HARDENING REPORT

Project: Quantarix Labs – Major Project
Environment: Azure (VM1 – Internal, VM2 – DMZ, VM3 – SIEM)

Structure

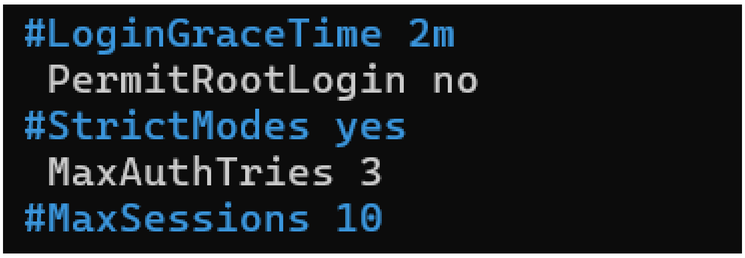
1 SSH Hardening

Commands:

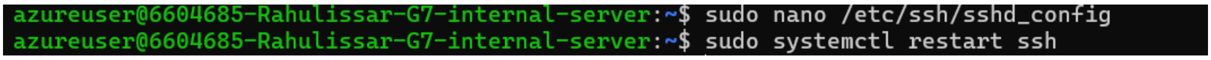
- `sudo nano /etc/ssh/sshd_config`

Changes:

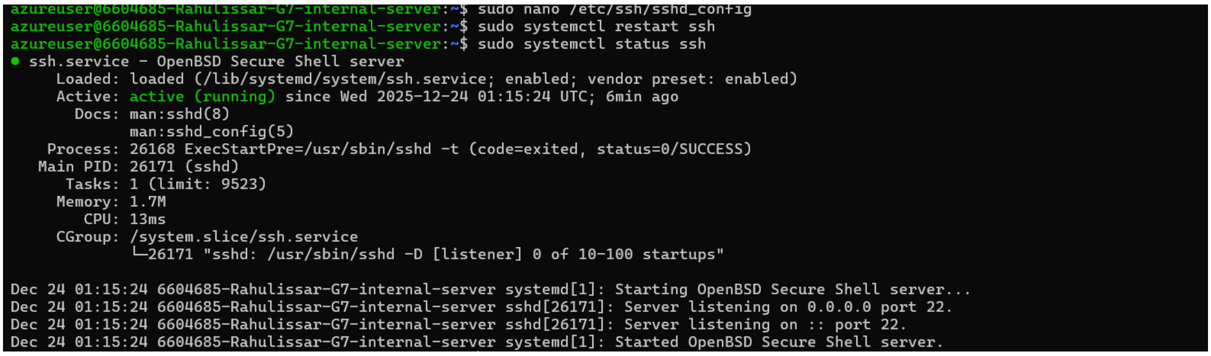
- `PermitRootLogin no`
- `PasswordAuthentication no`
- `Port 2222`
- `sudo systemctl restart ssh`



```
#LoginGraceTime 2m
 PermitRootLogin no
#StrictModes yes
 MaxAuthTries 3
#MaxSessions 10
```



```
azureuser@6604685-Rahulissar-G7-internal-server:~$ sudo nano /etc/ssh/sshd_config
azureuser@6604685-Rahulissar-G7-internal-server:~$ sudo systemctl restart ssh
```



