenie filtrów za pomocą Tcpdump (277)
 - o Konfiguracja programu Ethereal do przechwytywania pakietów w sieci (277)
 - o Przeglądanie ruchu w sieci komputerowej pomiędzy serwerami za pomocą EtherApe (277)
- Najczęściej zadawane pytania (FAQ) (278)

Rozdział 6. Autoryzacja i szyfrowanie w sieci komputerowej (281)

- Wprowadzenie (281)
- Podstawy autoryzacji w sieci komputerowej (282)
 - o Atakowanie zaszyfrowanych protokołów (283)
- Tworzenie rozwiązań wykorzystujących autoryzację oraz szyfrowanie (285)
- Implementacja haseł jednorazowych (OTP oraz OPIE) (286)
 - o Jakie pliki zastępuje OPIE? (286)
 - o W jaki sposób działa OPIE? (287)
 - o Pliki i aplikacje OPIE (287)
 - opiepasswd (288)
 - Postać hasła (289)
 - Używanie opiekey (290)
 - o Używanie opieinfo oraz opiekey do tworzenia listy haseł (290)
 - o Instalacja OPIE (291)
 - Opcje konfiguracyjne (291)
 - Opcje instalacji (291)
 - o Odinstalowywanie OPIE (292)
 - Ćwiczenie: instalacja programu OPIE (292)
 - Ćwiczenie: instalacja klienta OPIE na zdalnym serwerze (294)
 - Ćwiczenie: używanie opie-tk i zezwalanie użytkownikom systemu Windows na stosowanie OPIE (295)
 - Ćwiczenie: instalacja opieftpd (296)
- Implementacja programu Kerberos w wersji 5 (297)
 - o Dlaczego Kerberos jest tak ważny? (299)
 - o Terminologia Kerberos (299)
 - o Zarządcy Kerberos (299)
 - o Proces autoryzacji Kerberos (301)
 - o W jaki sposób informacje przesyłane są przez sieć? (301)
 - o Tworzenie bazy danych systemu Kerberos (302)
 - o Wykorzystanie kadmin.local (302)
 - Wykorzystanie kadmin (303)
 - Używanie programu kadmin na komputerze klienta (305)
- Wykorzystanie polecenia kadmin do tworzenia haseł klientów Kerberos (306)
 - o Ustawianie strategii (306)
 - o Używanie kinit (306)
 - Polecenie kinit i ograniczenia czasowe (308)
 - o Zarządzanie danymi uwierzytelniającymi klienta Kerberos (308)
 - o Polecenie kdestroy (309)
 - Ćwiczenie: konfiguracja KDC (309)
- Ustanowienie zaufanej relacji klienta Kerberos za pomocą kadmin (312)
 - o Dodatkowe nazwy zarządców demonów (313)

- Logowanie do demona serwera Kerberos (314)
 - o Rozwiązywanie powszechnych problemów z klientem systemu Kerberos (315)
 - o Aplikacje klientów systemu Kerberos (316)
 - o Autoryzacja systemu Kerberos oraz klogin (316)
 - Ćwiczenie: konfiguracja klienta Kerberos (317)
- Podsumowanie (319)
- Szybki przegląd rozwiązań (319)
 - o Podstawy autoryzacji w sieci komputerowej (319)
 - o Tworzenie rozwiązań wykorzystujących autoryzację oraz szyfrowanie (319)
 - o Implementacja haseł jednorazowych (OTP oraz OPIE) (320)
 - o Implementacja programu Kerberos w wersji 5 (320)
 - o Wykorzystanie polecenia kadmin do tworzenia haseł klientów Kerberos (321)
 - o Ustanowienie zaufanej relacji klienta Kerberos za pomocą kadmin (321)
 - o Logowanie do demona serwera Kerberos (321)
- Najczęściej zadawane pytania (FAQ) (322)

Rozdział 7. Zapobieganie przechwytywaniu pakietów w sieci poprzez szyfrowanie (325)

