

Twórcy książki (7)

Wstęp (9)

Rozdział 1. Bezpieczeństwo systemu Unix (13)

- 1. Zabezpieczenie punktów montowania (13)
- 2. Wynajdywanie programów z ustawionymi bitami SUID i SGID (15)
- 3. Wynajdywanie udostępnionych katalogów (16)
- 4. Tworzenie elastycznych hierarchii uprawnień za pomocą list ACL standardu POSIX (17)
- 5. Zabezpieczenie dzienników zdarzeń przed modyfikacją (20)
- 6. Podział zadań administracyjnych (22)
- 7. Automatyczna kryptograficzna weryfikacja sygnatury (24)
- 8. Odnalezienie nasłuchujących usług (26)
- 9. Zapobieganie wiązaniu się usług z interfejsami (28)
- 10. Ograniczenie usług do środowiska sandbox (30)
- 11. Użycie serwera proftpd z MySQL jako źródłem danych uwierzytelniających (33)
- 12. Zabezpieczenie się przed atakami rozbicia stosu (35)
- 13. grsecurity - zabezpieczenie na poziomie jądra (37)
- 14. Ograniczanie aplikacji za pomocą łatki grsecurity (41)
- 15. Ograniczanie wywołań systemowych za pomocą mechanizmu sysrtrace (44)
- 16. Automatyczne tworzenie zasad mechanizmu sysrtrace (47)
- 17. Kontrola logowania za pomocą modułów PAM (50)
- 18. Środowiska ograniczonych powłok (54)
- 19. Ograniczenie użytkownikom i grupom użycia zasobów (55)
- 20. Automatyczne uaktualnianie systemu (57)

Rozdział 2. Bezpieczeństwo systemu Windows (59)

- 21. Kontrola zainstalowanych poprawek (60)
- 22. Lista otwartych plików oraz procesów, które ich używają (65)
- 23. Lista działających usług i otwartych portów (66)
- 24. Uruchomienie inspekcji (67)
- 25. Zabezpieczenie dzienników zdarzeń (69)
- 26. Zmiana maksymalnej wielkości dzienników zdarzeń (69)
- 27. Wyłączenie udziałów domyślnych (71)
- 28. Zaszyfrowanie folderu Temp (72)
- 29. Czyszczenie pliku stronicowania podczas zamykania systemu (73)
- 30. Ograniczenie aplikacji dostępnych użytkownikom (75)

Rozdział 3. Bezpieczeństwo sieci (79)

- 31. Wykrywanie fałszowania odpowiedzi ARP (79)
- 32. Tworzenie statycznych tablic ARP (82)
- 33. Zapora sieciowa Netfilter (84)
- 34. Zapora sieciowa PacketFilter systemu OpenBSD (88)
- 35. Tworzenie bramy uwierzytelniającej (93)
- 36. Zapora sieciowa w systemie Windows (96)
- 37. Sieć z ograniczeniem na wyjściu (99)
- 38. Testowanie zapory sieciowej (100)
- 39. Filtrowanie adresów MAC za pomocą zapory sieciowej Netfilter (103)

- 40. Uniemożliwienie rozpoznawania systemu operacyjnego (104)
- 41. Wprowadzanie w błąd programów identyfikujących systemy operacyjne (107)
- 42. Inwentaryzacja sieci (110)
- 43. Wyszukiwanie słabych punktów sieci (113)
- 44. Synchronizacja zegarów serwerów (118)
- 45. Tworzenie własnego ośrodka certyfikacyjnego (120)
- 46. Rozpowszechnienie certyfikatu CA wśród klientów (123)
- 47. Szyfrowanie usług IMAP i POP za pomocą SSL (124)
- 48. Konfiguracja serwera SMTP wykorzystującego szyfrowanie TLS (126)
- 49. Wykrywanie szperaczy działających w sieci Ethernet (128)
- 50. Instalacja serwera Apache z rozszerzeniem SSL i z trybem suEXEC (133)
- 51. Zabezpieczenie serwera BIND (136)
- 52. Zabezpieczenie bazy danych MySQL (139)
- 53. Bezpieczne udostępnianie plików w systemie Unix (141)

