

## Wstęp (11)

## Rozdział 1. Metody obrony przed atakami prowadzonymi w warstwie dostępu do sieci (15)

- Sniffing w sieci o fizycznej topologii magistrali i w sieci wykorzystującej koncentratory (16)
  - o Programy wykorzystywane do podsłuchu (16)
    - Tcpdump (16)
    - Ethereal (17)
    - Sniff v. 1.4 (18)
  - o Konfiguracja sieci testowej (18)
  - o Przeprowadzenie ataku (20)
- Sniffing w sieci zbudowanej przy wykorzystaniu przełączników (22)
  - o Konfiguracja sieci testowej (23)
  - o Sniffing w sieci zbudowanej przy wykorzystaniu przełączników - ARP-spoofing (24)
    - Przeprowadzenie ataku (25)
  - o Sniffing w sieci zbudowanej z wykorzystaniem przełączników - MAC-flooding (26)
    - Przeprowadzenie ataku (27)
  - o Sniffing w sieci zbudowanej przy wykorzystaniu przełączników - duplikacja adresu fizycznego (29)
    - Przeprowadzenie ataku (29)
- Antysniffing (30)
  - Zabezpieczenie nr 1. Wykrywanie sniffingu za pomocą testu ARP (31)
  - Zabezpieczenie nr 2. Wykrywanie sniffingu za pomocą testu ARP-Cache (34)
  - Zabezpieczenie nr 3. Wykrywanie sniffingu za pomocą testu ICMP (37)
  - Zabezpieczenie nr 4. Wykrywanie sniffingu za pomocą testu DNS (39)
  - Zabezpieczenie nr 5. Wykrywanie sniffingu za pomocą pomiarów czasów latencji (41)
  - Zabezpieczenie nr 6. Wykrywanie podsłuchu metodami reflektometrycznymi (45)
  - Zabezpieczenie nr 7. Wykrywanie ataku ARP-spoofing za pomocą programu arpwatch (46)
  - Zabezpieczenie nr 8. Ochrona przed atakiem ARP-spoofing za pomocą statycznej tablicy ARP (48)
  - Zabezpieczenie nr 9. Wykrywanie ataku ARP-spoofing za pomocą programu ARP-Analyzer (51)
  - Zabezpieczenie nr 10. Lokalne wykrywanie sniffingu (54)
  - Zabezpieczenie nr 11. Ochrona przed podsłuchem przy użyciu technologii VLAN (55)
  - Zabezpieczenie nr 12. Przełączniki zarządzalne jako zabezpieczenie przed podsłuchem (59)
  - Zabezpieczenie nr 13. Wirtualne sieci prywatne jako zabezpieczenie przed podsłuchem (59)
  - Zabezpieczenie nr 14. Wykrywanie ataku MAC-flooding za pomocą programu MACManipulator (66)

- Zabezpieczenie nr 15. Szyfrowanie połączenia sieciowego z wykorzystaniem protokołu SSL (68)
- Zabezpieczenie nr 16. Szyfrowanie połączenia sieciowego z wykorzystaniem protokołu TLS (77)

