

O Autorach (13)

Przedmowa (15)

Część I Tworzenie sieci komputerowej w oparciu o system Linux (19)

Rozdział 1. Przykłady sieci komputerowych (21)

- Przykłady sieci komputerowych (22)
 - o Bezpośrednie połączenie z siecią internetową (DCI) (22)
 - o Połączenie z siecią internetową za pośrednictwem strefy zdemilitaryzowanej (DMZI) (23)
- Opis funkcji serwera (25)
 - o Podstawy konfiguracji sieci DCI (26)
 - o Podstawy konfiguracji DMZI (28)
- Dodawanie podsieci do obu przykładowych sieci komputerowych (29)
- Podsumowanie (30)

Rozdział 2. Konfiguracja usług sieciowych w systemie Red Hat (33)

- Podstawy protokołu internetowego IP (34)
 - o Usługi sieciowe a model OSI (34)
 - o Podstawy protokołów warstwy transportowej (35)
- Podstawy protokołów warstwy sieci (przekazywanie pakietów IP) (36)
- Działanie protokołów warstwy łącza (ramki w sieci Ethernet) (37)
- Wygląd sieci opartej na systemie Red Hat Linux (38)
 - o Ważne pliki konfiguracyjne sieci (38)
 - o Ważne aplikacje oraz skrypty (42)
 - o arp/rarp (42)
 - o ifconfig (43)
 - o netstat (44)
 - o nmap (44)
 - o ping (44)
 - o redhat-config-network-druid/ redhat-config-network-cmd (45)
 - o route (45)
 - o sysctl (46)
 - o tcpdump (47)
 - o modprobe (47)
- Konfiguracja jednej lub większej liczby kart sieciowych (48)
 - o Przykład 1: Konfiguracja pojedynczego interfejsu sieciowego (48)
 - o Przykład 2: Konfiguracja dwóch interfejsów sieciowych (dwie podsieci) (52)
 - o Przykład 3: Konfiguracja routera w oparciu o system Red Hat Linux (55)
- Podsumowanie (59)

Rozdział 3. Nawiązywanie połączenia z siecią Internet przy użyciu łącza DSL (61)

- Podstawy technologii DSL (62)
- Terminologia stosowana w technologii DSL (66)
 - o Ogólne definicje (66)
 - o Rodzaje usług DSL (70)
- Tworzenie połączenia z siecią Internet przy użyciu łącza DSL (71)
 - o Uzyskiwanie połączenia internetowego DSL (71)
 - o Fizyczne podłączanie modemu DSL (71)

- o Konfiguracja wyposażenia udostępnianego przez dostawcę usługi DSL (73)
- Podstawowe wskazówki przydatne podczas rozwiązywania problemów (79)
- Podsumowanie (83)

Rozdział 4. Tworzenie systemu zapory sieciowej (85)

- Podstawy systemów zapór sieciowych (85)
 - o Zapory sieciowe filtrujące pakiety (86)
 - o Zapory pośredniczące (87)
 - o Zapory hybrydowe (88)
 - o Podstawy translacji adresów (NAT) (88)
 - o Wyjaśnienie przepływu pakietów w sieci Internet (89)
 - o Podstawy stanowych filtrów pakietów (Netfilter/iptables) (91)
- Tworzenie systemu zapory sieciowej (97)
 - o Ochrona sieci za pomocą prostego zestawu reguł (97)
 - o Zacieśnianie zapory sieciowej przy użyciu łańcuchów definiowanych przez użytkownika (104)
- Wpuszczanie z zewnątrz połączeń SSH (109)
 - o Konfiguracja serwera SSH (112)
 - o Modyfikacja serwera zapory sieciowej (atlas) w celu umożliwienia korzystania z usługi SSH (114)
- Zarządzanie systemem zapory sieciowej (116)
- Podsumowanie (117)

Rozdział 5. Rozwiązywanie prostych problemów (119)

