**Attack, Detect & Secure the Environment**

Attack – Detect – Secure Using Wazuh SIEM

# Cover Page

ERP No.: 6604722

# Executive Summary

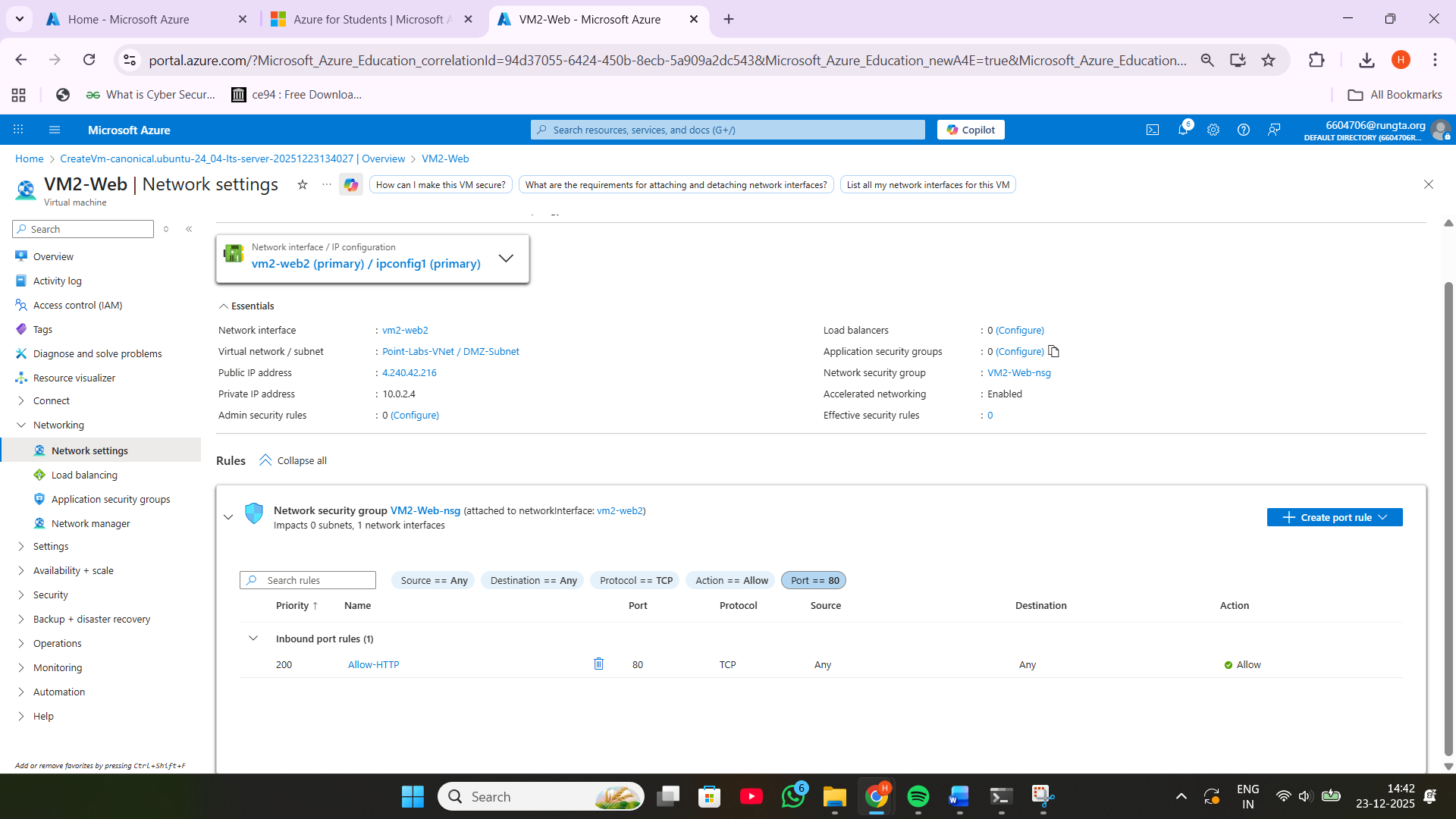
This project simulates a real-world enterprise cybersecurity operation involving offensive attacks (Red Team) and defensive monitoring & hardening (Blue Team).   
A three-tier Azure environment was deployed consisting of a Web Server (VM2), Domain/Internal Services (VM1), and SIEM Server (VM3). Multiple real-world cyber-attacks were executed including SSH brute force, privilege escalation, and web reconnaissance.  
  
The attacks were successfully detected using Wazuh SIEM. Logs were analyzed, Indicators of Compromise (IOCs) documented, misconfigurations identified, and full system hardening implemented.   
Post-hardening validation showed significant security improvement with reduced attack surface, enhanced visibility, and improved detection response.

# 1️⃣ Environment Architecture

Insert Architecture screenshots here.

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Purpose | IP | OS |
| VM1 | Internal / Domain | 4.247.138.166 | Ubuntu |
| VM2 | Web Server (Apache) | 4.240.42.216 | Ubuntu |
| VM3 | Wazuh SIEM | 4.213.69.222 | Ubuntu |
| Kali | Attacker Machine |  | Kali Linux |

