

Spis treści

O autorze	13
O recenzencie	14
Przedmowa	15
Rozdział 1. Problemy bezpieczeństwa w systemie Linux	21
Polityka bezpieczeństwa	22
Opracowanie polityki bezpieczeństwa	22
Mity związane z bezpieczeństwem systemu Linux	22
Konfigurowanie zabezpieczeń serwerów	23
Jak to zrobić...	24
Jak to działa...	25
Polityka bezpieczeństwa — bezpieczeństwo serwera	26
Jak to zrobić...	26
Jak to działa...	27
Definiowanie listy kontrolnej bezpieczeństwa	28
Jak to zrobić...	28
Jak to działa...	29
Sprawdzanie integralności nośnika instalacyjnego za pomocą funkcji skrótu	30
Przygotuj się	30
Jak to zrobić...	30
Jak to działa...	31
Zobacz również	31
Szyfrowanie dysków z użyciem mechanizmu LUKS	31
Przygotuj się	32
Jak to zrobić...	32
Co dalej?	35

Zastosowanie pliku sudoers — konfiguracja dostępu do polecenia sudo	36
Przygotuj się	36
Jak to zrobić...	36
Jak to działa...	38
Co dalej?	38
Skanowanie hostów za pomocą programu Nmap	39
Przygotuj się	39
Jak to zrobić...	39
Jak to działa...	43
Zobacz również	43
Zdobywanie uprawnień użytkownika root w podatnym na ataki systemie Linux	43
Przygotuj się	43
Jak to zrobić...	44
Jak to działa...	46
Co dalej?	47
Brak planu tworzenia kopii zapasowych	47
Przygotuj się	47
Jak to zrobić...	47
Jak to działa...	49
 Rozdział 2. Konfigurowanie bezpiecznego i zoptymalizowanego jądra systemu	 51
Tworzenie nośnika startowego USB	52
Przygotuj się	52
Jak to zrobić...	52
Jak to działa...	53
Pobieranie kodu źródłowego jądra systemu	53
Przygotuj się	54
Jak to zrobić...	54
Jak to działa...	55
Konfigurowanie i budowanie jądra systemu	55
Przygotuj się	55
Jak to zrobić...	56
Jak to działa...	60
Instalowanie i uruchamianie nowego jądra	60
Przygotuj się	60
Jak to zrobić...	61
Jak to działa...	62
Testowanie nowego jądra i usuwanie błędów	63
Konfigurowanie konsoli do debugowania przy użyciu modułu Netconsole	63
Przygotuj się	64
Jak to zrobić...	65
Jak to działa...	69
Co dalej?	69
Debugowanie procesu uruchamiania jądra	70
Jak to zrobić...	70
Błędy jądra	71
Przyczyny powstawania błędów jądra	71
Analizowanie ustawień i parametrów jądra za pomocą programu Lynis	73
Przygotuj się	73
Jak to zrobić...	74

Rozdział 3. Bezpieczeństwo lokalnego systemu plików	77
Wyświetlanie szczegółowych informacji o plikach i katalogach za pomocą polecenia ls	78
Przygotuj się	78
Jak to zrobić...	78
Jak to działa...	80
Zastosowanie polecenia chmod do ustawiania praw dostępu do plików i katalogów	80
Przygotuj się	80
Jak to zrobić...	81
Jak to działa...	83
Co dalej?	83
Zastosowanie polecenia chown do zmiany właściciela plików i katalogów	84
Jak to zrobić...	84
Co dalej?	86
Zastosowanie list ACL do ustawiania praw dostępu do plików	86
Przygotuj się	86
Jak to zrobić...	87
Co dalej?	89
Operacje na plikach z użyciem polecenia mv (przenoszenie plików i zmiana ich nazw)	90
Przygotuj się	90
Jak to działa...	90
Wdrażanie systemu obowiązkowej kontroli dostępu (MAC)	
z wykorzystaniem rozszerzenia SELinux	95
Przygotuj się	95
Jak to zrobić...	96
Jak to działa...	97
Co dalej?	97
Zastosowanie rozszerzonych atrybutów plików do ochrony plików wrażliwych	98
Przygotuj się	98
Jak to zrobić...	99
Instalowanie i konfigurowanie prostego serwera LDAP w systemie Ubuntu Linux	100
Przygotuj się	100
Jak to zrobić...	100
Jak to działa...	106
Rozdział 4. Uwierzytelnianie lokalne w systemie Linux	107
Uwierzytelnianie i logowanie się użytkowników	107
Przygotuj się	107
Jak to zrobić...	108
Jak to działa...	110
Ograniczanie możliwości logowania się użytkowników	110
Przygotuj się	110
Jak to zrobić...	111
Jak to działa...	113
Blokowanie możliwości logowania się użytkowników	113
Przygotuj się	114
Jak to zrobić...	114
Jak to działa...	116