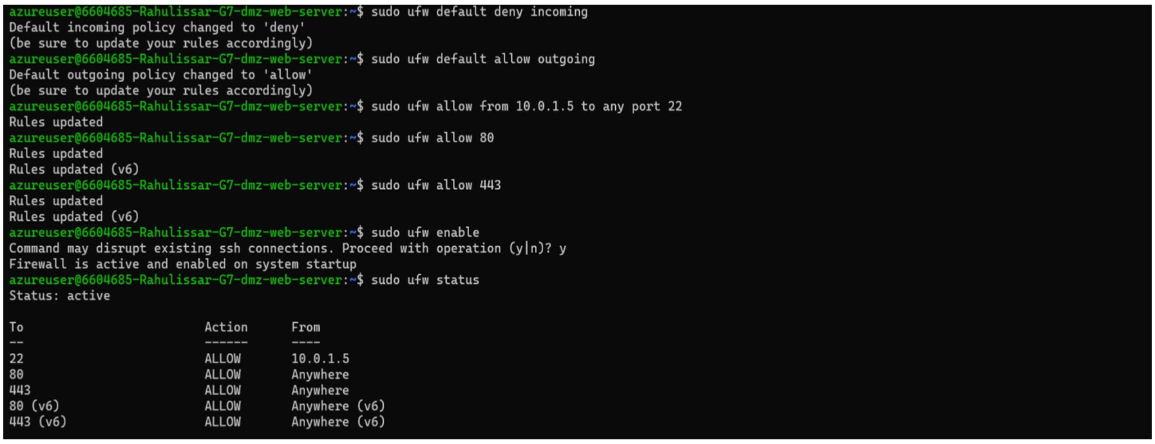
```
azureuser@6604685-Rahulissar-G7-internal-server:~$ sudo nano /etc/ssh/sshd_config
azureuser@6604685-Rahulissar-G7-internal-server:~$ sudo systemctl restart ssh
azureuser@6604685-Rahulissar-G7-internal-server:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2025-12-24 01:15:24 UTC; 6min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 26168 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 26171 (sshd)
      Tasks: 1 (limit: 9523)
     Memory: 1.7M
        CPU: 13ms
     CGroup: /system.slice/ssh.service
             └─26171 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 24 01:15:24 6604685-Rahulissar-G7-internal-server systemd[1]: Starting OpenBSD Secure Shell server...
Dec 24 01:15:24 6604685-Rahulissar-G7-internal-server sshd[26171]: Server listening on 0.0.0.0 port 22.
Dec 24 01:15:24 6604685-Rahulissar-G7-internal-server sshd[26171]: Server listening on :: port 22.
Dec 24 01:15:24 6604685-Rahulissar-G7-internal-server systemd[1]: Started OpenBSD Secure Shell server.
```