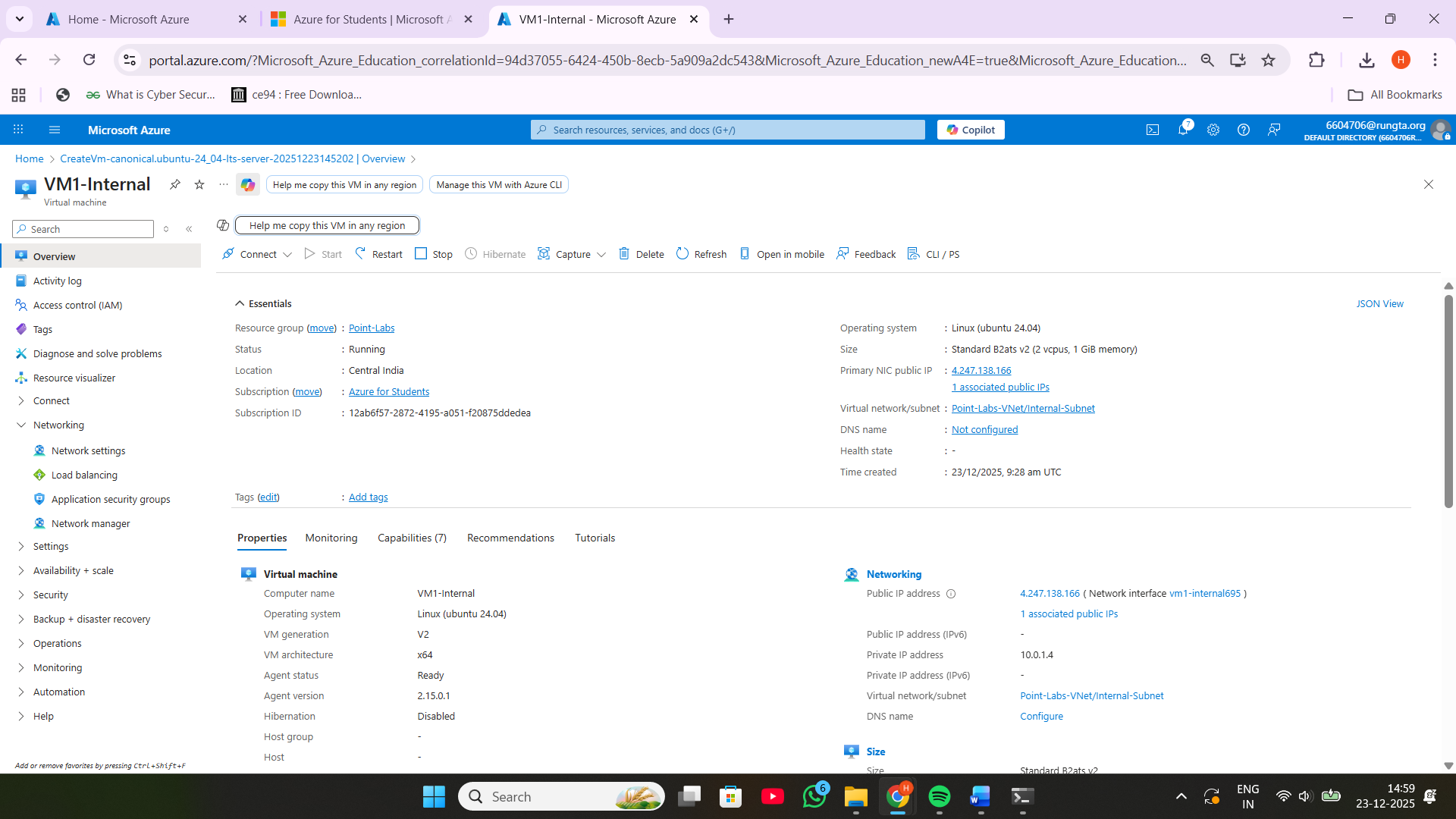
# 

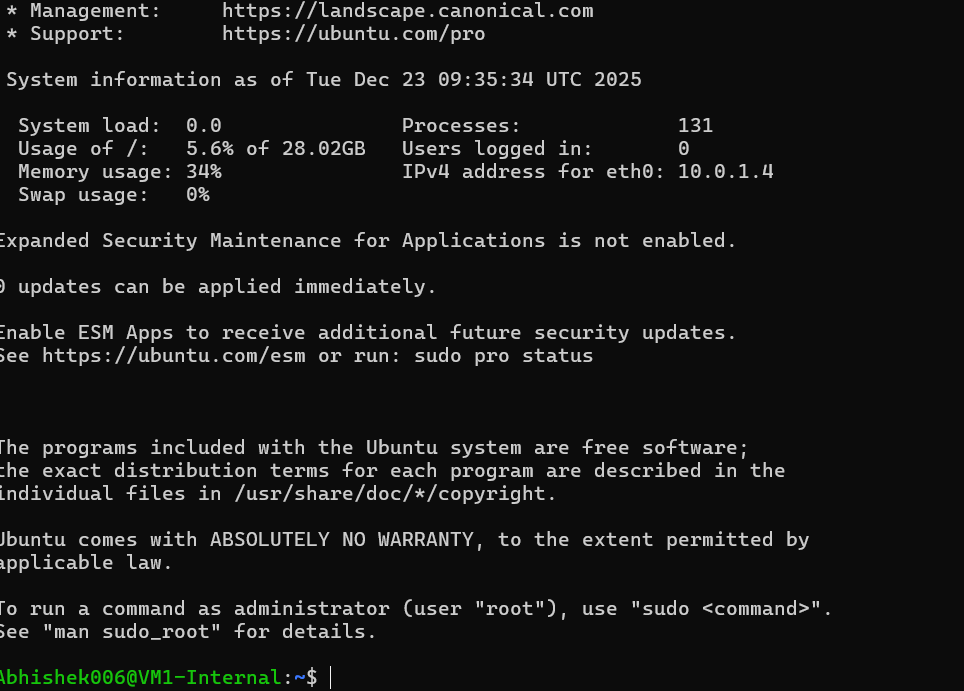


# 

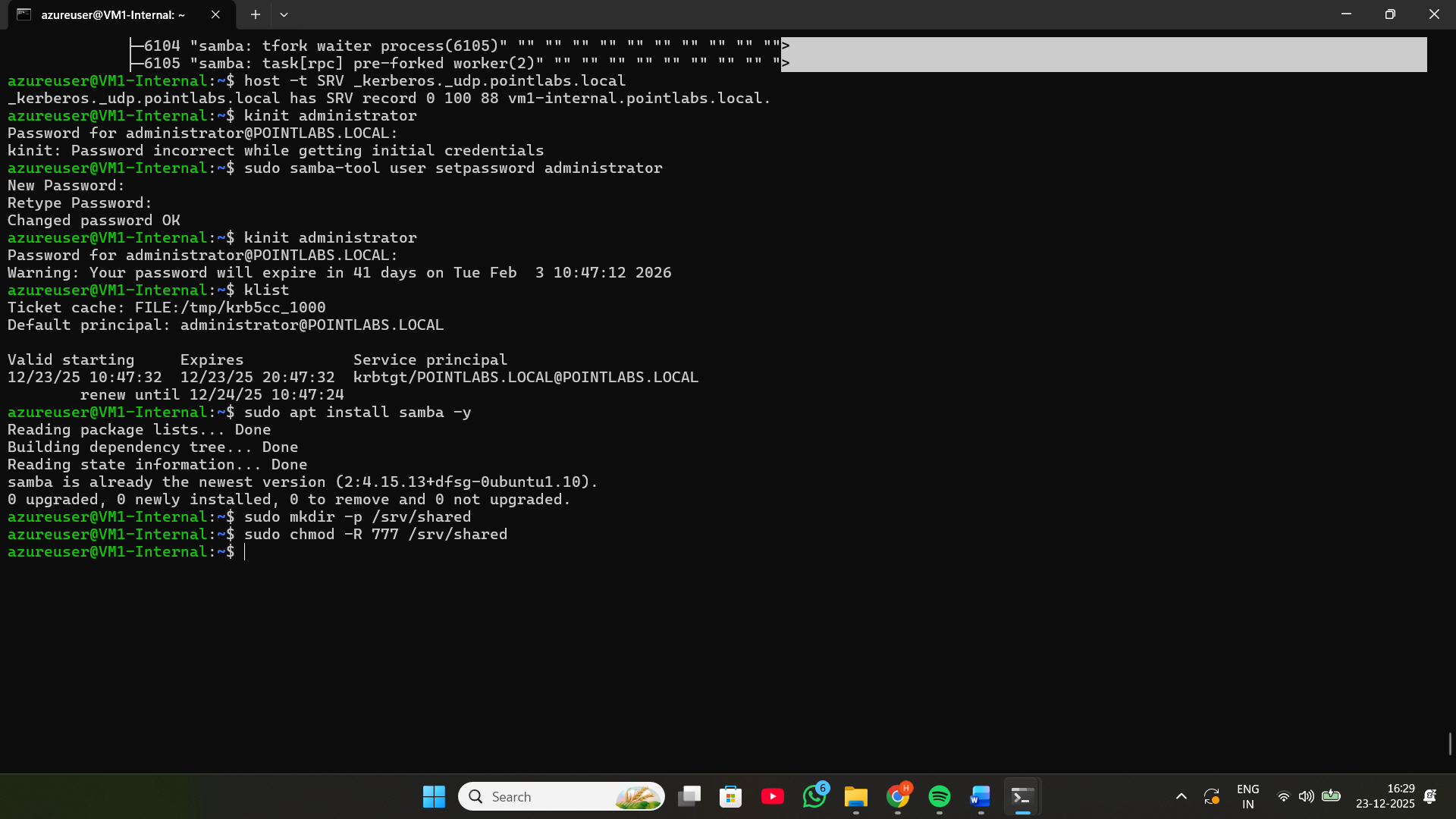
# 

# VM1-Internal

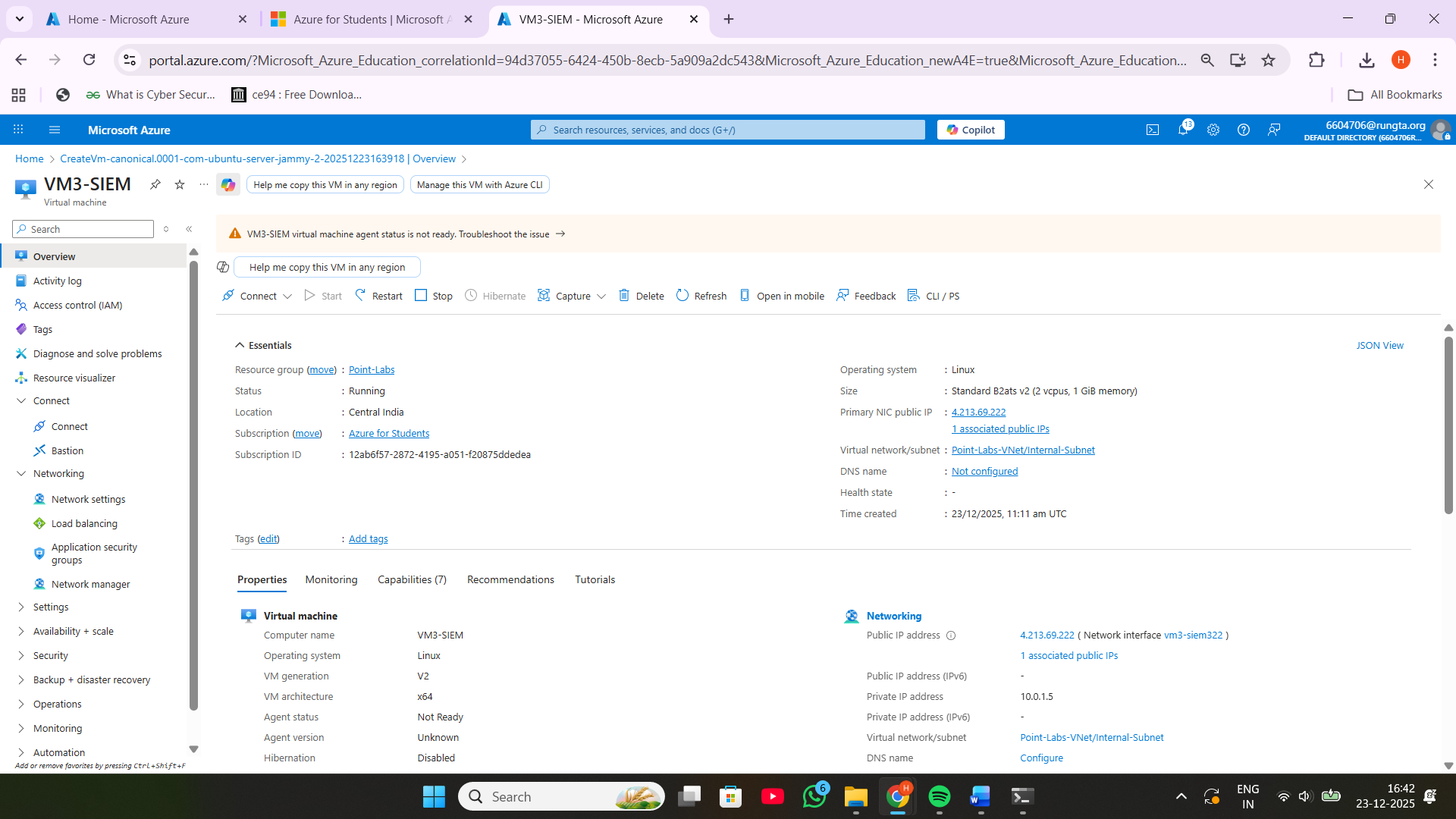


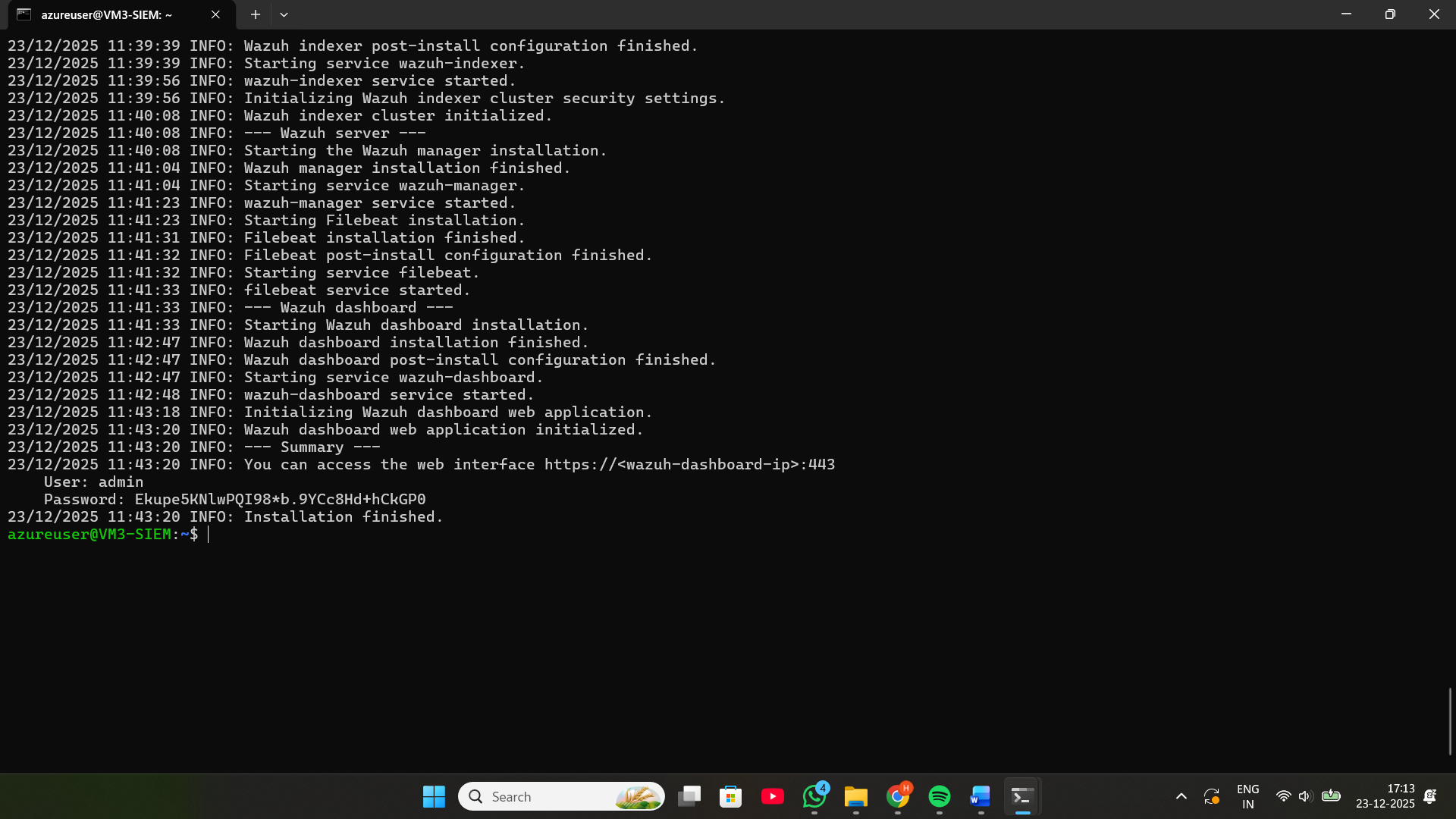


