

SPIS TREŚCI

Od Autora	19
Podziękowania	21
Od Wydawcy	23
Linux Early Access: podziękowania	23
Konwencje stosowane w książce	25
Wstęp Leszek Miś	29
Dlaczego z lektury Twierdzy... skorzysta początkujący?	30
Twierdza... dla eksperta	31
Nie ma na tym świecie człowieka, który o Linuksie wie wszystko	33
1. Linux i bezpieczeństwo z lotu ptaka: o czym jest ta książka	35
Co to jest [GNU/]Linux?	37
Nazewnictwo w książce	40
Bezpieczeństwo systemu: co to właściwie znaczy?	41
Po co zabezpieczenia?	42
Atak na system linuksowy z lotu ptaka	44
Przed kim się bronimy?	45
Reguły postępowania w zabezpieczaniu systemów	47
Ciągły proces, nie jednorazowe działanie	48
Model F/LOSS a bezpieczeństwo	49
2. Źródła i aktualność oprogramowania	51
Po co te wszystkie aktualizacje?	53
Okres wsparcia dystrybucji	54
Wersja dystrybucji a wersja jądra	58
Samodzielna kompilacja jądra	59
Aktualizowanie jądra w locie: livepatching	61
Różne źródła programów i ich wpływ na bezpieczeństwo	62
Pakiety .deb/.rpm i mechanizm repozytoriów APT/RPM	65
DNF: szczegóły konfiguracji	68
APT: szczegóły konfiguracji	70

Repozytoria inne niż bazowe	73
Serwery lustrzane	75
Bezpieczeństwo pojedynczych pakietów	76
Jak przeanalizować zawartość pliku .deb lub .rpm	77
Weryfikacja pochodzenia i spójności plików zainstalowanych z pakietów	79
Pochodzenie plików i mechanizm alternatyw	80
Jak skutecznie ustalić listę zainstalowanych pakietów?	81
Aktualizacje automatyczne dla „małych i prostych” systemów	83
Mechanizmy Snap i Flatpak	84
Dystrybucje typu niezmiennego (immutable/atomic)	87
Deklaratywne (functional) menedżery pakietów: Nix i Guix	88
Bezpieczeństwo oprogramowania z innych źródeł	90
Pojedyncze pliki binarne (np. Applmage), binarne instalatory, skrypty instalacyjne	90
Programy kompilowane ze źródeł	92
Menedżery pakietów/bibliotek specyficzne dla języków programowania	93
Docker i inne mechanizmy konteneryzacji	94
Serwery aplikacji dla Javy, Pythona i innych oraz pozostałe aplikacje serwerowe	95
Wtyczki, dodatki, rozszerzenia	95
Pliki konfiguracyjne środowiska i bibliotek	96
Kiedy restart po aktualizacji jest konieczny?	97
Co należy odinstalować?	97
Ataki na łańcuch dostaw (supply chain attacks)	99
Checklista: źródła i aktualność oprogramowania	101

3. Konta, użytkownicy, uprawnienia **105**

Linuksowy model uprawnień – przypomnienie	107
Uprawnienia w praktyce: przykłady i problemy	110
„Ślepe przejście” przez katalog	110
Pliki wykonywalne a setuid (u+s) i setgid (g+s)	111
Uprawnienia nowo tworzonych plików: umask, setgid na katalogu	112
Czy można kasować cudze pliki? Czyli o sticky bit	114
Nadawanie uprawnień, zmiana właściciela – czy rozumiesz, co robisz?	114
Mechanizm ACL: listy kontroli dostępu	115
Użytkownicy i grupy	118
Systemowa baza kont	118
Zarządzanie kontami: kwestie praktyczne	120
Zawartość katalogu domowego nowo tworzonego użytkownika	120
Imię i nazwisko użytkownika lub pełna nazwa usługi	120