## **Rozdział 2. Metody obrony przed atakami prowadzonymi w warstwach internetu i host-to-host (79)**

- Skanowanie portów (79)
  - o Nmap (80)
    - Instalacja Nmapa (80)
    - Instalacja Nmapa w systemie Linux (80)
    - Instalacja Nmapa w systemie Windows (81)
  - o Techniki skanowania portów (82)
    - Skanowanie TCP-connect (83)
    - Zabezpieczenie nr 17. NAT jako składnik zapory sieciowej (83)
    - Zabezpieczenie nr 18. Usługi pośredniczenia (proxy) w roli zapory sieciowej (87)
  - o Pośredniczenie za pomocą Socks (88)
    - Konfiguracja komputera B (88)
    - Konfiguracja komputera A (92)
    - Testowanie działania usługi pośredniczącej (94)
    - Zabezpieczenie nr 19. Wykorzystanie zapory sieciowej IPTables do blokowania prób skanowania TCP-connect (96)
    - Skanowanie TCP SYN (99)
    - Zabezpieczenie nr 20. Wykorzystanie zapory sieciowej iptables do blokowania prób skanowania TCP SYN (99)
    - Skanowanie TCP FIN (100)
    - Zabezpieczenie nr 21. Wykorzystanie systemu IDS Snort do wykrywania prób skanowania TCP FIN (100)
    - Zabezpieczenie nr 22. Wykorzystanie zapory sieciowej IPTables do blokowania prób skanowania TCP FIN (101)
    - Skanowanie TCP ACK (103)
    - Zabezpieczenie nr 23. Wykorzystanie systemu IDS Snort do wykrywania prób skanowania TCP ACK (104)
    - Zabezpieczenie nr 24. Wykorzystanie zapory sieciowej iptables do blokowania prób skanowania TCP ACK (104)
    - Skanowanie TCP NULL (105)
    - Zabezpieczenie nr 25. Wykorzystanie systemu IDS Snort do wykrywania prób skanowania TCP NULL (105)
    - Zabezpieczenie nr 26. Wykorzystanie zapory sieciowej iptables do blokowania prób skanowania TCP NULL (105)
    - Skanowanie TCP XMAS (106)
    - Zabezpieczenie nr 27. Wykorzystanie systemu IDS Snort do wykrywania prób skanowania TCP XMAS (106)
    - Zabezpieczenie nr 28. Wykorzystanie zapory sieciowej iptables do blokowania prób skanowania TCP XMAS (107)
    - Skanowanie FTP-bounce (107)
    - Zabezpieczenie nr 29. Obrona przed skanowaniem FTP-bounce (110)

- Zabezpieczenie nr 30. Narzędzie Portsentry jako obrona przed skanowaniem portów w systemie Linux (111)
- Przeprowadzenie próby skanowania portów komputera zabezpieczonego przez Portsentry (115)
- Zabezpieczenie nr 31. Osobiste zapory sieciowe jako obrona przed skanowaniem portów w systemach Windows (116)
- Skanowanie UDP (128)
- Zabezpieczenie nr 32. Wykorzystanie zapory sieciowej iptables do blokowania prób skanowania pakietami UDP (129)
- Skanowanie ICMP (129)
- Zabezpieczenie nr 33. Wykorzystanie zapory sieciowej iptables do blokowania prób skanowania pakietami ICMP (129)
  - o Techniki ukrywania przez napastnika skanowania portów (130)
- Metody wykrywania systemu operacyjnego (ang. OS fingerprinting) (131)
  - o Pasywne wykrywanie systemu operacyjnego (131)
    - Pasywna analiza stosu TCP/IP (132)
  - o Aktywne wykrywanie systemu operacyjnego (134)
    - Zabezpieczenie nr 34. Zmiana parametrów stosu TCP/IP w systemie Linux w celu utrudnienia fingerprintingu (136)
- IP-spoofing (137)
  - Zabezpieczenie nr 35. Filtrowanie ruchu na zaporze sieciowej jako zabezpieczenie przed atakami wykorzystującymi IP-spoofing (137)
  - Zabezpieczenie nr 36. Weryfikacja adresu źródłowego za pomocą funkcji rp\_filter (141)
- Atak wyboru trasy (ang. Source routing) (142)
  - Zabezpieczenie nr 37. Wyłączenie opcji source routing (142)
  - Zabezpieczenie nr 38. Wykorzystanie uwierzytelniania RIPv2 jako ochrona przed atakami na routery (143)

### **Rozdział 3. Metody obrony przed atakami DoS i DDoS (155)**

- Ataki DoS (155)
  - o Ping of Death (156)
    - Zabezpieczenie nr 39. Ochrona przed atakiem Ping of Death za pomocą filtrowania na zaporze sieciowej (156)
  - o Teardrop (157)
    - Zabezpieczenie nr 40. Ochrona przed atakiem teardrop za pomocą systemu Snort (158)
    - Zabezpieczenie nr 41. Ochrona przed atakiem teardrop za pomocą filtrowania pakietów (158)
  - o Atak SYN-flood (158)
    - Zabezpieczenie nr 42. Ochrona przed atakiem SYN-flood wychodzącym z naszej sieci za pomocą zapory sieciowej (159)
    - Zabezpieczenie nr 43. Ochrona przed atakami SYN-flood i Naptha na usługi w naszej sieci za pomocą iptables (160)
  - o Atak Land (160)
    - Zabezpieczenie nr 44. Ochrona przed atakiem Land za pomocą programu Snort (161)
    - Zabezpieczenie nr 45. Ochrona przed atakiem Land za pomocą programu Snort (reguła systemu IDS) (162)

