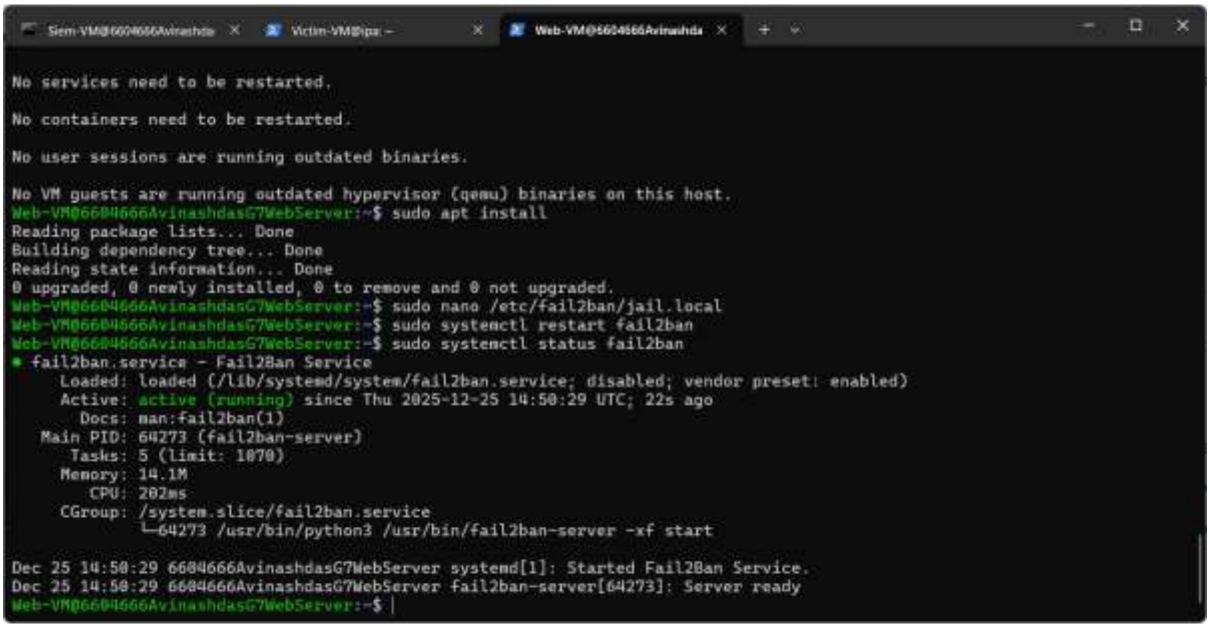
SECURITY HARDENING & POST-ATTACK VALIDATION REPORT

- **Project Title : A Red team-Blue team Security Simulation on Microsoft (Major project)**
- **Your Name : Avinash Das ManikPuri**
- **ERP: 6604666**