- Wprowadzenie (326)
- Podstawy szyfrowania danych w sieci (326)
- Przechwytywanie i analiza niezaszyfrowanych pakietów w sieci (327)
- Wykorzystanie OpenSSH do szyfrowania pakietów przesyłanych pomiędzy dwoma serwerami (332)
 - o Pakiet OpenSSH (334)
- Instalacja OpenSSH (334)
- Konfiguracja SSH (338)
 - o W jaki sposób działa SSH (338)
 - Niezabezpieczona autoryzacja zdalnych poleceń (339)
 - Bezpieczna autoryzacja SSH (341)
- Wykorzystanie SSH do zabezpieczenia transmisji danych poprzez niezabezpieczoną sieć (343)
 - o Rozpowszechnianie klucza publicznego (345)
- Przechwytywanie i analiza zaszyfrowanych pakietów w sieci (349)
- Podsumowanie (352)
- Szybki przegląd rozwiązań (353)
 - o Podstawy szyfrowania sieci (353)
 - o Przechwytywanie i analiza niezaszyfrowanych pakietów w sieci (354)
 - o Wykorzystanie OpenSSH w celu zaszyfrowania pakietów przesyłanych pomiędzy dwoma serwerami (354)
 - o Instalacja i konfiguracja SSH na dwóch komputerach sieciowych (354)
 - o Wykorzystanie SSH do zabezpieczania transmisji danych poprzez niezabezpieczoną sieć komputerową (355)
 - o Przechwytywanie i analiza zaszyfrowanych pakietów w sieci (355)
- Najczęściej zadawane pytania (FAQ) (355)

Rozdział 8. Tworzenie wirtualnych sieci prywatnych (359)

- Wprowadzenie (359)
- Bezpieczne tunelowanie w wirtualnych sieciach prywatnych (360)
 - o Zdalne połączenie VPN (360)

- o Sieć VPN typu ruter-ruter (361)
 - o Sieć VPN typu serwer-serwer (362)
 - o Protokoły tunelowania (362)
- Wyjaśnienie architektury bezpieczeństwa IP (363)
 - o Stosowanie IPSec wraz z protokołem tunelowania VPN (367)
 - o Protokół wymiany kluczy internetowych (IKE) (368)
- Tworzenie wirtualnych sieci prywatnych przy użyciu FreeS/WAN (368)
 - o Pobieranie i rozpakowywanie FreeS/WAN (370)
 - o Kompilacja jądra w celu uruchomienia FreeS/WAN (372)
 - o Ponowna kompilacja FreeS/WAN w nowym jądrze (380)
 - o Konfiguracja programu FreeS/WAN (383)
 - Testowanie sieci (383)
 - Konfiguracja szyfrowania za pomocą klucza publicznego oraz bezpiecznej autoryzacji na końcach sieci VPN (387)
 - Uruchamianie tunelu (394)
 - Przechwytywanie ruchu w tunelu VPN (396)
 - Zamykanie tunelu VPN (397)
- Podsumowanie (398)
- Szybki przegląd rozwiązań (399)
 - o Bezpieczne tunelowanie poprzez wirtualne sieci prywatne (VPN) (399)
 - o Wyjaśnienie architektury bezpieczeństwa IP (399)
 - o Tworzenie wirtualnych sieci prywatnych przy użyciu FreeS/WAN (399)
- Najczęściej zadawane pytania (FAQ) (400)

Rozdział 9. Implementacja zapory sieciowej za pomocą Ipchains i Iptables (403)

