

Environment Details

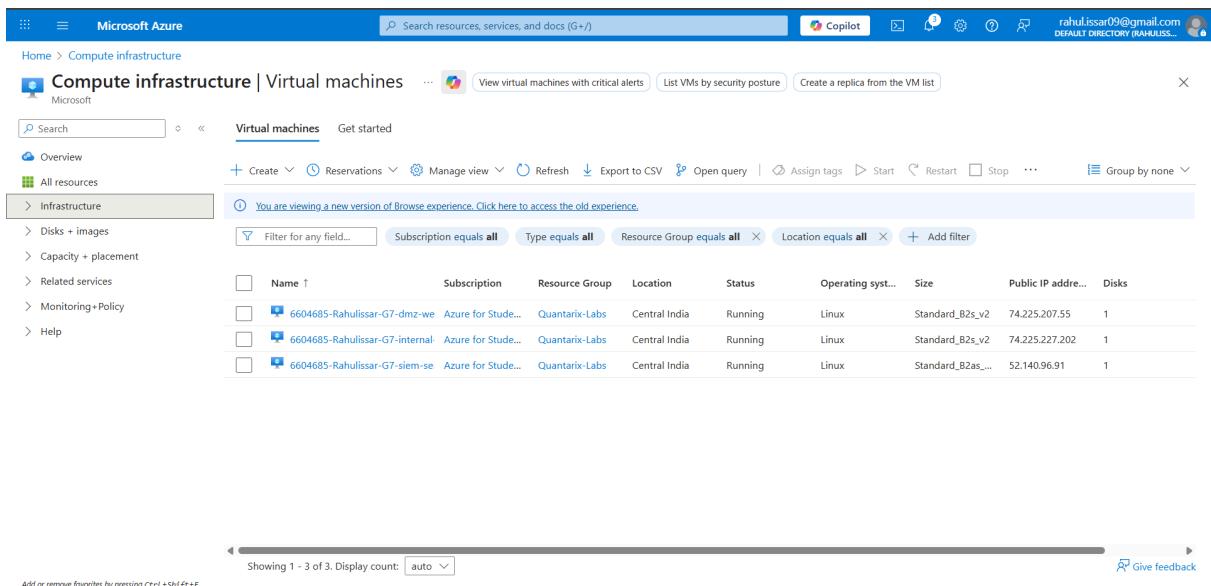
SIEM Server: Azure VM (Wazuh SIEM)

Internal Server (VM1): Ubuntu 22.04

DMZ Web Server (VM2): Ubuntu 22.04 (Apache/Nginx)

Attacker Machine: Kali Linux

- Azure portal showing **VM names**



The screenshot shows the Microsoft Azure Compute Infrastructure Virtual machines page. The left sidebar is collapsed, and the main area displays a list of virtual machines. The list includes:

Name	Subscription	Resource Group	Location	Status	Operating system	Size	Public IP address	Disk count
6604685-Rahulissar-G7-dmz-we	Azure for Students	Quantarix-Labs	Central India	Running	Linux	Standard_B2s_v2	74.225.207.55	1
6604685-Rahulissar-G7-internal	Azure for Students	Quantarix-Labs	Central India	Running	Linux	Standard_B2s_v2	74.225.227.202	1
6604685-Rahulissar-G7-siem-se	Azure for Students	Quantarix-Labs	Central India	Running	Linux	Standard_B2as_v2	52.140.96.91	1

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

```
azureuser@6604685-Rahulissar-G7-internal-server:~$ hostname
6604685-Rahulissar-G7-internal-server
azureuser@6604685-Rahulissar-G7-internal-server:~$ |
```

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

```
azureuser@6604685-Rahulissar-G7-internal-server:~$ hostname
6604685-Rahulissar-G7-internal-server
azureuser@6604685-Rahulissar-G7-internal-server:~$ |
```

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

```
azureuser@6604685-Rahulissar-G7-siem-server:~$ hostname
6604685-Rahulissar-G7-siem-server
```