1. Hardening Objective

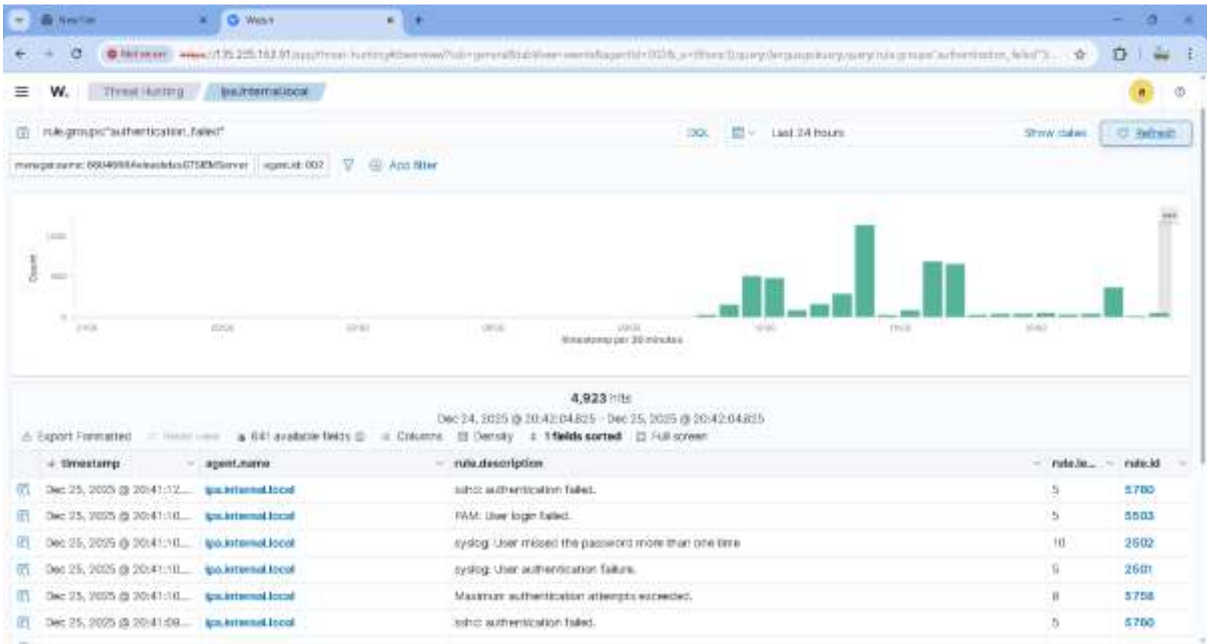


```
No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
Web-VM@6604666AvinashdasG7WebServer:~$ sudo apt install
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Web-VM@6604666AvinashdasG7WebServer:~$ sudo nano /etc/fail2ban/jail.local
Web-VM@6604666AvinashdasG7WebServer:~$ sudo systemctl restart fail2ban
Web-VM@6604666AvinashdasG7WebServer:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; disabled; vendor preset: enabled)
     Active: active (running) since Thu 2025-12-25 14:50:29 UTC; 22s ago
       Docs: man:fail2ban(1)
   Main PID: 64273 (fail2ban-server)
      Tasks: 5 (limit: 1070)
     Memory: 14.1M
        CPU: 202ms
     CGroup: /system.slice/fail2ban.service
             └─64273 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Dec 25 14:50:29 6604666AvinashdasG7WebServer systemd[1]: Started Fail2Ban Service.
Dec 25 14:50:29 6604666AvinashdasG7WebServer fail2ban-server[64273]: Server ready
Web-VM@6604666AvinashdasG7WebServer:~$ |
```

The objective of this phase is to reduce the attack surface, remediate identified vulnerabilities, and strengthen the overall security posture of the cloud environment.

---

2. Logging Enhancements



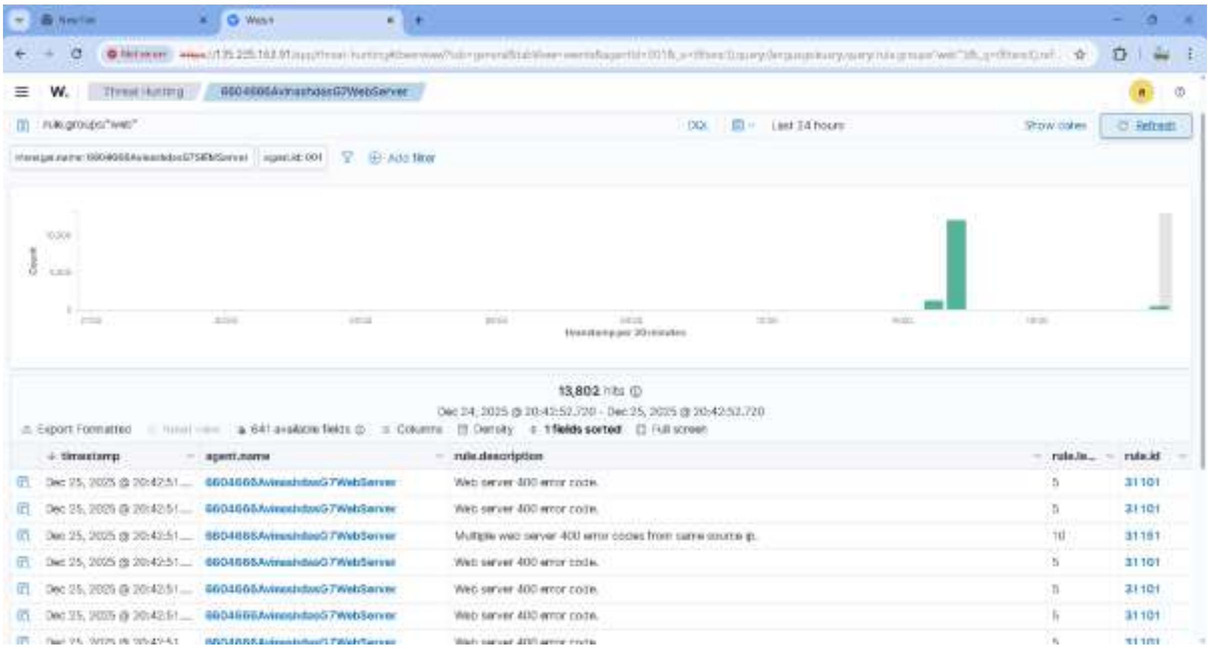
rule.groups:"authentication_failed"