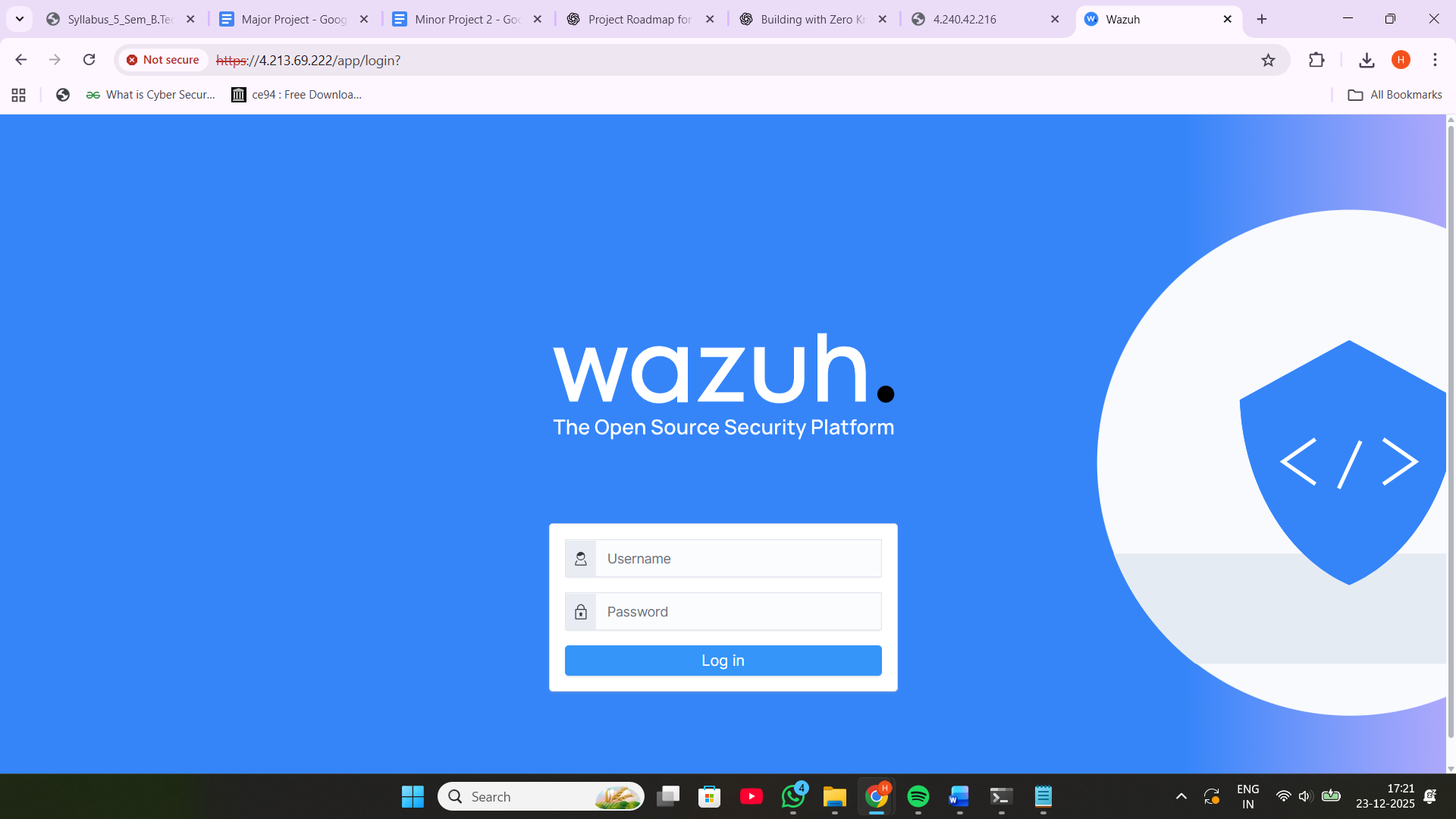
# 

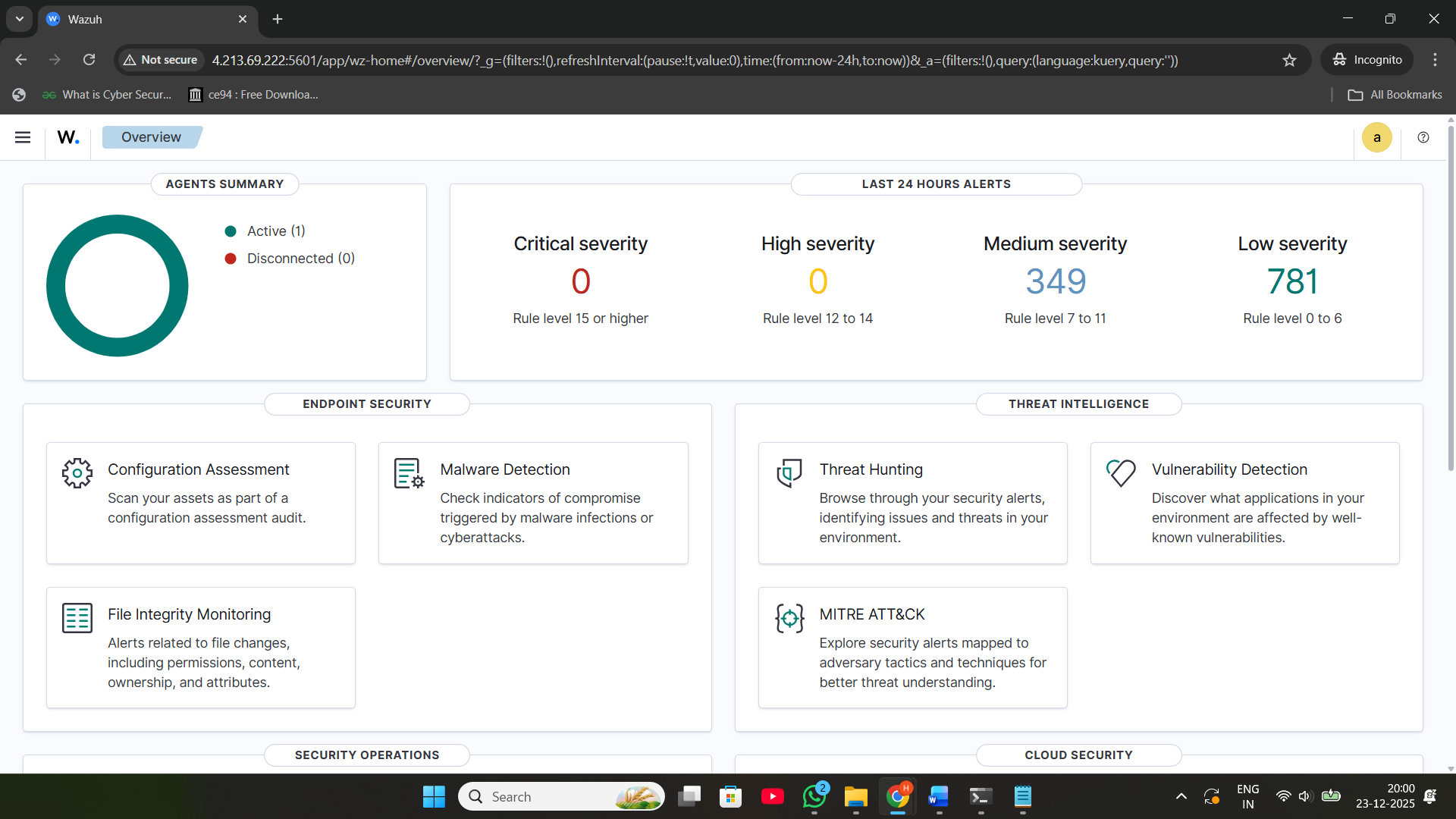


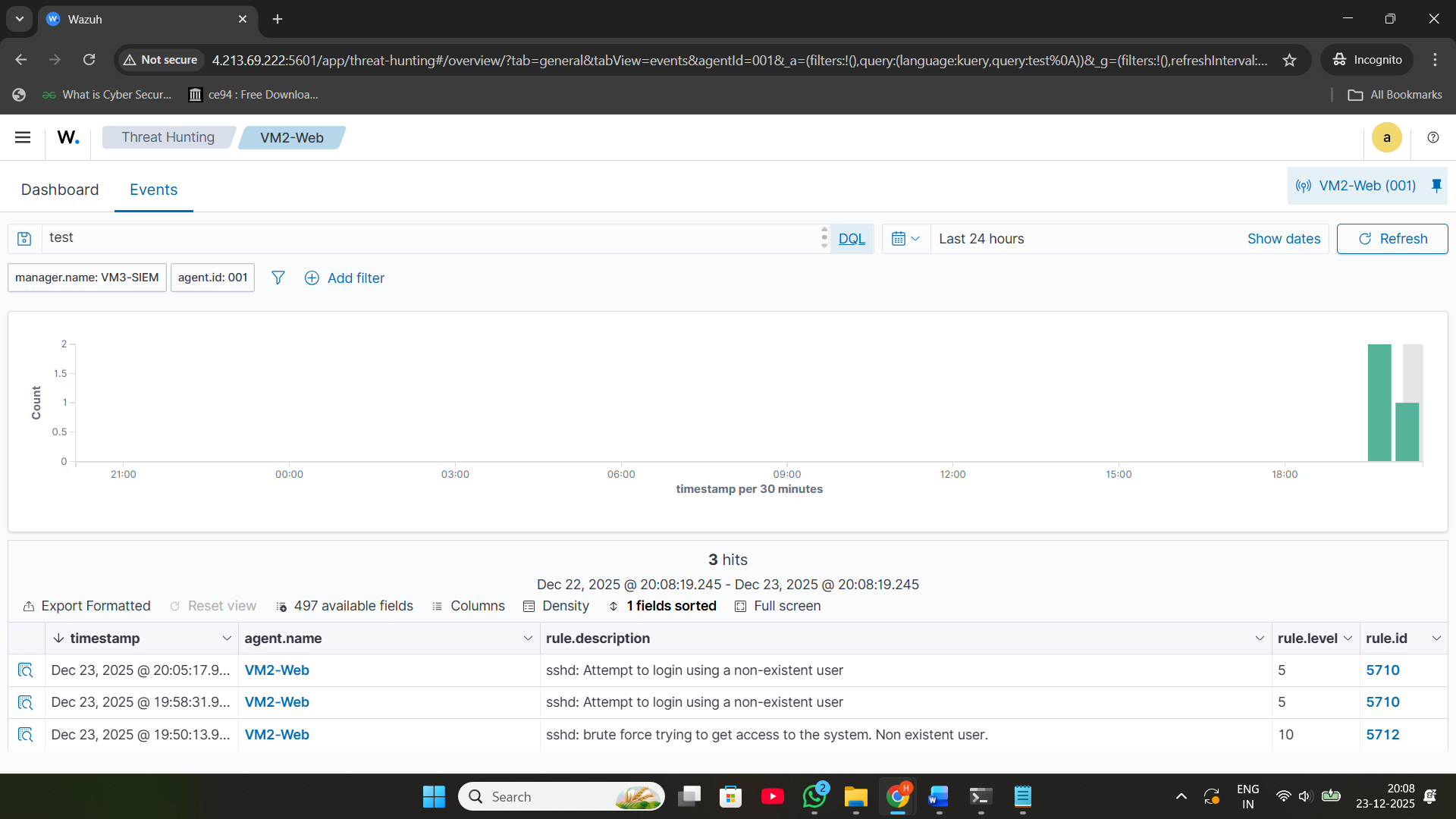
* **VM3-SIEM**

****







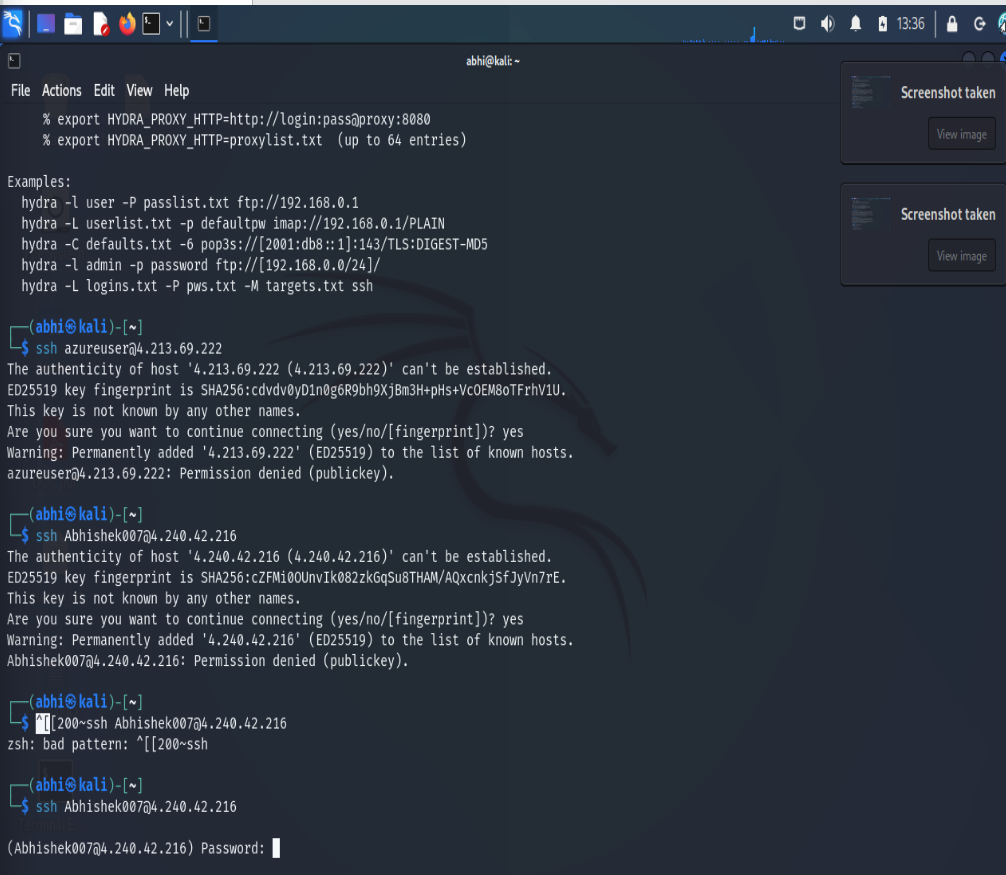


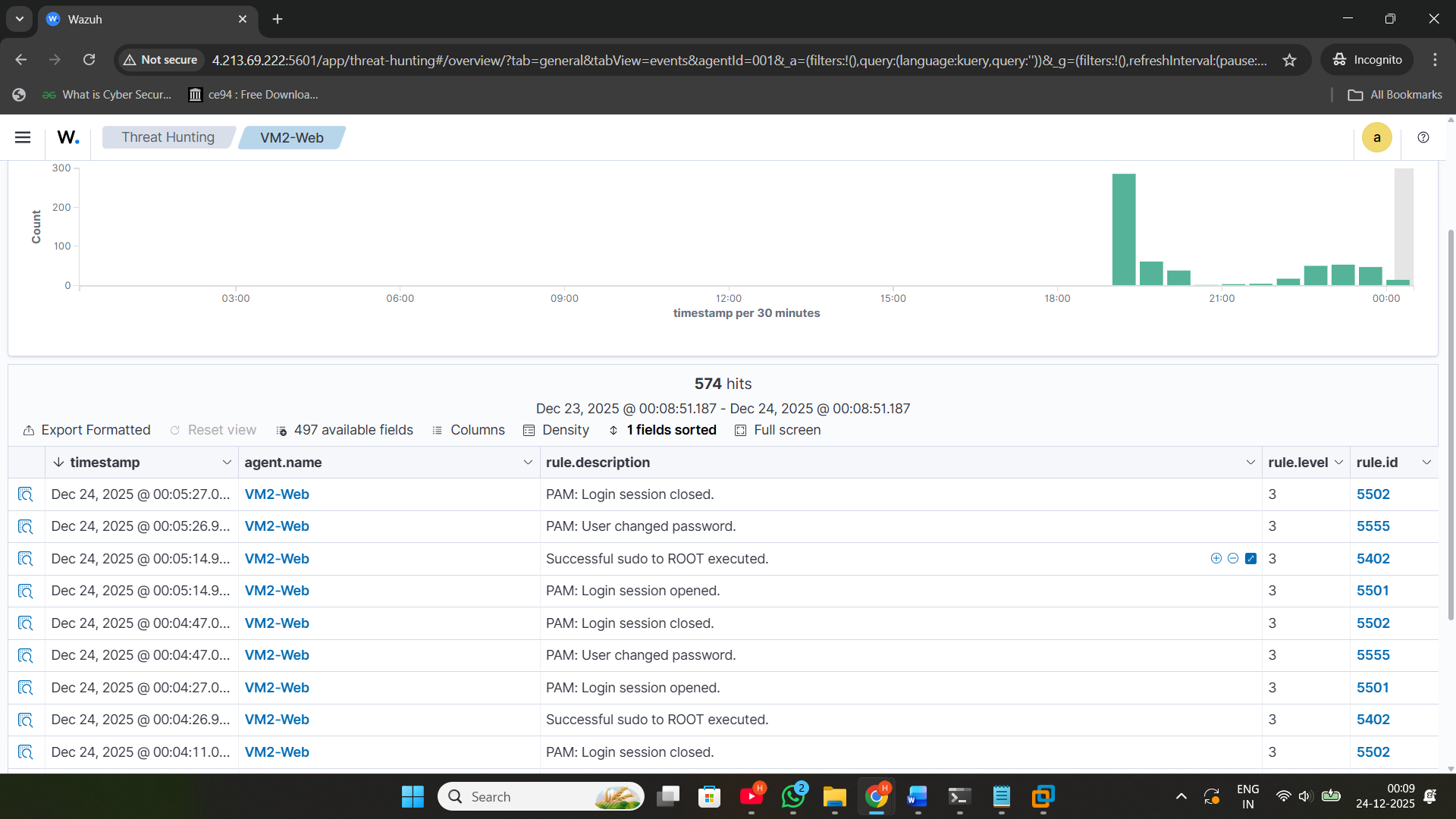
