

Spis treści |

O autorze	15
O recenzentach	16
Przedmowa	17

CZĘŚĆ 1.

Podstawy zabezpieczeń systemu Linux

ROZDZIAŁ 1.

Uruchamianie systemu Linux w środowisku wirtualnym	23
Przegląd zagrożeń	24
Dlaczego dochodzi do naruszeń bezpieczeństwa?	25
Bądź na bieżąco z wiadomościami dotyczącymi bezpieczeństwa	25
Różnice między konfiguracjami systemu: fizyczną, wirtualną i w chmurze	26
VirtualBox i Cygwin	27
Instalowanie maszyny wirtualnej w VirtualBox	28
Instalowanie repozytorium EPEL na maszynie wirtualnej CentOS 7	32
Instalacja repozytorium EPEL na maszynach wirtualnych AlmaLinux 8/9	33
Konfigurowanie sieci w maszynach wirtualnych VirtualBox	33
Tworzenie migawki maszyny wirtualnej za pomocą VirtualBox	34
Używanie Cygwin do łączenia się z maszynami wirtualnymi	35
Korzystanie z klienta SSH systemu Windows 10 do łączenia się z maszynami wirtualnymi działającymi z systemem Linux	36
Korzystanie z klienta SSH systemu Windows 11 do łączenia się z maszynami wirtualnymi z systemem Linux	39
Aktualizowanie systemów Linux	39
Aktualizowanie systemów opartych na Debianie	40
Konfigurowanie automatycznych aktualizacji dla Ubuntu	40
Aktualizowanie systemów opartych na Red Hat 7	43
Aktualizowanie systemów opartych na Red Hat8/9	46
Zarządzanie aktualizacjami w przedsiębiorstwie	47

Podsumowanie	48
Pytania	48
Lektura uzupełniająca	49
Odpowiedzi	49

ROZDZIAŁ 2.

Zabezpieczanie kont użytkowników administracyjnych	50
Niebezpieczeństwa związane z logowaniem się jako użytkownik root	50
Zalety korzystania z sudo	51
Konfigurowanie uprawnień sudo dla pełnych użytkowników administracyjnych	52
Dodawanie użytkowników do predefiniowanej grupy administratorów	53
Tworzenie wpisu w pliku zasad sudo	54
Konfigurowanie sudo dla użytkowników z wybranymi oddelegowanymi uprawnieniami	55
Ćwiczenie: przypisywanie ograniczonych uprawnień sudo	58
Zaawansowane wskazówki i porady dotyczące korzystania z sudo	60
Minutnik sudo	60
Wyświetlanie swoich uprawnień sudo	61
Uniemożliwianie użytkownikom dostępu do powłoki root	62
Uniemożliwianie użytkownikom ucieczki do powłoki	63
Jak uniemożliwić użytkownikom skorzystanie z innych niebezpiecznych programów?	65
Ograniczanie działań użytkownika do wykonywania określonych poleceń	66
Umożliwianie działania w imieniu innego użytkownika	67
Zapobieganie nadużyciom poprzez skrypty powłoki użytkownika	67
Wykrywanie i usuwanie domyślnych kont użytkowników	69
Nowe funkcje sudo	70
Specjalne uwagi dotyczące sudo dla SUSE i OpenSUSE	70
Podsumowanie	72
Pytania	73
Lektura uzupełniająca	74
Odpowiedzi	74

ROZDZIAŁ 3.**Zabezpieczanie kont zwykłych użytkowników 75**

Zabezpieczanie katalogów domowych użytkowników w systemach Red Hat	75
Zabezpieczanie katalogów domowych użytkowników w systemach Debian i Ubuntu	76
useradd w Debian/Ubuntu	77
adduser w systemach Debian/Ubuntu	78
Wymuszenie korzystania z silnych haseł	79
Instalowanie i konfigurowanie pwquality	81
Ustawianie i używanie mechanizmu wygasania haseł i kont	84
Konfigurowanie domyślnych danych wygasania haseł przy użyciu pliku useradd (tylko dla rodziny systemów Red Hat)	86
Ustawianie danych związanych z wygasaniem dla poszczególnych kont za pomocą useradd i usermod	87
Ustawianie opcji wygasania poszczególnych kont za pomocą chage	89
Ćwiczenie: ustawianie wygasania konta i hasła	90
Zapobieganie atakom siłowym na hasła	91
Konfigurowanie modułu pam_tally2 PAM w systemie CentOS 7	92
Konfigurowanie pam_faillock na AlmaLinux 8/9	94
Konfiguracja pam_faillock dla Ubuntu 20.04 i Ubuntu 22.04	96
Blokowanie kont użytkowników	96
Używanie usermod do blokowania konta użytkownika	97
Używanie passwd do blokowania kont użytkowników	97
Blokowanie konta użytkownika root	98
Konfigurowanie wiadomości z ostrzeżeniem	99
Korzystanie z pliku motd	99
Korzystanie z pliku issue	100
Korzystanie z pliku issue.net	101
Wykrywanie ujawnionych haseł	101
Ćwiczenie: wykrywanie ujawnionych haseł	104
Scentralizowane zarządzanie użytkownikami	105
Microsoft Active Directory	105
Samba w systemie Linux	106
FreeIPA — zarządzanie tożsamością na dystrybucjach typu RHEL	107
Podsumowanie	108
Pytania	108
Lektura uzupełniająca	109
Odpowiedzi	110

