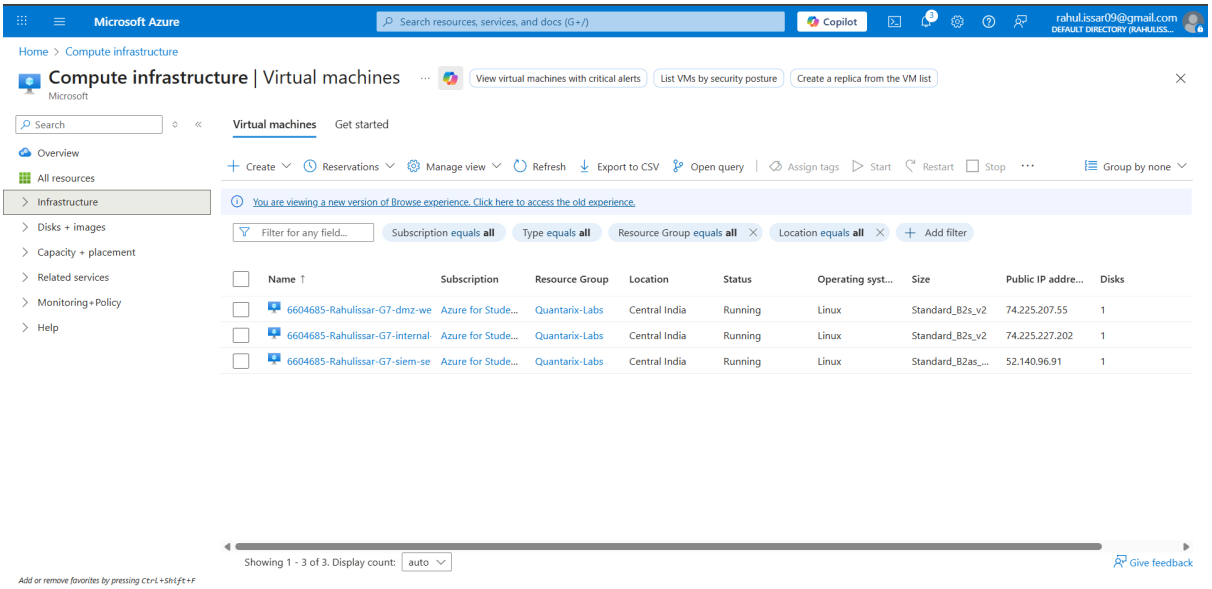
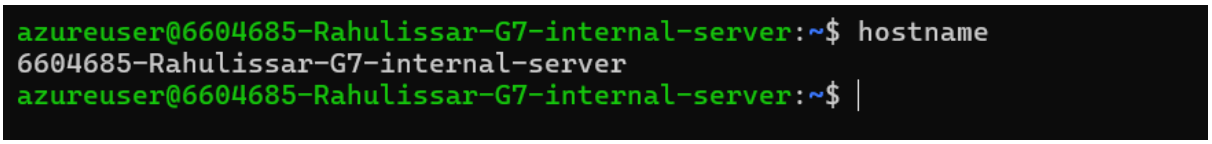
Environment Details

SIEM Server: Azure VM (Wazuh SIEM)
Internal Server (VM1): Ubuntu 22.04
DMZ Web Server (VM2): Ubuntu 22.04 (Apache/Nginx)
Attacker Machine: Kali Linux