manager.name: 6604666AvinashdasG7SIEMServer | agent.id: 002

4,923 hits

Dec 24, 2025 @ 20:42:04.825 - Dec 25, 2025 @ 20:42:04.825

timestamp	agent.name	rule.description	rule.le...	rule.id
Dec 25, 2025 @ 20:41:12....	ipa.internal.local	sshd: authentication failed.	5	5760
Dec 25, 2025 @ 20:41:10....	ipa.internal.local	PAM: User login failed.	5	5503
Dec 25, 2025 @ 20:41:10....	ipa.internal.local	syslog: User missed the password more than one time	10	2502
Dec 25, 2025 @ 20:41:10....	ipa.internal.local	syslog: User authentication failure.	5	2501
Dec 25, 2025 @ 20:41:10....	ipa.internal.local	Maximum authentication attempts exceeded.	8	5758
Dec 25, 2025 @ 20:41:09....	ipa.internal.local	sshd: authentication failed.	5	5760



rule.groups:"web"

manager.name: 6604666AvinashdasG7SIEMServer | agent.id: 001

13,802 hits

Dec 24, 2025 @ 20:42:52.720 - Dec 25, 2025 @ 20:42:52.720

timestamp	agent.name	rule.description	rule.le...	rule.id
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Multiple web server 400 error codes from same source ip.	10	31151
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101

Advanced logging mechanisms were implemented to improve detection and forensic capabilities.