- o Atak Naptha (162)
  - Zabezpieczenie nr 46. Wykorzystanie systemu IDS Snort do wykrywania ataku Naptha (164)
- o Atak Smurf (165)
  - Zabezpieczenie nr 47. Ochrona od strony pośrednika przed atakiem Smurf za pomocą zapory sieciowej (167)
  - Zabezpieczenie nr 48. Ochrona przed atakiem Smurf od strony ofiary za pomocą zapory sieciowej (168)
- o UDP-flood ("Pepsi") (168)
  - Zabezpieczenie nr 49. Ochrona przed atakiem Pepsi za pomocą zapory sieciowej (169)
  - Zabezpieczenie nr 50. Ochrona przed atakiem Pepsi za pomocą programu Snort (170)
- o Smbnuke (170)
  - Zabezpieczenie nr 51. Ochrona przed atakiem Smbnuke za pomocą filtra pakietów (170)
  - Zabezpieczenie nr 52. Ochrona przed atakiem Smbnuke za pomocą programu Snort (171)
- o Zalewanie maszyny połączeniami na określonym porcie - Connection-flood (171)
  - Zabezpieczenie nr 53. Ochrona przed atakiem Connection-flood za pomocą zapory sieciowej (173)
- o Fraggle (173)
  - Zabezpieczenie nr 54. Ochrona przed atakiem fraggle za pomocą zapory sieciowej (174)
- o Jolt (175)
  - Zabezpieczenie nr 55. Ochrona przed atakiem Jolt za pomocą zapory sieciowej (175)
  - Zabezpieczenie nr 56. Ochrona przed atakiem Jolt za pomocą programu Snort (175)
- Rozproszone ataki typu "odmowa usługi" (DDoS) (175)
  - Faza powstawania sieci DDoS (178)
  - Właściwa faza ataku (179)
  - o Szczegółowa charakterystyka ataków DDoS (179)
    - Atak Trinoo (179)
    - Atak Tribe Flood Network (180)
    - Atak TFN 2000 (180)
    - Atak Stacheldraht (drut kolczasty) (181)
    - Atak Shaft (181)
    - Atak Mstream (182)
- Obrona przed atakami DDoS (182)
  - Zabezpieczenie nr 57. Ręczne wykrywanie i usuwanie demona Wintrinoo (183)
  - Zabezpieczenie nr 58. Wykrywanie demona Wintrinoo za pomocą programu wtrinscan (184)
  - Zabezpieczenie nr 59. Wykrywanie narzędzi DDoS za pomocą programu Zombie Zapper (184)
  - Zabezpieczenie nr 60. Wykrywanie demona trinoo za pomocą programu wtrinscan (186)

- Zabezpieczenie nr 61. Wykrywanie i unieszkodliwianie demona trinoos narzędziem netcat (187)
- Zabezpieczenie nr 62. Wykrywanie demona i węzła Trinoo za pomocą programu find\_ddos (191)
- Zabezpieczenie nr 63. Zdalne i lokalne usuwanie z systemu demona Trinoo (192)
- Zabezpieczenie nr 64. Wykrywanie narzędzi DDoS za pomocą programu DDoSPing (193)
- Zabezpieczenie nr 65. Wykrywanie narzędzi DDoS przez analizę ruchu sieciowego (195)
- Zabezpieczenie nr 66. Wykorzystanie systemu IDS Snort do wykrywania ataku Trinoo (200)
- Zabezpieczenie nr 67. Wykorzystanie systemu IDS Snort do wykrywania ataku Tribe Flood Network (204)
- Zabezpieczenie nr 68. Wykorzystanie systemu IDS Snort do wykrywania ataku Tribe Flood Network 2000 (204)
- Zabezpieczenie nr 69. Wykorzystanie systemu IDS Snort do wykrywania ataku Stacheldraht (205)
- Zabezpieczenie nr 70. Wykorzystanie systemu IDS Snort do wykrywania ataku Shaft (205)
- Zabezpieczenie nr 71. Wykorzystanie systemu IDS Snort do wykrywania ataku Mstream (206)