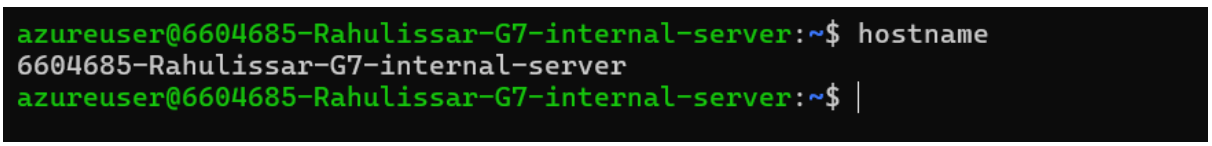
- Azure portal showing **VM names**



- SSH terminal showing **hostname (VM 1)**



- SSH terminal showing **hostname (VM 2)**



- SSH terminal showing **hostname (VM 3)**

Attack Scenarios Executed

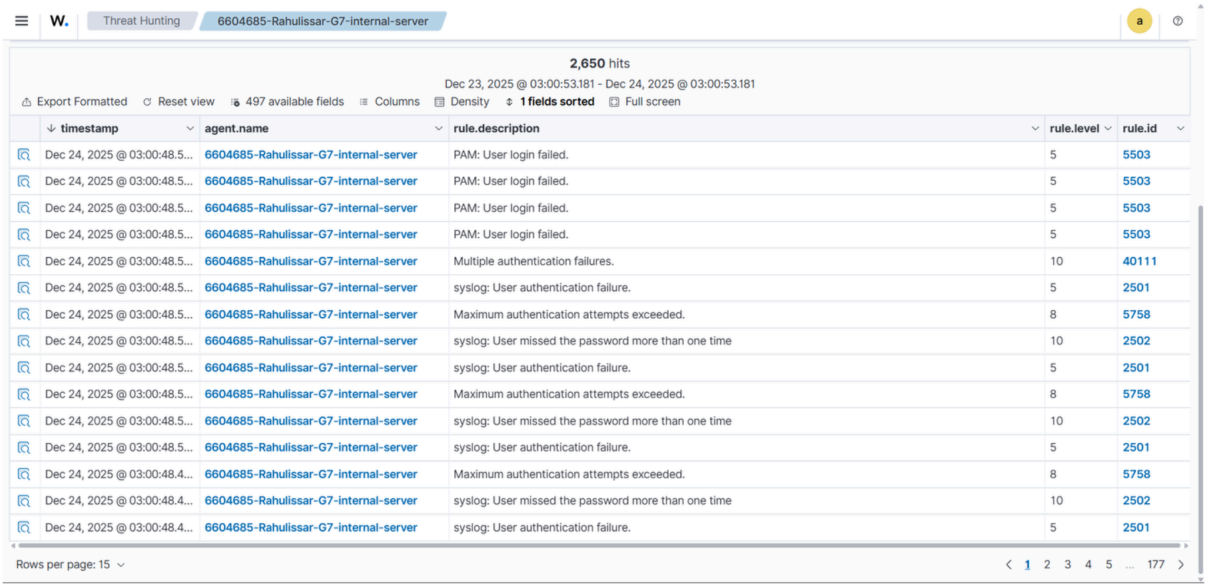
Attack 1: SSH Brute Force (VM1 & VM2)

VM 1 :

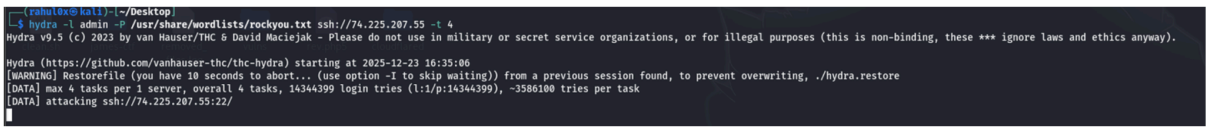
Command used:

- hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://74.225.227.202 -t 4

Wazuh:
Threat Hunting → Events
Filter:
rule.groups: authentication_failed



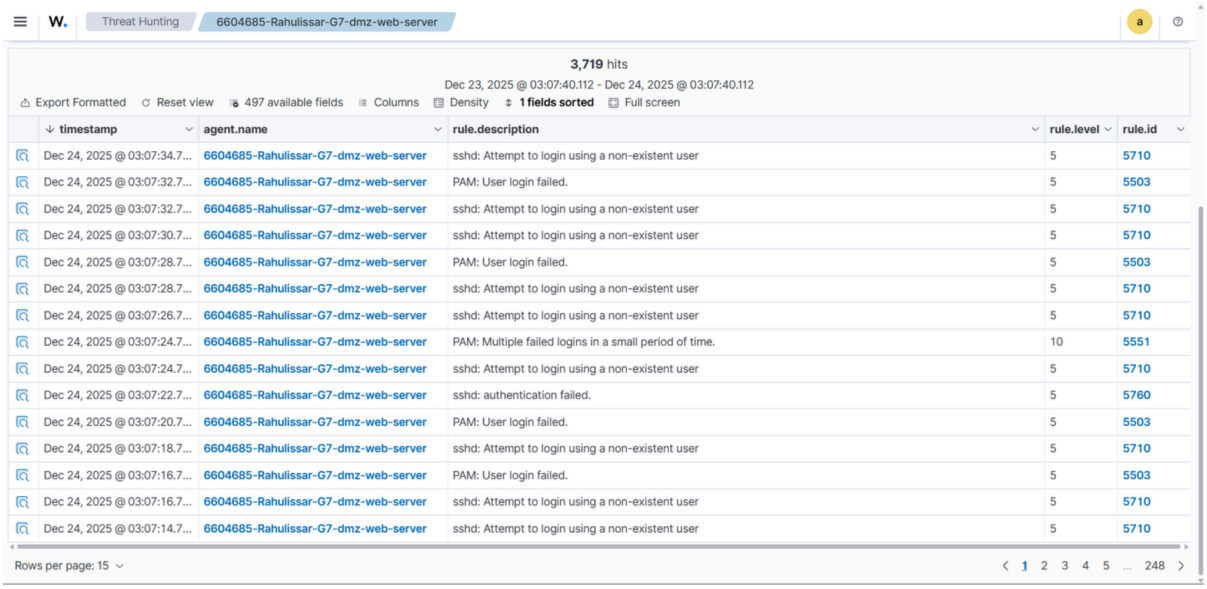
VM 2 :



Command used:

- hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://74.225.207.55 -t 4

Wazuh:
Threat Hunting → Events
Filter:
rule.groups: authentication_failed



timestamp	agent.name	rule.description	rule.level	rule.id
Dec 24, 2025 @ 03:07:34.7...	6604685-Rahulissar-G7-dmz-web-server	sshd: Attempt to login using a non-existent user	5	5710
Dec 24, 2025 @ 03:07:32.7...	6604685-Rahulissar-G7-dmz-web-server	PAM: User login failed.	5	5503
Dec 24, 2025 @ 03:07:32.7...	6604685-Rahulissar-G7-dmz-web-server	sshd: Attempt to login using a non-existent user	5	5710
Dec 24, 2025 @ 03:07:30.7...	6604685-Rahulissar-G7-dmz-web-server	sshd: Attempt to login using a non-existent user	5	5710
Dec 24, 2025 @ 03:07:28.7...	6604685-Rahulissar-G7-dmz-web-server	PAM: User login failed.	5	5503
Dec 24, 2025 @ 03:07:28.7...	6604685-Rahulissar-G7-dmz-web-server	sshd: Attempt to login using a non-existent user	5	5710
Dec 24, 2025 @ 03:07:26.7...	6604685-Rahulissar-G7-dmz-web-server	sshd: Attempt to login using a non-existent user	5	5710
Dec 24, 2025 @ 03:07:24.7...	6604685-Rahulissar-G7-dmz-web-server	PAM: Multiple failed logins in a small period of time.	10	5551
Dec 24, 2025 @ 03:07:24.7...	6604685-Rahulissar-G7-dmz-web-server	sshd: Attempt to login using a non-existent user	5	5710
Dec 24, 2025 @ 03:07:22.7...	6604685-Rahulissar-G7-dmz-web-server	sshd: authentication failed.	5	5760
Dec 24, 2025 @ 03:07:20.7...	6604685-Rahulissar-G7-dmz-web-server	PAM: User login failed.	5	5503
Dec 24, 2025 @ 03:07:18.7...	6604685-Rahulissar-G7-dmz-web-server	sshd: Attempt to login using a non-existent user	5	5710
Dec 24, 2025 @ 03:07:16.7...	6604685-Rahulissar-G7-dmz-web-server	PAM: User login failed.	5	5503
Dec 24, 2025 @ 03:07:16.7...	6604685-Rahulissar-G7-dmz-web-server	sshd: Attempt to login using a non-existent user	5	5710
Dec 24, 2025 @ 03:07:14.7...	6604685-Rahulissar-G7-dmz-web-server	sshd: Attempt to login using a non-existent user	5	5710