- Rozwiązywanie problemów przy użyciu drzewa decyzyjnego (120)
- Rozwiązywanie problemów sieciowych w systemie Red Hat Linux (121)
 - o Czy zostało włączone zasilanie? (121)
 - o Czy nie została uszkodzona fizyczna instalacja sieci komputerowej? (122)
 - o Czy przełącznik sieciowy lub koncentrator jest skonfigurowany w sposób poprawny? (122)
 - o Czy interfejs sieciowy został skonfigurowany w sposób prawidłowy? (122)
- Rozwiązywanie problemów z połączeniem DSL (129)
 - o Sprawdzanie konfiguracji modemu DSL (routera) po stronie użytkownika (130)
 - o Sprawdzanie konfiguracji dostawcy usługi DSL (131)
 - o Sprawdzanie konfiguracji ISP (132)
- Rozwiązywanie problemów z bramką i zaporą sieciową (132)
 - o Sprawdzanie konfiguracji sieciowej w systemie Red Hat Linux (133)
 - o Sprawdzanie tras bramki oraz przekazywania pakietów IP (134)
 - o Sprawdzanie skryptów zapory sieciowej (136)
 - o Sprawdzanie modułów jądra oraz znaczników (137)
 - o Wykorzystywanie narzędzi podsłuchujących ruch w sieci (137)
- Dodatkowe informacje (139)
- Podsumowanie (139)

Część II Tworzenie serwera WWW (141)

Rozdział 6. Prosta konfiguracja serwera Apache (143)

- Podstawy języka HTML oraz protokołu HTTP (143)
 - o Protokół HTTP (143)
 - o Język HTML (HTML nie jest protokołem) (144)
- Serwer WWW Apache (148)
 - o Dyrektywy konfiguracyjne serwera Apache (149)
 - o Plik konfiguracyjny serwera Apache (149)
- Tworzenie prostej witryny WWW (158)
 - o Instalacja serwera Apache (158)
 - o Konfiguracja serwera Apache (159)
 - o Kontrolowanie działania serwera Apache (162)
 - o Używanie serwera Apache (163)
 - o Kontrola dostępu do serwera WWW za pomocą plików .htaccess oraz .htpasswd (163)
- Uruchamianie wirtualnego serwera WWW (164)
- Stosowanie protokołu SSL z serwerem Apache (167)
 - o Instalacja pakietu mod_ssl (168)
 - o Negocjacja SSL oraz certyfikaty (168)
 - o Centra autoryzacji (169)
 - o Konfiguracja serwera Apache w celu wykorzystywania protokołu HTTP z SSL (169)
- Tworzenie certyfikatów podpisanych przez CA (170)
- Rozwiązywanie problemów (171)
 - o Sprawdzanie systemowych plików dziennika systemu Linux (172)
 - o Sprawdzanie plików dziennika serwera Apache (172)
 - o Połączenie lokalne (173)
 - o Sprawdzanie konfiguracji serwera Apache (173)
 - o Jeśli mamy taką możliwość, należy użyć uproszczonego pliku httpd.conf (173)
 - o Stopniowe dodawanie nowych dyrektyw (174)
- Podsumowanie (174)

Rozdział 7. Tworzenie połączenia z bazą danych (175)

- Podstawy języka SQL (175)
- Instalacja oraz konfiguracja bazy MySQL (177)
- Dostęp do serwera SQL (178)
 - o Tworzenie bazy danych (179)
 - o Wykorzystywanie bazy danych MySQL (181)
- Wymiana danych z serwerem SQL przy użyciu skryptów (182)
 - o Wyświetlanie danych z bazy danych MySQL (183)
 - o Wstawianie danych do bazy danych MySQL (186)
 - o Modyfikacja danych w bazie danych MySQL (187)
 - o Wykorzystywanie skryptu CGI w celu dostępu do bazy danych SQL za pomocą przeglądarki (190)
- Zabezpieczanie bazy danych MySQL (195)
- Podsumowanie (196)

Rozdział 8. Tworzenie prostego serwera multimedialnego (197)

- Wprowadzenie do technologii strumieniowej (197)
- Fundacja Xiph.org (198)

- Udostępnianie strumieni danych dźwiękowych przy użyciu serwera Icecast (200)
 - o Instalacja oraz konfiguracja serwera Icecast (200)
 - o Instalacja oraz konfiguracja źródła Ices (202)
 - o Udostępnianie strumieni MP3 (203)
 - o Udostępnianie strumieni Ogg Vorbis (205)
- Rozwiązywanie problemów (218)
- Podsumowanie (220)

Część III Udostępnianie prostych usług internetowych (221)

Rozdział 9. Tworzenie serwera DNS (223)