# 2️⃣ Red Team Attack Phase

## SSH Brute Force Attack

Tool Used: Hydra  
  
Command:  
hydra -l Payal007 -P rockyou.txt ssh//4.240.42.216  
  
Source IP: Kali  
Target: VM2  
Severity: HIGH

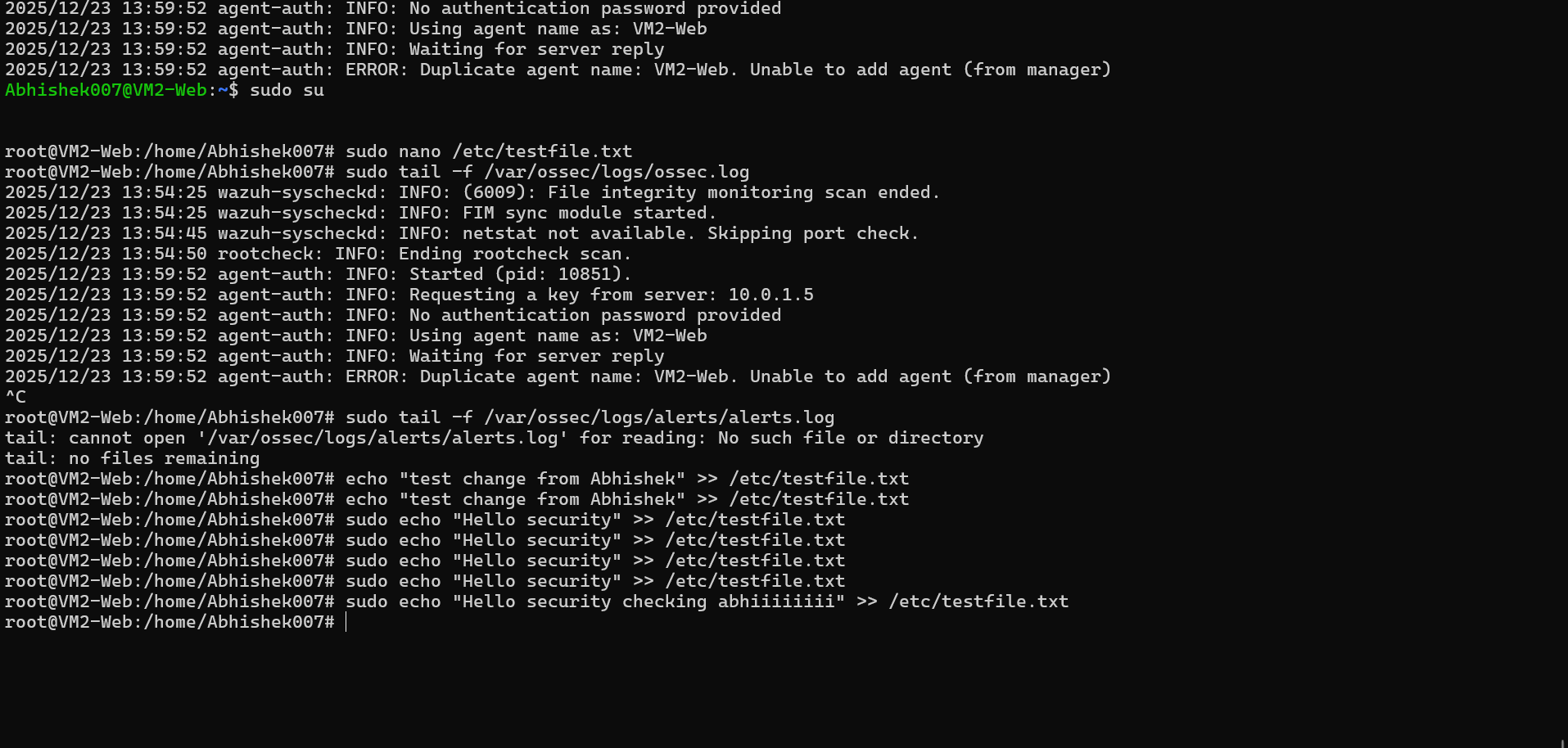


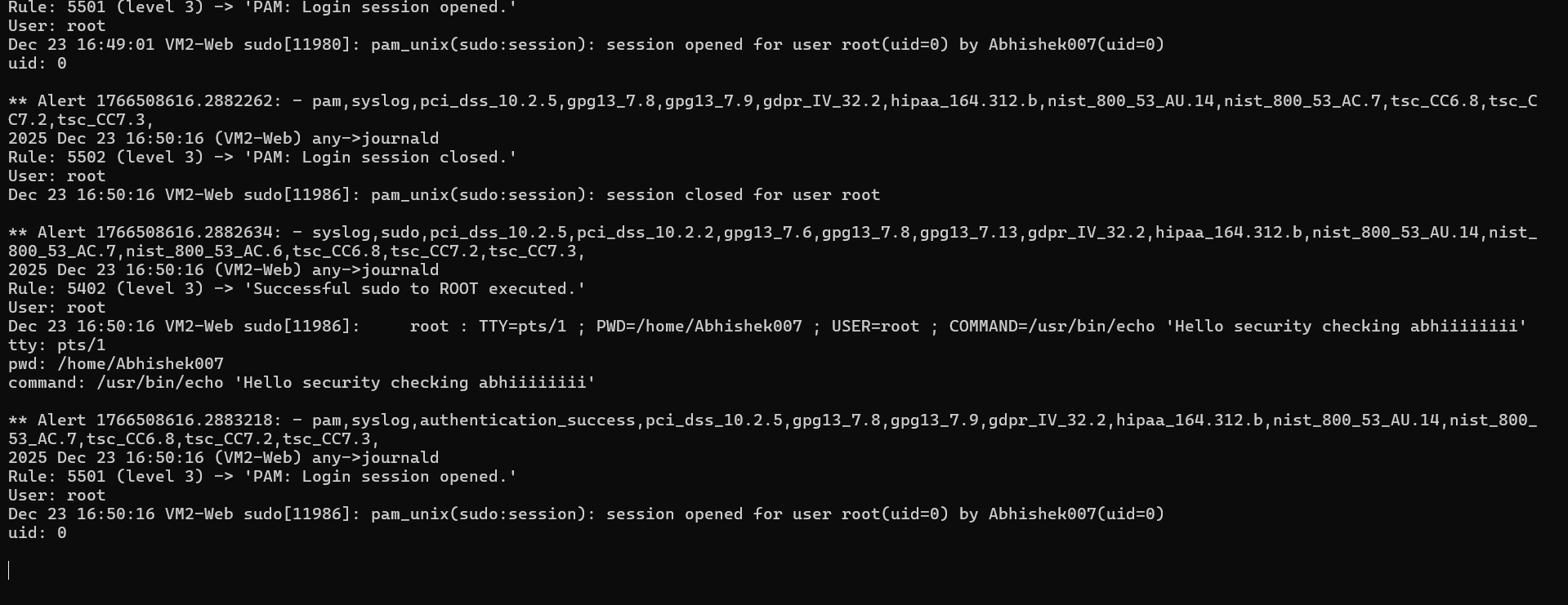