ROZDZIAŁ 4.**Zabezpieczanie serwera za pomocą zapory sieciowej — część I 111**

Wymagania techniczne	111
Podstawy działania zapory sieciowej w systemie Linux	112
Narzędzie iptables	113
Podstawy iptables	114
Blokowanie ruchu ICMP za pomocą iptables	118
Blokowanie wszystkiego, co nie jest dozwolone, za pomocą iptables	120
Blokowanie nieprawidłowych pakietów za pomocą iptables	123
Przywracanie usuniętych reguł	129
Ochrona IPv6	131
nftables — bardziej uniwersalny typ zapory sieciowej	135
Co nieco o tabelach i łańcuchach w nftables	136
Konfiguracja nftables w Ubuntu	136
Używanie poleceń nft	140
Podsumowanie	146
Pytania	147
Lektura uzupełniająca	148
Odpowiedzi	148

ROZDZIAŁ 5.**Zabezpieczanie serwera za pomocą zapory sieciowej — część II 149**

Wymagania techniczne	149
Nieskomplikowana zaporę sieciową dla systemów Ubuntu	150
Konfigurowanie ufw	150
Praca z plikami konfiguracyjnymi ufw	152
firewalld dla systemów z rodziny Red Hat	156
Weryfikacja statusu firewalld	157
Praca ze strefami firewalld	158
Dodawanie usług do strefy firewalld	161
Dodawanie portów do strefy firewalld	165
Blokowanie ICMP	166
Korzystanie z trybu „panika”	168
Rejestrowanie porzuconych pakietów	169
Korzystanie z „bogatego” języka reguł firewalld	170
Przeglądanie reguł iptables w firewalld w RHEL/CentOS 7	172
Bezpośrednie tworzenie reguł w firewalld RHEL/CentOS 7	174
Rzut oka na reguły nftables w firewalld RHEL/AlmaLinux 8 i 9	176
Tworzenie bezpośrednich reguł w RHEL/AlmaLinux firewalld	177

Podsumowanie	179
Pytania	180
Lektura uzupełniająca	181
Odpowiedzi	181

ROZDZIAŁ 6.

Technologie szyfrowania	182
GNU Privacy Guard (GPG)	183
Ćwiczenie: tworzenie kluczy GPG	184
Ćwiczenie: symetryczne szyfrowanie własnych plików	186
Ćwiczenie: szyfrowanie plików za pomocą kluczy publicznych	188
Ćwiczenie: podpisywanie pliku (bez szyfrowania)	192
Szyfrowanie partycji za pomocą Linux Unified Key Setup (LUKS)	192
Szyfrowanie dysku podczas instalacji systemu operacyjnego	193
Konfigurowanie partycji LUKS do automatycznego montowania	199
Ćwiczenie: konfigurowanie partycji LUKS do automatycznego montowania	200
Szyfrowanie katalogów za pomocą eCryptfs	201
Ćwiczenie: szyfrowanie katalogu domowego dla nowego konta użytkownika	201
Tworzenie prywatnego katalogu w istniejącym katalogu domowym	201
Ćwiczenie: szyfrowanie innych katalogów za pomocą eCryptfs	203
Szyfrowanie partycji wymiany za pomocą eCryptfs	205
Korzystanie z VeraCrypt do wieloplatformowego udostępniania zaszyfrowanych kontenerów	205
Ćwiczenie: pobieranie i instalowanie VeraCrypt	206
Korzystanie z VeraCrypt z graficznym interfejsem użytkownika	209
OpenSSL i infrastruktura klucza publicznego	210
Instytucje wydające komercyjne certyfikaty	211
Tworzenie kluczy, żądań podpisania certyfikatów i certyfikatów	214
Tworzenie lokalnego urzędu certyfikacji	219
Dodawanie urzędu certyfikacji do systemu operacyjnego	223
OpenSSL i serwer internetowy Apache	225
Konfigurowanie uwierzytelniania wzajemnego	231
Wprowadzenie algorytmów odpornych na obliczenia kwantowe	231
Podsumowanie	232
Pytania	233
Lektura uzupełniająca	234
Odpowiedzi	235