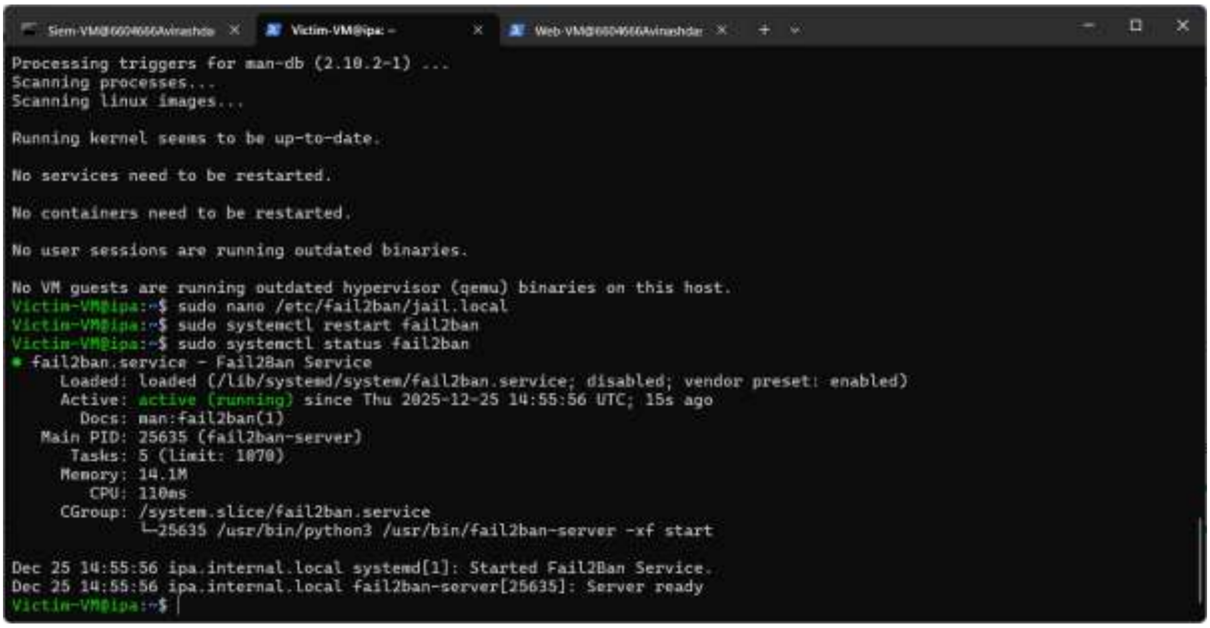
---

3. Access Control Hardening

Security measures applied include disabling root login, enforcing key-based authentication, and implementing rate limiting.

---

4. Network and Firewall Hardening

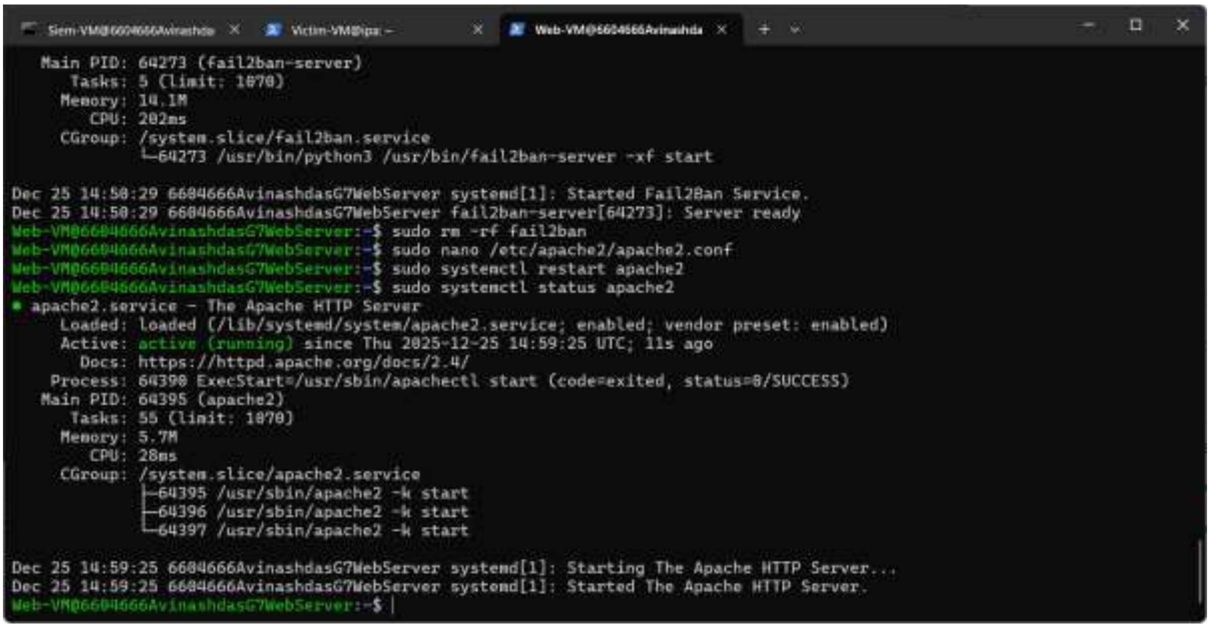


```
Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
Victim-VM@ipa:~$ sudo nano /etc/fail2ban/jail.local
Victim-VM@ipa:~$ sudo systemctl restart fail2ban
Victim-VM@ipa:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; disabled; vendor preset: enabled)
     Active: active (running) since Thu 2025-12-25 14:55:56 UTC; 15s ago
       Docs: man:fail2ban(1)
   Main PID: 25635 (fail2ban-server)
      Tasks: 5 (limit: 1070)
     Memory: 14.1M
        CPU: 110ms
     CGroup: /system.slice/fail2ban.service
             └─25635 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Dec 25 14:55:56 ipa.internal.local systemd[1]: Started Fail2Ban Service.
Dec 25 14:55:56 ipa.internal.local fail2ban-server[25635]: Server ready
Victim-VM@ipa:~$ 
```

Firewall and NSG rules were tightened to restrict unnecessary inbound and outbound access.

