

Spis treści

O autorze	13
O recenzencie	14
Przedmowa	15
Część I. Podstawy Linuksa	23
Rozdział 1. Witamy w rodzinie Linuksa	25
Dlaczego Linux jest dobrym wyborem dla zespołu ds. sieci?	26
Dlaczego Linux jest ważny?	27
Historia Linuksa	28
Popularne odmiany Linuksa dla centrów danych	29
Red Hat	30
Oracle/Scientific Linux	30
SUSE	30
Ubuntu	31
BSD/FreeBSD/OpenBSD	31
Wyspecjalizowane dystrybucje Linuksa	32
Zapory open source	32
Kali Linux	32
SIFT	33
Security Onion	33
Wirtualizacja	33
Linux i przetwarzanie danych w chmurze	33
Wybieranie dystrybucji Linuksa dla swojej organizacji	34
Podsumowanie	35
Dalsza lektura	36

Rozdział 2. Podstawowa konfiguracja i obsługa sieci w Linuksie	37
— praca z interfejsami lokalnymi	
Wymagania techniczne	38
Praca z ustawieniami sieci — dwa zbiory poleceń	38
Wyświetlanie informacji o interfejsie IP	40
Wyświetlanie informacji o trasach	43
Adresy IPv4 i maski podsieci	44
Adresy specjalnego przeznaczenia	45
Adresy prywatne — RFC 1918	48
Przypisywanie adresu IP do interfejsu	48
Dodawanie trasy	50
Dodawanie trasy tradycyjnym sposobem	51
Wyłączanie i włączanie interfejsu	52
Ustawianie jednostki MTU interfejsu	52
Więcej o poleceniu nmcli	53
Podsumowanie	55
Pytania	55
Dalsza lektura	56
 Część II. Linux jako węzeł sieciowy	
i platforma diagnostyczna	57
 Rozdział 3. Używanie Linuksa i linuksowych narzędzi do diagnostyki sieci	59
Wymagania techniczne	60
Podstawy sieci — model OSI	61
Warstwa 2. — kojarzenie adresów IP i MAC za pomocą protokołu ARP	63
Wartości OUI adresów MAC	68
Warstwa 4. — jak działają porty TCP i UDP?	69
Warstwa 4. — TCP i potrójne uzgodnienie	70
Wylizywanie portów lokalnych — do czego jestem podłączony? Czego nasłuchuję?	72
Wylizywanie portów zdalnych za pomocą natywnych narzędzi	80
Wylizywanie zdalnych portów i usług — Nmap	86
Skrypty Nmap	91
Czy Nmap ma jakieś ograniczenia?	97
Diagnozowanie łączności bezprzewodowej	98
Podsumowanie	103
Pytania	104
Dalsza lektura	104
 Rozdział 4. Zapora Linuksa	105
Wymagania techniczne	106
Konfigurowanie zapory iptables	106
Ogólny opis zapory iptables	107
Tabela NAT	111
Tabela mangle	113
Kolejność operacji w iptables	114

Konfigurowanie zapory nftables	115
Podstawowa konfiguracja nftables	117
Używanie plików include	118
Usuwanie konfiguracji zapory	119
Podsumowanie	119
Pytania	120
Dalsza lektura	120
 Rozdział 5. Standardy bezpieczeństwa Linuksa na praktycznych przykładach	 121
Wymagania techniczne	122
Dlaczego trzeba zabezpieczać hosty linuksowe?	122
Kwestie bezpieczeństwa specyficzne dla chmury	123
Często spotykane branżowe standardy bezpieczeństwa	124
Krytyczne środki kontroli Center for Internet Security	125
Krytyczne środki kontroli CIS nr 1 i 2 — pierwsze kroki	130
OSQuery — krytyczne środki kontroli nr 1 i 2 uzupełnione o nr 10 i 17	136
Wzorce Center for Internet Security	140
Stosowanie wzorca CIS — zabezpieczanie SSH w Linuksie	141
SELinux i AppArmor	147
Podsumowanie	149
Pytania	149
Dalsza lektura	150
 Część III. Usługi sieciowe w Linuksie	 151
 Rozdział 6. Usługi DNS w Linuksie	 153
Wymagania techniczne	154
Co to jest DNS?	154
Dwa główne zastosowania serwera DNS	154
„Wewnętrzny” serwer DNS organizacji (i przegląd systemu DNS)	155
Internetowy serwer DNS	158
Często używane implementacje DNS	160
Podstawowa instalacja: BIND do użytku wewnętrznego	160
BIND: implementacja do użytku internetowego	163
Diagnozowanie i rekonesans DNS	165
DoH	166
DoT	168
knot-dnsutils	170
Implementacja DoT w Nmap	172
DNSSEC	172
Podsumowanie	174
Pytania	174
Dalsza lektura	175