ROZDZIAŁ 7.**Utwarczanie SSH 236**

Upewnianie się, że protokół SSH 1 jest wyłączony	237
Tworzenie kluczy do logowania bez hasła i zarządzanie kluczami	237
Tworzenie zestawu kluczy SSH użytkownika	238
Przesyłanie klucza publicznego do zdalnego serwera	241
Wyłączanie logowania użytkownika root	244
Wyłączanie logowania przy użyciu nazwy użytkownika i hasła	246
Włączanie uwierzytelniania dwuskładnikowego	247
Konfigurowanie Secure Shell z silnymi algorytmami szyfrowania	252
Skanowanie w poszukiwaniu włączonych algorytmów SSH	256
Wyłączenie słabych algorytmów szyfrowania SSH	257
Ustawianie zasad szyfrowania na poziomie całego systemu operacyjnego w systemach RHEL 8/9 i AlmaLinux 8/9	260
Konfigurowanie bardziej szczegółowego rejestrowania	262
Konfigurowanie kontroli dostępu za pomocą białych list i TCP Wrappers	264
Konfigurowanie białych list w sshd_config	265
Konfigurowanie białych list za pomocą TCP Wrappers	267
Konfigurowanie automatycznego wylogowywania i wiadomości ostrzegawczych	268
Konfigurowanie automatycznego wylogowywania dla użytkowników lokalnych i zdalnych	268
Konfigurowanie automatycznego wylogowywania w sshd_config	269
Tworzenie wiadomości ostrzegawczej wyświetlanej przed logowaniem	269
Konfigurowanie innych ustawień zabezpieczeń	270
Wyłączanie przekierowania X11	270
Wyłączanie tunelowania SSH	270
Zmiana domyślnego portu SSH	271
Zarządzanie kluczami SSH	272
Ustawianie różnych konfiguracji dla różnych użytkowników i grup	275
Tworzenie różnych konfiguracji dla różnych hostów	276
Konfigurowanie środowiska chroot dla użytkowników SFTP	277
Tworzenie grupy i konfiguracja pliku sshd_config	277
Udostępnianie katalogu za pomocą SSHFS	280
Ćwiczenie: udostępnianie katalogu z SSHFS	280
Zdalne łączenie się z komputerów stacjonarnych z systemem Windows	282
Podsumowanie	286
Pytania	286
Lektura uzupełniająca	288
Odpowiedzi	289

CZĘŚĆ 2.

Kontrola dostępu do plików i katalogów (DAC)

ROZDZIAŁ 8.

Uznaniowa kontrola dostępu (DAC)	293
Używanie chown do zmiany własności plików i katalogów	293
Używanie chmod do ustawiania uprawnień na plikach i katalogach	295
Ustawianie uprawnień za pomocą metody symbolicznej	296
Ustawianie uprawnień metodą numeryczną	297
Używanie SUID i SGID na zwykłych plikach	298
Wpływ uprawnień SUID i SGID na bezpieczeństwo	300
Wyszukiwanie niepożądanych plików z ustawionym SUID lub SGID	300
Zapobieganie używaniu SUID i SGID na partycji	302
Używanie rozszerzonych atrybutów plików do ochrony wrażliwych plików	303
Ustawianie atrybutu a	304
Ustawianie atrybutu i	305
Zabezpieczanie plików konfiguracyjnych systemu	306
Podsumowanie	309
Pytania	309
Lektura uzupełniająca	312
Odpowiedzi	312

ROZDZIAŁ 9.

Listy kontroli dostępu i zarządzanie udostępnionymi katalogami	314
Tworzenie listy ACL dla użytkownika lub grupy	314
Tworzenie dziedziczonej listy ACL dla katalogu	317
Usuwanie określonego uprawnienia przy użyciu maski ACL	318
Używanie opcji tar --acls, aby zapobiec utracie list ACL podczas tworzenia kopii zapasowej	319
Tworzenie grupy użytkowników i dodawanie do niej członków	321
Dodawanie członków podczas tworzenia kont użytkowników	322
Użycie usermod, by dodać do grupy konto istniejącego użytkownika	322
Dodawanie użytkowników do grupy poprzez edycję pliku /etc/group	323
Tworzenie udostępnionego katalogu	323
Ustawienie bitu SGID i lepkiego bitu na udostępnionym katalogu	325
Korzystanie z list ACL w celu ustawienia uprawnień dostępu do plików w udostępnionym katalogu	327
Ustawianie uprawnień i tworzenie listy ACL	327

Podsumowanie	330
Pytania	330
Lektura uzupełniająca	332
Odpowiedzi	332

CZĘŚĆ 3.