MITRE ATT&CK: T1110 Brute Force

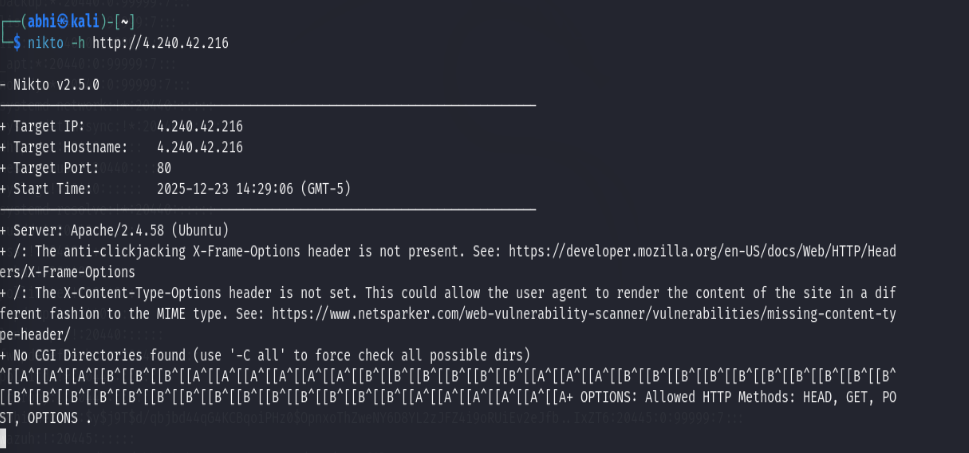
**Changes In File in VM-2**

****

****

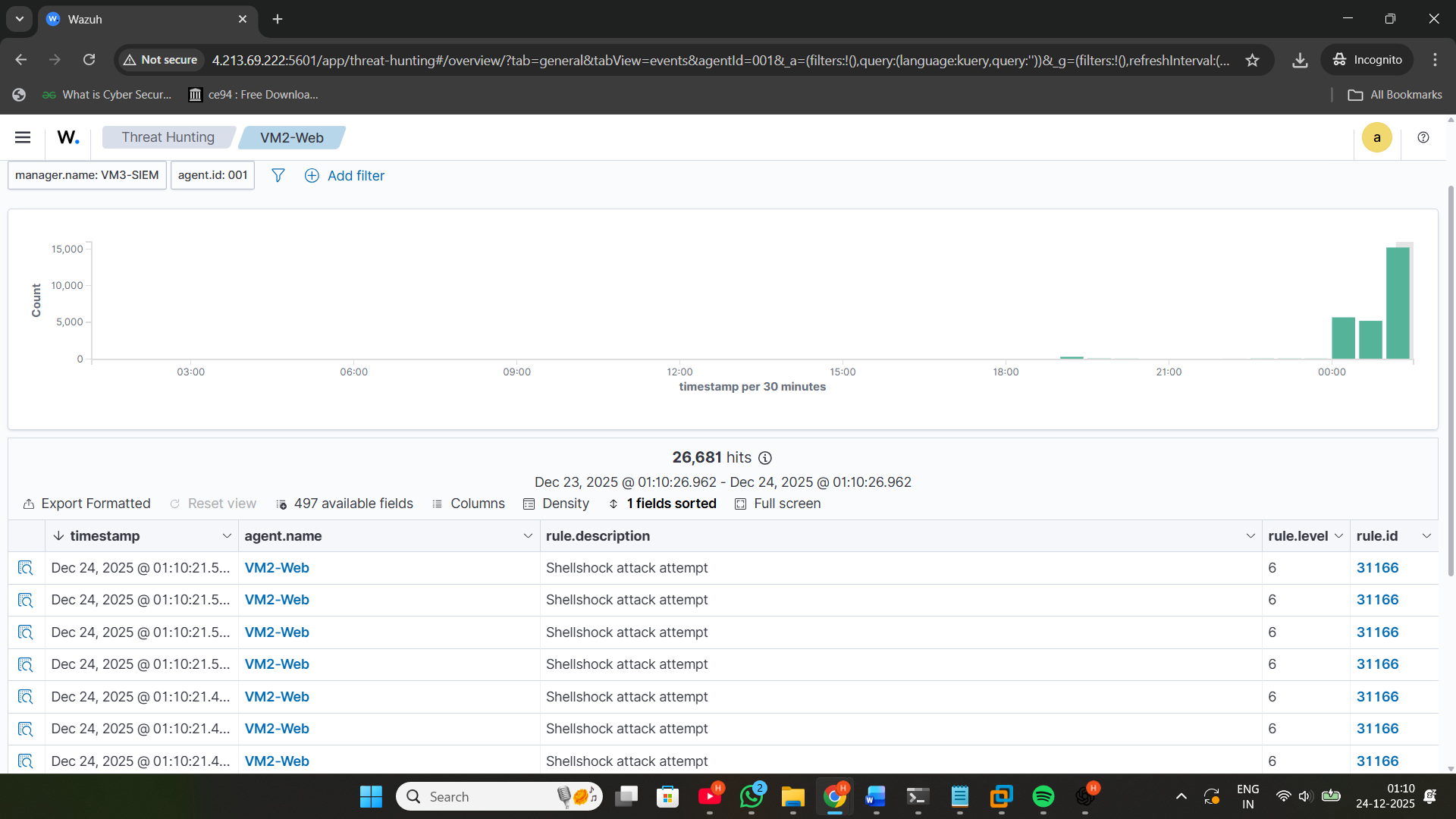
## Web Vulnerability Scan - Nikto

Tool: Nikto  
  
Findings:  
Missing headers  