Okresy ważności kont	121
Powłoka konta	122
Członkostwo w grupach	122
Grupy dające podwyższone uprawnienia	123
Konta usług/systemowe	124
Usuwanie kont a właścicielstwo plików	124
Limity zasobów użytkowników	125
Sudo i su	125
Pozornie bezpieczne: sudo a funkcjonalność narzędzi	127
Pozornie bezpieczne: symbole wieloznaczne w regułach	128
Program su	129
Inne narzędzia służące do wykonywania poleceń z podniesionymi uprawnieniami	130
Atrybuty (lsattr, chattr)	131
Capabilities	132
Nadawanie capabilities wybranym użytkownikom za pomocą PAM	135
PAM – moduły uwierzytelnienia	136
Wywołania modułów	136
Przykład: wzmocnienie wymagań dla haseł	139
Przykład: uwierzytelnianie kluczami a przeterminowane hasła	141
Ograniczenie uruchamiania aplikacji: fapolicyd	142
Checklista: konta i uprawnienia	142
4. Bezpieczeństwo SSH i dostępu zdalnego	145
Czym jest SSH	147
Po pierwsze: protokół bezpiecznej komunikacji	147
Po drugie: protokoły aplikacyjne zaimplementowane jako część SSH	148
Implementacje serwera	149
Implementacje klienta	149
Jak nawiązywane jest bezpieczne połączenie SSH klient-serwer	150
Konfiguracja i zabezpieczenie serwera	153
Port 22 czy inny?	154
Protokoły szyfrowania i klucze serwera	155
Zaufanie do klucza serwera, atak MitM, rekordy DNS SSHFP	158
Ograniczanie uprawnień kont i grup	161
Blokada/zezwoleń na logowanie kont i grup	161
Selektywne ograniczanie uprawnień kont i grup	162
Konta przeznaczone tylko do transferu plików (SFTP-only)	163
Ochrona przed atakami DDoS i brute-force	164

Tunele (forwardowanie połączeń)	165
Wyłączenie logowania hasłem dla konta root	168
Inne istotne ustawienia serwera	169
Konfiguracja innych mechanizmów systemu a SSH	170
SSH po stronie klienta	171
Konfiguracja klienta OpenSSH	171
Generowanie pary kluczy klienta na potrzeby uwierzytelnienia	173
Logowanie kluczami	175
Plik authorized_keys	176
Agent SSH	177
Tunelowanie połączeń do agenta SSH, czyli jak pracować wygodnie i nadal trzymać klucze przy sobie	178
Ilu kluczy potrzebuje jedna osoba?	179
Czy model działania agenta SSH jest bezpieczny?	180
Agent w trybie potwierdzania, czyli kontrola zamiast wygody	181
PuTTY i WinSCP a klucze i agent	182
MFA i klucze sprzętowe	183
Checklisty: SSH	185
Serwer	185
Klient	186

5. Powłoka i GUI – jak pracować bezpiecznie

BHPS: bezpieczeństwo i higiena powłoki oraz skryptów	192
W jakim języku rozmawiamy?	192
Co ja właściwie uruchamiam?	194
Używaj cudzysłowów, waliduj wejście	195
O filozofii porównań i naturze nawiasu	197
Zmienne – bezpieczniej	199
Włączanie zawartości z zewnętrznych plików	200
Sekrety na widoku	201
Nie przeszkadzać sąsiadom, nie zostawiać po sobie śmieci	201
Znaleźć i nie zgubić: find, -exec oraz xargs	202
Jeszcze raz: nie zostawiać po sobie śmieci	204
Od A do... czego?	204
Debugging skryptów	205
Hardening skryptów – przydatne opcje	207
Praca interaktywna w powłoce: porady	207
Wygoda i ergonomia środowiska	208

