

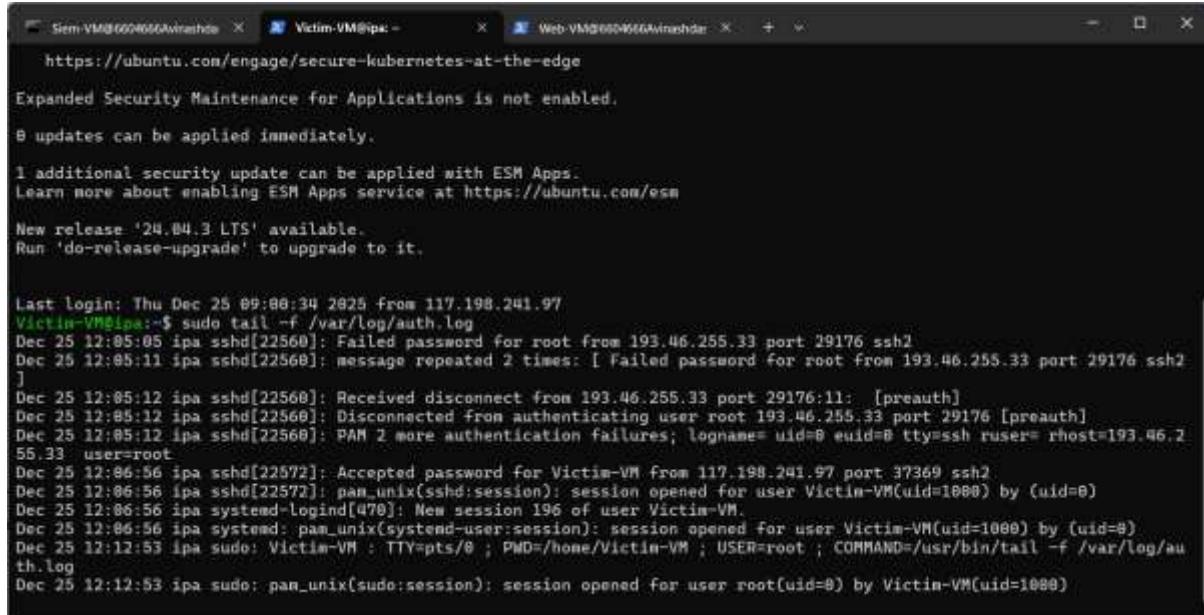
BLUE TEAM INVESTIGATION & DETECTION REPORT

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

1. Blue Team Objective

The objective of the Blue Team phase is to detect, analyze, and investigate malicious activities using centralized logging and SIEM-based monitoring.