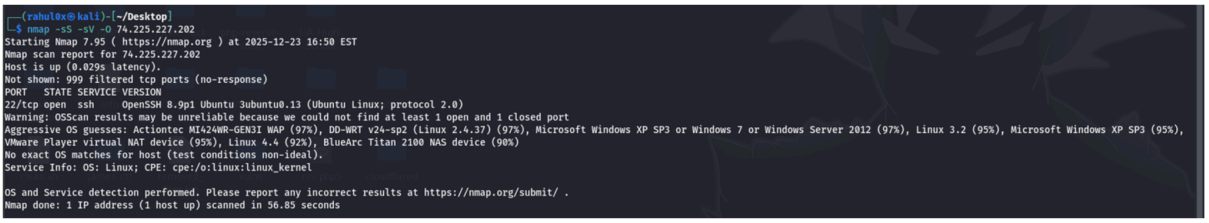
Rows per page: 15 1 2 3 4 5 ... 248

Attack 2: Port Scanning

VM 1:

Command used:

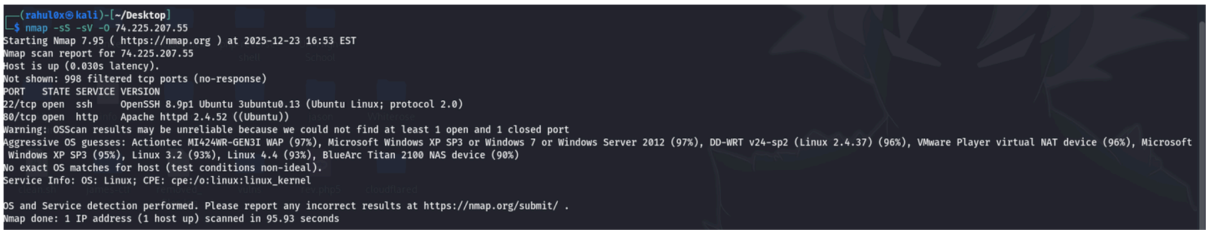
- nmap -sS -sV -O 74.225.227.202



VM 2:

Command used:

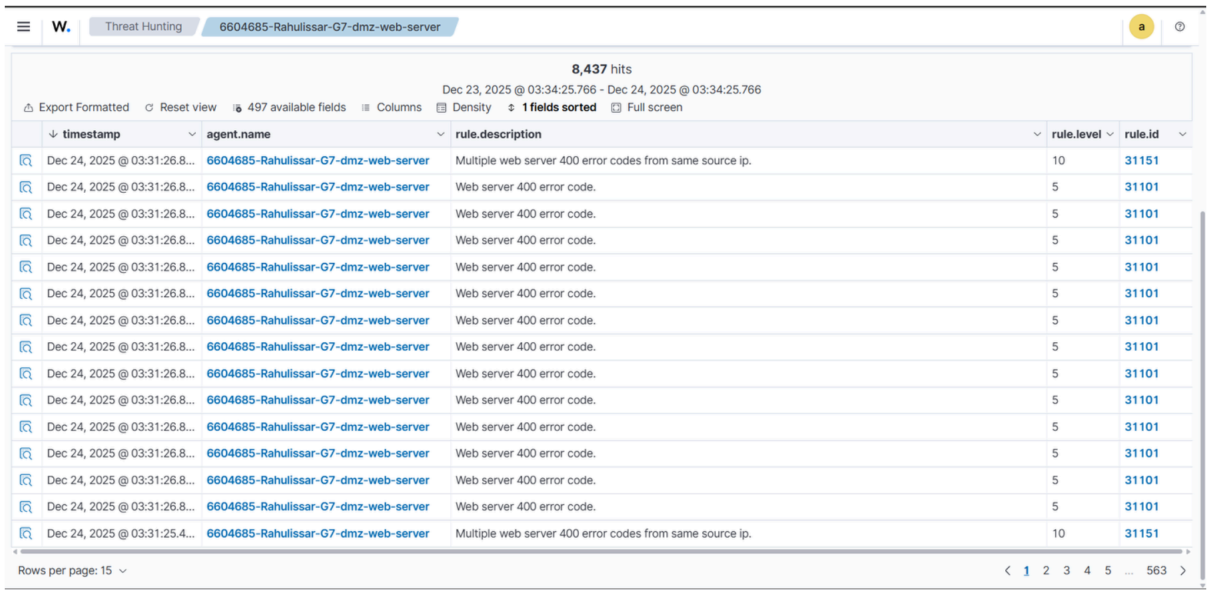
- nmap -sS -sV -O 74.225.207.55



Attack 3: Web Enumeration (VM2)

Command used:

