KARTA PRACY UCZNIA • TECHNIK CYBERBEZPIECZEŃSTWA

Utwardzona instalacja systemu Linux

Partycjonowanie GPT • UEFI i Secure Boot • konfiguracja po instalacji

PRZEDMIOT / KWALIFIKACJA	CZAS PRACY	ŚRODOWISKO
Systemy operacyjne / INF.11	5 × 45 min (225 min)	Ubuntu Desktop 24.04 LTS w VirtualBox 7.2

MISJA: Jesteś administratorem nowej stacji roboczej w firmie. Masz pobrać system z wiarygodnego źródła, sprawdzić obraz instalacyjny, świadomie przygotować partycje i uruchomić podstawowe zabezpieczenia.

Po wykonaniu laboratorium potrafisz

- zweryfikować integralność pliku ISO przy użyciu SHA-256;
- utworzyć maszynę wirtualną z UEFI i odróżnić UEFI od Secure Boot;
- zaprojektować dysk GPT i oddzielne punkty montowania / oraz /home;
- zainstalować Linux, utworzyć konto i sprawdzić stan zabezpieczonego rozruchu;
- zaktualizować system, skonfigurować UFW oraz sprawdzić uprawnienia kont.

Reguły bezpieczeństwa na tych zajęciach

UWAGA: Pracuj tylko na nowym wirtualnym dysku. Nie uruchamiaj instalatora na fizycznym dysku laptopa i nie wybieraj opcji kasowania dysku gospodarza. Hasła pozostają prywatne; nie umieszczaj ich na zrzutach ekranu.

Imię i nazwisko: .....

Klasa / grupa: ..... Data: .....

Dowody wykonania: zapisz 6–8 zrzutów ekranu do folderu LINUX_INF11_[inicjały] i dołącz krótki raport zgodnie z tabelą na końcu instrukcji.

LEKCJA 1 / 5 • 45 MINUT

Pobieranie ISO i kontrola integralności

CEL: Pobierz oficjalny obraz i udowodnij, że plik nie został przypadkowo zmieniony.

Zadanie 1. Pobierz sprawdzoną dystrybucję

KROK 1. Uruchom przeglądarkę na szkolnym komputerze. Wejdź na https://releases.ubuntu.com/noble/ (seria 24.04 LTS).

KROK 2. Pobierz plik ubuntu-24.04.x-desktop-amd64.iso (nazwa końcowa zależy od aktualnego wydania punktowego) lub użyj obrazu udostępnionego przez nauczyciela.

KROK 3. Z tej samej oficjalnej strony otwórz plik SHA256SUMS i znajdź wiersz odpowiadający dokładnie Twojej nazwie ISO.

DLACZEGO TO WAŻNE? SHA-256 służy do wykrywania zmian w pliku. Zgodność skrótu potwierdza integralność względem opublikowanego pliku kontrolnego. Samo pobranie SHA256SUMS przez HTTPS nie jest pełną weryfikacją autentyczności podpisu; podpis SHA256SUMS.gpg to osobny etap zaawansowany.

Zadanie 2. Porównaj skrót SHA-256

KROK 4. W systemie Windows otwórz PowerShell w folderze z ISO (Shift + kliknięcie prawym przyciskiem → terminal / PowerShell).

```
Get-FileHash .\ubuntu-24.04*.iso -Algorithm SHA256
```

KROK 5. Porównaj 64 znaki szesnastkowe wyniku z ciągiem obok nazwy obrazu w SHA256SUMS.

☐ Skróty są identyczne → można kontynuować instalację.

☐ Skróty są różne → przerwij pracę i poinformuj nauczyciela.

Krótka odpowiedź

Czy zgodność SHA-256 wystarcza do całkowitego potwierdzenia tożsamości autora pliku? Dlaczego?

Dowód 1: wynik polecenia Get-FileHash (bez ujawniania innych danych).

LEKCJA 2 / 5 • 45 MINUT

Nowa maszyna i podstawy rozruchu

CEL: Utwórz izolowany komputer wirtualny, prawidłowo dobierz zasoby i tryb rozruchu.

Zadanie 3. Skonfiguruj VirtualBox

KROK 1. Uruchom Oracle VirtualBox 7.2 i wybierz Nowa. Nazwa maszyny: INF11-Linux-[inicjały].

