Spis treści

Przedmowa **13**

O autorze **15**

Część I Filtrowanie pakietów i podstawowe środki bezpieczeństwa **17**

Rozdział 1. Wstępne koncepcje dotyczące działania zapór sieciowych filtrujących pakiety **19**

Model sieciowy OSI 22
Protokoły bezpołączeniowe i połączeniowe 23
Następne kroki 24
Protokół IP 24
Adresowanie IP i podsieciowanie 24
Fragmentacja IP 28
Broadcasting i multicasting 28
ICMP 29
Mechanizmy transportowe 31
Protokół UDP 32
Protokół TCP 32
Nie zapominajmy o protokole ARP 35
Nazwy hostów i adresy IP 36
Adresy IP oraz adresy ethernetowe 36
Routing: przekazywanie pakietu z jednego miejsca do drugiego 37
Porty usług: drzwi dla programów w Twoim systemie 37
Typowe połączenie TCP: odwiedzanie zdalnej witryny 39
Podsumowanie 42

Rozdział 2. Koncepcje związane z filtrowaniem pakietów **43**

Zapora sieciowa filtrująca pakiety 45
Wybór domyślnej polityki filtrowania pakietów 47
Odrzucanie pakietu w porównaniu z blokowaniem pakietu 49

Filtrowanie pakietów przychodzących 50
Filtrowanie zdalnych adresów źródłowych 50
Filtrowanie lokalnych adresów docelowych 53
Filtrowanie zdalnego portu źródłowego 54
Filtrowanie lokalnego portu docelowego 54
Filtrowanie stanu przychodzących połączeń TCP 55
Sondy i skanowanie 55
Ataki DoS 60
Pakiety routowane źródłowo 67
Filtrowanie pakietów wychodzących 67
Filtrowanie lokalnych adresów źródłowych 68
Filtrowanie zdalnych adresów docelowych 68
Filtrowanie lokalnych portów źródłowych 69
Filtrowanie zdalnych portów docelowych 69
Filtrowanie stanów wychodzących połączeń TCP 70
Usługi sieci prywatnej i publicznej 70
Ochrona niezabezpieczonych usług lokalnych 71
Wybór uruchamianych usług 72
Podsumowanie 72

Rozdział 3. iptables: starszy program do administrowania zaporą sieciową systemu Linux 73
Różnice pomiędzy mechanizmami zapory sieciowej IPFW i Netfilter 74
Trawersacja pakietów w zaporze sieciowej IPFW 75
Trawersacja pakietów w zaporze sieciowej Netfilter 76
Podstawowa składnia polecenia iptables 77
Funkcje programu iptables 78
Funkcje tabeli nat 81
Funkcje tabeli mangle 83
Składnia polecenia iptables 84
Polecenia tabeli filter 85
Rozszerzenia celu tabeli filter 90
Rozszerzenia dopasowywania tabeli filter 92
Rozszerzenia celu tabeli nat 103
Polecenia tabeli mangle 106
Podsumowanie 106

Rozdział 4. nftables: program do administrowania zaporą sieciową systemu Linux 109
Różnice pomiędzy iptables i nftables 109
Podstawowa składnia nftables 109
Funkcje programu nftables 110
Składnia nftables 111
Składnia tabeli 112
Składnia łańcucha 113

Składnia reguły 114
Podstawowe operacje nftables 118
Składnia plików nftables 119
Podsumowanie 119

Rozdział 5. Budowa i instalacja samodzielnej zapory sieciowej 121
Programy do administrowania zaporą sieciową systemu Linux 122
Jądro systemu Linux: standardowe czy niestandardowe 124
Opcje adresowania źródłowego i docelowego 125
Inicjowanie zapory sieciowej 126
Symboliczne stałe używane w przykładach zapory sieciowej 127
Włączanie obsługi monitorowania w jądrze 128
Usunięcie wszelkich istniejących reguł 130
Resetowanie domyślnych polityk i zatrzymywanie zapory sieciowej 131
Włączanie interfejsu pętli zwrotnej 132
Definiowanie domyślnej polityki 133
Wykorzystywanie stanu połączenia do omijania sprawdzania reguł 135
Fałszowanie adresów źródłowych i inne złe adresy 136
Ochrona usług na przypisanych portach nieuprzywilejowanych 141
Typowe usługi lokalne TCP przypisane do nieuprzywilejowanych portów 142
Typowe usługi lokalne UDP przypisane do nieuprzywilejowanych portów 144
Włączenie podstawowych, wymaganych usług internetowych 147
Włączenie usługi DNS (UDP/TCP port 53) 147
Włączenie typowych usług TCP 152
E-mail (TCP SMTP port 25, POP port 110, IMAP port 143) 153
SSH (port TCP 22) 159
FTP (porty TCP 21, 20) 161
Ogólna usługa TCP 164
Włączanie typowych usług UDP 165
Dostęp do serwera DHCP dostawcy usług internetowych (porty UDP 67, 68) 166
Dostęp do zdalnych sieciowych serwerów czasu (port UDP 123) ... 168
Rejestrowanie porzuconych pakietów przychodzących 169
Rejestrowanie porzuconych pakietów wychodzących 170
Instalowanie zapory sieciowej 170
Wskazówki dla debugowania skryptu zapory sieciowej 171
Uruchamianie zapory sieciowej przy starcie systemu — Red Hat i SUSE 172
Uruchamianie zapory sieciowej przy starcie systemu — Debian 173
Instalowanie zapory sieciowej z dynamicznym adresem IP 173
Podsumowanie 174