Version disclosure  
Exposure risk  
  
MITRE ATT&CK: T1595 Active Scanning



## Privilege Escalation Monitoring

Privilege Escalation was monitored via sudo events.  
MITRE ATT&CK: T1068

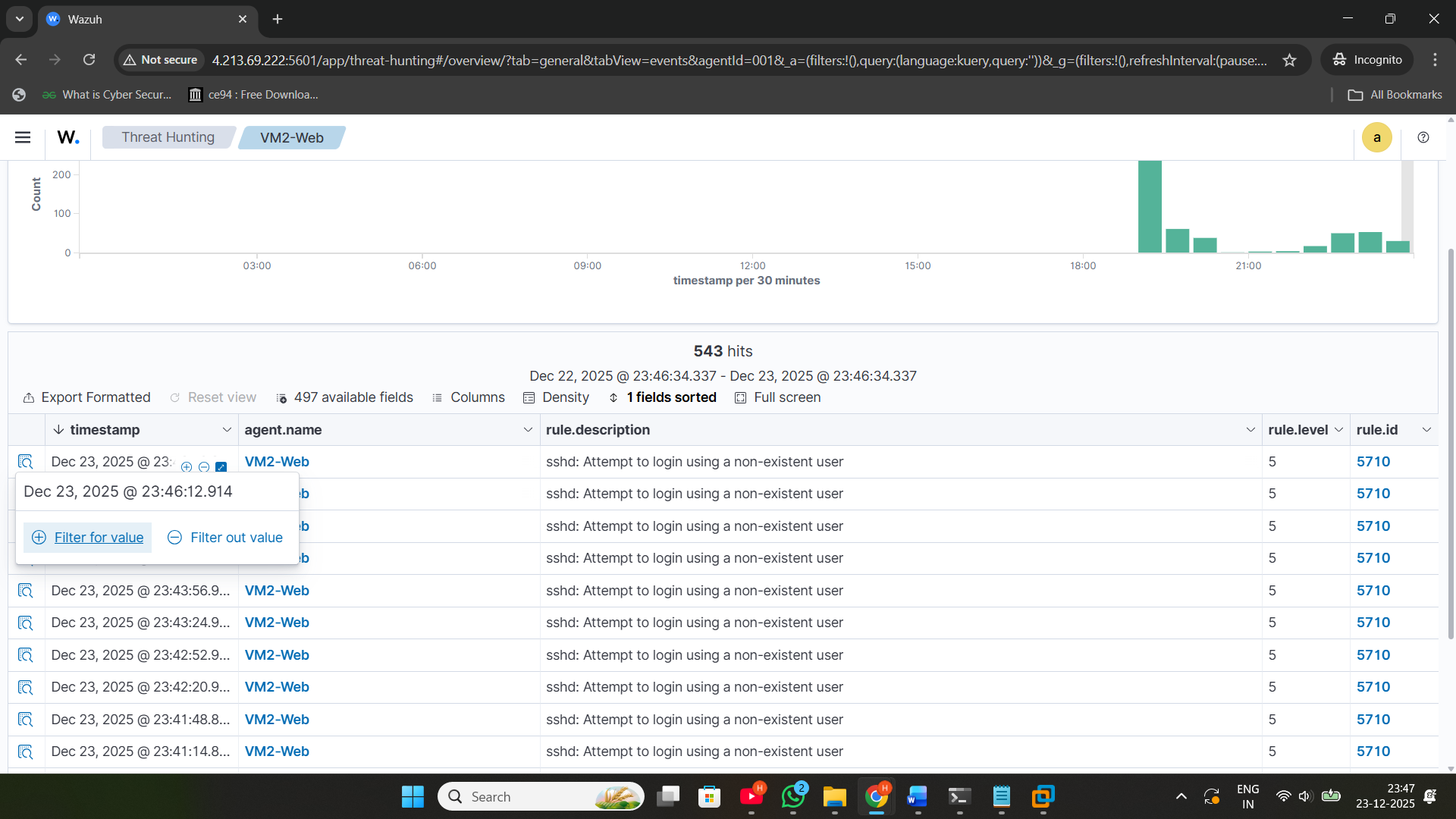