KROK 2. Wskaż pobrany obraz ISO. Jeżeli pojawi się „instalacja nienadzorowana” (Unattended), zaznacz opcję pominięcia instalacji nienadzorowanej - partycje wykonasz samodzielnie.

KROK 3. Ustaw: 4096 MB RAM, 2 wirtualne procesory, nowy dysk VDI 50 GB dynamicznie przydzielany, sieć NAT.

KROK 4. Wejdź w Ustawienia → System → Płyta główna i włącz UEFI. Znajdź też Secure Boot. Przed startem sprawdź jego stan z nauczycielem.

KROK 5. Nie włączaj katalogów współdzielonych ani schowka dwukierunkowego, jeżeli nie są niezbędne do ćwiczenia. Maszynę uruchom z podłączonym obrazem ISO.

Parametr	Wartość zadana	Moja konfiguracja
Typ systemu	Ubuntu (64-bit)	.....
Pamięć	4096 MB	.....
CPU	2 vCPU	.....
Dysk	50 GB VDI, dynamiczny	.....
Firmware	UEFI	.....
Sieć	NAT	.....

Rozpoznaj trzy pojęcia

Pojęcie	Znaczenie
UEFI	Firmware uruchamiający komputer; zastępuje starszy tryb BIOS/Legacy.
GPT	Sposób opisu tablicy partycji dysku; nie jest to format systemu plików.
Secure Boot	Mechanizm UEFI, który weryfikuje podpisy elementów łańcucha rozruchu.

WAŻNE: Samo uruchomienie maszyny w UEFI nie dowodzi, że Secure Boot jest aktywny. Stan potwierdzisz komendą mokutil --sb-state na 4. lekcji.

Dowód 2: zrzut ustawień VM (bez haseł).

LEKCJA 3 / 5 • 45 MINUT

Ręczne partycjonowanie GPT

CEL: Zaprojektuj układ partycji przeznaczony do instalacji UEFI i oddziel dane użytkownika.

Zadanie 4. Wejdź do instalatora

KROK 1. Uruchom z ISO i wybierz Install Ubuntu / Zainstaluj Ubuntu. Zmień język/klawiaturę według potrzeb, wybierz instalację interaktywną i podstawowy zestaw programów.

KROK 2. W kroku dotyczącym dysku wybierz ręczne partycjonowanie (Manual installation / Manual partitioning). Upewnij się, że widzisz nowy pusty dysk wirtualny 50 GB.

KROK 3. Jeśli instalator oferuje wybór tablicy partycji, użyj GPT. Następnie utwórz poniższy układ; wartości mogą różnić się minimalnie z powodu jednostek GB/GiB.

Partycja	Wielkość	System plików	Punkt montowania
1. EFI System (ESP)	512 MiB	FAT32	/boot/efi
2. System	28 GiB	ext4	/
3. Dane użytkownika	pozostałe ~21 GiB	ext4	/home

PAMIĘTAJ: Dla partycji EFI ustaw typ EFI System Partition / użycie „EFI”, jeśli instalator udostępnia taką opcję. Sama partycja FAT32 bez prawidłowego typu i punktu montowania może nie wystarczyć.

Po co aż trzy partycje?

• /boot/efi – miejsce plików uruchomieniowych UEFI (ESP);

• / – katalog główny systemu operacyjnego i programów;

• /home – pliki i konfiguracje użytkowników; wydzielenie pomaga w administracji i reinstalacji.

KROK 4. Na ekranie podsumowania skontroluj partycje. Przed kliknięciem Instaluj pokaż układ nauczycielowi. Dopiero potem zatwierdź zmiany.

Dowód 3: zrzut schematu partycji przed zatwierdzeniem instalacji.

Kontrola układu partycji

Wypełnij tabelę na podstawie konfiguracji zapisanej w instalatorze. Nie wpisuj tu numerów partycji z dysku komputera-gospodarza.

Element	Moja obserwacja	Dlaczego jest potrzebny?
Rodzaj tablicy	.....	.....
ESP: typ + rozmiar	.....	.....
Partycja /	.....	.....
Partycja /home	.....	.....

Pytania kontrolne

1. Czym różni się system plików ext4 od tablicy partycji GPT?

2. Czy wolno sformatować istniejącą partycję z Windows, jeśli pojawi się na liście? Wyjaśnij.

NA TEMAT SZYFROWANIA: W tym wariancie ćwiczenia partycjonujemy ręcznie i nie deklarujemy, że dysk jest szyfrowany. W instalatorze Ubuntu 24.04 opcja LVM + szyfrowanie jest oferowana przy automatycznym użyciu całego dysku – to alternatywny wariant, a nie krok do wykonania jednocześnie z przedstawionym schematem.