2. Log Collection and SIEM Setup



A screenshot of a terminal window titled 'Victim-VM@ip-172-16-0-1:~\$'. The window displays a log of system events from a Ubuntu system. The log shows multiple failed password attempts for root via SSH, successful logins by the user 'Victim-VM' (uid=1000), and a user named 'root' (uid=0) running a command to tail the auth.log file. The log entries are as follows:

```
https://ubuntu.com/engage/secure-kubernetes-at-the-edge
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Dec 25 09:00:34 2025 from 117.198.241.97
Victim-VM@ip-172-16-0-1:~$ sudo tail -f /var/log/auth.log
Dec 25 12:05:05 ipa sshd[22568]: Failed password for root from 193.46.255.33 port 29176 ssh2
Dec 25 12:05:11 ipa sshd[22568]: message repeated 2 times: [ Failed password for root from 193.46.255.33 port 29176 ssh2 ]
Dec 25 12:05:12 ipa sshd[22568]: Received disconnect from 193.46.255.33 port 29176:11: [preauth]
Dec 25 12:05:12 ipa sshd[22568]: Disconnected from authenticating user root 193.46.255.33 port 29176 [preauth]
Dec 25 12:05:12 ipa sshd[22568]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=193.46.255.33 users=root
Dec 25 12:06:56 ipa sshd[22572]: Accepted password for Victim-VM from 117.198.241.97 port 37369 ssh2
Dec 25 12:06:56 ipa sshd[22572]: pam_unix(sshd:session): session opened for user Victim-VM(uid=1000) by (uid=0)
Dec 25 12:06:56 ipa systemd-logind[479]: New session 196 of user Victim-VM.
Dec 25 12:06:56 ipa systemd: pam_unix(systemd-user:session): session opened for user Victim-VM(uid=1000) by (uid=0)
Dec 25 12:12:53 ipa sudo: Victim-VM : TTY=pts/0 ; PWD=/home/Victim-VM ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
Dec 25 12:12:53 ipa sudo: pam_unix(sudo:session): session opened for user root(uid=0) by Victim-VM(uid=1000)
```

```

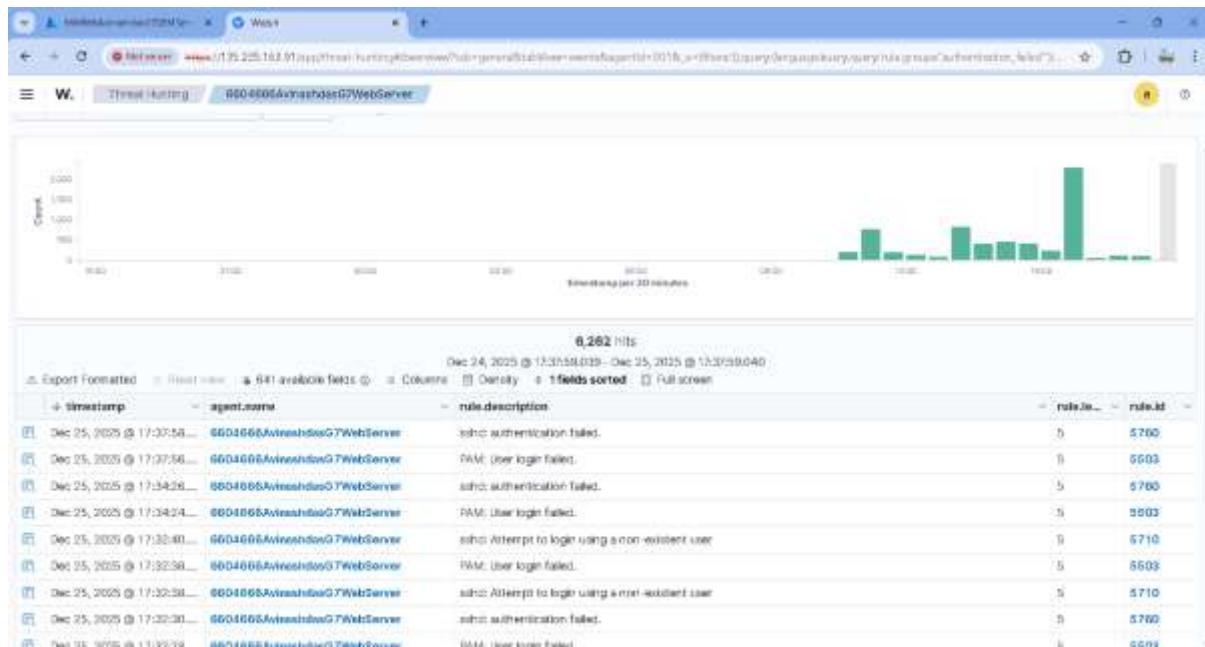
Sem-VM@660466Avinashdas: ~ Victim-VM@ps: ~ Web-VM@660466Avinashdas: ~ + ×
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

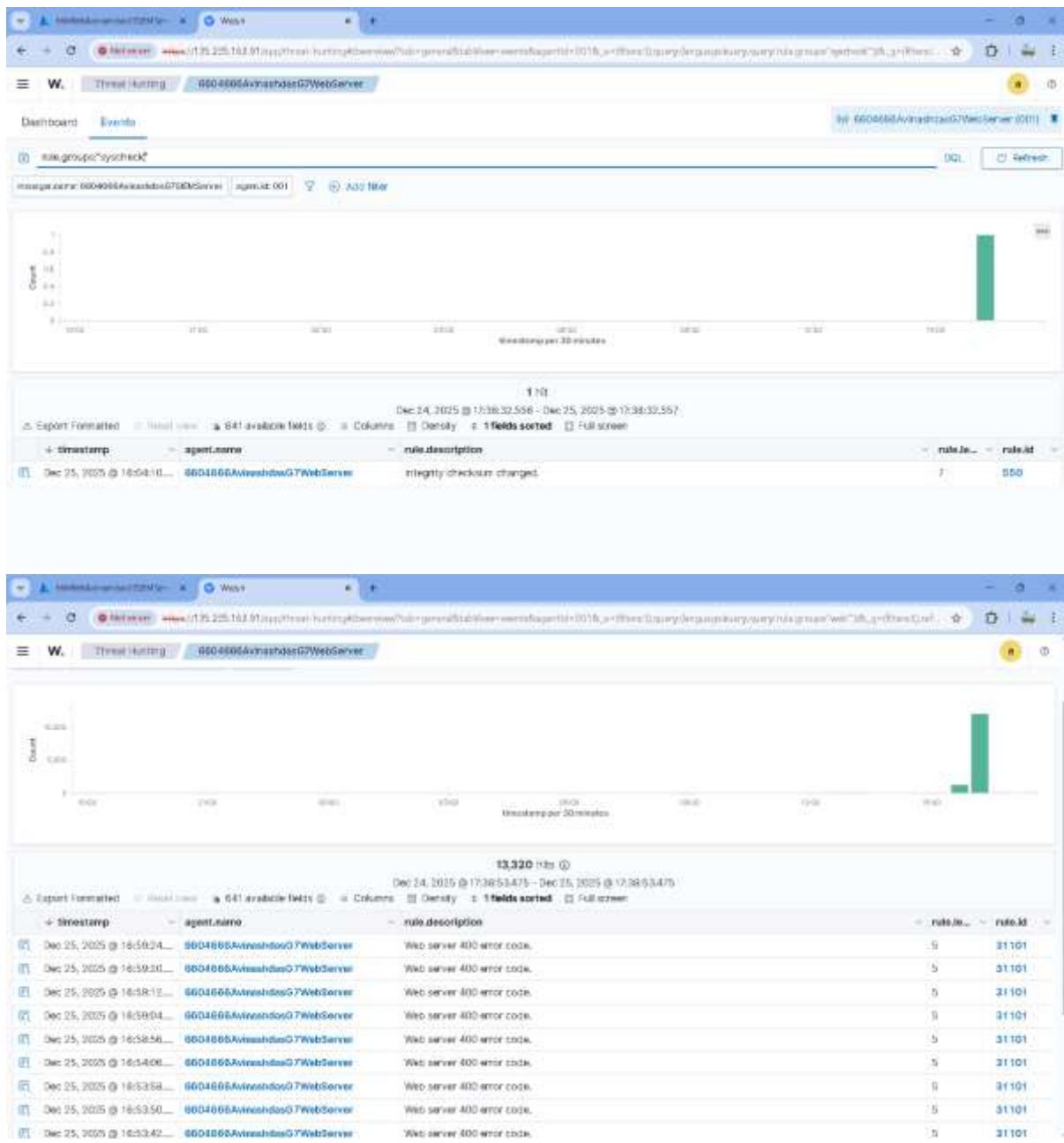
New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Dec 25 08:47:09 2025 from 117.198.241.97
Web-VM@660466Avinashdas$ sudo tail -f /var/log/apache2/access.log
87.121.84.154 - - [25/Dec/2025:11:23:48 +0000] "POST /_next/server HTTP/1.1" 404 456 "-" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.6998.135 Mobile Safari/537.36"
87.121.84.154 - - [25/Dec/2025:11:23:56 +0000] "POST /app HTTP/1.1" 404 456 "-" "Mozilla/5.0 (X11; CrOS x86_64 14541.0.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.8.0 Safari/537.36"
