Sveučilište u Zagrebu

Fakultet Organizacije i Informatike

Varaždin

Lynis Security Auditing Software

Kolegij: Sigurnost informacijskih sustava

Mentori: Izv. prof. dr. sc. Petra Grd, Izv. prof. dr. sc. Igor Tomičić

Tim: Lidija Mudri, Paula Narančić, Vito Petrinjak, Luka Pošta

Uvod

- Tema projekta je sigurnosna analiza pomoću alata Lynis
- Lynis je besplatan alat koji se koristi za provjeru sigurnosti operacijskih sustava poput Linuxa, macOS-a ili FreeBSD-a
- Glavni cilj projekta je pronaći sigurnosne propuste u sustavima, razumjeti njihove uzroke i pokazati kako ih ispraviti
- Cilj projekta je da na kraju postignemo bolju sigurnosnu ocjenu sustava i manje pronađenih upozorenja
- Ovaj projekt pokazuje kako se u praksi radi sustavno testiranje i „učvršćivanje” (hardening) sustava, što je važan dio posla sistem administratora i sigurnosnih stručnjaka

Postavljanje okruženja

- Za rad koristimo alat za virtualizaciju VirtualBox
- Unutar njega kreiramo jedno virtualno računalo s operacijskim sustavom Ubuntu 22.04
- On radi kao odvojeno računalo i ponaša se kao pravi server
- Dobiva oko 2 GB RAM-a, 2 procesora i 25 GB diska, što je dovoljno za testiranje

Instalacija i priprema sustava

- Nakon što je virtualni sustav pokrenut, na njemu napravimo osnovno ažuriranje i instaliramo osnovne alate
- Zatim instaliramo Lynis

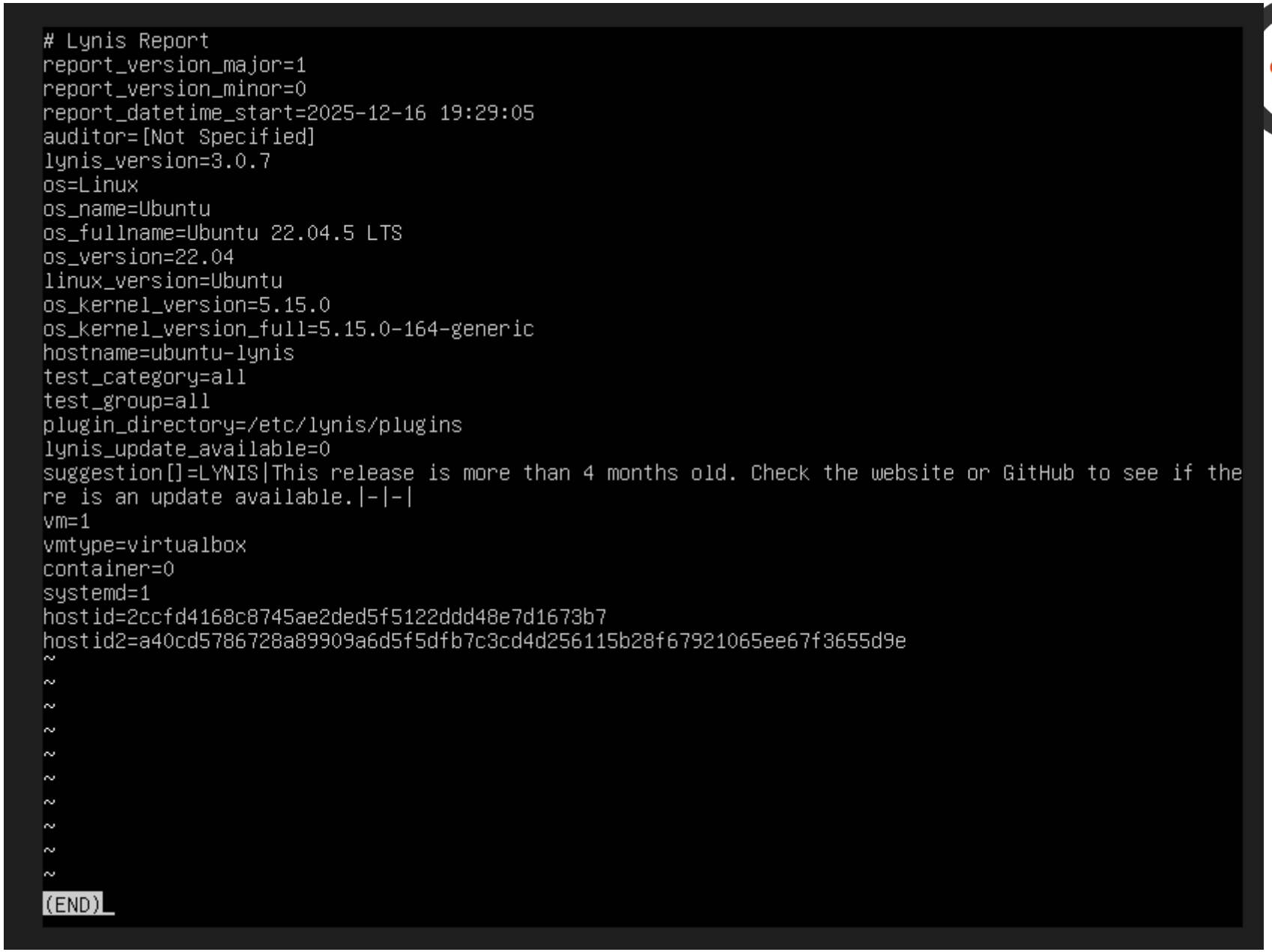
```
sudo apt update
sudo apt install lynis -y
```

```
/var/log/lynis.log
/var/log/lynis-report.dat
```