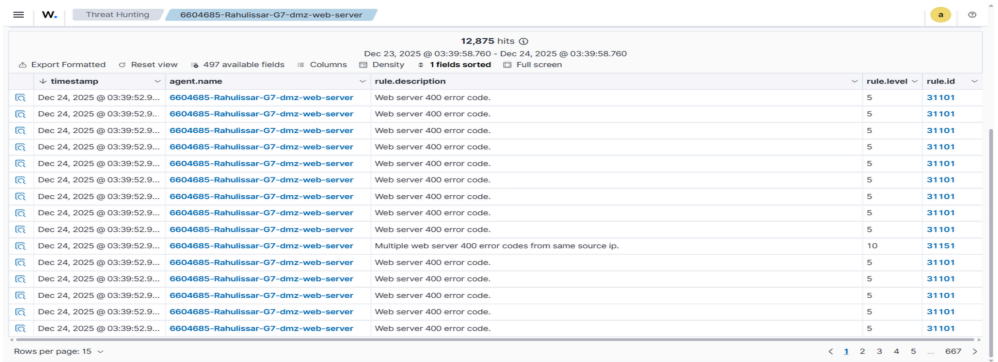
- gobuster dir -u http://74.225.207.55 -w /usr/share/wordlists/dirb/common.txt



Vulnerability Scan

Command used:

- nikto -h http://74.225.207.55

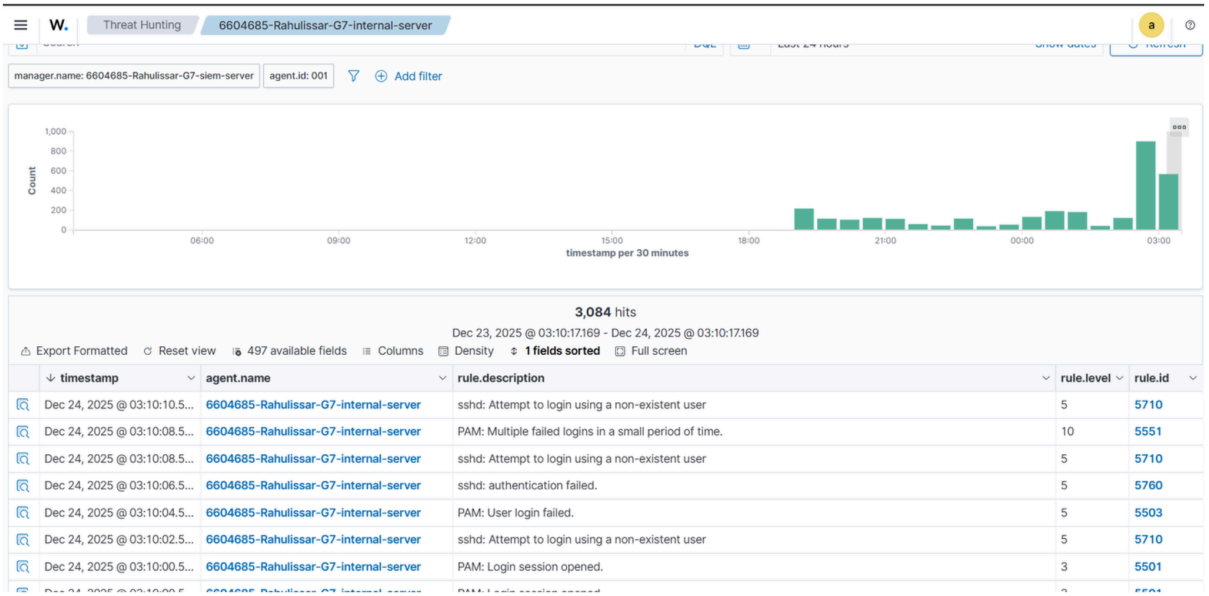


Attack 4: Privilege Escalation Attempts

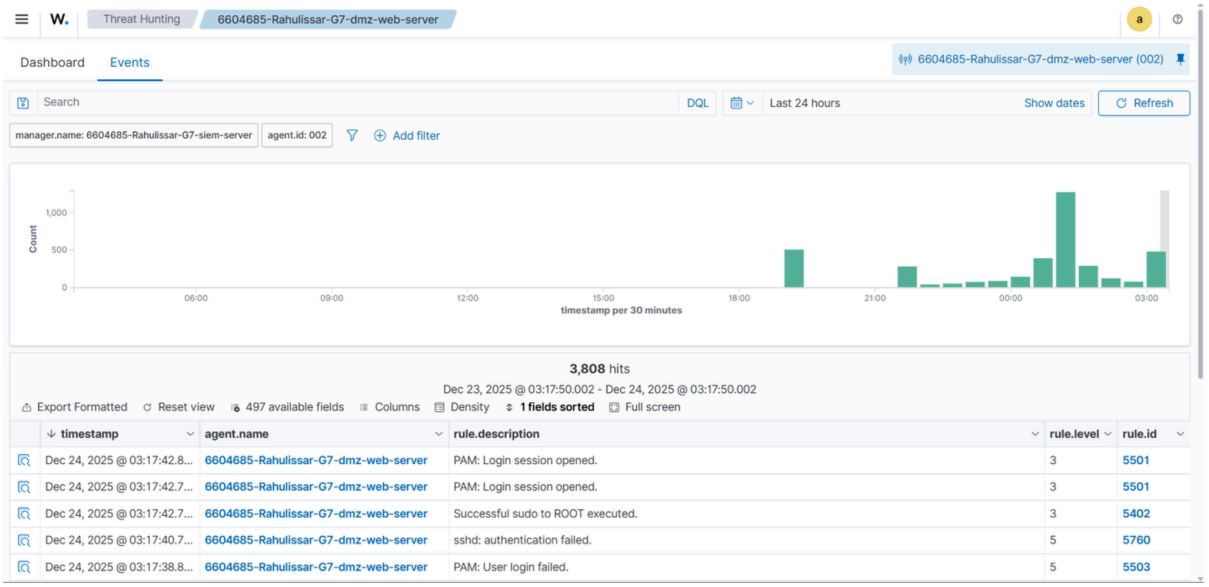
Command used:

- sudo -l
- find / -perm -4000 2>/dev/null

VM 1:



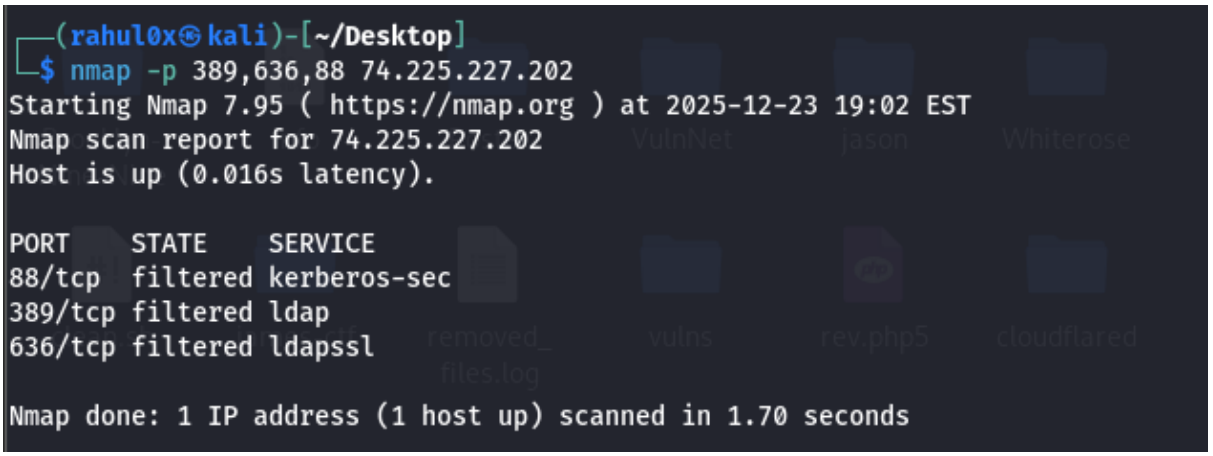
VM 2:



Attack 5: Enumeration (FreeIPA / Services)

Command used:

- nmap -p 389,636,88 74.225.227.202



Summary Table

Attack	Tool	Target	Logs Generated
SSH Brute Force	Hydra	VM 1	auth.log
Port Scan	Nmap	VM 1	syslog
Web Attack	Nikto	VM 2	apache
Priv Esc	sudo	VM 1	pam