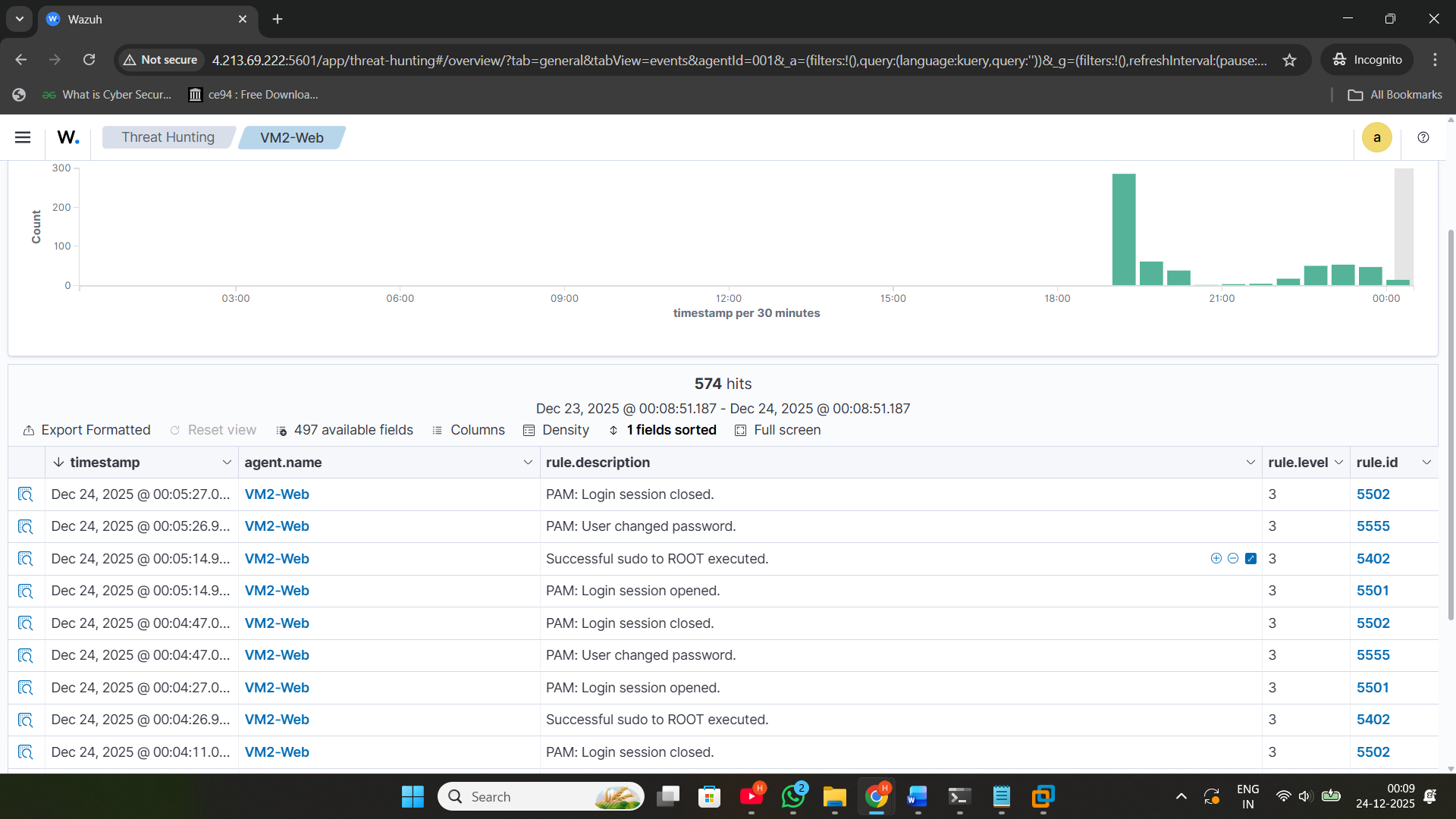
# 

# 

# 3️⃣ SOC Investigation

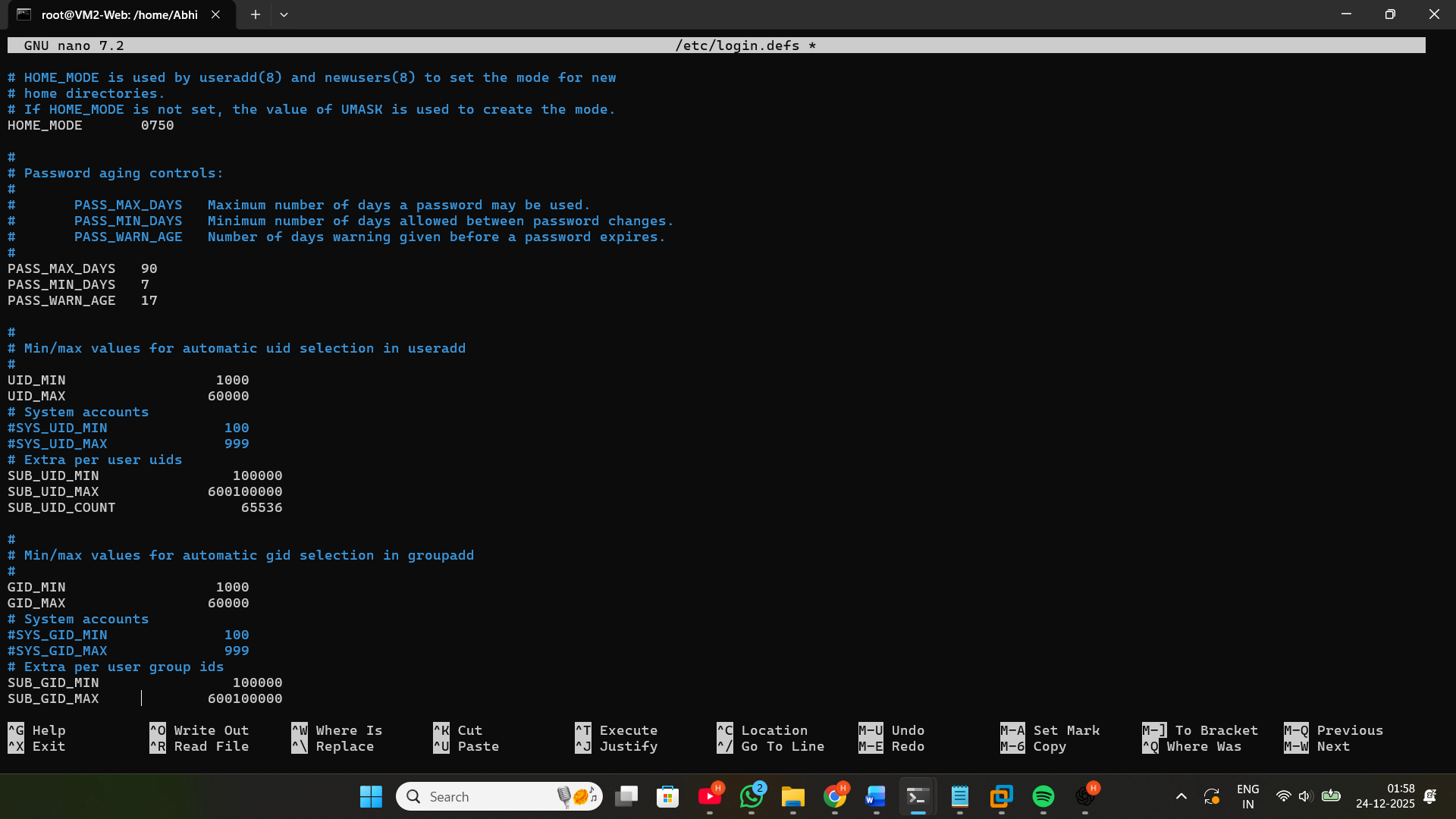
Threat hunting was performed using Wazuh SIEM.  
Indicators of Compromise were captured.  
Logs analyzed include:  
- Syslog  
- Auth.log  
- Wazuh alerts