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

```
(rahul0x㉿kali)-[~/Desktop]
└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://74.225.227.202 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-23 16:28:05
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:/1:p:14344399), -3586100 tries per task
[DATA] attacking ssh://74.225.227.202:22/
[STATUS] 72.00 tries/min, 72 tries in 00:01h, 14344327 to do in 3320:27h, 4 active
```

Wazuh:

Threat Hunting → Events

Filter:

rule.groups: authentication_failed

2,650 hits				
Dec 23, 2025 @ 03:00:53.181 - Dec 24, 2025 @ 03:00:53.181				
timestamp	agent.name	rule.description	rule.level	rule.id
Dec 24, 2025 @ 03:00:48.5...	6604685-Rahulissar-G7-internal-server	PAM: User login failed.	5	5503
Dec 24, 2025 @ 03:00:48.5...	6604685-Rahulissar-G7-internal-server	PAM: User login failed.	5	5503
Dec 24, 2025 @ 03:00:48.5...	6604685-Rahulissar-G7-internal-server	PAM: User login failed.	5	5503
Dec 24, 2025 @ 03:00:48.5...	6604685-Rahulissar-G7-internal-server	PAM: User login failed.	5	5503
Dec 24, 2025 @ 03:00:48.5...	6604685-Rahulissar-G7-internal-server	Multiple authentication failures.	10	40111
Dec 24, 2025 @ 03:00:48.5...	6604685-Rahulissar-G7-internal-server	syslog: User authentication failure.	5	2501
Dec 24, 2025 @ 03:00:48.5...	6604685-Rahulissar-G7-internal-server	Maximum authentication attempts exceeded.	8	5758
Dec 24, 2025 @ 03:00:48.5...	6604685-Rahulissar-G7-internal-server	syslog: User missed the password more than one time	10	2502
Dec 24, 2025 @ 03:00:48.5...	6604685-Rahulissar-G7-internal-server	syslog: User authentication failure.	5	2501
Dec 24, 2025 @ 03:00:48.5...	6604685-Rahulissar-G7-internal-server	Maximum authentication attempts exceeded.	8	5758
Dec 24, 2025 @ 03:00:48.5...	6604685-Rahulissar-G7-internal-server	syslog: User missed the password more than one time	10	2502
Dec 24, 2025 @ 03:00:48.5...	6604685-Rahulissar-G7-internal-server	syslog: User authentication failure.	5	2501
Dec 24, 2025 @ 03:00:48.4...	6604685-Rahulissar-G7-internal-server	Maximum authentication attempts exceeded.	8	5758
Dec 24, 2025 @ 03:00:48.4...	6604685-Rahulissar-G7-internal-server	syslog: User missed the password more than one time	10	2502
Dec 24, 2025 @ 03:00:48.4...	6604685-Rahulissar-G7-internal-server	syslog: User authentication failure.	5	2501

Rows per page: 15 < 1 2 3 4 5 ... 177 >

VM 2 :

```
(rahul0x㉿kali)-[~/Desktop]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://74.225.207.55 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-23 16:35:06
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:/1:p:14344399), -3586100 tries per task
[DATA] attacking ssh://74.225.207.55:22/
```

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

3,719 hits					
Dec 23, 2025 @ 03:07:40.112 - Dec 24, 2025 @ 03:07:40.112					
Export	Formatted	Reset view	497 available fields	Columns	Density
rule.level	rule.id				
5	5710				
5	5503				
5	5710				
5	5710				
5	5503				
5	5710				
5	5710				
10	5551				
5	5710				
5	5760				
5	5503				
5	5710				
5	5503				
5	5710				
5	5710				
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

```
(rahul@kali) [~/Desktop]
$ nmap -sS -sV -O 74.225.227.202
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-23 16:50 EST
Nmap scan report for 74.225.227.202
Host is up (0.029s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Actiontec M1424WR-GEN3I WAP (97%), DD-WRT v24-sp2 (Linux 2.4.37) (97%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (97%), Linux 3.2 (95%), Microsoft Windows XP SP3 (95%), VMware Player virtual NAT device (95%), Linux 4.4 (92%), BlueArc Titan 2100 NAS device (90%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 56.85 seconds
```