- Wprowadzenie (404)
- Potrzeba stosowania zapory sieciowej (405)
 - o Tworzenie własnej zapory (407)
 - Wyjaśnienie terminologii związanej z filtrowaniem pakietów (407)
 - Wybór komputera pod zaporę działającą na podstawie systemu Linux (409)
 - Ochrona zapory sieciowej (410)
- Wykorzystywanie przekazywania i maskarady pakietów IP (411)
 - o Maskarada (413)
- Konfiguracja zapory sieciowej jako filtra pakietów sieciowych (414)
 - o Konfiguracja jądra (416)
 - Rozliczanie pakietów (416)
- Podstawy tabel i łańcuchów wykorzystywanych w zaporach sieciowych w systemie Linux (416)
 - o Obiekty wbudowane i łańcuchy definiowane przez użytkownika (417)
 - Określanie interfejsu (418)
 - Strategie ustawień (419)
 - o Wykorzystanie Ipchains do maskarady połączeń (421)
 - Moduły maskujące Ipchains (422)
 - o Wykorzystanie Iptables do maskarady połączeń (422)
 - Moduły Iptables (423)
 - Ćwiczenie: maskarada połączeń z wykorzystaniem Ipchains lub Iptables (424)
- Rejestrowanie pakietów na poziomie zapory sieciowej (424)

- o Ustalanie ograniczeń przy tworzeniu plików dziennika (425)
 - o Dodawanie i usuwanie reguł filtrowania pakietów (425)
 - Rodzaje ICMP (426)
 - Ćwiczenie: stworzenie osobistej zapory sieciowej i łańcucha definiowanego przez użytkownika (427)
 - o Przekierowanie portów za pomocą Ipchains i Iptables (429)
- Konfiguracja zapory sieciowej (430)
 - o Przygotowanie właściwych podstaw (430)
 - Tworzenie reguł zabezpieczających przed przechwytywaniem pakietów (430)
- Statystyki przepustowości zapory sieciowej (433)
 - o Wyświetlanie i zerowanie liczników (434)
 - Ustalanie rodzaju usług na routerze opartym na systemie Linux (434)
 - Ustawianie wartości określającej rodzaj usługi w Ipchains i Iptables (435)
- Używanie i uzyskiwanie zautomatyzowanych skryptów zapory sieciowej i narzędzi graficznych (437)
 - o Prace związane z zaporami sieciowymi będące w toku (439)
 - Ćwiczenie: korzystanie z aplikacji Firestarter w celu stworzenia własnej zapory sieciowej (439)
 - Ćwiczenie: korzystanie z zaawansowanych możliwości aplikacji Firestarter (446)
- Podsumowanie (447)
- Szybki przegląd rozwiązań (447)
 - o Potrzeba stosowania zapory sieciowej (447)
 - o Wykorzystywanie przesyłania i maskarady pakietów IP (448)
 - o Konfiguracja zapory sieciowej jako filtra pakietów sieciowych (449)
 - o Podstawy tabel i łańcuchów wykorzystywanych w zaporach sieciowych w systemie Linux (449)
 - o Rejestrowanie pakietów na poziomie zapory sieciowej (449)
 - o Konfiguracja zapory sieciowej (450)
 - o Statystyki używania zapory sieciowej (450)
 - o Używanie i uzyskiwanie zautomatyzowanych skryptów zapory sieciowej i narzędzi graficznych (451)
- Najczęściej zadawane pytania (FAQ) (451)

Rozdział 10. Instalacja serwera proxy przy użyciu programu Squid (455)

- Wprowadzenie (455)
- Korzyści wynikające ze stosowania serwera proxy (456)
 - o Pamięć podręczna serwera proxy (456)
 - o Tłumaczenie adresów sieciowych (NAT) (457)
- Odróżnianie filtra pakietów od serwera proxy (459)
- Implementacja internetowego serwera proxy przy użyciu programu Squid (460)
 - o Specyfikacja wymagań systemowych dla serwera proxy (463)
 - o Instalacja programu Squid (463)
 - o Konfiguracja programu Squid (466)
 - Znacznik http_port (467)
 - Znacznik cache_dir (468)
 - Znacznik acl (470)

- Znacznik http_access (472)
 - o Uruchamianie programu Squid i sprawdzanie jego działania (474)
- Konfiguracja klientów serwera proxy (475)
 - o Konfiguracja programów Netscape Navigator oraz Lynx (475)
 - Konfiguracja programu Netscape Navigator (475)
 - Konfiguracja programu Lynx (477)
 - o Konfiguracja programu Internet Explorer (opcjonalna) (478)
- Podsumowanie (479)
- Szybki przegląd rozwiązań (481)
 - o Korzyści wynikające ze stosowania serwera proxy (481)
 - o Odróżnianie filtra pakietów od serwera proxy (481)
 - o Implementacja internetowego serwera proxy przy użyciu programu Squid (481)
 - o Konfiguracja klientów serwera proxy (482)
- Najczęściej zadawane pytania (FAQ) (482)