Miniwyzwanie (bez klikania)

Masz laptop firmowy, który może zostać skradziony. Co ochroni dane lepiej przed odczytem po wyjęciu dysku: samo hasło logowania, Secure Boot czy szyfrowanie dysku (LUKS)? Uzasadnij.

Moja odpowiedź:

LEKCJA 4 / 5 • 45 MINUT

Instalacja i weryfikacja Secure Boot

CEL: Zainstaluj system i sprawdź, czy system wystartował w UEFI oraz czy działa weryfikacja rozruchu.

Zadanie 5. Dokończ instalację

KROK 1. Ustaw strefę czasową Warszawa i utwórz konto użytkownika uczen-[inicjały]. Nazwa komputera: ubuntu-inf11-[inicjały].

KROK 2. Nadaj silne, własne hasło (nie udostępniaj go innym uczniom). Wybierz wymagaj hasła podczas logowania, bez automatycznego logowania.

KROK 3. Rozpocznij instalację. Po jej zakończeniu usuń wirtualny napęd instalacyjny, gdy program o to poprosi, i uruchom ponownie maszynę.

KROK 4. Zaloguj się i otwórz terminal skrótem Ctrl + Alt + T.

Zadanie 6. Sprawdź firmware i system plików

```
test -d /sys/firmware/efi && echo UEFI || echo LEGACY

lsblk -o NAME,SIZE,FSTYPE,MOUNTPOINTS

findmnt /

findmnt /home

findmnt /boot/efi
```

Wynik UEFI wskazuje rozruch w tym trybie. W poleceniu lsblk odszukaj vda/sda i partycje EFI, systemową i /home (nazwy urządzeń mogą się różnić).

Zadanie 7. Sprawdź Secure Boot

```
sudo apt update

sudo apt install -y mokutil

mokutil --sb-state
```

Zanotuj wynik dosłownie: SecureBoot enabled oznacza włączony mechanizm; SecureBoot disabled – brak aktywnego zabezpieczonego rozruchu. Komunikat o braku zmiennych EFI wymaga sprawdzenia trybu UEFI.

PROBLEM Z SECURE BOOT? Jeśli nie można aktywować tej funkcji, nie przełączaj samodzielnie firmware i nie kasuj kluczy. Zgłoś wynik nauczycielowi. W VirtualBox samo zaznaczenie Secure Boot może nie wystarczyć, jeśli wirtualny magazyn UEFI nie ma wymaganych kluczy.

Dowody 4–5: terminal z wynikiem UEFI/lsblk oraz wynik mokutil (mogą być dwa zrzuty).

Co faktycznie chroni Secure Boot?

Analizę wykonaj po sprawdzeniu stanu komendami — to nie jest tylko definicja z podręcznika.

Pytanie	Odpowiedź
Czy UEFI = Secure Boot?	Nie. Można uruchamiać system przez UEFI przy wyłączonym Secure Boot.
Co jest weryfikowane?	Podpisane elementy łańcucha startowego, m.in. shim, GRUB, jądro.
Czy Secure Boot szyfruje /home?	Nie. Ochrona integralności startu nie zastępuje szyfrowania danych.
Czy Secure Boot zastępuje aktualizacje?	Nie. Nie usuwa podatności programów lub usług po starcie.

Łańcuch rozruchowy – wpisz brakujące elementy

UEFI firmware → ..... → GRUB → ..... → system

W podanej konfiguracji Ubuntu elementem pośrednim jest zwykle shim, a później weryfikowane jest jądro Linux.

Sprawdzenie kontrolne

1. Jaki wynik zwróciło u Ciebie mokutil --sb-state? Czy ten wynik jest zgodny z ustawieniami maszyny?

2. Co powinien zrobić administrator, jeżeli instalacja dodatkowego modułu jądra jest blokowana przez Secure Boot?

W PRAKTYCE: Na komputerach produkcyjnych nie wyłącza się Secure Boot „żeby działało”. Najpierw należy ustalić, czy sterownik/moduł jest podpisany i jak bezpiecznie zarejestrować właściwy klucz; w laboratorium decyzję podejmuje nauczyciel.