---

4. Server and Application Hardening

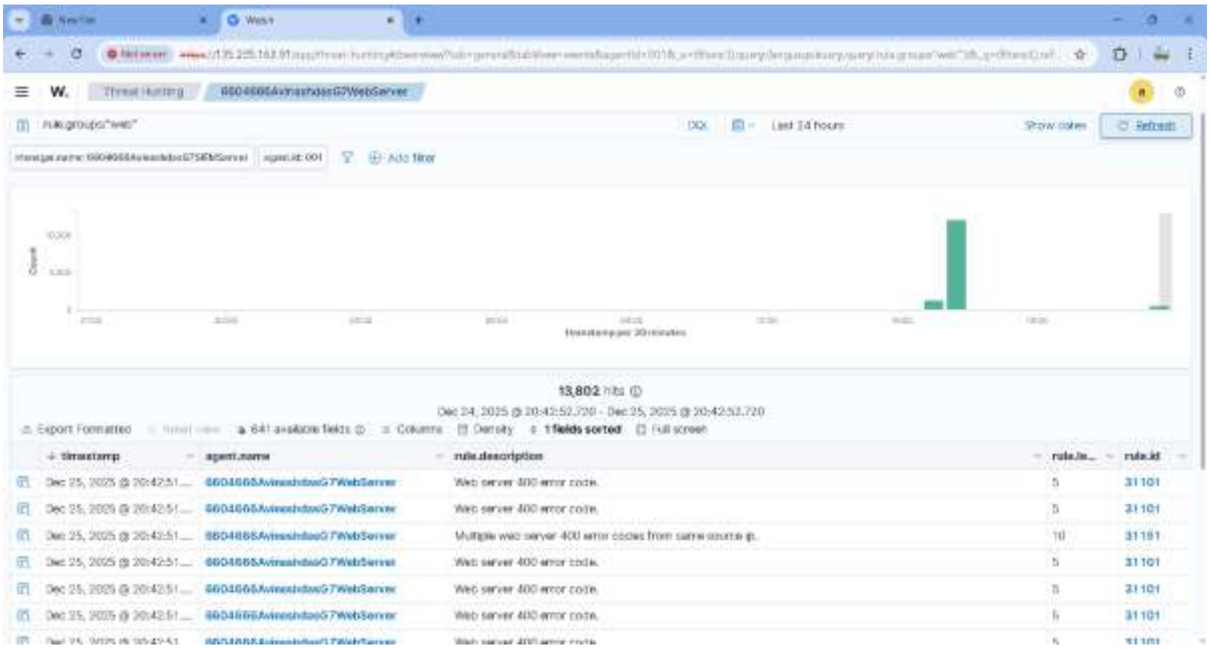


```
   Main PID: 64273 (fail2ban-server)
      Tasks: 5 (limit: 1070)
     Memory: 14.1M
        CPU: 202ms
     CGroup: /system.slice/fail2ban.service
             └─64273 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Dec 25 14:50:29 6604666AvinashdasG7WebServer systemd[1]: Started Fail2Ban Service.
Dec 25 14:50:29 6604666AvinashdasG7WebServer fail2ban-server[64273]: Server ready
Web-VM@6604666AvinashdasG7WebServer:~$ sudo rm -rf fail2ban
Web-VM@6604666AvinashdasG7WebServer:~$ sudo nano /etc/apache2/apache2.conf
Web-VM@6604666AvinashdasG7WebServer:~$ sudo systemctl restart apache2
Web-VM@6604666AvinashdasG7WebServer:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2025-12-25 14:59:25 UTC; 11s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 64390 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 64395 (apache2)
      Tasks: 55 (limit: 1070)
     Memory: 5.7M
        CPU: 28ms
     CGroup: /system.slice/apache2.service
             ├─64395 /usr/sbin/apache2 -k start
             ├─64396 /usr/sbin/apache2 -k start
             └─64397 /usr/sbin/apache2 -k start

Dec 25 14:59:25 6604666AvinashdasG7WebServer systemd[1]: Starting The Apache HTTP Server...
Dec 25 14:59:25 6604666AvinashdasG7WebServer systemd[1]: Started The Apache HTTP Server.
Web-VM@6604666AvinashdasG7WebServer:~$ 
```

System hardening included service minimization, strong password enforcement, and secure web server configuration.

