

Spis treści

1. Linux i bezpieczeństwo z lotu ptaka: o czym jest ta książka

Zagadnienia:

Co to jest [GNU/]Linux?

Bezpieczeństwo systemu – co to właściwie znaczy i po co to robić

Atak: przed czym i przed kim się bronimy?

Reguły postępowania w zabezpieczaniu systemów, modelowanie zagrożeń

Bezpieczeństwo – ciągły proces, nie jednorazowe działanie

Model F/OSS a bezpieczeństwo

2. Źródła i aktualność oprogramowania

Zagadnienia:

Po co te wszystkie aktualizacje?

Okres wsparcia dystrybucji

Wersja dystrybucji a wersja jądra

Samodzielna kompilacja jądra – czy warto?

Aktualizowanie jądra w locie – livepatching

Różne źródła programów i ich wpływ na bezpieczeństwo

Pakiety .rpm/.deb i mechanizm repozytoriów APT/RPM

DNF i APT – szczegóły bezpiecznej konfiguracji

Którym repozytorium ufać

Jak przeanalizować zawartość pliku .deb lub .rpm

Aktualizacje automatyczne

Mechanizmy Snap i Flatpak

Dystrybucje typu niezmiennego (immutable)

Deklaratywne (functional) menedżery pakietów: Nix i Guix

Bezpieczeństwo oprogramowania z innych źródeł

Applmage, binarne instalatory, skrypty instalacyjne

Programy kompilowane ze źródeł

Menedżery specyficzne dla języków programowania (pip, npm...)

Docker i inne mechanizmy konteneryzacji

Serwery aplikacyjne Javy, Pythona i innych oraz pozostałe aplikacje serwerowe

Wtyczki, dodatki, rozszerzenia

Malware w oficjalnych repozytoriach i pakietach?

Czego należy się pozbyć z systemu

Ataki na łańcuch dostaw (supply chain attacks)

Checklista

3. Konta, użytkownicy, uprawnienia

Zagadnienia:

Linuksowy model uprawnień – przypomnienie

Uprawnienia w praktyce: przykłady i problemy

ACL: listy kontroli dostępu

Użytkownicy i grupy

 Zarządzanie kontami: kwestie praktyczne

 Najczęstsze błędy i problemy

 Grupy dające podwyższone uprawnienia

 Konta usług/systemowe

Sudo i su

 Pułapki bezpieczeństwa w konfiguracji sudo

 Inne narzędzia służące wykonywaniu poleceń z podniesionymi uprawnieniami

Atrybuty

Capabilities

Pluggable Authentication Modules (PAM)

 Wzmacnianie systemowej polityki haseł

fapolicyd – mechanizm application whitelisting

Checklista

4. Bezpieczeństwo SSH i dostępu zdalnego

Zagadnienia:

Czym jest SSH

 Protokół transportowy i protokoły wewnętrzne

 Implementacje serwera

 Implementacje klienta

Konfiguracja i zabezpieczenie serwera

 Port 22 czy inny?

 Protokoły szyfrowania i klucze serwera

 Zaufanie do klucza serwera i rekordy DNS SSHFP

 Ograniczanie uprawnień kont i grup

 Ochrona przed atakami DDoS i brute-force

 Tunele (forwardowanie połączeń)

 Inne istotne ustawienia serwera

SSH po stronie klienta

 Konfiguracja klienta OpenSSH

 Logowanie kluczami, dodatkowe możliwości i ograniczenia

 Serwery pośrednie, agent SSH i jak uczynić taki model działania bezpiecznym

 PuTTY i WinSCP a klucze i agent

 MFA i klucze sprzętowe

Checklisty

5. Powłoka i GUI – jak pracować bezpiecznie

Zagadnienia:

Bezpieczeństwo pracy w powłoce

Wygoda i ergonomia środowiska a bezpieczeństwo

Pisanie bezpiecznych skryptów powłoki

Najczęstsze błędy i problemy

Walidacja wejścia

Czy hardening skryptów powłoki jest możliwy

Jak testować/debugować skrypty

Co może pójść nie tak przy pracy w środowisku graficznym

Linux dla całej rodziny

Czy mój system mnie śledzi?

6. Utwarczanie konfiguracji usług

Zagadnienia:

Co i dlaczego działa w systemie?

Systemd i jego jednostki (unity) konfiguracyjne w szczegółach

Bezpieczna konfiguracja usług – zasady ogólne

Checklista

Porady dla poszczególnych typów usług

NTP

SMTP

Cron / atd / timery systemd

Serwery WWW (Apache, Nginx, PHP, load balancery i reverse proxy

Java i jej serwery aplikacyjne

Bazy danych (MySQL/MariaDB, PostgreSQL, NoSQL)

Wirtualizacja

Konteneryzacja

Systemy kopii zapasowych i monitoringu

Usługi zarządzania zdalnego

FTP

rsyncd

Network File System (NFS) i usługi towarzyszące

Usługi druku – CUPS i LPD

inetd i xinetd, proces init (systemd) nasłuchujący na TCP

Środowisko graficzne

Hardening usług z poziomu systemd: cgroups, namespaces i inne

7. Mechanizmy bezpieczeństwa w jądrze

Zagadnienia:

Jądro a przestrzeń użytkownika

Konfiguracja i zabezpieczenia ładowania i konfiguracji modułów

Ustawienia systemctl istotne dla bezpieczeństwa

Moduły zabezpieczeń LSM (Linux Security Modules)

- Yama: ograniczenie debugowania (ptrace)

- Landlock

- Kernel lockdown mode

eBPF: extended Berkeley Packet Filter

- Inspekcja działających programów eBPF

- Prosty przykład zabezpieczania istniejących usług

Mechanizmy izolacji aplikacji (sandboxing)