Zaawansowane techniki utwardzania systemu

ROZDZIAŁ 10.

Wdrażanie obligatoryjnej kontroli dostępu

za pomocą SELinux i AppArmor	337
Jak SELinux może wspomóc administratora systemu?	338
Ustawianie kontekstu zabezpieczeń dla plików i katalogów	339
Instalowanie narzędzi dla SELinux	341
Tworzenie plików zawierających treści publikowane w Internecie z włączonym SELinux	342
Poprawianie nieprawidłowego kontekstu SELinux	344
Rozwiązywanie problemów za pomocą setroubleshoot	349
Wyświetlanie komunikatów setroubleshoot	349
Korzystanie z narzędzia setroubleshoot w interfejsie graficznym	350
Rozwiązywanie problemów w trybie pobłażliwym	352
Praca z zasadami SELinux	354
Wyświetlanie wartości logicznych	354
Ustawianie wartości logicznych	356
Ochrona serwera WWW	357
Ochrona portów sieciowych	358
Tworzenie niestandardowych modułów zasad	360
Jak AppArmor może pomóc administratorowi systemu	363
Profile w AppArmor	363
Praca z narzędziami wiersza poleceń AppArmor	366
Rozwiązywanie problemów z AppArmor	369
Rozwiązywanie problemów z profilem AppArmor w Ubuntu 16.04	370
Rozwiązywanie problemów z profilem AppArmor w Ubuntu 18.04	372
Rozwiązywanie problemów z Sambą w Ubuntu 22.04	374
Atak na system za pomocą odpowiednio przygotowanego kontenera Dockera	375
Ćwiczenie: tworzenie „niegrzecznego” kontenera Dockera	376
Podsumowanie	378

Pytania	378
Lektura uzupełniająca	380
Odpowiedzi	381

ROZDZIAŁ 11.

Utwardzanie jądra i izolowanie procesów 382

System plików /proc	383
Przegląd procesów w trybie użytkownika	383
Przeglądanie informacji o jądrze	385
Ustawianie parametrów jądra za pomocą sysctl	387
Konfiguracja pliku sysctl.conf	388
Konfiguracja sysctl.conf — Ubuntu	389
Konfiguracja sysctl.conf — CentOS i AlmaLinux	392
Ustawianie dodatkowych parametrów utwardzających jądro	393
Zapobieganie wzajemnemu podglądaniu swoich procesów przez użytkowników	396
O izolacji procesów	397
Grupy kontrolne (cgroups)	397
Izolacja przestrzeni nazw	401
Mechanizmy CAP jądra	402
Zrozumienie SECCOMP i wywołań systemowych	406
Korzystanie z izolacji procesów w kontenerach Dockera	408
Uruchamianie w piaskownicy z Firejail	409
Uruchamianie w piaskownicy ze Snappy	412
Uruchamianie w piaskownicy z Flatpak	416
Podsumowanie	418
Pytania	418
Lektura uzupełniająca	420
Odpowiedzi	422

ROZDZIAŁ 12.

Skanowanie, monitoring i utwardzanie 423

Instalowanie i aktualizowanie ClamAV i maldet	424
Ćwiczenie: instalacja ClamAV i maldet	425
Ćwiczenie: konfiguracja maldet	426
Aktualizowanie ClamAV i maldet	428
Skanowanie za pomocą ClamAV i maldet	430
Uwagi związane z SELinux	431