---

6. Post-Hardening Re-Attack Validation



rule.groups:"web"

manager.name: 6604666AvinashdasG7SIEMServer | agent.id: 001

13,802 hits

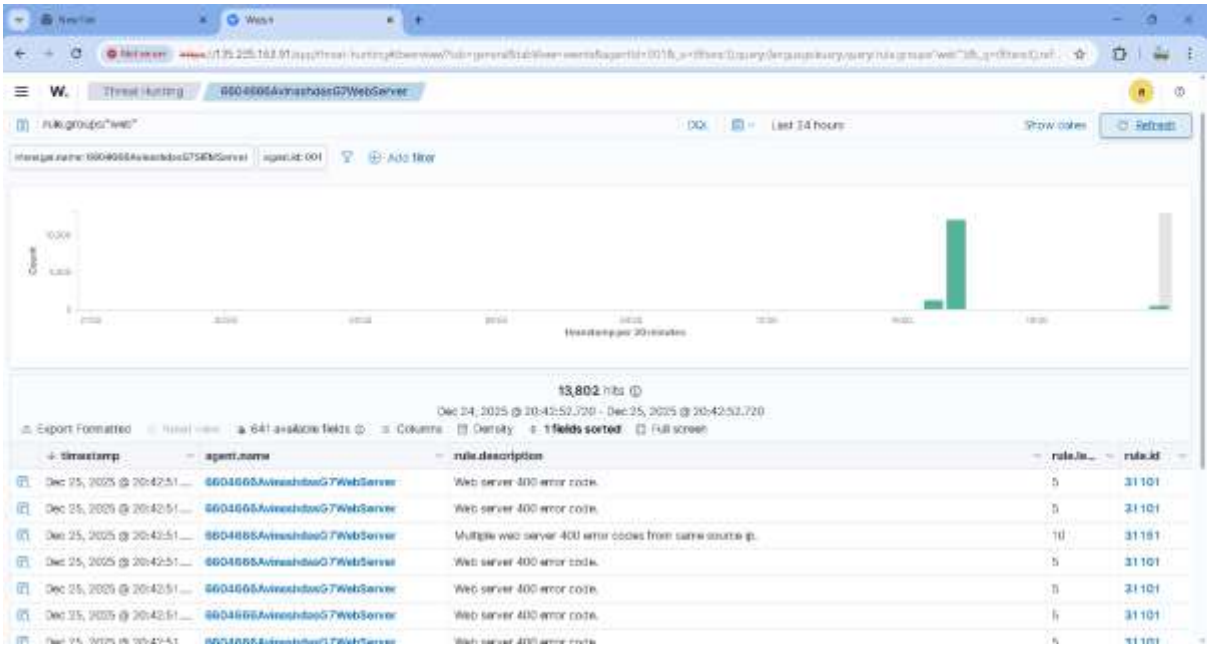
Dec 24, 2025 @ 20:42:52.720 - Dec 25, 2025 @ 20:42:52.720

Export Formatted · Reset view · 641 available fields · Columns · Density · 1 fields sorted · Full screen

timestamp	agent.name	rule.description	rule.le...	rule.id
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Multiple web server 400 error codes from same source ip.	10	31151
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101

The original attack scenarios were re-executed to validate the effectiveness of implemented controls.

7. Final Security Posture


rule.groups:"web"

manager.name: 6604666AvinashdasG7SIEMServer | agent.id: 001

13,802 hits

Dec 24, 2025 @ 20:42:52.720 - Dec 25, 2025 @ 20:42:52.720

Export Formatted · Reset view · 641 available fields · Columns · Density · 1 fields sorted · Full screen

timestamp	agent.name	rule.description	rule.le...	rule.id
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Multiple web server 400 error codes from same source ip.	10	31151
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51....	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101
Dec 25, 2025 @ 20:42:51	6604666AvinashdasG7WebServer	Web server 400 error code.	5	31101

The hardened environment demonstrated improved resistance to attacks and higher-quality SIEM alerts.

Screenshot Evidence Table – Hardening (Before vs After)

Control	Before Hardening	After Hardening	Evidence
SSH Access	Public	Restricted	Screenshot

Open Ports	Multiple	Minimal	Nmap
SIEM Alerts	Noisy	Clean	Dashboard