87.121.84.154 - - [25/Dec/2025:11:24:05 +0000] "POST /api/route HTTP/1.1" 404 456 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136"
87.121.84.154 - - [25/Dec/2025:11:28:58 +0000] "POST / HTTP/1.1" 200 415 "-" "Mozilla/5.0 (Linux; Android 14; SM-F9560 B build/UPRA.231005.007; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/127.0.6533.183 Mobile Safari/537.36"
87.121.84.154 - - [25/Dec/2025:11:28:55 +0000] "POST /_next/server HTTP/1.1" 404 456 "-" "Mozilla/5.0 (Linux; U; Android 4.2.2; he-il; NEO-X5-116A Build/JQ039) AppleWebKit/534.38 (KHTML, like Gecko) Version/4.0 Safari/534.38"
87.121.84.154 - - [25/Dec/2025:11:29:02 +0000] "POST /api/route HTTP/1.1" 404 456 "-" "Mozilla/5.0 (Linux; Android 9; AFTMMST22 Build/P57233; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/88.0.4324.152 Mobile Safari/537.36"
87.121.84.154 - - [25/Dec/2025:11:29:11 +0000] "POST /_next/server HTTP/1.1" 404 456 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136"
87.121.84.154 - - [25/Dec/2025:11:29:18 +0000] "POST /app HTTP/1.1" 404 456 "-" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.6998.135 Mobile Safari/537.36"
87.121.84.154 - - [25/Dec/2025:11:29:23 +0000] "POST /api/route HTTP/1.1" 404 456 "-" "Mozilla/5.0 (Linux; Android 9; AFTMMST22 Build/P57233; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/88.0.4324.152 Mobile Safari/537.36"
204.76.203.219 - - [25/Dec/2025:11:39:33 +0000] "GET / HTTP/1.1" 200 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4430.85 Safari/537.36 Edg/90.0.818.46"
```

Logs were collected from all virtual machines and forwarded to the SIEM platform, including system logs, authentication logs, audit logs, and web server logs.

3. Security Event Analysis





The SIEM was used to identify abnormal patterns such as repeated failed login attempts, suspicious web requests, and enumeration behavior.

4. Indicators of Compromise (IOC)

Identified indicators of compromise included:

- Attacker IP addresses
- Brute-force authentication patterns
- Malicious payloads in HTTP requests

5. Root Cause Analysis

The investigation revealed misconfigurations related to authentication policies, network access rules, and insufficient logging controls.

Screenshot Evidence Table – Blue Team Analysis

Screenshot No.	Log Type	SIEM Alert	Observation
1	Auth Logs	Brute Force Alert	Multiple failures
2	Web Logs	SQLi Attempt	Malicious payload
3	Audit Logs	Privilege Attempt	Unauthorized access