Wstydliva historia	211
Jak szybko i prosto uruchomić malware... przez przypadek	212
Procesy i sesje w tle a blokowanie sesji terminalowej	212
Konsola współdzielona przez Internet	212
Co może pójść nie tak przy pracy w środowisku graficznym	213
GUI a dostęp zdalny do systemu	215
Linux dla całej rodziny	217
Czy mój system mnie śledzi?	218
6. Utwardzanie konfiguracji usług	223
Co i dlaczego działa w systemie?	225
Lista procesów	225
Spis usług	226
Otwarte porty i nasłuchujące procesy	227
Systemd i jego jednostki (unity) konfiguracyjne	227
Jak całkowicie zablokować start usługi bez jej odinstalowywania	229
Checklista: bezpieczna konfiguracja usługi – zasady ogólne	229
Checklista: przegląd systemu pod kątem zainstalowanych i działających usług	233
Checklisty i porady dla poszczególnych typów usług	233
Ustawienie i synchronizacja czasu (NTP)	234
Poczta: lokalne SMTP	236
Automatyczne uruchamianie zadań	237
Cron	238
atd	239
Timery mechanizmu systemd	239
Serwery WWW	241
PHP na serwerze WWW	243
Load balancery i reverse proxy	245
Java i jej serwery aplikacyjne (Tomcat, JBoss i inne)	245
Bazy danych (MySQL/MariaDB, PostgreSQL)	246
Bazy NoSQL (np. Redis, MongoDB)	247
Wirtualizacja	248
Konteneryzacja	250
Systemy kopii zapasowych i monitoringu infrastruktury	252
Usługi zarządzania zdalnego	253
FTP	254
rsyncd	254
Network File System (NFS) i usługi towarzyszące	255

Usługi druku: CUPS i LPD	257
inetd i xinetd, proces init (systemd) nasłuchujący na TCP/UDP	257
Baza plików locate	258
Środowisko graficzne i polkit (PolicyKit)	258
Hardening usług z poziomu systemd	260
Poprawna edycja i tworzenie jednostek .service	260
Jak ograniczyć usługę i jej środowisko wykonawcze	262

7. Mechanizmy bezpieczeństwa w jądrze

Jądro, przestrzeń użytkownika i wywołania systemowe	269
Moduły jądra	270
Konfiguracja jądra i modułów	271
Bezpieczeństwo ładowania i konfiguracji modułów	273
Ustawienia sysctl istotne dla bezpieczeństwa	274
Moduły zabezpieczeń LSM (Linux Security Modules)	277
Yama: ograniczenie debugowania (ptrace)	281
Landlock	282
Kernel lockdown mode	282
eBPF: extended Berkeley Packet Filter	283
Inspekcja działających programów eBPF	285
Prosty przykład zabezpieczania istniejących usług	286
Mechanizmy izolacji aplikacji (sandboxing)	287
Control groups (cgroups)	288
Przestrzeń nazw (namespaces)	289
Secure computing (seccomp i seccomp-bpf)	290
Historycznie: chroot	290
Jak tego użyć, czyli izolacja aplikacji w praktyce	291
Mechanizm ulimit	292
Fork-bomba w powłoce: jak się zabezpieczyć	293
Słowo o tworzeniu i pakowaniu aplikacji	294
Ochrona przed zapełnieniem systemu plików	294
Ukrywanie procesów i ochrona systemu plików /proc	295
Utwardzanie jądra: czy można zrobić jeszcze więcej?	297
LKRG: Linux Kernel Runtime Guard	298
Checklista: bezpieczeństwo jądra	299

8. SELinux i AppArmor, czyli dwa najważniejsze LSM	301
SELinux	304
Koncepcja SELinux z lotu ptaka	305
Tryby działania i podstawowe polityki	305
Włączanie, wyłączanie i zmiana trybu pracy SELinux	306
Etykiety (konteksty) zasobów	306
Źródło, cel, domena	310
Przełączniki (booleans)	311
W praktyce: konfiguracja i rozwiązywanie typowych problemów	313
Podręcznik systemowy	313
Jak czytać logi	314
Konteksty (etykiety) plików – przykład 1	316
Konteksty (etykiety) plików – przykład 2	317
„Samoistna” zmiana kontekstów plików: autorelabel i restorecond	318
Konteksty (etykiety) portów – przykład	319
Dostosowanie polityki do potrzeb: audit2allow	319
Selektywne luzowanie restrikcji: permissive domains	322
Reguły dontaudit, czyli czego nie widać w logach	323
SELinux a virtualizacja i konteneryzacja: użycie MCS w praktyce	323
Jak bezpiecznie wrócić do trybu enforcing, jeśli SELinux jest wyłączony	325
Polityka dla nowej aplikacji: od czego zacząć	326
Źródła wiedzy	326
AppArmor	327
Koncepcja	327
Profile	327
Tryby profili	327
W praktyce	328
Logi zdarzeń	329
Konstrukcja profili	329
Diagnostyka, przełączanie trybu profilu	331
Samodzielne tworzenie profili	332
Podprofile, czyli kapelusze (hats)	333
Ochrona mechanizmów wirtualizacji i konteneryzacji	333
Czy można to obejść?	334
Gdzie szukać pomocy	334

