1. POSTAVLJANJE SIEM I IDS OKRUŽENJA

1.1. Korištene tehnologije:

- Ubuntu Server 22.04 LTS

- Wazuh (Manager, Indexer, Dashboard)

- Suricata IDS

- Bash skripta za automatizaciju

1.2. Postupak:

1. Pokrenuti SIEM VM pomoću alata VirtualBox ili VMWare Workstation

2. Uzeti IP adresu Ubuntu LTS pomoću naredbe **ip a**

   Info: uzeti IP adresu iz dijela inet 192.168.XX.XX/24

3. Spojiti se sa primarnog windows uređaja putem SSH Clienta

   Preduvjet: potrebno je instalirati SSH Client na Windows 10/11 uređaj te napraviti reboot

   Info: otvoriti Powershell s admin pravima te spojiti se komadom **ssh user@SIEM_IP**.
   Lozinka je unaprijed postavljena te je ona **niko**.

4. Kreirati instalacijsku skriptu install_siem.sh i zalijepiti njezin sadržaj iz github repo dokumenta.

   Info: napraviti skriptu naredbom **nano install_siem.sh** te zalijepiti sadržaj sa datoteke iz github repozitorija

5. Pokrenuti setup SIEM skriptu naredbom **sudo bash install_siem.sh**

6. Pristupiti online Wazuh dashboardu

   Info: Na Wazuh dashboard se spaja na web stranici **https://SIEM_IP**
   Napomena: bit će ispisano sigurnosno upozerenje, treba ga prihvatiti I nastaviti na stranicu

7. Logirati se u Wazuh s kredencijalima

   Info: username je unaprijed postavljen te je on **admin**,
   a lozinka je random te se ona generira i ispisuje u konzoli pri pokretanju install_siem.sh skripte.

   Red u konzoli sa lozinkom izgleda ovako:
   23/12/2025 19:07:18 INFO: The password for user admin is xxxxxxxxxxxx

1.3. Pristup Dashboardu:

https://IP_ADRESA_SIEM_POSLUŽITELJA

user -> admin

pass -> ispisan u konzoli pri pokretanju skripte install_siem.sh

1.4. Napomena:

Zbog korištenja self-signed certifikata, preglednik će prikazati sigurnosno upozorenje koje je mpotrebno prihvatiti.

2. ENDPOINT (WINDOWS VM)

2.1. Priprema Windows virtualnog stroja

Info: treba omogućiti mrežni pristup prema SIEM poslužitelju i testirati povezanost naredbom **ping SIEM_IP**

Primjer valjanog odgovora:
ping 192.168.54.135

Pinging 192.168.54.135 with 32 bytes of data:
Reply from 192.168.54.135: bytes=32 time<1ms TTL=64
Reply from 192.168.54.135: bytes=32 time<1ms TTL=64
Reply from 192.168.54.135: bytes=32 time<1ms TTL=64
Reply from 192.168.54.135: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.54.135:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

2.2. Instalacija Wazuh agenta (Spajanje Windowsa sa Wazuh SIEM)

Preduvjeti:

- Admin privilegije
- IP SIEM-a
- Wazuh Dashboard radi na https://SIEM_IP
- Admin login radi na Dashboardu

Deploy Wazuh agenta:

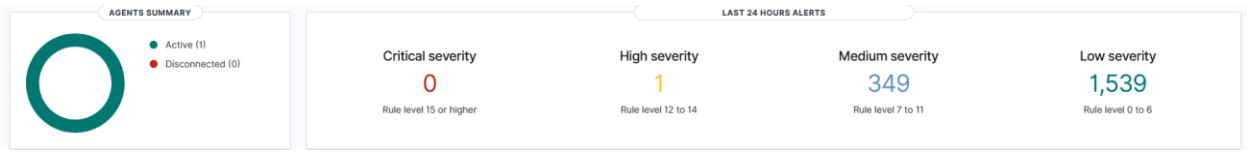
A) Na SIEM Dashboardu

1. Otvoriti Wazuh Dashboard
2. Odabrati Agents -> Deploy new Agent
3. Odabrati Windows MSI 32/64 bits
4. Pod server address staviti SIEM IP adresu
5. Pod optional settings postaviti logičan i nedvosmislen naziv agenta
6. Kopirati komandu koju treba pokrenuti na Windows VM-u

B) Na Windows VM-u

1. Otvoriti Windows Powershell sa admin privilegijama
2. Pokrenuti kopiranu komadu (primjer izgleda, **NE KOPIRATI** ovu):
   Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.54.135'
3. Pokrenuti agenta sa komandom **net start wazuh**

Nakon ovih koraka dashboard mora imati jednog aktivnog agenta pod dijelom “Agent Summary” te to izgleda ovako:



Bez uspostave Sysmona, trenutno SIEM zapisuje:

- Windows Event Logove
- Login / logout
- System evente
- Security baseline evente

2.3. Endpoint telemetrija – Sysmon

Za dodatnu telemtriju poput process creation, network events itd., potrebno je instalirati Sysmon.

Instalacijski koraci na Windows VM-u:

1. Preuzmi Sysmon:
   dvije komande:
   - **Invoke-WebRequest https://download.sysinternals.com/files/Sysmon.zip -OutFile Sysmon.zip**
   - **Expand-Archive Sysmon.zip -DestinationPath Sysmon**

2. Preuzmi osnovni config:

- **Invoke-WebRequest https://raw.githubusercontent.com/SwiftOnSecurity/sysmon-config/master/sysmonconfig-export.xml -OutFile sysmon.xml**

3. Instalacija:
   - **.\Sysmon\Sysmon64.exe -accepteula -i sysmon.xml**
4. Provjera radi li servis:

   Get-Service Sysmon64

   Ako servis radi, biti će ovako ispisano ui konzoli (bitno je da piše Running):

   Status Name DisplayName

   Running Sysmon64 Sysmon64

2.4. HoneyPot

Honeypot je namjerno izložen i lažno ranjiv sustav čija je svrha:

- privući napadače
- bilježiti njihove aktivnosti
- ne štititi sustav, nego učiti iz napada

Koristio sam Cowrie SSH Honeypot.

1. Setup na SIEM Ubunutu sustavu:

sudo apt update
sudo apt install -y git python3-venv python3-pip
git clone https://github.com/cowrie/cowrie.git
cd cowrie
python3 -m venv cowrie-env
source cowrie-env/bin/activate
pip install -r requirements.txt python -m
pip install --upgrade pip python -m pip install -e . cowrie start
cowrie status

Kad se pokrenu sve naredbe te ako sve prođe bez grešaka, kad se pokrene naredba **cowrie status**, dobiva se sljedeći ispis: **cowrie is running (PID: 136876)**.

Ako pak cowrie ne radi, potrebno ga je pokrenuti naredbom **cowrie start**.

2. Testiranje honeypota

Preduvjet: potrebno je znati Honeypot IP.

Spajanje s drugog stroja pomoću naredbe: **ssh root@HONEYPOT_IP -p 2222**

Pri prijavi sustav će tražiti lozinku, može se napisati bilo šta, a sustav zatim bilježi lozinku u logovima na lokaciji: ~/cowrie/var/log/cowrie/cowrie.log. Ovi logovi su dodani u Wazuh:

```
<localfile>
  <log_format>syslog</log_format>
  <location>/home/niko/cowrie/var/log/cowrie/cowrie.log</location>
</localfile>
```