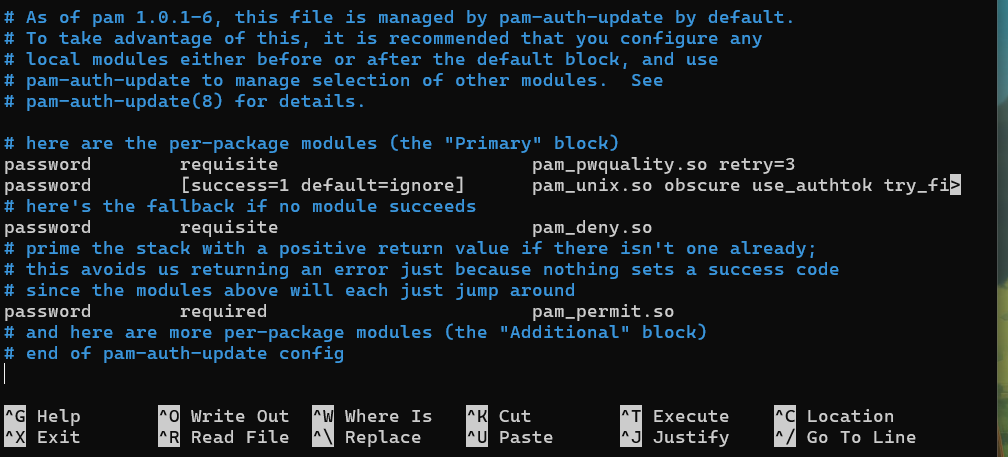
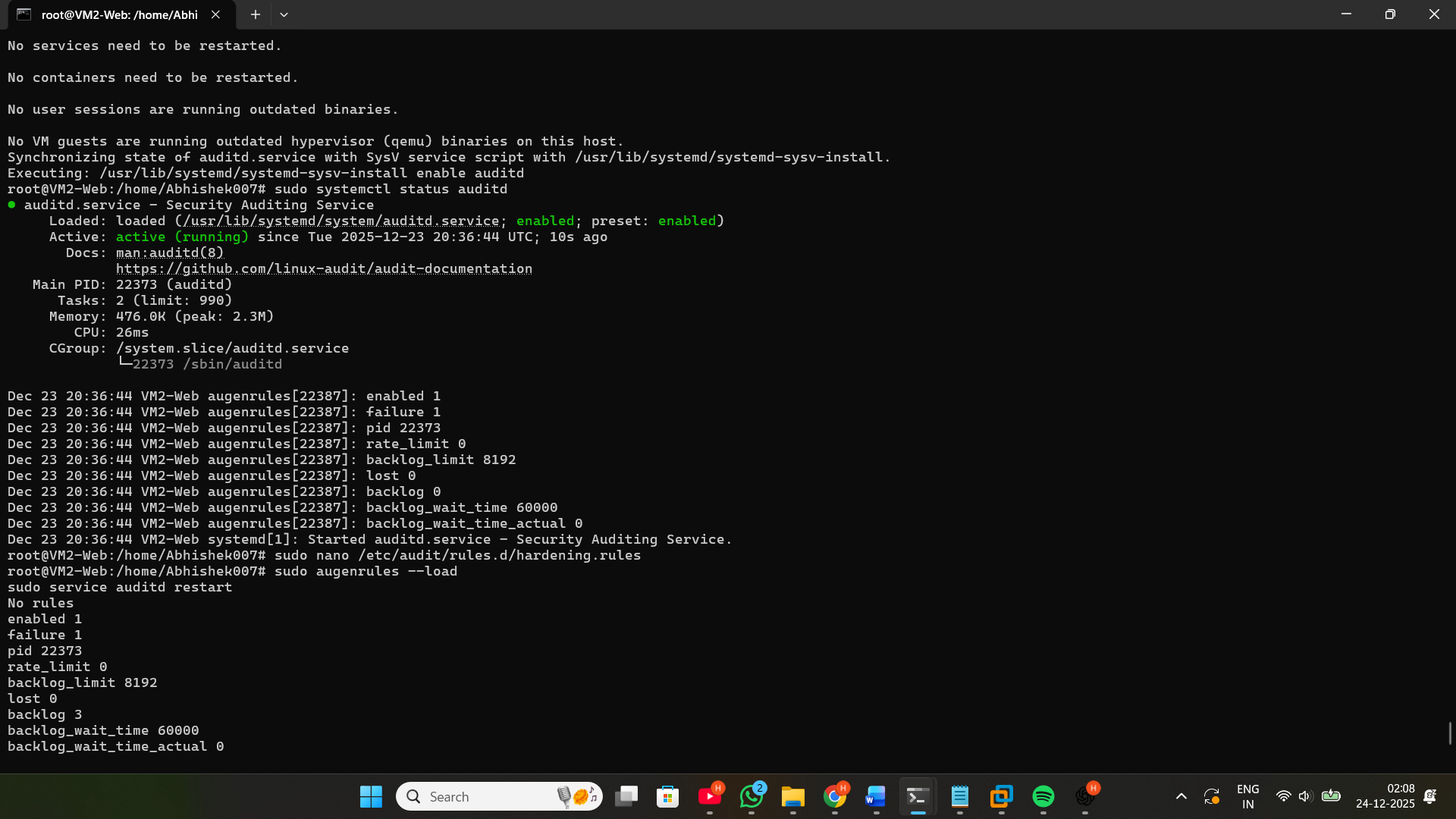




# 4️⃣ System Hardening

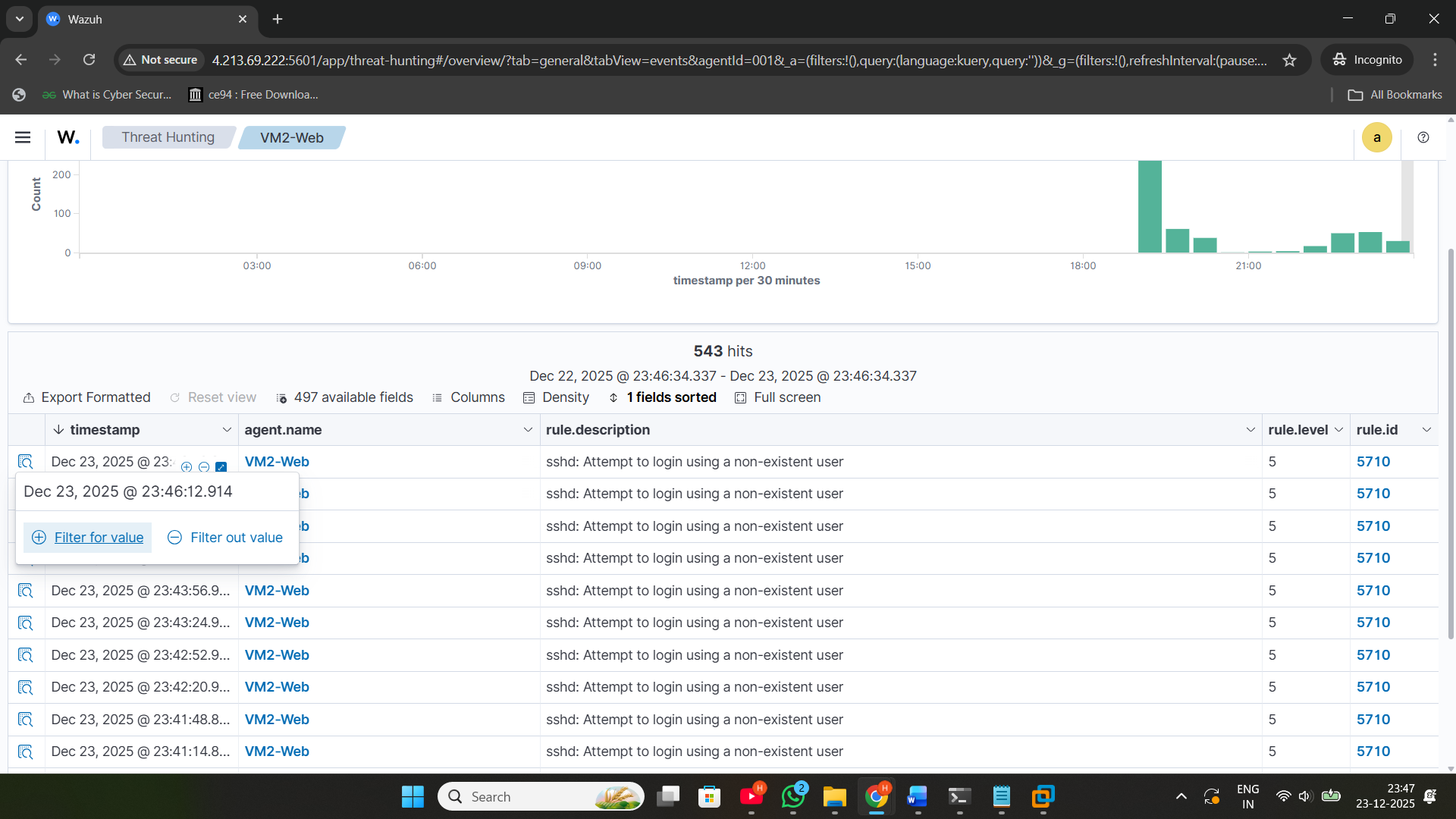
SSH Hardening:  
- Disable root login  
- Change SSH Port  
- Enable Key Authentication  
- Disable Password Login  
- Allow SSH only from SIEM Server  
  
Firewall Hardening:  
- Allow required traffic only  
- Block external SSH except SIEM  
  
Web Hardening:  
- Added security headers  
- Disabled server signature





# 5️⃣ Validation (Re-Attack)

Re-attacks were performed.  
Before vs After comparison shows:  
- SSH brute force blocked  
- Web exposure reduced  
- Logs improved



# Conclusion

This project successfully demonstrated cyber-attack simulation, SIEM-based detection, log analysis, security hardening, and improved defense posture.