LEKCJA 5 / 5 • 45 MINUT

Pierwsze utwardzenie systemu

> CEL: Zaktualizuj system, włącz podstawową zaporę i sprawdź konta oraz uruchomione usługi.

Zadanie 8. Aktualizacje

KROK 1. W terminalu sprawdź listę pakietów i zainstaluj aktualizacje. Poczekaj na zakończenie; w razie potrzeby uruchom VM ponownie.

```
sudo apt update

sudo apt upgrade -y
```

KROK 2. Sprawdź, czy aktualizacje automatyczne są w systemie dostępne. Jeśli pakiet nie jest zainstalowany, zainstaluj go.

```
sudo apt install -y unattended-upgrades

systemctl is-enabled unattended-upgrades
```

Zapisz wynik. Aktywne aktualizacje zmniejszają czas, w którym system pozostaje podatny na znane błędy.

Zadanie 9. Zapora sieciowa UFW

KROK 3. Ustaw politykę blokowania nowych połączeń przychodzących, a następnie aktywuj zaporę. Nie otwieraj portu SSH – nie uruchamiamy serwera SSH.

```
sudo apt install -y ufw

sudo ufw default deny incoming

sudo ufw default allow outgoing

sudo ufw enable

sudo ufw status verbose
```

W poprawnym wyniku szukaj Status: active oraz Default: deny (incoming).

Zadanie 10. Uprawnienia i konta

KROK 4. Sprawdź grupy swojego konta i utwórz dodatkowe konto testowe bez roli administratora.

```
id

sudo adduser audyt

groups audyt
```

Podczas tworzenia konta wpisz osobne hasło; dodatkowe pytania o dane osobowe można pominąć. Użytkownik audyt nie powinien znaleźć się w grupie sudo.

Dowody 6–8: aktualizacje, status zapory, grupy użytkownika audyt.

Test końcowy: czy stacja jest gotowa?

Zadanie 11. Odczyt konfiguracji

```
hostnamectl

sudo ss -tulpen

sudo ufw status verbose

lsblk -f

mokutil --sb-state
```

Użyj wyników poleceń do wypełnienia listy audytowej. Nie zmieniaj ustawień na ślepo.

Kontrola	Wynik / uwagi
Dystrybucja i wersja	.....
Rozruch: UEFI czy Legacy?	.....
Secure Boot: enabled / disabled	.....
ESP oraz osobne / i /home	.....
Zapora UFW	.....
Konto audyt bez sudo	.....
Aktualizacje	.....

Zadania na samodzielne myślenie

1. Dlaczego blokowanie połączeń przychodzących jest bezpieczniejszą polityką domyślną?

2. Wymień dwie rzeczy, których nie zabezpiecza samo włączenie Secure Boot.

3. Jakie dwa dodatkowe zabezpieczenia warto wdrożyć na laptopie przechowującym dane uczniów?

Dla chętnych: drugi wariant instalacji

Po zakończeniu obowiązkowej części możesz porównać ręcznie partycjonowany dysk z instalacją wykorzystującą szyfrowanie. Wymaga to drugiej, nowej maszyny wirtualnej lub osobnego dysku testowego — nigdy nie nadpisuj gotowego laboratorium.

Wariant B – szyfrowanie pełnego dysku LVM + LUKS

KROK 1. Utwórz nową maszynę INF11-Linux-LUKS-[inicjały] z osobnym pustym dyskiem wirtualnym (minimum 35 GB).

KROK 2. Uruchom instalator Ubuntu Desktop 24.04. Wybierz automatyczną instalację na całym nowym dysku wirtualnym.

KROK 3. Otwórz funkcje zaawansowane i wybierz opcję Use LVM and encryption (LVM + szyfrowanie), jeśli jest dostępna.

KROK 4. Ustaw odrębne silne hasło do odblokowania dysku. Sprawdź, czy przy kolejnym uruchomieniu system prosi o to hasło.

```
lsblk -f

sudo cryptsetup status ubuntu--vg-ubuntu--lv
```

Polecenie cryptsetup status używa przykładowej nazwy urządzenia, która nie musi istnieć w Twojej instalacji; rzeczywistą nazwę ustala się z lsblk -f, dlatego nie wykonuj go bez sprawdzenia.