Skanowanie w poszukiwaniu rootkitów za pomocą Rootkit Hunter	432
Ćwiczenie: instalacja i aktualizacja Rootkit Hunter	433
Skanowanie w poszukiwaniu rootkitów	434
Przeprowadzanie szybkiej analizy złośliwego oprogramowania przy użyciu ciągów znaków i VirusTotal	435
Przeanalizuj plik z ciągami znaków	435
Skanowanie złośliwego oprogramowania za pomocą VirusTotal	436
Demon auditd	437
Tworzenie reguł monitorowania	438
Monitorowanie pliku	438
Monitorowanie katalogu	440
Monitorowanie wywołań systemowych	441
Korzystanie z ausearch i aureport	442
Wyszukiwanie powiadomień o zmianie pliku	442
Wyszukiwanie naruszeń reguł dostępu do katalogu	445
Wyszukiwanie naruszeń reguł wywołań systemowych	449
Generowanie raportów uwierzytelniania	451
Korzystanie z predefiniowanych zestawów reguł	452
Ćwiczenie: korzystanie z auditd	453
Ćwiczenie: Używanie wstępnie skonfigurowanych reguł z auditd	454
Monitorowanie plików i katalogów za pomocą inotifywait	455
Stosowanie zasad OpenSCAP za pomocą oscap	456
Instalacja OpenSCAP	457
Przeglądanie plików profilu	457
Pobieranie brakujących profili dla Ubuntu	458
Skanowanie systemu	459
Poprawianie konfiguracji systemu	460
Korzystanie ze SCAP Workbench	462
Wybór profilu OpenSCAP	463
Zastosowanie profilu OpenSCAP podczas instalacji systemu	465
Podsumowanie	467
Pytania	467
Lektura uzupełniająca	469
Odpowiedzi	470

ROZDZIAŁ 13.

Rejestrowanie i bezpieczeństwo dzienników	471
Pliki dzienników systemu Linux	471
Dziennik systemowy i dziennik uwierzytelniania	472
Pliki utmp, wtmp, btmp i lastlog	475

Jak działa rsyslog	477
Reguły rejestrowania rsyslog	478
System journald	480
Ułatwianie sobie pracy dzięki Logwatch	482
Ćwiczenie: instalacja Logwatch	482
Konfigurowanie zdalnego serwera dzienników	484
Ćwiczenie: konfigurowanie podstawowego serwera dzienników	484
Tworzenie szyfrowanego połączenia z serwerem dzienników	486
Rozdzielanie komunikatów klientów do ich własnych plików	490
Utrzymywanie dzienników w dużych przedsiębiorstwach	491
Podsumowanie	491
Pytania	492
Lektura uzupełniająca	493
Odpowiedzi	494

ROZDZIAŁ 14.

Skanowanie pod kątem podatności i wykrywanie włamań

Wprowadzenie do Snorta i Security Onion	495
Pobieranie i instalowanie Snorta	496
Korzystanie z zabezpieczeń Onion	498
IPFire i jego wbudowany system zapobiegania włamaniom (IPS)	499
Ćwiczenie: tworzenie maszyny wirtualnej IPFire	501
Skanowanie i utwardzanie za pomocą Lynis	505
Instalacja Lynis w Red Hat/ CentOS	505
Instalacja Lynis w Ubuntu	505
Skanowanie za pomocą Lynis	506
Znajdowanie podatności za pomocą Greenbone Security Assistant	509
Skanowanie serwerów WWW za pomocą Nikto	516
Nikto w Kali Linux	516
Podsumowanie	520
Pytania	520
Lektura uzupełniająca	521
Odpowiedzi	522

ROZDZIAŁ 15.

Zapobieganie uruchamianiu niepożądanych programów

Montowanie partycji z opcjami „no”	523
Jak działa fapolicyd	530
Reguły fapolicyd	532
Instalowanie fapolicyd	534

Podsumowanie	535
Lektura uzupełniająca	535
Pytania	536
Odpowiedzi	537

ROZDZIAŁ 16.

Wskazówki i porady dotyczące bezpieczeństwa dla zapracowanych 538

Wymagania techniczne	538
Monitorowanie usług systemowych	538
Monitorowanie usług systemowych za pomocą systemctl	539
Monitorowanie usług sieciowych za pomocą netstat	540
Monitorowanie usług sieciowych za pomocą Nmap	545
Ochrona programu ładującego GRUB2 hasłem	552
Ćwiczenie: resetowanie hasła dla Red Hat/ CentOS/ AlmaLinux	553
Ćwiczenie: resetowanie hasła w Ubuntu	555
Zapobieganie edycji parametrów jądra w systemach Red Hat/ CentOS/ AlmaLinux	558
Blokowanie możliwości modyfikowania parametrów jądra lub dostępu do trybu odzyskiwania w Ubuntu	559
Wyłączanie podmenu dla Ubuntu	562
Bezpieczna konfiguracja BIOS/UEFI	563
Korzystanie z listy kontrolnej bezpieczeństwa podczas konfiguracji systemu	566
Podsumowanie	568
Pytania	569
Lektura uzupełniająca	571
Odpowiedzi	571