BLUE TEAM INVESTIGATION & DETECTION REPORT

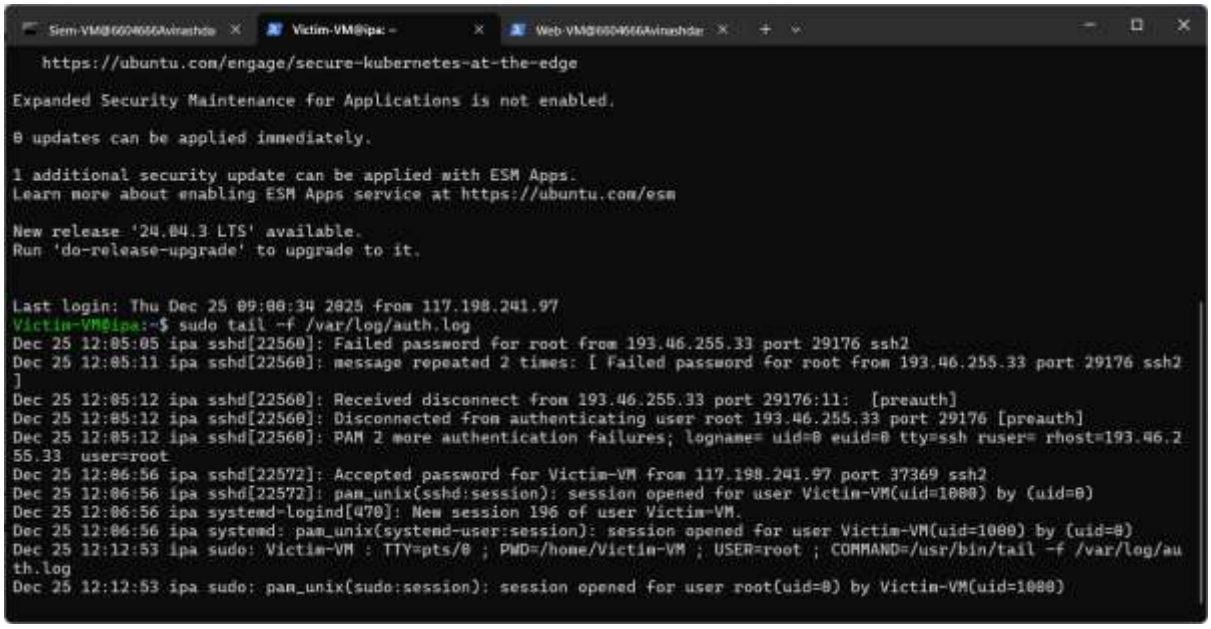
- **Project Title : A Red team-Blue team Security Simulation on Microsoft (Major project)**
- **Your Name : Avinash Das ManikPuri**
- **ERP: 6604666**