- Pokrenemo prvi audit i dobivamo prvi izvještaj o sigurnosti sustava

```
sudo lynis audit system
```

Lynis Report



Početni audit – baseline analiza

- Prvi audit služi kao početno stanje, tzv. baseline
- Lynis tada prolazi kroz stotine provjera: gleda postavke mreže, SSH konfiguraciju, dozvole na datotekama, stanje firewall-a, logove, korisničke račune i ažuriranja
- Rezultat je popis upozorenja i prijedlozi

Lynis Baseline

(Početni audit)

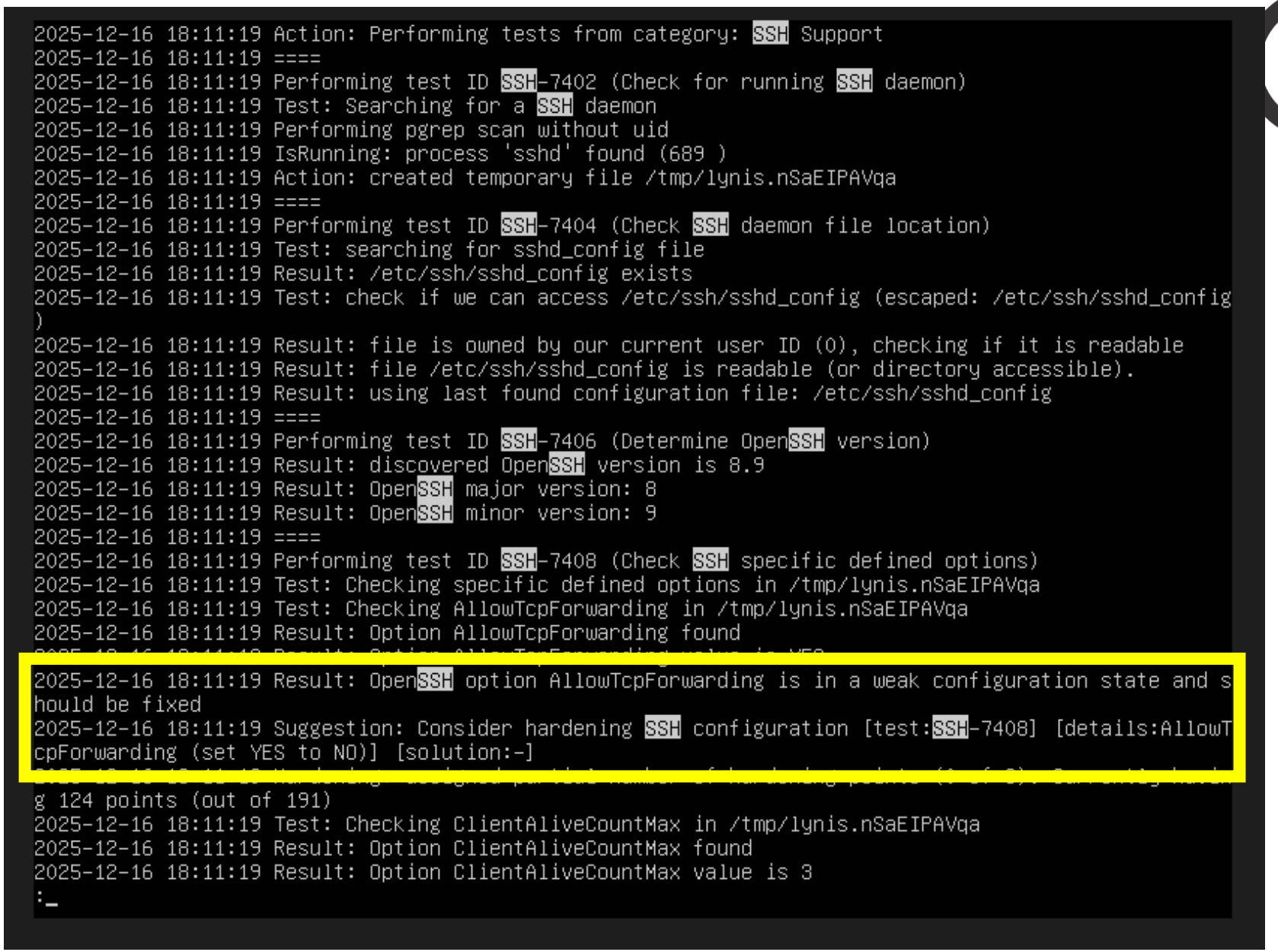
```
2025-12-16 18:11:33 Hardening index : [60] [############        ]
2025-12-16 18:11:33 Hardening strength: System has been hardened, but could use additional hardening
2025-12-16 18:11:33 ====
2025-12-16 18:11:34 Checking permissions of /usr/share/lynis/include/tool_tips
2025-12-16 18:11:35 File permissions are OK
2025-12-16 18:11:35 Tool tips: enabled
2025-12-16 18:11:35 ================================================================================
2025-12-16 18:11:35 Tests performed:     255
2025-12-16 18:11:35 Total tests:         450
2025-12-16 18:11:35 Active plugins:      1
2025-12-16 18:11:35 Total plugins:       1
2025-12-16 18:11:35 ================================================================================