Część II Zaawansowane zagadnienia, wiele zapór sieciowych oraz strefy ograniczonego zaufania ...175

Rozdział 6. Optymalizacja zapory sieciowej 177

Organizacja reguł 177
Rozpocznij od reguł blokujących ruch na portach o dużych numerach 178
Użyj modułu stanu dla dopasowań ESTABLISHED i RELATED 178
Uwzględnij protokół transportowy 178
Reguły zapory sieciowej dla bardzo popularnych usług umieszczaj jak najwyżej w łańcuchu 180
Użyj przepływu ruchu do określenia, gdzie umieścić reguły dla wielu interfejsów sieciowych 180
Łańcuchy definiowane przez użytkownika 181
Zoptymalizowane przykłady 184
Zoptymalizowany skrypt iptables 184
Inicjowanie zapory sieciowej 186
Instalowanie łańcuchów 188
Budowanie definiowanych przez użytkownika łańcuchów EXT-input i EXT-output 190
Łańcuch tcp-state-flags 199
Łańcuch connection-tracking 200
Łańcuchy local-dhcp-client-query i remote-dhcp-server-response 200
Łańcuch source-address-check 201
Łańcuch destination-address-check 201
Rejestrowanie porzuconych pakietów za pomocą polecenia iptables 202
Zoptymalizowany skrypt nftables 204
Inicjowanie zapory sieciowej 204
Budowanie plików reguł 205
Rejestrowanie porzuconych pakietów za pomocą polecenia nftables 209
Co dała optymalizacja? 210
Optymalizacja iptables 210
Optymalizacja nftables 211
Podsumowanie 212

Rozdział 7. Przekazywanie pakietów 213

Ograniczenia samodzielnej zapory sieciowej 213
Podstawowe konfiguracje bramy z zaporą sieciową 215
Kwestie bezpieczeństwa sieci LAN 217
Opcje konfiguracyjne dla zaufanej domowej sieci LAN 218
Dostęp sieci LAN do bramy z zaporą sieciową 220
Dostęp sieci LAN do innych sieci LAN: przekazywanie ruchu pomiędzy wieloma sieciami LAN 221

Opcje konfiguracyjne dla większych lub mniej zaufanych sieci LAN 223
Dzielenie przestrzeni adresowej w celu tworzenia wielu sieci 224
Selektywny dostęp wewnętrzny na podstawie hosta, zakresu adresów lub portu 226
Podsumowanie 231

Rozdział 8. Przekazywanie pakietów 233
Koncepcyjne tło powstania translacji NAT 233
Semantyka translacji NAT w programach iptables i nftables 238
NAT źródłowy 240
NAT docelowy 242
Przykłady translacji SNAT i prywatnych sieci LAN 244
Maskowanie ruchu LAN kierowanego do internetu 244
Stosowanie standardowej translacji NAT do ruchu LAN kierowanego do internetu 245
Przykłady translacji DNAT, sieci LAN i serwerów proxy 246
Przekierowanie hostów 246
Podsumowanie 248

Rozdział 9. Debugowanie reguł zapory sieciowej 249
Ogólne wskazówki dotyczące tworzenia zapory sieciowej 249
Wyświetlanie listy reguł zapory sieciowej 251
Przykład wyświetlania zawartości tabel iptables 252
Przykład wyświetlania zawartości tabel nftables 255
Interpretacja wpisów dziennika systemowego 256
Konfiguracja syslog 256
Znaczenie komunikatów dziennika zapory sieciowej 259
Sprawdzanie otwartych portów 263
Polecenie netstat -a [-n -p -A inet] 263
Użycie polecenia fuser do sprawdzania procesu powiązanego z konkretnym portem 266
Nmap 266
Podsumowanie 267

Rozdział 10. Wirtualne sieci prywatne — VPN 269
Przegląd wirtualnych sieci prywatnych 269
Protokoły VPN 269
PPTP i L2TP 270
IPsec 270
System Linux i produkty VPN 273
Openswan/Libreswan 273
OpenVPN 273
PPTP 273
VPN i zapory 274
Podsumowanie 275