9. Firewall i ochrona warstwy sieciowej	337
Co powinna robić zaporą?	339
Przykładowy zestaw reguł firewalla	340
Stateful kontra stateless	341
Połączenia wychodzące: zezwalać czy blokować?	342
Dwa słowa o blokowaniu ruchu ICMP	344
Firewall na Linuksie, czyli co?	344
iptables (czyli netfilter)	344
nftables (czyli... netfilter wiele lat później)	346
eBPF w roli narzędzia do filtrowania i kształtowania ruchu	346
Nakładki ułatwiające zarządzanie zaporą	347
firewalld (firewall-cmd, firewall-config)	347
(Pseudo)usługa nftables i jej starsze rodzeństwo	347
Generatory reguł (nakładki)	348
Skrypty tworzone ręcznie	349
Specjalizowane dystrybucje sieciowe	350
System otwarty na przestrzał: od czego zacząć?	350
TCP wrappers: pliki hosts.deny i hosts.allow	350
Blokowanie dużej liczby adresów IP lub podsieci	351
Automatyczne blokowanie ataków brute-force	352
Fail2ban	352
sshguard	353
Zapora w praktyce: porady i sugestie	354
Co dalej?	355
Checklista: konfiguracja firewalla	356
10. Między sprzętem a systemem	359
Proces uruchamiania systemu i jego słabe punkty	362
Serwis niekoniecznie sprząający, czyli co może napastnik z fizycznym dostępem	365
Weryfikacja integralności systemu i mechanizm Secure Boot	368
Secure Boot w środowisku linuksowym	372
Łańcuch zaufania na Linuksie	374
Dziury w bootie	376
Krok dalej: atestacja, zdalna weryfikacja integralności	378
Kontrowersje wokół Secure Boot i podobnych rozwiązań	378
Alternatywna droga: otwartoźródłowy lub własny firmware	380
Linux a oprogramowanie sprzętowe	381
Linux Vendor Firmware Service (LVFS) i fwupd	381

Edycja ustawień i analiza zabezpieczeń	382
Aktualizacje mikrokodu CPU, odporność na ataki Spectre/Meltdown	383
Układ partycji, systemy plików, opcje montowania	384
Parametry montowania a bezpieczeństwo	386
Bezpieczniejsze montowanie dysków przenośnych	387
Obszar wymiany w pliku	388
Szyfrowanie dysków	389
Wstęp: LUKS – jak to działa	391
Nagłówek LUKS i sloty	393
W praktyce: tworzenie i obsługa szyfrowanych woluminów	396
Plik /etc/crypttab i automatyczne montowanie urządzeń LUKS przy starcie	399
Hasło w postaci pliku-klucza (keyfile)	399
Zmiana hasła (i niektórych parametrów slotu)	401
FDE – pełne szyfrowanie dysku podczas instalacji	401
Dla zaawansowanych: czy można schować /boot wewnątrz LUKS?	404
Integracje dla niełubiących haseł: TPM2, FIDO2, sieciowy serwer kluczy	406
Klucze sprzętowe i systemd-cryptenroll	406
Clevis: TPM, SSS, Tang i NBDE	407
Co jeszcze potrafi cryptsetup	408
Co może pójść nie tak	410
Podstawy: bezpieczne hasła, klucze, nagłówki	410
Wydobycie klucza woluminu z RAM, czyli atak cold boot	412
Kradzież kluczy z TPM	414
Atak z użyciem DMA	415
Fizyczna napaść podczas pracy	415
Jeśli nie FDE, to co?	416
Bezpieczne usuwanie danych	418
Dyski SSD a nadpisywanie danych	420
Wymazywanie dysku za pomocą funkcji firmware'u	421
Ile razy zamazywać?	422
Blokowanie nieautoryzowanych urządzeń	423
Filtrowanie USB z użyciem USBGuard	424
Jak zaplanować i wykonać bezpieczną instalację systemu	426
Nośniki instalacyjne i obrazy bazowe systemu	428
Weryfikacja podpisu ISO instalacyjnego	429
Obrazy bazowe i pliki odpowiedzi dla instalatora	434
Profile bezpieczeństwa (CIS, STIG, FIPS)	435
Checklisty	436