VM 2:

Command used:

- nmap -sS -sV -O 74.225.207.55

```
(rahul@kali) [~/Desktop]
$ nmap -sS -sV -O 74.225.207.55
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-23 16:53 EST
Nmap scan report for 74.225.207.55
Host is up (0.030s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
20/tcp    open  ftp   Apache httpd 2.4.52 ((Ubuntu))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Actiontec M1424WR-GEN3I WAP (97%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (97%), DD-WRT v24-sp2 (Linux 2.4.37) (96%), VMware Player virtual NAT device (96%), Microsoft Windows XP SP3 (95%), Linux 3.2 (93%), Linux 4.4 (93%), BlueArc Titan 2100 NAS device (90%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 95.93 seconds
```

Attack 3: Web Enumeration (VM2)

Command used:

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

W.		Threat Hunting			6604685-Rahulissar-G7-dmz-web-server		a	
8,437 hits								
<input type="checkbox"/> Export Formatted	<input type="radio"/> Reset view	<input checked="" type="radio"/> 497 available fields	<input type="checkbox"/> Columns	<input type="checkbox"/> Density	<input checked="" type="checkbox"/> 1 fields sorted	<input type="checkbox"/> Full screen		
↓ timestamp	↑ agent.name	↓ rule.description					↑ rule.level	↑ rule.id
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Multiple web server 400 error codes from same source ip.					10	31151
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Web server 400 error code.					5	31101
Dec 24, 2025 @ 03:31:26.8...	6604685-Rahulissar-G7-dmz-web-server	Multiple web server 400 error codes from same source ip.					10	31151

Vulnerability Scan

Command used:

- nikto -h <http://74.225.207.55>

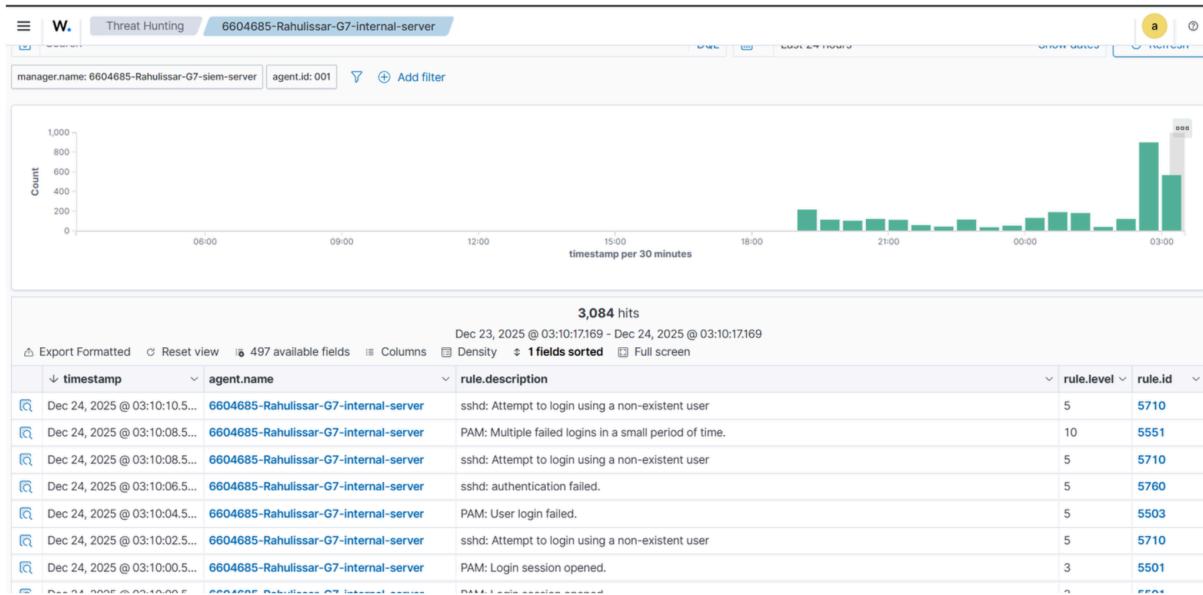
```
[rahul0@kali:~/Desktop]$ php reverse-shell -U http://74.225.207.55  
- Nikto v2.5.0  
  
-----  
* Target IP: 74.225.207.55  
* Target Hostname: 74.225.207.55  
* Target Port: 80  
* Start Time: 2025-12-23 17:05:53 (GMT-5)  
  
+ Server: Apache/2.4.52 (Ubuntu)  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scan/nervulnerabilities/missing-content-type-header/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ /: Server may leak inodes via ETags, header found with file /, inode: 970, size: 6468f2c9cd081, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418  
+ Apache/2.4.52 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.  
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
```