Monitorowanie aktywności użytkowników przy użyciu pakietu acct	116
Przygotuj się	116
Jak to zrobić...	118
Jak to działa...	119
Uwierzytelnianie użytkowników za pomocą klucza USB i mechanizmu PAM	120
Przygotuj się	120
Jak to zrobić...	120
Jak to działa...	124
Co dalej?	124
Sprawdzanie autoryzacji użytkowników	125
Przygotuj się	125
Jak to zrobić...	125
Jak to działa...	128
Zarządzanie dostępem za pomocą systemu IDAM	128
Przygotuj się	128
Jak to zrobić...	130
Jak to działa...	132
 Rozdział 5. Uwierzytelnianie zdalne	 133
Zdalny dostęp do serwera/hosta przy użyciu połączenia SSH	133
Przygotuj się	133
Jak to zrobić...	134
Jak to działa...	136
Włączanie lub blokowanie możliwości logowania się użytkownika root za pośrednictwem sesji SSH	137
Przygotuj się	137
Jak to zrobić...	137
Jak to działa...	139
Co dalej?	139
Ograniczanie zdalnego dostępu z użyciem sesji SSH opartej na kluczach	140
Przygotuj się	140
Jak to zrobić...	140
Jak to działa...	142
Zdalne kopiowanie plików	143
Przygotuj się	143
Jak to zrobić...	143
Jak to działa...	146
Konfiguracja serwera Kerberos na platformie Ubuntu	147
Przygotuj się	147
Jak to zrobić...	147
Jak to działa...	155
Zastosowanie serwera LDAP do uwierzytelniania użytkowników i zarządzania nimi	155
Przygotuj się	155
Jak to zrobić...	156

Rozdział 6. Bezpieczeństwo sieciowe	161
Zarządzanie sieciami TCP/IP	161
Przygotuj się	161
Jak to zrobić...	162
Jak to działa...	165
Zastosowanie analizatora pakietów do monitorowania ruchu w sieci	165
Przygotuj się	166
Jak to zrobić...	166
Jak to działa...	169
Zastosowanie zapory sieciowej iptables	169
Przygotuj się	169
Jak to zrobić...	170
Jak to działa...	174
Blokowanie połączeń ze sfałszowanych adresów IP	174
Przygotuj się	174
Jak to zrobić...	175
Jak to działa...	177
Blokowanie ruchu przychodzącego	178
Przygotuj się	178
Jak to zrobić...	178
Jak to działa...	181
Konfigurowanie i stosowanie pakietu TCP Wrappers	182
Przygotuj się	182
Jak to zrobić...	182
Jak to działa...	186
Blokowanie ruchu sieciowego z danego kraju przy użyciu zapory ModSecurity	186
Przygotuj się	186
Jak to zrobić...	186
Zabezpieczanie ruchu sieciowego przy użyciu protokołu SSL	191
Przygotuj się	191
Jak to zrobić...	191
Jak to działa...	195
Rozdział 7. Narzędzia bezpieczeństwa	197
sXID	197
Przygotuj się	198
Jak to zrobić...	198
Jak to działa...	200
PortSentry	200
Przygotuj się	200
Jak to zrobić...	200
Jak to działa...	204
Squid Proxy	204
Przygotuj się	204
Jak to zrobić...	205
Jak to działa...	208

Serwer OpenSSL	208
Przygotuj się	209
Jak to zrobić...	209
Jak to działa...	213
Co dalej?	213
Tripwire	215
Przygotuj się	215
Jak to zrobić...	215
Jak to działa...	220
Shorewall	220
Przygotuj się	220
Jak to zrobić...	221
Jak to działa...	224
OSSEC	224
Przygotuj się	225
Jak to zrobić...	225
Jak to działa...	232
Snort	232
Przygotuj się	232
Jak to zrobić...	233
Jak to działa...	237
Rsync i Grsync — narzędzia do tworzenia kopii zapasowych	237
Przygotuj się	238
Jak to zrobić...	238
Jak to działa...	243
 Rozdział 8. Dystrybucje systemu Linux związane z bezpieczeństwem	 245
Kali Linux	245
pfSense	251
Przygotuj się	251
Jak to zrobić...	252
Jak to działa...	257
DEFT Linux	257
Jak to działa...	259
NST Linux	259
Przygotuj się	259
Jak to zrobić...	260
Jak to działa...	263
Security Onion Linux	263
Przygotuj się	263
Jak to zrobić...	264
Jak to działa...	270
Tails Linux	270
Przygotuj się	270
Jak to zrobić...	270
Qubes Linux	273
Przygotuj się	273
Jak to zrobić...	274
Jak to działa...	280

