Przedmowa (9)
Rozdział 1. Tripwire i migawki systemu (17)

- 1.0. Wprowadzenie (17)
- 1.1. Konfiguracja Tripwire (20)
- 1.2. Wyświetlanie założeń i konfiguracji (22)
- 1.3. Modyfikacja założeń i konfiguracji (22)
- 1.4. Podstawowe sprawdzanie spójności (24)
- 1.5. Sprawdzanie spójności w trybie tylko do odczytu (25)
- 1.6. Zdalne sprawdzanie spójności (26)
- 1.7. Superskrupulatne sprawdzanie spójności (28)
- 1.8. Drogie i superskrupulatne sprawdzanie spójności (30)
- 1.9. Automatyczne sprawdzanie spójności (30)
- 1.10. Odczytywanie najnowszego raportu Tripwire (31)
- 1.11. Uaktualnianie bazy danych (32)
- 1.12. Dodawanie plików do bazy danych (33)
- 1.13. Usuwanie plików z bazy danych (35)
- 1.14. Sprawdzanie systemów plików Windows VFAT (35)
- 1.15. Sprawdzanie plików zainstalowanych za pomocą menedżera pakietów RPM (36)
- 1.16. Sprawdzanie spójności za pomocą programu rsync (37)
- 1.17. Ręczne sprawdzanie spójności (38)

Rozdział 2. Zapory sieciowe: oprogramowanie iptables i ipchains (41)

- 2.0. Wprowadzenie (41)
- 2.1. Weryfikacja adresu źródłowego (43)
- 2.2. Blokowanie sfałszowanych adresów (45)
- 2.3. Blokowanie całego ruchu sieciowego (47)
- 2.4. Blokowanie ruchu przychodzącego (48)
- 2.5. Blokowanie ruchu wychodzącego (49)
- 2.6. Blokowanie przychodzących żądań usług (50)
- 2.7. Blokowanie dostępu z określonego hosta zdalnego (51)
- 2.8. Blokowanie dostępu do określonego hosta zdalnego (52)
- 2.9. Blokowanie dostępu do wszystkich serwerów WWW określonej zdalnej sieci (53)
- 2.10. Blokowanie połączeń z komputerów zdalnych, zezwalanie na lokalne (54)
- 2.11. Kontrola dostępu na podstawie adresów MAC (55)
- 2.12. Zezwalanie wyłącznie na dostęp SSH (56)
- 2.13. Blokowanie wychodzących połączeń Telnet (57)
- 2.14. Zabezpieczanie wydzielonego serwera (58)
- 2.15. Blokowanie pingów (59)
- 2.16. Wyświetlanie reguł zapory sieciowej (60)
- 2.17. Usuwanie reguł zapory sieciowej (61)
- 2.18. Wstawianie reguł zapory sieciowej (62)
- 2.19. Zapisywanie konfiguracji zapory sieciowej (63)
- 2.20. Ładowanie konfiguracji zapory sieciowej (64)
- 2.21. Testowanie konfiguracji zapory sieciowej (66)
- 2.22. Budowanie złożonych drzew reguł (67)
- 2.23. Uproszczone rejestrowanie (69)

Rozdział 3. Kontrola dostępu do sieci (71)

- 3.0. Wprowadzenie (71)
- 3.1. Wyświetlanie interfejsów sieciowych (74)
- 3.2. Włączanie i wyłączanie interfejsu sieciowego (75)
- 3.3. Włączanie i wyłączanie usługi (xinetd) (76)
- 3.4. Włączanie i wyłączanie usługi (inetd) (77)
- 3.5. Dodawanie nowej usługi (xinetd) (78)
- 3.6. Dodawanie nowej usługi (inetd) (79)
- 3.7. Ograniczanie dostępu zdalnym użytkownikom (80)
- 3.8. Ograniczanie dostępu zdalnym hostom (xinetd) (82)
- 3.9. Ograniczanie dostępu zdalnym hostom (xinetd z biblioteką libwrap) (83)
- 3.10. Ograniczanie dostępu zdalnym hostom (xinetd w połączeniu z tcpd) (84)
- 3.11. Ograniczanie dostępu zdalnym hostom (inetd) (85)
- 3.12. Ograniczanie dostępu o określonych porach dnia (86)
- 3.13. Ograniczanie określonym hostom dostępu do serwera SSH (88)
- 3.14. Ograniczanie dostępu do serwera SSH w zależności od konta systemowego (89)
- 3.15. Ograniczanie zasobów usług do określonych katalogów systemu plików (90)
- 3.16. Zapobieganie atakom powodującym odmowę obsługi (92)
- 3.17. Przekierowanie do innego gniazda (93)
- 3.18. Rejestrowanie przypadków korzystania z usług (94)
- 3.19. Uniemożliwianie logowania się przez terminal jako root (96)