Komputer fizyczny (desktop, laptop, serwer)	436
Maszyna wirtualna, instancja w chmurze	437
GRUB na x86 i start kernela	438
Urządzenia specjalizowane (router, SmartTV, odkurzacz) i IoT	438
Dwa osobiste apele autora	440
Apel do producentów i dostawców urządzeń	440
Apel do kupujących urządzenia	441

11. Wykrywanie incydentów i automatyzacja zabezpieczeń

Logi systemowe i aplikacji na Linuksie	450
Mechanizm syslog	451
Następca sysloga: journald	454
Wysyłka logów na zdalny serwer	455
Archiwizowanie (rotacja) logów	457
Narzędzia do procesowania logów	458
Mechanizm audytowy i usługa auditd	460
Konfiguracja reguł audytu	460
Reguły monitorowania plików	461
Reguły monitorujące wywołania systemowe	462
Reguły/opcje sterujące działaniem mechanizmu audytowego	466
Przegląd i analiza zdarzeń audytowych	468
Monitoring bezpieczeństwa bez SIEM	470
Klasyczny monitoring IT w służbie bezpieczeństwa	470
AIDE: proste narzędzie klasy HIDS	471
Wykrywanie złośliwego oprogramowania	474
Zewnętrzne usługi wspomagające	476
Mam SIEM/EDR/XYZ: co powinien wykrywać?	476
Jak przetestować zabezpieczenia systemu	477
Rejestrowanie aktywności użytkowników	480
Analiza konfiguracji i utrzymanie standardów	481
Narzędzia automatyzujące audyt konfiguracji	482
Standaryzacja zabezpieczeń: CIS, STIG i OpenSCAP	482
Zarządzanie większym środowiskiem	484
Checklista	485

12. Atak, infekcja, incydent	489
Opowieści z pamiętnika i notatnika	491
Młody i naiwny	491
Jak webserwer swoim własnym interfejsem ethernetowym został	492
All your localhost are belong to us	493
NoSQL czy NoScurity?	494
Ransomware	495
Log4Shell, czyli tysiąc małych trzęsień ziemi	496
XZ – jedno trzęsienie ziemi o przeciętnej magnitudzie	498
Wyciek	498
Przegląd linuksowego malware’u	499
Incydent bezpieczeństwa: co robić, gdy przytrafi się mnie?	502
Zabezpieczenie dowodów incydentu w systemie linuksowym	503
13. Bezpieczeństwo a ludzie (i organizacja, czyli też ludzie)	509
Użytkownicy też ludzie	511
IT i security: też ludzie	512
Wolne i otwartoźródłowe oprogramowanie tworzą ludzie	513
Bądź dla siebie człowiekiem	514
Słownik pojęć	517
Spis tabel	531
Spis rysunków	533
Źródła wiedzy	535
Zasoby internetowe	535
Bieżące newsy	535
Dokumentacja i przewodniki	536
Inne warte polecenia źródła wiedzy	536
Bibliografia	537