Rozdział 7. Usługi DHCP w Linuksie	177
Jak działa DHCP?	177
Podstawowe działanie DHCP	177
Żądania DHCP z innych podsieci (przełączniki DHCP)	179
Opcje DHCP	181
Zabezpieczanie usług DHCP	182
Nieautoryzowany serwer DHCP	183
Nieautoryzowany klient DHCP	186
Instalowanie i konfigurowanie serwera DHCP	186
Podstawowa konfiguracja	187
Rezerwacje statyczne	189
Proste rejestrowanie zdarzeń i diagnozowanie DHCP	190
Podsumowanie	191
Pytania	191
Dalsza lektura	192
Rozdział 8. Usługi certyfikatów w Linuksie	193
Wymagania techniczne	194
Czym są certyfikaty?	194
Pozyskiwanie certyfikatu	195
Używanie certyfikatu na przykładzie serwera WWW	197
Budowanie prywatnego urzędu certyfikacji	201
Budowanie urzędu CA z wykorzystaniem OpenSSL	202
Tworzenie i podpisywanie wniosku CSR	204
Zabezpieczanie infrastruktury urzędu certyfikacji	206
Tradycyjna, wypróbowana rada	206
Współczesna rada	207
Zagrożenia specyficzne dla urzędów CA działających w nowoczesnych infrastrukturach	208
Transparentność certyfikatów	208
Używanie usług CT do inwentaryzacji lub rekonesansu	209
Automatyzacja zarządzania certyfikatami i protokół ACME	211
Ściągawka z OpenSSL	212
Podsumowanie	214
Pytania	215
Dalsza lektura	215
Rozdział 9. Usługi RADIUS w Linuksie	216
Wymagania techniczne	216
Podstawy protokołu RADIUS — czym jest i jak działa?	217
Wdrażanie usług RADIUS z uwierzytelnianiem lokalnym	221
Usługi RADIUS z zapleczem LDAP/LDAPS	223
Uwierzytelnianie NTLM (AD) — wprowadzenie do CHAP	227
Unlang — niejęzyk	232
Zastosowania usług RADIUS	234
Uwierzytelnianie VPN za pomocą identyfikatora użytkownika i hasła	234
Dostęp administracyjny do urządzeń sieciowych	235

Dostęp administracyjny do routerów i przełączników	236
Konfigurowanie serwera RADIUS pod kątem uwierzytelniania EAP-TLS	237
Uwierzytelnianie w sieci bezprzewodowej za pomocą 802.1x/EAP-TLS	239
Uwierzytelnianie w sieci przewodowej za pomocą 802.1x/EAP-TLS	241
Używanie usługi Google Authenticator do uwierzytelniania MFA z wykorzystaniem serwera RADIUS	244
Podsumowanie	245
Pytania	245
Dalsza lektura	246
 Rozdział 10. Usługi równoważenia obciążenia w Linuksie	 248
Wymagania techniczne	249
Wprowadzenie do równoważenia obciążenia	249
Round Robin DNS (RRDNS)	249
Serwer proxy dla ruchu przychodzącego	
— równoważenie obciążenia w warstwie 7.	251
Translacja NAT połączeń przychodzących	
— równoważenie obciążenia w warstwie 4.	253
Równoważenie obciążenia z użyciem DSR	255
Algorytmy równoważenia obciążenia	257
Sprawdzanie kondycji serwerów i usług	258
Usługi równoważenia obciążenia w centrum danych — kwestie projektowe	259
Sieć w centrum danych a kwestie zarządzania	262
Budowanie usług równoważenia obciążenia typu NAT/proxy za pomocą HAProxy	266
Przed przystąpieniem do konfiguracji — karty sieciowe, adresowanie i routing	266
Przed przystąpieniem do konfiguracji — dostrajanie wydajności	267
Równoważenie obciążenia usług TCP — usługi WWW	269
Konfigurowanie trwałych połączeń	272
Nota wdrożeniowa	273
Przetwarzanie HTTPS na frontonie	273
Końcowe uwagi dotyczące bezpieczeństwa usług równoważenia obciążenia	275
Podsumowanie	277
Pytania	277
Dalsza lektura	278
 Rozdział 11. Przechwytywanie i analiza pakietów w Linuksie	 279
Wymagania techniczne	280
Wprowadzenie do przechwytywania pakietów — miejsca, w których należy szukać	280
Przechwytywanie po jednej ze stron	280
Użycie portu monitorowania	281
Pośredni host na ścieżce ruchu	282
Podśluch sieciowy	283
Złośliwe sposoby przechwytywania pakietów	284
Kwestie wydajnościowe podczas przechwytywania	287
Narzędzia do przechwytywania	289
tcpdump	289
Wireshark	289