2 Firewall Hardening

- `sudo ufw allow from <SIEM_IP> to any port 22`
- `sudo ufw deny 22`

- `sudo ufw enable`

- sudo ufw status

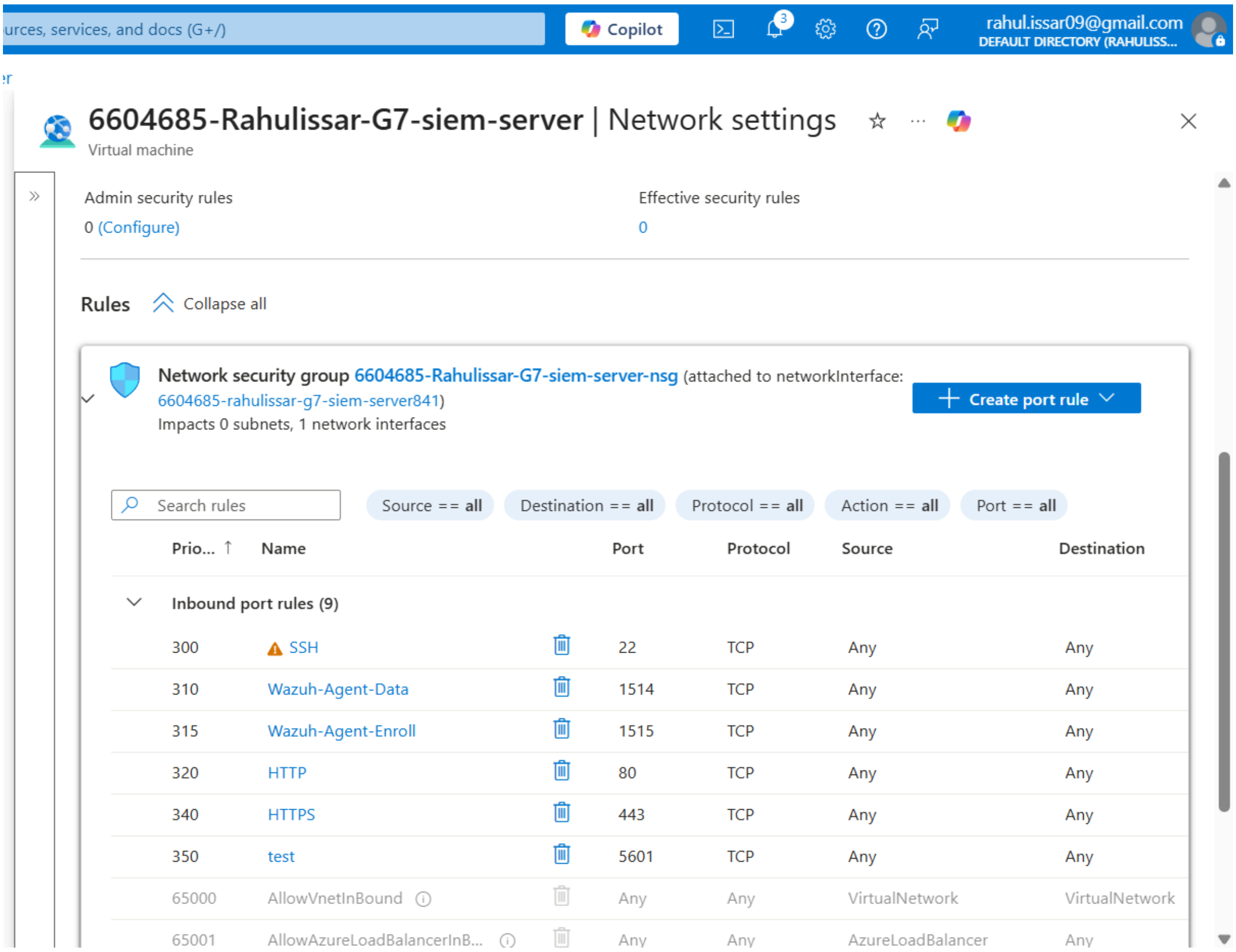


```
azureuser@6604685-Rahulissar-G7-dmz-web-server:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
azureuser@6604685-Rahulissar-G7-dmz-web-server:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
azureuser@6604685-Rahulissar-G7-dmz-web-server:~$ sudo ufw allow from 10.0.1.5 to any port 22
Rules updated
azureuser@6604685-Rahulissar-G7-dmz-web-server:~$ sudo ufw allow 80
Rules updated
Rules updated (v6)
azureuser@6604685-Rahulissar-G7-dmz-web-server:~$ sudo ufw allow 443
Rules updated
Rules updated (v6)
azureuser@6604685-Rahulissar-G7-dmz-web-server:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
azureuser@6604685-Rahulissar-G7-dmz-web-server:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       10.0.1.5
80                         ALLOW       Anywhere
443                        ALLOW       Anywhere
80 (v6)                    ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)
```

3 NSG Hardening (Azure)

Rules:

- Allow SSH only from SIEM
- Block public SSH



urces, services, and docs (G+/)
Copilot
3
rahul.issar09@gmail.com
DEFAULT DIRECTORY (RAHULISS...
Collapse all
Create port rule

6604685-Rahulissar-G7-siem-server | Network settings

Virtual machine

Admin security rules

0 (Configure)

Effective security rules

0

Rules

Network security group 6604685-Rahulissar-G7-siem-server-nsg (attached to networkInterface: 6604685-rahulissar-g7-siem-server841)