Rozdział 4. Techniki i infrastruktury uwierzytelniania (97)

- 4.0. Wprowadzenie (97)
- 4.1. Tworzenie aplikacji obsługującej infrastrukturę PAM (100)
- 4.2. Wymuszanie stosowania silnych haseł za pomocą oprogramowania PAM (101)
- 4.3. Tworzenie list kontroli dostępu za pomocą oprogramowania PAM (102)
- 4.4. Sprawdzanie poprawności certyfikatu SSL (104)
- 4.5. Odkodowywanie certyfikatu SSL (105)
- 4.6. Instalowanie nowego certyfikatu SSL (106)
- 4.7. Generowanie żądania podpisania certyfikatu SSL (CSR) (107)
- 4.8. Tworzenie samopodpisanego certyfikatu SSL (109)
- 4.9. Tworzenie organu certyfikującego (110)
- 4.10. Konwertowanie certyfikatów SSL z formatu DER do formatu PEM (113)
- 4.11. Rozpoczęcie pracy z oprogramowaniem Kerberos (114)
- 4.12. Dodawanie użytkowników do domeny Kerberos (119)
- 4.13. Dodawanie hostów do domeny Kerberos (120)
- 4.14. Korzystanie z uwierzytelniania Kerberos w usłudze SSH (121)
- 4.15. Korzystanie z uwierzytelniania Kerberos w usłudze Telnet (124)
- 4.16. Zabezpieczanie usługi IMAP technologią Kerberos (126)
- 4.17. Uwierzytelnianie użytkowników w systemie z użyciem technologii Kerberos i PAM (127)

Rozdział 5. Mechanizmy autoryzacji (131)

- 5.0. Wprowadzenie (131)
- 5.1. Logowanie do powłoki z przywilejami roota (133)
- 5.2. Uruchamianie programów X z przywilejami roota (134)
- 5.3. Uruchamianie poleceń jako inny użytkownik przez program sudo (135)
- 5.4. Jak obejść uwierzytelnianie hasłem w programie sudo (136)

- 5.5. Wymuszanie uwierzytelniania hasłem w sudo (138)
- 5.6. Autoryzacja w sudo z uwzględnieniem nazwy hosta (138)
- 5.7. Przydzielanie przywilejów grupie przez program sudo (140)
- 5.8. Uruchamianie przez sudo dowolnego programu w katalogu (140)
- 5.9. Blokowanie argumentów poleceń w sudo (141)
- 5.10. Współużytkowanie plików z użyciem grup (142)
- 5.11. Zezwalanie przez sudo na dostęp do współużytkowanego pliku w trybie tylko do odczytu (143)
- 5.12. Autoryzacja zmian haseł przez sudo (144)
- 5.13. Uruchamianie-zatrzymywanie demonów przez sudo (145)
- 5.14. Ograniczenie przywilejów roota za pomocą sudo (145)
- 5.15. Zabijanie procesów przez sudo (146)
- 5.16. Wyświetlanie prób wywołania programu sudo (148)
- 5.17. Zdalny dziennik sudo (148)
- 5.18. Udostępnianie przywilejów roota przez SSH (149)
- 5.19. Uruchamianie poleceń roota przez SSH (151)
- 5.20. Udostępnianie przywilejów roota przez Kerberos su (152)

Rozdział 6. Ochrona wychodzących połączeń sieciowych (155)