2025-12-16 18:11:35 Lynis 3.0.7
2025-12-16 18:11:35 2007-2021, CISOfy - https://cisofy.com/lynis/
2025-12-16 18:11:35 Enterprise support available (compliance, plugins, interface and tools)
2025-12-16 18:11:35 Program ended successfully
2025-12-16 18:11:35 ================================================================================
2025-12-16 18:11:35 PID file removed (/var/run/lynis.pid)
2025-12-16 18:11:35 Temporary files:  /tmp/lynis.2ZH3yCBBiF /tmp/lynis.NFiCkbSYoW /tmp/lynis.EIKwS6u
vXp /tmp/lynis.nSaEIPAVqa
2025-12-16 18:11:35 Action: removing temporary file /tmp/lynis.2ZH3yCBBiF
2025-12-16 18:11:35 Info: temporary file /tmp/lynis.NFiCkbSYoW was already removed
2025-12-16 18:11:35 Info: temporary file /tmp/lynis.EIKwS6uvXp was already removed
2025-12-16 18:11:35 Action: removing temporary file /tmp/lynis.nSaEIPAVqa
2025-12-16 18:11:35 Lynis ended successfully.
~
~
~
~
~
~
~
~
~
~
~
(END)
```

Odabir i analiza propusta

- Nakon što pogledamo izvještaj, odabiremo najvažnije i najrealnije propuste koje ćemo ispraviti
- Tada slijedi faza hardeninga, odnosno „učvršćivanja” sustava

Lynis Baseline

(Početni audit)