- Control groups (cgroups)

- Przestrzeń nazw (namespaces)

- Secure computing (seccomp i seccomp-bpf)

- Historycznie: chroot

- Jak tego użyć, czyli izolacja aplikacji w praktyce

Mechanizm ulimit

Słowo o tworzeniu i pakowaniu aplikacji

Ochrona przed zapełnieniem systemu plików

Ukrywanie procesów i ochrona systemu plików /proc

Utwardzanie jądra

- LKRG: Linux Kernel Runtime Guard

Checklista

8. SELinux i AppArmor, czyli dwa najważniejsze LSM

Zagadnienia:

SELinux

- Koncepcja

 - Tryby działania i podstawowe polityki

 - Etykiety (konteksty) zasobów

 - Źródło, cel, domena

 - Przełączniki (booleans)

- W praktyce: konfiguracja i rozwiązywanie typowych problemów na przykładach

 - Dostosowanie systemowej polityki do potrzeb

 - Selektywne luzowanie restrykcji

- Jak bezpiecznie wrócić do trybu enforcing, jeśli SELinux jest wyłączony

- SELinux a wirtualizacja i konteneryzacja – MCS w praktyce

- Polityka dla nowej aplikacji – od czego zacząć

AppArmor

- Koncepcja

 - Profile

 - Tryby profili

- W praktyce

- Konstrukcja profili
- Diagnostyka, przełączanie trybu profilu
- Samodzielne tworzenie profili
- Podprofile, czyli kapelusze (hats)
- Ochrona mechanizmów wirtualizacji i konteneryzacji
- Czy można to obejść?

9. Firewall i ochrona warstwy sieciowej

Zagadnienia:

Firewall na Linuksie, czyli co?

- iptables (czyli netfilter)

- nftables (czyli... netfilter wiele lat później)

- eBPF

- Nakładki ułatwiające zarządzanie zaporą

Co powinna robić zaporą?

- Przykładowy zestaw reguł firewalla

- Stateful kontra stateless

- Połączenia wychodzące: zezwalać czy blokować?

- System otwarty na przestrzał – od czego zacząć?

Blokowanie dużej liczby adresów IP lub podsieci

Automatyczne blokowanie ataków brute-force

TCP wrappers

Porady i sugestie

Checklista

10. Między sprzętem a systemem

Zagadnienia:

Proces uruchamiania systemu i jego słabe punkty

Weryfikacja integralności systemu

- Secure Boot w środowisku linuksowym

- Łańcuch zaufania na Linuksie

- Krok dalej: atestacja, zdalna weryfikacja integralności

- Alternatywne drogi: otwartoźródłowy lub własny firmware

Linux a oprogramowanie sprzętowe

- Linux Vendor Firmware Service (LVFS) i fwupd

- Aktualizacje mikro kodu CPU, odporność na ataki Spectre/Meltdown

Układ partycji, systemy plików, opcje montowania

Szyfrowanie dysków

- Teoria: LUKS – jak to działa

- Praktyka: Tworzenie i obsługa szyfrowanych woluminów

- FDE – pełne szyfrowanie dysku podczas instalacji

- Integracje dla nie lubiących haseł:

- TPM2, klucze sprzętowe (FIDO2), klucze dzielone (SSS), sieciowy serwer kluczy (NBDE)
- Co może pójść nie tak
 - Podstawy obrony: bezpieczne hasła, klucze, nagłówki
 - Atak cold boot, kradzież kluczy z TPM, atak z użyciem DMA
 - Fizyczna napaść podczas pracy
- Jeśli nie LUKS, to co?
- Bezpieczne usuwanie danych
 - Dyski SSD a nadpisywanie danych
 - Ile razy zamazywać?
- Blokowanie nieautoryzowanych urządzeń
 - Filtrowanie USB z użyciem usbguard
- Jak zaplanować i wykonać bezpieczną instalację systemu
 - Weryfikacja nośników instalacyjnych
 - Profile bezpieczeństwa (CIS, STIG, FIPS)
- Checklisty

11. Wykrywanie incydentów i automatyzacja zabezpieczeń

- Zagadnienia:
 - Logi systemowe i aplikacji na Linuksie
 - syslog i journald
 - Wysyłka logów na zdalny serwer
 - Archiwizowanie (rotacja) logów
 - Narzędzia do procesowania logów
 - Mechanizm audytowy i usługa auditd
 - Konfiguracja reguł audytu
 - Przegląd i analiza zdarzeń audytowych
 - Monitoring bezpieczeństwa bez SIEM
 - Klasyczny monitoring IT w służbie bezpieczeństwa
 - AIDE – proste narzędzie klasy HIDS
 - Wykrywanie złośliwego oprogramowania
 - Zewnętrzne usługi wspomagające
 - Mam SIEM/EDR/XYZ. Co powinien wykrywać i jak to przetestować?
 - Rejestrowanie aktywności użytkowników
 - Audyt konfiguracji i utrzymanie standardów
 - Standaryzacja zabezpieczeń: CIS, STIG i OpenSCAP
- Checklista

12. Atak, infekcja, incydent

- Zagadnienia:
 - Incydenty i katastrofy – historie prawdziwe
 - Przegląd linuksowego malware
 - Incydent bezpieczeństwa – co robić?

13. Bezpieczeństwo a ludzie

Zagadnienia:

Użytkownicy też ludzie

Zespoły IT i security to też ludzie

Wolne i otwartoźródłowe oprogramowanie tworzą ludzie

Bądź dla siebie człowiekiem

14. Źródła wiedzy

Bieżące newsy

Dokumentacja i przewodniki

Inne wartościowe źródła informacji

Indeks

Bibliografia