> PORÓWNAJ: Szyfrowanie danych (np. LUKS) ogranicza odczyt informacji z wyłączonego urządzenia bez klucza. Secure Boot ogranicza uruchamianie nieautoryzowanego kodu podczas rozruchu. Te mechanizmy odpowiadają na różne zagrożenia.

Pytania rozszerzające

Jakie zagrożenie ogranicza Secure Boot, a jakie szyfrowanie dysku?

Raport z laboratorium i kryteria oceniania

Oddaj folder LINUX_INF11_[inicjały] z plikiem raport.pdf (lub dokumentem tekstowym) oraz 6–8 opisanymi zrzutami ekranu. Oceniana jest konfiguracja i jej wyjaśnienie, nie tylko liczba zrzutów.

Dowód	Co powinno być widoczne
01_ISO	Zgodny hash SHA-256 oraz nazwa ISO.
02_VM	Parametry VM: dysk, RAM, UEFI.
03_PARTYCJE	Układ GPT: ESP, / oraz /home przed instalacją.
04_SYSTEM	System po pierwszym uruchomieniu; lsblk i punkty montowania.
05_BOOT	Polecenie mokutil --sb-state i jego rzeczywisty wynik.
06_UPDATE	Wynik aktualizacji / stan unattended-upgrades.
07_UFW	Status active, polityka deny incoming.
08_KONTA	Grupy użytkownika audyt, bez sudo.

Kryteria: maksymalnie 100 punktów

Obszar	Punkty
Pobranie obrazu i porównanie SHA-256	10
Konfiguracja VM: zasoby, ISO, UEFI, NAT	10
Schemat GPT: EFI, /, /home z prawidłowymi systemami plików	25
Instalacja i bezpieczne ustawienia konta	10
Sprawdzenie UEFI/Secure Boot i interpretacja	15
Aktualizacje i stan mechanizmu aktualizacji	10
Zapora UFW i poprawna polityka ruchu	10
Konto bez uprawnień administratora i raport	10

Próg zaliczenia: 75/100 punktów. Jeżeli Secure Boot nie może zostać włączony z przyczyn środowiskowych, poprawna diagnoza i udokumentowanie problemu pozwalają otrzymać punkty za tę część — nie ma obowiązku wyłączania zabezpieczeń komputera gospodarza.

Ściąga administratora: Linux

Polecenie	Do czego służy
`lsblk -f`	Dyski, partycje, systemy plików i punkty montowania.
`findmnt /home`	Sprawdza, czy /home jest osobnym systemem plików.
`mokutil --sb-state`	Odczytuje stan Secure Boot z perspektywy systemu.
`sudo apt update`	Aktualizuje informacje o dostępnych pakietach.
`sudo apt upgrade -y`	Instaluje dostępne aktualizacje pakietów.
`sudo ufw status verbose`	Pokazuje stan zapory i polityki domyślne.
`id`	Pokazuje identyfikator konta i jego grupy.
`sudo ss -tulpen`	Pokazuje nasłuchujące porty i gniazda.

Najczęstsze problemy

Sytuacja	Co zrobić
Instalator sam wybiera partycje	Przerwij i wybierz instalację ręczną; pomiń Unattended w VirtualBox.
Nie ma /home na liście	Sprawdź konfigurację przed zatwierdzeniem; nie zaczynaj kasowania danych na ślepo.
mokutil: disabled	Sprawdź UEFI i klucze Secure Boot z nauczycielem. Nie usuwaj kluczy z VM samodzielnie.
apt nie działa	Sprawdź NAT, DNS i połączenie; poproś o lokalne ISO/źródło pakietów.
VM pracuje bardzo wolno	Zamknij inne programy; nie zwiększaj RAM VM kosztem Windows.
Po restarcie powrót do instalatora	Odłącz ISO od wirtualnego napędu.

Materiały źródłowe (do samodzielnej nauki)

Ubuntu 24.04 – obrazy ISO i sumy: releases.ubuntu.com/noble/

Oficjalna instalacja Ubuntu: ubuntu.com/desktop/docs/en/24.04/tutorial/install-ubuntu-desktop/

Ubuntu Secure Boot: documentation.ubuntu.com/security/security-features/platform-protections/secure-boot/

VirtualBox 7.2 – ustawienia VM: docs.oracle.com/en/virtualization/virtualbox/7.2/user/working-with-vms.html

UFW: ubuntu.com/server/docs/firewalls/