Rozdział 9. Usuwanie luk w zabezpieczeniach powłoki bash	281
Powłoka bash — ataki z wykorzystaniem luki Shellshock	281
Przygotuj się	282
Jak to zrobić...	282
Jak to działa...	284
Kwestie bezpieczeństwa — ataki z wykorzystaniem luki Shellshock	285
Przygotuj się	285
Jak to zrobić...	286
Jak to działa...	290
System zarządzania aktualizacjami i poprawkami bezpieczeństwa	291
Przygotuj się	291
Jak to zrobić...	291
Jak to działa...	297
Instalowanie aktualizacji i poprawek bezpieczeństwa w systemie Linux	297
Przygotuj się	297
Jak to zrobić...	298
Jak to działa...	300
Inne znane podatności i luki w zabezpieczeniach systemu Linux	300
Jak to zrobić...	300
Jak to działa...	302
Rozdział 10. Monitorowanie systemu i rejestrowanie zdarzeń	303
Przeglądanie plików dziennika i zarządzanie nimi za pomocą programu Logcheck	303
Przygotuj się	304
Jak to zrobić...	304
Jak to działa...	306
Monitorowanie sieci za pomocą skanera Nmap	307
Przygotuj się	307
Jak to zrobić...	308
Jak to działa...	311
Zastosowanie pakietu Glances do monitorowania systemu	311
Przygotuj się	312
Jak to zrobić...	312
Jak to działa...	315
Monitorowanie dzienników zdarzeń za pomocą programu MultiTail	315
Przygotuj się	315
Jak to zrobić...	316
Jak to działa...	318
Zastosowanie narzędzi systemowych — polecenie whowatch	318
Przygotuj się	318
Jak to zrobić...	319
Jak to działa...	321
Zastosowanie narzędzi systemowych — polecenie stat	322
Przygotuj się	322
Jak to zrobić...	322
Jak to działa...	325

Zastosowanie narzędzi systemowych — polecenie Isof	325
Przygotuj się	325
Jak to zrobić...	325
Jak to działa...	327
Zastosowanie narzędzi systemowych — polecenie strace	328
Przygotuj się	328
Jak to zrobić...	328
Jak to działa...	331
Monitorowanie sieci LAN w czasie rzeczywistym za pomocą pakietu IPTraf	331
Przygotuj się	331
Jak to zrobić...	332
Jak to działa...	336
Monitorowanie bezpieczeństwa sieci za pomocą pakietu Suricata	336
Przygotuj się	336
Jak to zrobić...	337
Monitorowanie sieci za pomocą pakietu OpenNMS	341
Przygotuj się	341
Jak to zrobić...	344
Jak to działa...	348
 Rozdział 11. Bezpieczeństwo serwera Linux	 349
Serwer WWW — usługa HTTPD	349
Przygotuj się	349
Jak to zrobić...	349
Jak to działa...	351
Logowanie zdalne — usługa Telnet	352
Przygotuj się	352
Jak to zrobić...	352
Jak to działa...	354
Bezpieczne logowanie zdalne — usługa SSH	354
Przygotuj się	354
Jak to zrobić...	355
Bezpieczeństwo przesyłania plików — usługa FTP	356
Bezpieczne przesyłanie poczty elektronicznej — usługa SMTP	358
Przygotuj się	358
Jak to zrobić...	358
Jak to działa...	363
 Rozdział 12. Skanowanie i audytowanie systemu Linux	 365
Instalowanie programu antywirusowego w systemie Linux	365
Przygotuj się	366
Jak to zrobić...	366
Jak to działa...	368
Skanowanie systemu za pomocą programu ClamAV	368
Przygotuj się	369
Jak to zrobić...	369
Jak to działa...	372

Wykrywanie rootkitów	372
Przygotuj się	372
Jak to zrobić...	372
Jak to działa...	376
Zastosowanie usługi auditd	376
Przygotuj się	376
Jak to zrobić...	376
Jak to działa...	377
Zastosowanie programów ausearch i aureport do przeglądania dzienników audytu	378
Przygotuj się	378
Jak to zrobić...	378
Jak to działa...	382
Audytowanie usług systemowych za pomocą polecenia systemctf	382
Przygotuj się	382
Jak to zrobić...	383
Jak to działa...	384
 Rozdział 13. Skanowanie w poszukiwaniu luk i podatności oraz wykrywanie włamań	 385
Monitorowanie bezpieczeństwa sieci z użyciem systemu Security Onion Linux	385
Przygotuj się	386
Jak to zrobić...	386
Jak to działa...	389
Wyszukiwanie luk i podatności na ataki z użyciem pakietu OpenVAS	389
Przygotuj się	389
Jak to zrobić...	389
Jak to działa...	394
Zastosowanie programu Nikto do skanowania serwerów WWW	395
Przygotuj się	395
Jak to zrobić...	395
Jak to działa...	397
Utwierdzanie systemu przy użyciu programu Lynis	397
Przygotuj się	397
Jak to zrobić...	398
Jak to działa...	400
 Skorowidz	 401