#### **Rozdział 4. Obrona przed atakami w warstwie procesów i aplikacji oraz atakami przeciwko systemom i aplikacjom sieciowym (209)**

- Robaki, wirusy, spyware (210)
  - Zabezpieczenie nr 72. Wykrywanie programów typu rootkit w systemie Linux (211)
  - Zabezpieczenie nr 73. Lokalne wykrywanie koni trojańskich (212)
  - Zabezpieczenie nr 74. Wykrywanie modyfikacji plików z zapisem logowania użytkowników w systemie Linux (216)
- DNS-spoofing i ataki Man-in-the-Middle na sesje szyfrowane (217)
- DNS-spoofing (218)
  - Zabezpieczenie nr 75. Ochrona przed atakiem DNS-spoofing za pomocą statycznych odwzorowań nazw (220)
  - Zabezpieczenie nr 76. Ochrona przed niechcianymi banerami, plikami cookies za pomocą odwzorowań w pliku hosts (221)
  - Zabezpieczenie nr 77. Obrona przed atakiem Man-in-The-Middle (221)
- Łamanie haseł (229)
  - o Proces logowania (229)
  - o Narzędzia do łamania haseł (230)
    - L0pht Crack (230)
    - John the Ripper (230)
    - Łamacz 1.1 (230)
    - Advanced ZIP Password Recovery (231)
  - o Zdalne odgadywanie haseł użytkownika (234)
    - Zabezpieczenie nr 78. Polityka silnych haseł (235)
    - Zabezpieczenie nr 79. Hasła jednorazowe (238)

- Przykład implementacji haseł jednorazowych w systemie Knoppix 3.4 z wykorzystaniem usługi SSH (243)
- Zabezpieczenie nr 80. Bezpieczne uwierzytelnianie za pomocą serwera RADIUS (247)
- Zabezpieczenie nr 81. Bezpieczne uwierzytelnianie za pomocą protokołu Kerberos (249)
- SPAM i ataki na usługi pocztowe (251)
  - Zabezpieczenie nr 82. Uwierzytelnianie użytkownika końcowego SMTP oraz ograniczenia na wysyłane listy (252)
  - Zabezpieczenie nr 83. Szyfrowana transmisja POP (IMAP) i SMTP (253)
  - Zabezpieczenie nr 84. Zamykanie przekaźnika (relay) (254)
  - Zabezpieczenie nr 85. Filtrowanie poczty przychodzącej (255)
  - Zabezpieczenie nr 86. Programy kontroli rodzicielskiej (257)
  - Przykładowa konfiguracja programu Cyber Patrol (259)
  - Zabezpieczenie nr 87. Usuwanie lub fałszowanie etykiet wyświetlanych przez usługi sieciowe (264)
- Protokół DHCP (267)
  - Zabezpieczenie nr 88. Zabezpieczenie klienta przed nielegalnym serwerem DHCP w sieci (268)
  - Zabezpieczenie nr 89. Alokacja manualna adresów DHCP (270)
  - Zabezpieczenie nr 90. Honeypot (274)
  - Zabezpieczenie nr 91. Zabezpieczenie przed atakiem buffer overflow za pomocą biblioteki libsafe (287)

## **Rozdział 5. Dziesięć dobrych rad dla administratora (291)**

- Zabezpieczenie 92. Wykonuj regularnie kopie bezpieczeństwa (291)
- o Uaktualnianie systemu Windows (294)
  - Zabezpieczenie 93. Uaktualnij swój system (294)
- o Uaktualnianie systemu Linux (dystrybucja Knoppix 3.4) (304)
  - APT - narzędzie do zarządzania pakietami (309)
- o Uaktualnianie systemów Novell NetWare (314)
- o Integralność systemu plików (322)
  - Zabezpieczenie 94. Sprawdź integralność systemu plików (322)
- o Program FastSum w systemach Windows (338)
  - Zabezpieczenie 95. Ogranicz fizyczny dostęp do serwera (340)
  - Zabezpieczenie 96. - wykonuj i czytaj logi systemowe (342)
- o Analiza logów systemowych w systemie Linux (342)
  - Zabezpieczenie 97. Wykonaj audyt bezpieczeństwa (353)
  - Zabezpieczenie 98. Zaszzyfruj swój system plików (375)
  - Zabezpieczenie 99. Skorzystaj z internetowych serwisów skanujących (378)
- o Kontrola dostępu do usług (382)
  - Zabezpieczenie 100. Ogranicz zakres świadczonych usług (382)
  - Zabezpieczenie 101. Zarządzaj pasmem (389)
- o Podsumowanie (400)