Impacts 0 subnets, 1 network interfaces

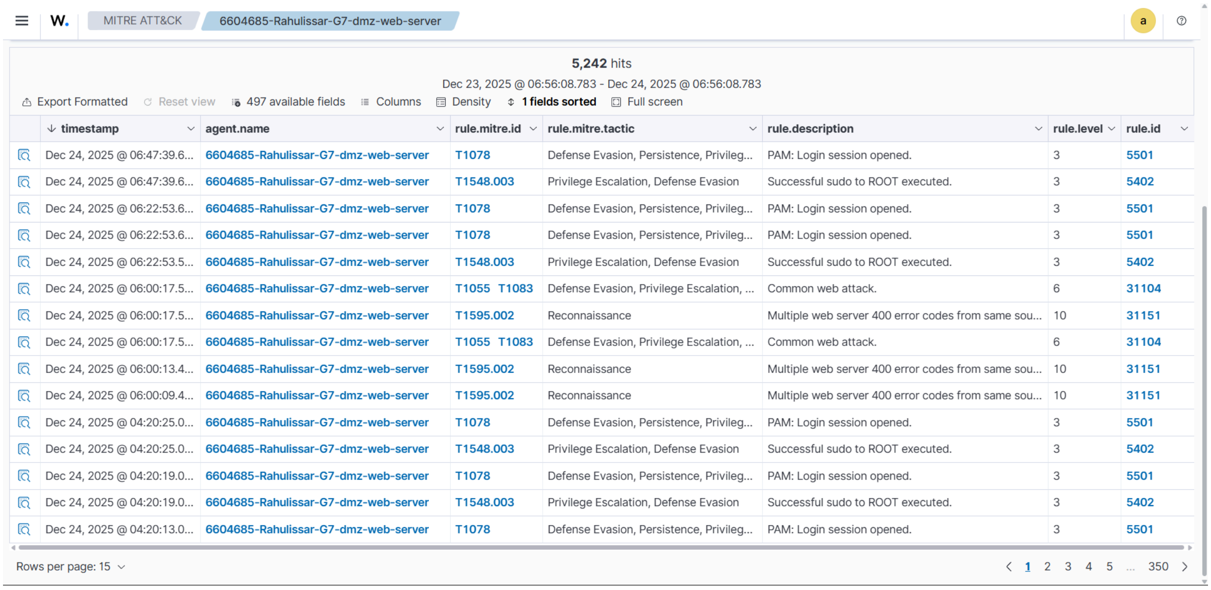
Search rules | Source == all | Destination == all | Protocol == all | Action == all | Port == all

Inbound port rules (9)

Prio... ↑	Name	Port	Protocol	Source	Destination
300	⚠ SSH	22	TCP	Any	Any
310	Wazuh-Agent-Data	1514	TCP	Any	Any
315	Wazuh-Agent-Enroll	1515	TCP	Any	Any
320	HTTP	80	TCP	Any	Any
340	HTTPS	443	TCP	Any	Any
350	test	5601	TCP	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any

4️⃣ Logging Enhancements

- `sudo apt install auditd audispd-plugins`
- `sudo auditctl -w /etc/passwd -p wa`



5,242 hits

Dec 23, 2025 @ 06:56:08.783 - Dec 24, 2025 @ 06:56:08.783

timestamp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
Dec 24, 2025 @ 06:47:39.6...	6604685-Rahulissar-G7-dmz-web-server	T1078	Defense Evasion, Persistence, Privileg...	PAM: Login session opened.	3	5501
Dec 24, 2025 @ 06:47:39.6...	6604685-Rahulissar-G7-dmz-web-server	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
Dec 24, 2025 @ 06:22:53.6...	6604685-Rahulissar-G7-dmz-web-server	T1078	Defense Evasion, Persistence, Privileg...	PAM: Login session opened.	3	5501
Dec 24, 2025 @ 06:22:53.6...	6604685-Rahulissar-G7-dmz-web-server	T1078	Defense Evasion, Persistence, Privileg...	PAM: Login session opened.	3	5501
Dec 24, 2025 @ 06:22:53.5...	6604685-Rahulissar-G7-dmz-web-server	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
Dec 24, 2025 @ 06:00:17.5...	6604685-Rahulissar-G7-dmz-web-server	T1055 T1083	Defense Evasion, Privilege Escalation, ...	Common web attack.	6	31104
Dec 24, 2025 @ 06:00:17.5...	6604685-Rahulissar-G7-dmz-web-server	T1595.002	Reconnaissance	Multiple web server 400 error codes from same sou...	10	31151
Dec 24, 2025 @ 06:00:17.5...	6604685-Rahulissar-G7-dmz-web-server	T1055 T1083	Defense Evasion, Privilege Escalation, ...	Common web attack.	6	31104
Dec 24, 2025 @ 06:00:13.4...	6604685-Rahulissar-G7-dmz-web-server	T1595.002	Reconnaissance	Multiple web server 400 error codes from same sou...	10	31151
Dec 24, 2025 @ 06:00:09.4...	6604685-Rahulissar-G7-dmz-web-server	T1595.002	Reconnaissance	Multiple web server 400 error codes from same sou...	10	31151
Dec 24, 2025 @ 04:20:25.0...	6604685-Rahulissar-G7-dmz-web-server	T1078	Defense Evasion, Persistence, Privileg...	PAM: Login session opened.	3	5501
Dec 24, 2025 @ 04:20:25.0...	6604685-Rahulissar-G7-dmz-web-server	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
Dec 24, 2025 @ 04:20:19.0...	6604685-Rahulissar-G7-dmz-web-server	T1078	Defense Evasion, Persistence, Privileg...	PAM: Login session opened.	3	5501
Dec 24, 2025 @ 04:20:19.0...	6604685-Rahulissar-G7-dmz-web-server	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
Dec 24, 2025 @ 04:20:13.0...	6604685-Rahulissar-G7-dmz-web-server	T1078	Defense Evasion, Persistence, Privileg...	PAM: Login session opened.	3	5501