- Podstawy systemu DNS (223)
 - o Domeny (224)
 - o Strefy (224)
 - o Autorytatywne serwery nazw (225)
 - o Podstawy procesu tłumaczenia nazwy przez klienta (226)
 - o Analiza prostego żądania przetłumaczenia nazwy (227)
- Rekordy zasobów (230)
 - o Stosowanie rekordu SOA (230)
 - o Definiowanie rekordów zasobów strefy (232)
 - o Instrukcje konfiguracyjne oraz parametry demona bind (232)
 - o Pliki konfiguracyjne /var/named/ (234)
- Konfiguracja prostego serwera DNS (235)
 - o Konfiguracja nadrzędnego serwera nazw (236)
 - o Konfiguracja pomocniczego serwera nazw (240)
- Dodawanie środków bezpieczeństwa (241)
 - o Stosowanie list ACL (241)
 - o Stosowanie podpisów cyfrowych podczas wymiany stref (243)
 - o Uruchamianie demona named w środowisku chroot (244)
 - o Uruchamianie oraz zatrzymywanie działania serwera nazw (245)
- Tworzenie wielu plików stref (246)
- Konfiguracja serwera rozdzielonej domeny (248)
 - o Konfiguracja serwera nazw dla sieci prywatnej w konfiguracji rozdzielonej domeny (249)
 - o Konfiguracja serwera nazw dla sieci DMZ w konfiguracji domeny podzielonej (251)
- Rozwiązywanie problemów (252)
 - o named-checkzone (252)
 - o named-checkconf (252)
 - o dig (253)
 - o host (253)
 - o tcpdump (254)
- Podsumowanie (254)

Rozdział 10. Konfiguracja serwera pocztowego SMTP (255)

- Trochę teorii na temat poczty elektronicznej (255)
 - o Kompatybilność (256)
 - o Wydajność (257)
 - o Wykorzystanie (257)

- Kolejki (257)
- Parametry konfiguracyjne (257)
 - o Składnia parametrów (258)
 - o Wartości bezpośrednie (258)
 - o Pliki (258)
 - o Bazy danych i tablice (258)
- Obsługa niechcianej poczty (259)
- Najważniejsze parametry z pliku main.cf (259)
 - o queue_directory (259)
 - o command_directory (259)
 - o daemon_directory (260)
 - o mail_owner (260)
 - o default_privs (260)
 - o myhostname (261)
 - o mydomain (261)
 - o myorigin (261)
 - o inet_interfaces (261)
 - o mydestination (262)
 - o local_recipient_maps (262)
 - o masquerade_domains (262)
 - o masquerade_exceptions (262)
 - o local_transport (263)
 - o alias_maps (263)
 - o alias_database (263)
 - o home_mailbox (263)
 - o mail_spool_directory (263)
 - o mailbox_command (264)
 - o mailbox_transport (264)
 - o fallback_transport (264)
 - o luser_relay (264)
 - o smtpd_recipient_limit (265)
 - o smtpd_timeout (265)
 - o mynetworks_style (265)
 - o mynetworks (266)
 - o allow_untrusted_routing (266)
 - o maps_rbl_domains (266)
 - o smtpd_client_restrictions (266)
 - o smtpd_sender_restrictions (267)
 - o smtpd_recipient_restrictions (267)
 - o smtpd_helo_required (267)
 - o smtpd_helo_restrictions (267)
 - o smtpd_delay_reject (268)
 - o strict_rfc821_envelopes (268)
 - o header_checks (268)
 - o body_checks (268)
 - o message_size_limit (269)
 - o relay_domains (269)
 - o mynetworks (269)
 - o smtpd_banner (269)
 - o local_destination_concurrency_limit (270)

- o default_destination_concurrency_limit (270)
 - o debug_peer_list (270)
 - o debug_peer_level (270)
 - o debugger_command (270)
 - o disable_vrfy_command (271)
- Konfiguracja podstawowych plików (271)
 - o Konfiguracja pliku master.cf (271)
 - o Konfiguracja pliku aliases (271)
 - o Konfiguracja pliku virtual (272)
 - o Konfiguracja pliku canonical (272)
 - o Konfiguracja pliku access (272)
- Wykorzystanie poleceń administracyjnych (273)
- Terminologia serwerów poczty elektronicznej (273)
 - o Programy typu Mail User Agent (274)
 - o Skład poczty (274)
 - o Programy typu Mail Transport Agent (274)
 - o Nagłówki poczty (275)
 - o Koperta (275)
- Przykładowe konfiguracje (276)
 - o Przykład 1: Wysyłanie poczty (276)
 - o Przykład 2: Przyjmowanie poczty dla różnych domen (276)
 - o Przykład 3: Wirtualne domeny w stylu systemu Postfix (277)
 - o Przekazywanie poczty między adresami wirtualnymi (278)
 - o Przykład 4: Weryfikacja ustawień DNS dla serwera poczty (280)
 - o Przykład 5: Przekazywanie całej poczty przez serwer centralny (287)
 - o Przykład 6: Konfiguracja serwera centralnego (288)
 - o Przykład 7: Minimalizacja ilości niechcianej poczty (288)
 - o Podstawy systemu spamassassin (290)
- Podsumowanie (291)