## **Dodatek A Podstawy komunikacji sieciowej (401)**

- Pojęcia podstawowe (401)
- Modele łączenia systemów (404)
- Model referencyjny ISO/OSI - warstwy: fizyczna i łączenia danych, protokoły z rodziny Ethernet (407)
- Model referencyjny ISO/OSI - warstwa sieciowa, protokół IP, hermetyzacja (419)
- Model referencyjny ISO/OSI - warstwa transportowa, protokoły TCP i UDP, stos protokołów TCP/IP (432)
- Model referencyjny ISO/OSI - warstwy: sesji, prezentacji i aplikacji, protokoły warstw wyższych (439)

## **Dodatek B Zapory sieciowe (451)**

- Technologie zapór sieciowych (453)
  - o Filtrowanie pakietów (ang. packet filtering) (453)
  - o Usługi pośredniczenia (proxy) (458)
    - Proxy warstwy aplikacji (ang. application-level proxies) (459)
    - Proxy obwodowe (ang. circuit level gateway) (460)
  - o Translacja adresów sieciowych (ang. Network Address Translation - NAT) (461)
  - o Wirtualne sieci prywatne (ang. Virtual Private Network - VPN) (463)
- Architektury zapór sieciowych (467)
  - o Router ekranujący (ang. screening router) (467)
  - o Host dwusieciowy (ang. dual-homed host) (467)
  - o Host bastionowy (ang. bastion host) (468)
  - o Ekranowany host (ang. screened host) (469)
  - o Ekranowana podsieć (ang. screened subnet) (470)
  - o Host trzysieciowy (ang. tri-homed host) (471)
  - o Wiele ekranowanych podsieci (ang. split-screened subnet) (471)
- Dwa popularne filtry pakietów: Ipfiler i Iptables (472)
  - o Ipfiler (472)
  - o Iptables (484)
    - Przygotowanie skryptu z regułami filtrowania (491)
    - Konfiguracja systemu linux Redhat 9.0 (493)
    - Konfiguracja systemu Linux Knoppix (494)

## **Dodatek C Systemy wykrywania intruzów IDS (497)**

- Techniki wykrywania intruzów stosowane w systemach IDS (498)
  - o Sygnatury (dopasowywanie wzorców) (498)
  - o Badanie częstości zdarzeń i przekraczania ich limitów w określonej jednostce czasu (499)
  - o Wykrywanie anomalii statystycznych (499)
  - o Zaawansowane techniki detekcji intruzów (499)
- Budowa, działanie i umieszczanie systemu IDS w sieci (500)
  - o Budowa i działanie systemu (500)
  - o Umieszczanie systemu w sieci (501)
  - o Klasyfikacja systemów IDS (502)
- Budowa i zasada działania programu Snort (503)
  - o Zasada działania (503)
  - o Preprocesory (504)

- o Możliwości wykrywania ataków oferowane przez SNORT-a (504)
- o Zasady tworzenia reguł dla programu Snort (504)
  - Podział ataków na klasy (509)
  - Reakcja na ataki (511)
  - Reakcja na typowy atak, wykrycie i zapis skanowania portów (511)
  - Zdalne logowanie na użytkownika root (512)
  - Statystyki oferowane przez Snorta (512)
- Konfiguracja systemu dynamicznie reagującego na włamania (516)
  - o Konfiguracja i uruchomienie Snorta (516)
    - Sniffer (516)
    - Logowanie pakietów (517)
    - NIDS (518)
    - Wykrywanie i dynamiczna reakcja (521)
  - o Podsumowanie (524)

**Dodatek D Instalowanie systemu Knoppix 3.4. na dysku twardym (525)**

**Zakończenie (529)**

**Bibliografia (531)**

**Skorowidz (539)**