TShark	289
Inne narzędzia PCAP	289
Filtrowanie przechwytywanego ruchu	290
Filtry przechwytywania w programie Wireshark (przechwytywanie ruchu w sieci domowej)	290
Filtry przechwytywania tcpdump — telefonyVoIP i DHCP	292
Więcej filtrów przechwytywania — LLDP i CDP	297
Pozyskiwanie plików z przechwyconych pakietów	300
Diagnozowanie aplikacji — przechwytywanie połączenia telefonicznego VoIP	302
Filtry wyświetlania w programie Wireshark — wyodrębnianie konkretnych danych	306
Podsumowanie	309
Pytania	309
Dalsza lektura	310
 Rozdział 12. Monitorowanie sieci z wykorzystaniem Linuksa	 311
Wymagania techniczne	312
Rejestrowanie zdarzeń z wykorzystaniem usługi syslog	312
Rozmiar dziennika, rotacja i bazy danych	313
Analiza dzienników — znajdowanie „tego czegoś”	314
Alarmy dotyczące konkretnych zdarzeń	316
Przykładowy serwer syslog	319
Projekt Dshield	324
Zarządzanie urządzeniami sieciowymi za pomocą SNMP	327
Podstawowe zapytania SNMP	327
Przykład wdrożenia systemu SNMP NMS — LibreNMS	331
SNMPv3	335
Gromadzenie danych NetFlow w Linuksie	346
Co to jest NetFlow i jego „kuzyni” — SFLOW, J-Flow i IPFIX?	346
Koncepcje wdrożeniowe związane z gromadzeniem informacji o przepływach	347
Konfigurowanie routera lub przełącznika do gromadzenia informacji o przepływach	349
Przykładowy serwer NetFlow wykorzystujący NFDump i NFSen	351
Podsumowanie	361
Pytania	362
Dalsza lektura	362
Często używane identyfikatory SNMP OID	364
 Rozdział 13. Systemy zapobiegania włamaniom w Linuksie	 365
Wymagania techniczne	366
Co to jest IPS?	366
Opcje architektoniczne — umiejscowienie systemu IPS w centrum danych	367
Techniki unikania systemów IPS	372
Wykrywanie rozwiązań WAF	372
Fragmentacja i inne techniki unikania systemów IPS	373
Klasyczne/sieciowe rozwiązania IPS — Snort i Suricata	375
Przykładowy system IPS Suricata	376
Konstruowanie reguły IPS	385

Pasywne monitorowanie ruchu	389
Monitorowanie pasywne za pomocą POF — przykład	389
Przykład użycia monitora Zeek — gromadzenie metadanych dotyczących sieci	391
Podsumowanie	400
Pytania	401
Dalsza lektura	401
 Rozdział 14. Usługi honeypot w Linuksie	 402
Wymagania techniczne	402
Przegląd usług honeypot — co to jest honeypot i do czego może się przydać?	403
Architektura i scenariusze wdrożeniowe — gdzie umieścić honeypota?	405
Zagrożenia związane z wdrażaniem honeypotów	408
Przykładowe honeypoty	409
Podstawowe honeypoty alarmujące o próbach połączenia z portem — iptables, netcat i portspooof	410
Inne często używane honeypoty	413
Honeypot rozproszony/społecznościowy — projekt DShield prowadzony przez Internet Storm Center	414
Podsumowanie	425
Pytania	426
Dalsza lektura	426
 Sprawdziany wiadomości	 427
Rozdział 2., „Podstawowa konfiguracja i obsługa sieci w Linuksie — praca z interfejsami lokalnymi”	427
Rozdział 3., „Używanie Linuksa i linuksowych narzędzi do diagnostyki sieci”	428
Rozdział 4., „Zapora Linuksa”	430
Rozdział 5., „Standardy bezpieczeństwa Linuksa na praktycznych przykładach”	431
Rozdział 6., „Usługi DNS w Linuksie”	431
Rozdział 7., „Usługi DHCP w Linuksie”	432
Rozdział 8., „Usługi certyfikatów w Linuksie”	435
Rozdział 9., „Usługi RADIUS w Linuksie”	436
Rozdział 10., „Usługi równoważenia obciążenia w Linuksie”	438
Rozdział 11., „Przechwytywanie i analiza pakietów w Linuksie”	438
Rozdział 12., „Monitorowanie sieci z wykorzystaniem Linuksa”	439
Rozdział 13., „Systemy zapobiegania włamaniom w Linuksie”	441
Rozdział 14., „Usługi honeypot w Linuksie”	442
 Skorowidz	 443