Część III Wykraczając poza iptables i nftables 277

Rozdział 11. Wykrywanie włamań i reagowanie 279

Wykrywanie włamań 279
Objawy sugerujące, że system mógł zostać przejęty przez atakującego 281
Wskazania dziennika systemowego 281
Wskazania konfiguracji systemu 282
Wskazania systemu plików 282
Wskazania kont użytkowników 283
Wskazania narzędzi do audytu bezpieczeństwa 284
Wskazania wydajności systemu 284
Co zrobić, gdy Twój system zostanie przejęty 284
Zgłaszanie incydentów 286
Dlaczego zgłaszać incydenty? 287
Jakie rodzaje incydentów można zgłaszać? 288
Komu zgłaszać incydenty? 289
Jakie informacje należy dostarczyć? 290
Podsumowanie 291

Rozdział 12. Narzędzia do wykrywania włamań 293

Zestaw narzędzi do wykrywania włamań: narzędzia sieciowe 293
Różnica między przełącznikami i koncentratorami 295
ARPWatch 295
Narzędzia do wykrywania rootkitów 295
Uruchamianie programu Chkrootkit 296
Co zrobić, gdy Chkrootkit zgłasza, że komputer został zainfekowany? 298
Ograniczenia programu Chkrootkit i innych podobnych narzędzi 299
Bezpieczne korzystanie z programu Chkrootkit 300
Kiedy należy korzystać z programu Chkrootkit? 300
Integralność systemu plików 301
Monitorowanie plików dziennika 301
Swatch 302
Jak ustrzec się przed atakami 303
Często weryfikuj zabezpieczenia 304
Często przeprowadzaj aktualizacje 304
Często testuj 305
Podsumowanie 307

Rozdział 13. Monitorowanie sieci i wykrywanie ataków 309
Nasłuchiwanie eteru 309
Trzy cenne narzędzia 311
Prosty przegląd programu TCPDump 312
Pobieranie i instalowanie narzędzia TCPDump 313
Opcje narzędzia TCPDump 314
Wyrażenia TCPDump 316
Zaawansowana obsługa narzędzia TCPDump 319
Korzystanie z narzędzia TCPDump do przechwytywania konkretnych protokołów 319
Korzystanie z narzędzia TCPDump w prawdziwym świecie 320
Ataki z perspektywy TCPDump 328
Rejestrowanie ruchu za pomocą narzędzia TCPDump 333
Zautomatyzowane monitorowanie włamań za pomocą pakietu Snort 335
Pobieranie i instalowanie pakietu Snort 336
Konfiguracja pakietu Snort 337
Testowanie działania pakietu Snort 339
Otrzymywanie alertów 340
Końcowe uwagi na temat pakietu Snort 340
Monitorowanie za pomocą programu ARPWatch 341
Podsumowanie 343

Rozdział 14. Integralność systemu plików 345
Zdefiniowanie integralności systemu plików 345
Integralność systemu plików w praktyce 345
Instalacja programu AIDE 347
Konfiguracja AIDE 347
Tworzenie pliku konfiguracyjnego AIDE 347
Przykładowy plik konfiguracyjny AIDE 350
Inicjowanie bazy danych AIDE 351
Ustalanie harmonogramu automatycznego uruchamiania AIDE 351
Monitorowanie nieprawidłowości za pomocą AIDE 352
Czyszczenie bazy danych AIDE 353
Zmiana wyjścia dla raportu AIDE 355
Uzyskanie dokładniejszych informacji 356
Definiowanie makr w AIDE 357
Rodzaje kontroli AIDE 359
Podsumowanie 362

Dodatki **363**

Dodatek A **Zasoby dotyczące bezpieczeństwa** **365**
Źródła informacji dotyczących bezpieczeństwa 365
Opracowania źródłowe i najczęściej zadawane pytania 366

Dodatek B **Przykłady zapory sieciowej i skryptów do jej obsługi** **367**
Zapora sieciowa iptables z rozdziału 5. dla samodzielnego systemu 367
Zapora sieciowa nftables z rozdziału 5. dla samodzielnego systemu 380
Zoptymalizowana zapora sieciowa iptables z rozdziału 6. 384
Zapora sieciowa nftables z rozdziału 6. 397

Dodatek C **Słowniczek** **403**

Dodatek D **Licencja GNU Wolnej Dokumentacji** **417**
0. Preambuła 417
1. Zastosowanie i definicje 418
2. Kopiowanie dosłowne 419
3. Kopiowanie w dużej liczbie egzemplarzy 420
4. Modyfikacje 420
5. Łączenie dokumentów 423
6. Zbiory dokumentów 423
7. Agregacja z pracami niezależnymi 423
8. Tłumaczenie 424
9. Wygaśnięcie praw 424
10. Przyszłe wersje Licencji 425
11. Relicencjonowanie 425

Skorowidz **427**