- 6.0 Wprowadzenie (155)
- 6.1. Logowanie do zdalnego hosta (156)
- 6.2. Uruchamianie zdalnych programów (157)
- 6.3. Zdalne kopiowanie plików (158)
- 6.4. Uwierzytelnianie za pomocą klucza publicznego (OpenSSH) (161)
- 6.5. Uwierzytelnianie z użyciem klucza publicznego (Klient OpenSSH, serwer SSH2, klucz OpenSSH) (163)
- 6.6. Uwierzytelnianie z użyciem klucza publicznego (Klient OpenSSH, serwer SSH2, klucz SSH2) (165)
- 6.7. Uwierzytelnianie z użyciem klucza publicznego (Klient SSH2, serwer OpenSSH) (166)
- 6.8. Uwierzytelnianie przez mechanizm wiarygodnego hosta (167)
- 6.9. Uwierzytelnianie bez hasła (interaktywne) (171)
- 6.10. Uwierzytelnianie w zadaniach cron (173)
- 6.11. Wyłączanie agenta SSH po wylogowaniu (175)
- 6.12. Dostosowanie działania klienta SSH do poszczególnych hostów (175)
- 6.13. Zmiana domyślnych ustawień klienta SSH (176)
- 6.14. Tunelowanie innej sesji TCP przez SSH (178)
- 6.15. Panowanie nad hasłami (179)

Rozdział 7. Ochrona plików (181)

- 7.0. Wprowadzenie (181)
- 7.1. Stosowanie prawa dostępu do plików (182)
- 7.2. Zabezpieczanie współużytkowanego katalogu (183)
- 7.3. Blokowanie wyświetlania zawartości katalogu (184)
- 7.4. Szyfrowanie plików z użyciem hasła (185)
- 7.5. Rozszyfrowywanie plików (186)
- 7.6. Przygotowanie oprogramowania GnuPG do szyfrowania z użyciem klucza publicznego (187)

- 7.7. Wyświetlanie zawartości zbioru kluczy (189)
- 7.8. Ustawianie klucza domyślnego (190)
- 7.9. Udostępnianie kluczy publicznych (191)
- 7.10. Dodawanie kluczy do zbioru (192)
- 7.11. Szyfrowanie plików w celu wysłania innym (193)
- 7.12. Podpisywanie pliku tekstowego (194)
- 7.13. Podpisywanie i szyfrowanie plików (195)
- 7.14. Składanie podpisu w oddzielnym pliku (195)
- 7.15. Sprawdzanie sygnatury (196)
- 7.16. Zademonstrowanie kluczy publicznych (197)
- 7.17. Tworzenie kopii zapasowej klucza prywatnego (198)
- 7.18. Szyfrowanie katalogów (200)
- 7.19. Dodawanie klucza do serwera kluczy (200)
- 7.20. Wysyłanie nowych sygnatur na serwer kluczy (201)
- 7.21. Uzyskiwanie kluczy z serwera kluczy (201)
- 7.22. Anulowanie klucza (204)
- 7.23. Zarządzanie zaszyfrowanymi plikami za pomocą programu Emacs (205)
- 7.24. Zarządzanie zaszyfrowanymi plikami za pomocą programu vim (206)
- 7.25. Szyfrowanie kopii zapasowych (208)
- 7.26. Korzystanie z kluczy PGP w programie GnuPG (209)

Rozdział 8. Ochrona poczty elektronicznej (211)