Attack 4: Privilege Escalation Attempts

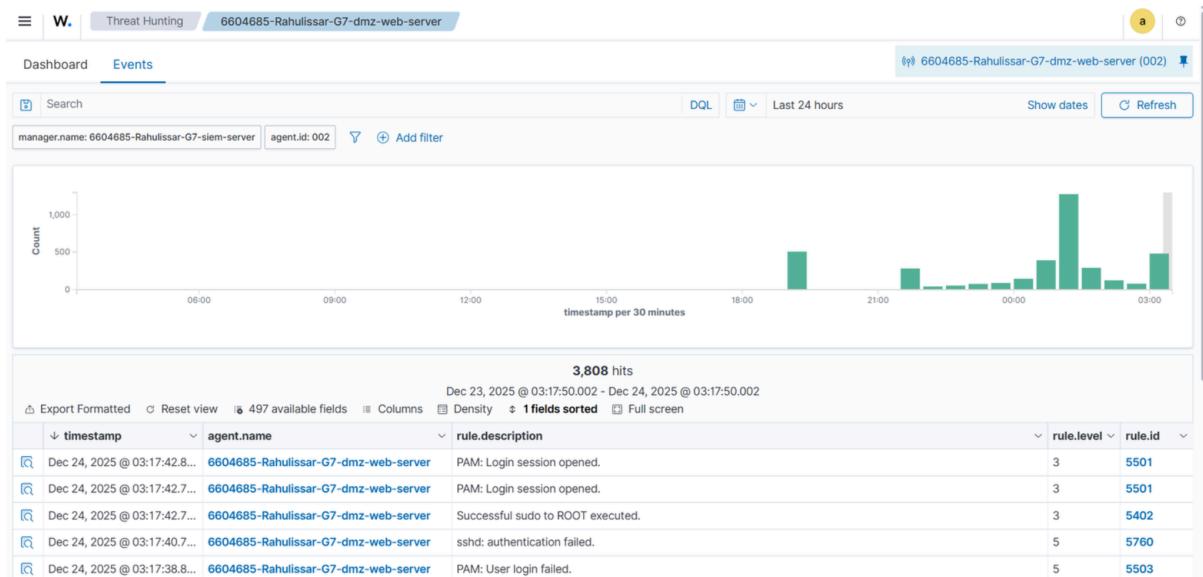
Command used:

- 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

```
(rahul0x㉿kali)-[~/Desktop]
$ nmap -p 389,636,88 74.225.227.202
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-23 19:02 EST
Nmap scan report for 74.225.227.202
Host is up (0.016s latency).

PORT      STATE      SERVICE
88/tcp    filtered  kerberos-sec
389/tcp   filtered  ldap
636/tcp   filtered  ldapssl
                           removed_
                           files.log

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
```

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