Odabir i analiza propusta

- Neaktivan firewall i mrežna filtracija

- Sustav nije imao aktivna firewall pravila, sav mrežni promet bio je dopušten bez ograničenja

- Slaba konfiguracija SSH servisa

- SSH je koristio zadane postavke koje povećavaju napadnu površinu, uključujući forwarding mehanizme, kompresiju i zadani port

- Neograničen SSH pristup korisnicima

- Nisu bila definirana ograničenja koji korisnici ili grupe se smiju prijavljivati putem SSH-a

- Neodgovarajuće dozvole SSH konfiguracije

- Konfiguracijska datoteka SSH servisa imala je preširoke dozvole pristupa

- Nedostatna politika lozinki

- Nisu bile definirane minimalne sigurnosne zahtjeve za jačinu, starost i način hashiranja lozinki

- Izostanak PAM kontrole jačine lozinki

- Sustav nije provodio tehničku provjeru kompleksnosti korisničkih lozinki

- Računi bez definiranog datuma isteka

- Korisnički računi nisu imali kontroliran životni ciklus

- Nezaštićen proces podizanja sustava (GRUB)

- Bootloader nije bio zaštićen lozinkom, što omogućuje neautorizirane izmjene pri podizanju sustava

- Neaktivan audit podsustav (auditd)

- Sustav nije bilježio detaljne sigurnosno relevantne događaje na razini jezgre

- Izostanak udaljenog zapisivanja logova

- Svi log zapisi pohranjivali su se isključivo lokalno, bez zaštite od brisanja u slučaju kompromitacije

Primjer hardeninga jednog propusta – „neaktivan firewall i mrežna filtracija”

1. sudo ufw status – provjerava trenutno stanje firewall sustava i pokazuje je li UFW aktivan ili ne
2. sudo ufw default deny incoming – postavlja zadanu politiku kojom se sav dolazni mrežni promet odbija ako nije izričito dopušten
3. sudo ufw default allow outgoing – dopušta sav odlazni mrežni promet sa sustava prema van
4. sudo ufw allow ssh – dopušta dolazne mrežne veze za SSH servis kako bi administratorski pristup ostao moguć
5. sudo ufw enable – aktivira UFW firewall i primjenjuje definirana pravila
6. sudo ufw status verbose – prikazuje detaljno stanje firewall sustava, uključujući zadane politike i aktivna pravila

Ponovni audit – provjera učinka

- Nakon primjene svih promjena ponovno smo pokrenuli Lynis
- Zatim uspoređujemo rezultate s prvim izvještajem

```
sudo lynis audit system
```

Kategorija	Baseline stanje	Post-hardening stanje
Hardening index	60	72
Firewall konfiguracija	Bez aktivnih pravila	Aktivna restriktivna politika
SSH konfiguracija	Slabe zadane postavke	Utvrđena i ograničena konfiguracija
Autentikacija i lozinke	Bez politike jačine i starosti	Aktivne PAM i password politike
Boot sigurnost	GRUB bez lozinke	GRUB zaštićen lozinkom
Logging i auditing	auditd neaktivan, bez remote logova	Aktiviran auditd i poboljšan nadzor

- Tako se vidi konkretan učinak mjera koje smo poduzeli

CIS Ubuntu Linux 22.04 LTS Benchmark

- CIS Benchmarks korišteni su kao referentni okvir za sigurnu konfiguraciju Ubuntu Server sustava
- Omogućuju strukturirano mapiranje identificiranih slabosti na preporučene hardening mjere
- Fokus na Level 1 preporuke, koje donose sigurnosna poboljšanja bez narušavanja funkcionalnosti
- CIS smjernice nisu primijenjene nekritički, već selektivno, u skladu s namjenom sustava
- Korištenje CIS Benchmarks osigurava usklađenost s industrijskim praksama i ponovljivost pristupa

Problemi s kojima smo se susreli

1. Previše upozorenja u prvom izvještaju
2. Lynis izvještaj prevelik i nepregledan
3. Promjene se ne primjenjuju (nepravilna implementacija)
4. Firewall ili SSH promjene uzrokuju gubitak pristupa
5. Snapshot nije napravljen i sustav se pokvari