Rozdział 11. FTP (293)

- Podstawy protokołu FTP (293)
- Washington University FTP (WU-FTPD) (294)
 - o Instalacja WU-FTPD (295)
 - o Plik konfiguracyjny /etc/xinetd.d/wu-ftp (296)
 - o Plik ftpaccess (298)
 - o Plik ftpconversions (302)
- Konfiguracja serwera FTP trybu rzeczywistego (303)
- Konfigurowanie kont gościnnych (303)
- Konfiguracja kont anonimowych (305)
 - o Konfiguracja kont anonimowych (305)
 - o Konfiguracja możliwości anonimowego przesyłania plików na serwer (306)
- Rozwiązywanie problemów z serwerem WU-FTPD (308)
 - o Kontrola na poziomie ogólnym (309)
 - o Problemy z trybem gościnnym (311)
 - o Problemy z trybem anonimowym (313)
- Podsumowanie (314)

Rozdział 12. Konfiguracja Samby (315)

- Wprowadzenie do Samby (315)
 - Składnia pliku smb.conf (317)
 - Parametry pliku smb.conf (317)
 - Struktura pliku smb.conf (318)
- Przykłady konfiguracji Samby (319)
 - Konfiguracja Samby w celu wykorzystania szyfrowanych haseł (319)
 - Tworzenie zasobów Samby (323)
 - Dostęp do macierzystych katalogów użytkowników (323)
 - Uprawnienia Linuksa i Samby (324)
 - Wykorzystanie makr Samby (330)
 - Udostępnianie drukarek sieciowych za pomocą Linuksa i Samby (331)
- Narzędzie SWAT (335)
- Rozwiązywanie problemów (335)
- Podsumowanie (336)

Część IV Zarządzanie serwerami linuksowymi (339)

Rozdział 13. Automatyzacja sieciowych kopii zapasowych (341)

- Wprowadzenie do systemu AMANDA (342)
- Szczegóły systemu AMANDA (343)
 - Części serwerowa i kliencka systemu AMANDA (343)
 - Serwisy sieciowe (344)
 - Pliki konfiguracyjne (345)
 - Narzędzia systemu AMANDA (347)
- Wykorzystanie systemu AMANDA (348)
 - Konfiguracja minimalistycznego systemu kopii zapasowych (349)
 - Konfiguracja prostego systemu kopii zapasowych (352)
 - Automatyzacja procesu wykonywania kopii zapasowych (357)
- Rozwiązywanie problemów (357)
- Podsumowanie (358)

Rozdział 14. Zwiększanie niezawodności serwera (361)

- Lokalizacja słabych punktów (361)
- Wykorzystanie systemu plików ext3 (363)
- Wykorzystanie macierzy RAID (365)
 - RAID programowy (365)
 - Implementacja programowej macierzy RAID (368)
- Tworzenie klastra o wysokiej dostępności (370)
 - Mechanizm działania HA (371)
 - Tryby przejęcia obsługi (371)
 - Tworzenie prostego klastra wysokiej dostępności na Linuksie (372)
 - Testowanie systemu Heartbeat (374)
- Podsumowanie (375)

Część V Zwiększanie bezpieczeństwa (379)

Rozdział 15. Podstawy bezpieczeństwa serwerów (381)

- Zrozumienie zagrożeń (381)
- Znaczenie poprawek systemowych (382)

- Identyfikacja napastników (384)
 - Kategorie napastników (384)
- Przewidywanie ataków (386)
- Sposoby obrony (389)
- Podsumowanie (396)

Rozdział 16. Podstawy bezpiecznej administracji systemów (397)

- Administrator systemu a administrator bezpieczeństwa (397)
- Automatyczna aktualizacja, łaty i zagrożenia (398)
- Środowisko produkcyjne i rozwojowe (400)
- Automatyczne instalowanie poprawek (402)
- Minimalizacja, standaryzacja i upraszczanie (404)
 - Zrozumieć minimalizację (404)
 - Trzy cnoty główne (407)
- Monitorowanie i bezpieczna zdalna administracja (407)
- Centralny system zarządzania (409)
- Monitorowanie stanu (410)
- Podsumowanie (411)

Rozdział 17. Wzmacnianie systemu (413)