Rozdział 4. Rejestracja zdarzeń (145)

- 54. Centralny serwer rejestracji zdarzeń (syslog) (146)
- 55. Konfigurowanie rejestracji zdarzeń (147)
- 56. Włączenie systemu Windows w infrastrukturę syslog (149)
- 57. Automatyczne streszczanie dzienników zdarzeń (156)
- 58. Automatyczne monitorowanie dzienników zdarzeń (157)
- 59. Zbieranie informacji o zdarzeniach ze zdalnych ośrodków (160)
- 60. Rejestracja działań użytkowników za pomocą systemu rozliczeń (165)

Rozdział 5. Monitorowanie i wyznaczanie trendów (169)

- 61. Monitorowanie dostępności usług (170)
- 62. Kreślenie trendów (177)
- 63. ntop - statystyki sieci w czasie rzeczywistym (179)
- 64. Monitorowanie ruchu sieciowego (181)
- 65. Gromadzenie statystyk za pomocą reguł zapory sieciowej (184)
- 66. Zdalne nasłuchiwanie ruchu sieciowego (185)

Rozdział 6. Bezpieczne tunele (189)

- 67. Konfiguracja protokołu IPsec w systemie Linux (189)
- 68. Konfiguracja protokołu IPsec w systemie FreeBSD (192)
- 69. Konfiguracja protokołu IPsec w systemie OpenBSD (194)
- 70. Tunelowanie PPTP (196)
- 71. Szyfrowanie oportunistyczne za pomocą FreeS/WAN (199)
- 72. Przekazywanie i szyfrowanie ruchu za pomocą protokołu SSH (201)
- 73. Szybkie logowanie za pomocą kluczy klienta SSH (203)
- 74. Proxy Squid w połączeniu SSH (205)
- 75. Użycie SSH jako proxy SOCKS 4 (207)
- 76. Szyfrowanie i tunelowanie ruchu za pomocą SSL (210)
- 77. Tunelowanie połączeń wewnątrz HTTP (212)
- 78. Tworzenie tunelu za pomocą VTun i SSH (214)
- 79. Generator plików vtund.conf (218)
- 80. Tworzenie sieci VPN łączących różne platformy systemowe (223)

- 81. Tunelowanie PPP (227)

Rozdział 7. Wykrywanie włamań do sieci (231)

- 82. Wykrywanie włamań za pomocą programu Snort (232)
- 83. Śledzenie alarmów (236)
- 84. Monitorowanie w czasie rzeczywistym (238)
- 85. Zarządzanie siecią sensorów (245)
- 86. Pisanie własnych reguł programu Snort (250)
- 87. Zapobieganie włamaniom za pomocą programu Snort_inline (255)
- 88. Sterowanie zaporą sieciową za pomocą programu SnortSam (258)
- 89. Wykrywanie nietypowego zachowania (261)
- 90. Automatyczne uaktualnianie reguł programu Snort (262)
- 91. Budowa sieci niewidzialnych sensorów (263)
- 92. Użycie programu Snort w wysoko wydajnych środowiskach sieciowych (265)
- 93. Wykrywanie i zapobieganie atakom na aplikacje WWW (268)
- 94. Symulacja sieci niezabezpieczonych komputerów (272)
- 95. Rejestracja aktywności komputera-pułapki (275)

Rozdział 8. Powrót do działania i reakcja (279)

- 96. Tworzenie obrazu systemu plików (279)
- 97. Weryfikacja integralności plików (281)
- 98. Wykrywanie zmodyfikowanych plików za pomocą pakietów RPM (285)
- 99. Poszukiwanie zainstalowanych zestawów rootkit (287)
- 100. Poszukiwanie właściciela sieci (288)

Skorowidz (291)