Rozdział 11. Utrzymywanie zapór sieciowych (487)

- Wprowadzenie (487)
- Sprawdzanie działania zapór sieciowych (488)
 - o Fałszowanie pakietów IP (489)
 - o Otwarte porty (demony) (490)
 - o Monitorowanie systemowych dysków twardych, pamięci RAM oraz procesorów (490)
 - o Podejrzani użytkownicy, operacje logowania oraz ich okresy (491)
 - o Sprawdź bazę danych zawierającą reguły (491)
 - o Sprawdzaj możliwość połączenia z kierownictwem firmy i użytkownikami (492)
 - o Śledź na bieżąco sprawy dotyczące systemu operacyjnego (492)
 - o Skanowanie portów (493)
- Testowanie zapór sieciowych przy użyciu aplikacji Telnet, Ipchains, Netcat oraz SendIP (494)
 - o Ipchains (494)
 - o Telnet (495)
 - Wykorzystanie wielu terminali (495)
 - o Netcat (496)
 - Proste polecenia programu Netcat (496)
 - Dodatkowe polecenia programu Netcat (498)
 - Ćwiczenie: wykorzystanie programu Netcat (499)
 - o SendIP: fałszerz pakietów (500)
 - Składnia programu SendIP (500)
 - Ćwiczenie: używanie programu SendIP do badania zapory sieciowej (502)
- Podstawy rejestrowania, blokowania oraz opcji alarmowych (504)
 - o Firewall Log Daemon (504)
 - Uzyskiwanie programu Firelogd (505)
 - Składnia i opcje konfiguracyjne (505)
 - Format wiadomości (506)
 - Personalizacja wiadomości (507)

- Czytanie plików dziennika utworzonych przez inne zapory sieciowe (508)
 - Ćwiczenie: konfiguracja i kompilacja programu Firelogd (508)
- o Program Fwlogwatch (509)
 - Tryby programu Fwlogwatch (510)
 - Opcje programu Fwlogwatch i tworzenie raportów (511)
 - Ćwiczenie: tworzenie plików dziennika opartych na HTML-u za pomocą programu Fwlogwatch (514)
- o Automatyzacja działania programu Fwlogwatch (515)
 - Plik konfiguracyjny programu Fwlogwatch (515)
 - Opcje powiadamiania (517)
 - Opcje odpowiedzi (519)
 - Ćwiczenie: konfiguracja programu Fwlogwatch w celu automatycznego wysyłania alarmów i blokowania użytkowników (520)
- o Używanie programu Fwlogwatch wraz ze skryptami CGI (522)
 - Uzyskiwanie większej ilości informacji (522)
 - Przeglądanie wyników (523)
 - Ćwiczenie: wykorzystanie programu Cron oraz skryptów CGI programu Fwlogwatch do tworzenia automatycznych raportów HTML (525)
 - Dodatkowe funkcje programu Fwlogwatch (526)
- Uzyskiwanie dodatkowych narzędzi rejestrujących ruch na zaporze sieciowej (527)
- Podsumowanie (528)
- Szybki przegląd rozwiązań (529)
 - o Sprawdzanie działania zapór sieciowych (529)
 - o Testowanie zapór sieciowych przy użyciu aplikacji Telnet, Ipchains, Netcat oraz SendIP (530)
 - o Podstawy rejestrowania, blokowania oraz opcji alarmowych (531)
 - o Uzyskiwanie dodatkowych narzędzi raportujących działanie zapory sieciowej (532)
- Najczęściej zadawane pytania (FAQ) (532)

Dodatek A Rejestr programu Bastille (535)

Dodatek B Hack Proofing Linux - szybki przegląd rozwiązań (539)

Skorowidz (569)