- Zrozumieć proces wzmacniania systemu (413)
 - Ręczne wzmacnianie systemu (415)
 - Blokowanie lub usuwanie niepotrzebnych programów (415)
 - Powtórka z procesu uruchamiania Linuksa (417)
 - Kontynuacja audytu demona sieciowego (422)
 - Automatyczne wzmacnianie systemu za pomocą Bastille Linux (435)
 - Moduł zabezpieczeń kont użytkowników (435)
 - Moduł bezpieczeństwa procesu uruchamiania systemu (436)
 - Konfiguracja ustawień mechanizmu PAM (436)
 - Moduł deaktywacji demonów (436)
 - Moduł blokujący dostęp do narzędzi (437)
 - Moduł uprawnień do plików (437)
 - Moduł dzienników (437)
 - Moduł wydruku (438)
 - Moduł zabezpieczania inetd lub xinetd (438)
 - Moduł zabezpieczenia katalogu tymczasowego (438)
 - Moduł Apache (439)
 - Moduł BIND (DNS) (439)
 - Moduł FTP (439)
 - Moduł sendmail (440)
 - Moduł zapory sieciowej (440)
 - Moduł detekcji skanowania portów (440)
- Podsumowanie (440)

Rozdział 18. Proste systemy wykrywania włamań (443)

- Sieciowe i systemowe wykrywanie włamań (443)
- Określenie zakresu odpowiedzialności (444)

- o Odpowiedzialność administratora (444)
 - o Odpowiedzialność oznacza władzę (446)
- Mechanizmy sieciowe (447)
 - o Pakiety (447)
 - o Adresy IP (449)
 - o Porty (451)
 - o ICMP (454)
 - o UDP (454)
 - o TCP (454)
 - o Rozpoznania i zagrożenia (456)
- Projektowanie defensywnej konfiguracji sieci (459)
 - o Filtrowanie na routerach oraz zapory sieciowe (459)
 - o Filtrowanie ingress i egress (460)
 - o DMZ (460)
 - o Hosty bastionowe (460)
 - o Dedykowane serwery (461)
- Projektowanie strategii wykrywania włamań (461)
- Ustalanie reguł (462)
 - o Detektory włamań nie wykrywają włamań (463)
 - o Pozytywne specyfikacje są złe (463)
 - o Negatywne specyfikacje nie są lepsze (463)
 - o Heurystyczne wykrywanie anomalii - Święty Graal (464)
- Przykładowy system NIDS - Snort (464)
 - o Opis i historia (464)
 - o Przegląd funkcji systemu Snort (wybrane opcje wiersza poleceń) (465)
- Podsumowanie (467)

Rozdział 19. Monitorowanie plików dziennika oraz reagowanie na zdarzenia (469)

- Odczytywanie systemowych plików dziennika (469)
- Rejestrowanie danych w plikach dziennika (470)
 - o Rejestrowanie danych w plikach dziennika aplikacji (471)
 - o Rejestrowanie danych w plikach dziennika systemu (472)
 - o Rejestrowanie danych w hybrydowych plikach dziennika (473)
 - o Syslog (474)
- Wykonywanie akcji wybranych przez selektor (475)
 - o Pola selektorów, jednostki oraz priorytety (475)
 - o Miejsca docelowe (477)
- Wykorzystywanie plików dziennika (478)
 - o Analiza bezpośrednia (479)
 - o Narzędzia przetwarzające pliki dziennika (479)
 - o egrep (480)
 - o Tworzenie raportów (482)
 - o Narzędzie monitorujące pliki dziennika (485)
- Zarządzanie odpowiedziami na zdarzenia (486)
 - o Najgorsza jest panika (486)
 - o Przewidywanie oznacza politykę bezpieczeństwa (487)
- Podsumowanie (487)

Dodatki (489)

Dodatek A Konfiguracja komutowanego połączenia typu dial-up z siecią Internet (491)

- Lokalizacja modemu (491)
 - o Nawiązywanie połączenia z siecią Internet (493)

Dodatek B Automatyzacja konfiguracji serwera (499)

- Instalacja systemu przy użyciu programu Kickstart (500)
- Tworzenie pliku konfiguracyjnego programu Kickstart (500)
- Tworzenie dyskietki startowej programu Kickstart (501)
- Instalacja przy użyciu programu Kickstart (503)
- Tworzenie własnych pakietów RPM (503)
 - o Wygląd pakietu RPM (504)
 - o Przykładowy pakiet RPM (504)

Dodatek C Stosowanie usługi DHCP (507)

- Instalacja dhcpd (507)
- Konfiguracja stacji roboczej działającej pod kontrolą systemu Red Hat Linux w celu korzystania z usługi DHCP (508)
- Konfiguracja komputera działającego pod kontrolą systemu Windows w charakterze klienta DHCP (509)

Skorowidz (511)