Rows per page: 15

Purpose of Hardening

After analyzing SIEM logs generated during the Red Team attack phase, several misconfigurations and weak security controls were identified.
The objective of hardening was to reduce attack surface, prevent successful exploitation, and improve detection quality.

HARDENING MEASURES IMPLEMENTED

A. SSH HARDENING (VM1 & VM2)

✅ What was implemented

- Disabled root login over SSH
- Enforced key-based authentication
- Disabled password-based SSH login
- Restricted SSH access to SIEM server only

Commands Used

- sudo nano /etc/ssh/sshd_config

Changes:

- PermitRootLogin no
- PasswordAuthentication no
- PubkeyAuthentication yes

Restart SSH:

- sudo systemctl restart ssh

Why this was implemented

- Prevent SSH brute-force attacks
- Stop unauthorized root access
- Reduce credential-based compromise risk

B. FIREWALL CONFIGURATION (UFW)

✅ What was implemented

- Enabled UFW firewall
- Allowed SSH **only from SIEM VM**
- Allowed HTTP only on DMZ web server
- Denied all other inbound traffic

Commands Used

- sudo ufw default deny incoming
- sudo ufw default allow outgoing

Allow SSH only from SIEM:

- `sudo ufw allow from <SIEM_PRIVATE_IP> to any port 22`

Allow HTTP (VM2 only):

- sudo ufw allow 80

Enable firewall:

- sudo ufw enable

Why this was implemented

- Prevent direct external access to internal servers
- Stop unauthorized lateral movement
- Enforce network segmentation

C. NETWORK SEGMENTATION (Azure NSG)

✅ What was implemented

- Restricted DMZ → Internal subnet traffic
- Allowed SSH to VM1 only from SIEM subnet
- Blocked public SSH to VM1

Why this was implemented

- Prevent attackers from jumping from web server to internal server
- Enforce Zero Trust model

D. APACHE / NGINX HARDENING (VM2)

✅ What was implemented

- Disabled directory listing
- Enabled detailed access and error logging
- Hid server version information

Commands Used

- `sudo nano /etc/apache2/apache2.conf`
- `ServerTokens Prod`
- `ServerSignature Off`

Disable directory listing:

- `sudo a2dismod autoindex`
- `sudo systemctl restart apache2`

Why this was implemented

- Prevent directory enumeration attacks
- Reduce information leakage
- Improve forensic logging

BEFORE HARDENING (Observed in SIEM)

Event	Evidence
SSH brute force attempts	Multiple auth failures

Web enumeration	HTTP 400 bursts
Privilege escalation	Repeated sudo events
No access restriction	Public SSH allowed

Impact:

- High noise
- Easy attacker access
- Weak prevention

SECURITY POSTURE IMPROVEMENT SUMMARY

Area	Before	After
SSH Security	Weak	Hardened
Firewall	Disabled	Enabled
Network Segmentation	None	Enforced
Logging	Basic	Advanced
Attack Visibility	Low	High

CONCLUSION

The applied hardening measures significantly reduced the system’s exposure to common attack techniques. Repeated attack attempts that previously generated high-severity alerts were successfully blocked or detected with clearer indicators. This validates the effectiveness of the implemented security controls and demonstrates measurable improvement in the organization’s security posture.