- 8.0. Wprowadzenie (211)
- 8.1. Szyfrowanie poczty elektronicznej w Emacsie (212)
- 8.2. Szyfrowanie poczty elektronicznej w vimie (214)
- 8.3. Szyfrowanie poczty elektronicznej w programie Pine (214)
- 8.4. Szyfrowanie poczty elektronicznej w programie Mozilla (216)
- 8.5. Szyfrowanie poczty elektronicznej w programie Evolution (217)
- 8.6. Szyfrowanie poczty elektronicznej w programie mutt (218)
- 8.7. Szyfrowanie poczty elektronicznej w programie elm (219)
- 8.8. Szyfrowanie poczty elektronicznej w programie MH (220)
- 8.9. Udostępnianie serwera pocztowego POP/IMAP z obsługą SSL (220)
- 8.10. Testowanie połączenia pocztowego przez SSL (225)
- 8.11. Zabezpieczanie transmisji POP/IMAP przez protokół SSL w programie Pine (226)
- 8.12. Zabezpieczanie transmisji POP/IMAP przez protokół SSL w programie mutt (228)
- 8.13. Zabezpieczanie transmisji POP/IMAP przez protokół SSL w programie Evolution (229)
- 8.14. Zabezpieczanie transmisji POP/IMAP przez program stunnel i protokół SSL (230)
- 8.15. Zabezpieczanie transmisji POP/IMAP za pomocą SSH (231)
- 8.16. Zabezpieczanie transmisji POP/IMAP za pomocą programów SSH i Pine (233)
- 8.17. Otrzymywanie poczty elektronicznej bez udostępniania serwera (235)
- 8.18. Udostępnienie serwera SMTP różnym klientom (237)

Rozdział 9. Testowanie i kontrolowanie (241)

- 9.0. Wprowadzenie (241)

- 9.1. Testowanie haseł kont (program John the Ripper) (242)
- 9.2. Testowanie haseł kont (CrackLib) (244)
- 9.3. Wyszukiwanie kont bez haseł (246)
- 9.4. Wyszukiwanie kont superużytkowników (246)
- 9.5. Sprawdzanie podejrzanych zachowań dotyczących kont (247)
- 9.6. Sprawdzanie podejrzanych zachowań dotyczących kont w wielu systemach (249)
- 9.7. Testowanie ścieżki wyszukiwania (251)
- 9.8. Efektywne przeszukiwanie systemów plików (253)
- 9.9. Wyszukiwanie programów z bitami setuid lub setgid (256)
- 9.10. Zabezpieczanie specjalnych plików urządzeń (258)
- 9.11. Poszukiwanie plików pozwalających na zapis (259)
- 9.12. Poszukiwanie rootkitów (261)
- 9.13. Poszukiwanie otwartych portów (262)
- 9.14. Badanie aktywności sieci w komputerze lokalnym (268)
- 9.15. Śledzenie procesów (274)
- 9.16. Obserwacja ruchu sieciowego (276)
- 9.17. Obserwacja ruchu sieciowego (z interfejsem graficznym) (282)
- 9.18. Wyszukiwanie łańcuchów w ruchu sieciowym (284)
- 9.19. Wykrywanie niezabezpieczonych protokołów sieciowych (287)
- 9.20. Rozpoczęcie pracy z programem Snort (293)
- 9.21. Podsłuchiwanie pakietów programem Snort (294)
- 9.22. Wykrywanie włamań programem Snort (295)
- 9.23. Rozkodowywanie komunikatów alarmowych programu Snort (298)
- 9.24. Rejestrowanie z użyciem programu Snort (300)
- 9.25. Dzielenie dzienników programu Snort na różne pliki (301)
- 9.26. Uaktualnianie i dostrajanie reguł programu Snort (302)
- 9.27. Przekierowanie komunikatów systemowych do dzienników (syslog) (304)
- 9.28. Testowanie konfiguracji syslog (308)
- 9.29. Rejestrowanie zdalne (309)
- 9.30. Rotacja plików dziennika (310)
- 9.31. Wysyłanie komunikatów do systemu rejestrującego (311)
- 9.32. Zapisywanie komunikatów w dziennikach ze skryptów powłoki (313)
- 9.33. Zapisywanie komunikatów w dziennikach z programów w Perlu (315)
- 9.34. Zapisywanie komunikatów w dziennikach z programów w C (316)
- 9.35. Łączenie plików dziennika (317)
- 9.36. Tworzenie raportów z dzienników: program logwatch (319)
- 9.37. Definiowanie filtra logwatch (320)
- 9.38. Nadzorowanie wszystkich wykonywanych poleceń (322)
- 9.39. Wyświetlanie wszystkich wykonywanych poleceń (324)
- 9.40. Przetwarzanie dziennika z księgowania procesów (326)
- 9.41. Odtwarzanie po włamaniu (328)
- 9.42. Zgłaszanie faktu włamania (329)

Skorowidz (333)