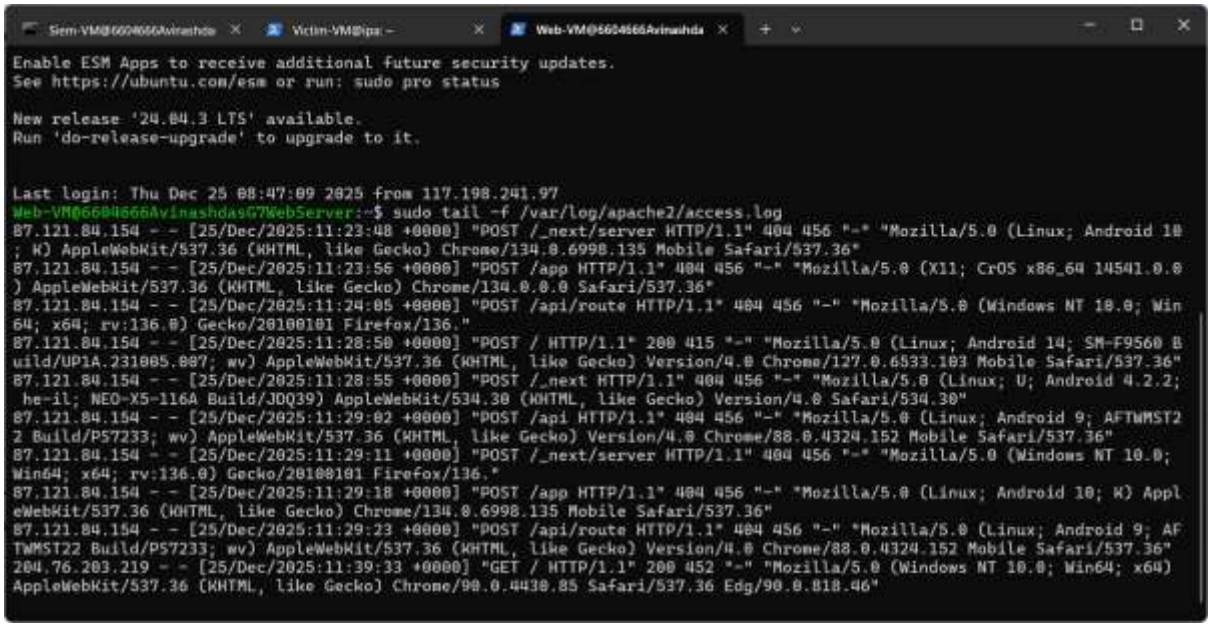
1. Blue Team Objective

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

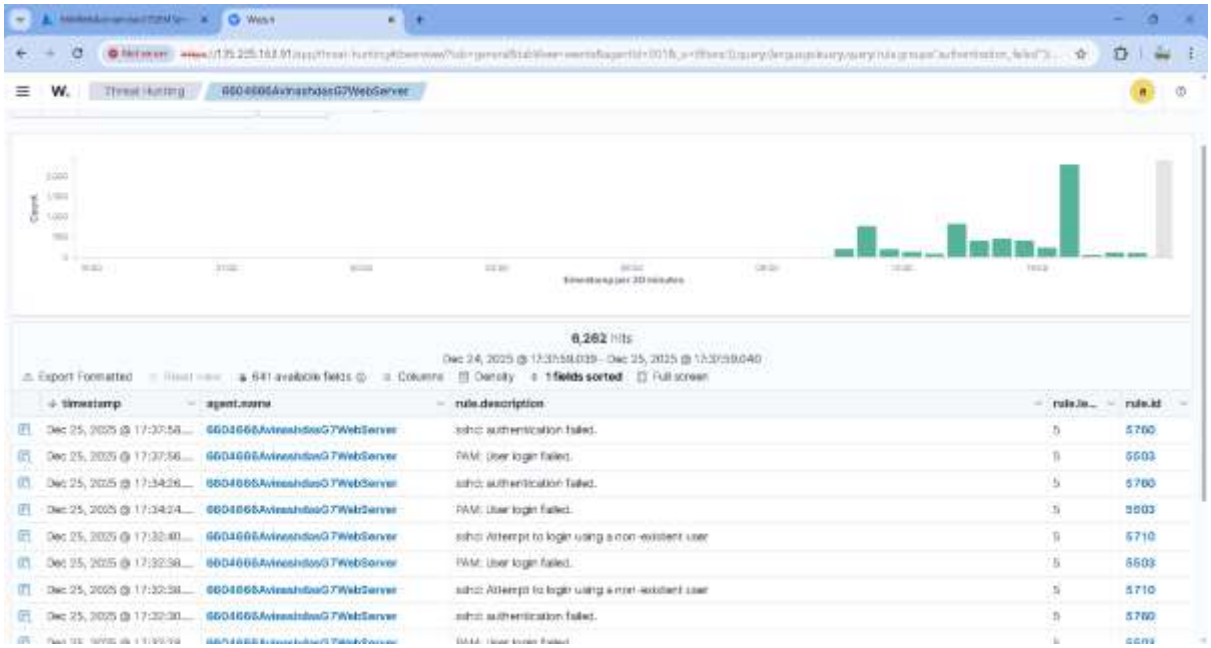


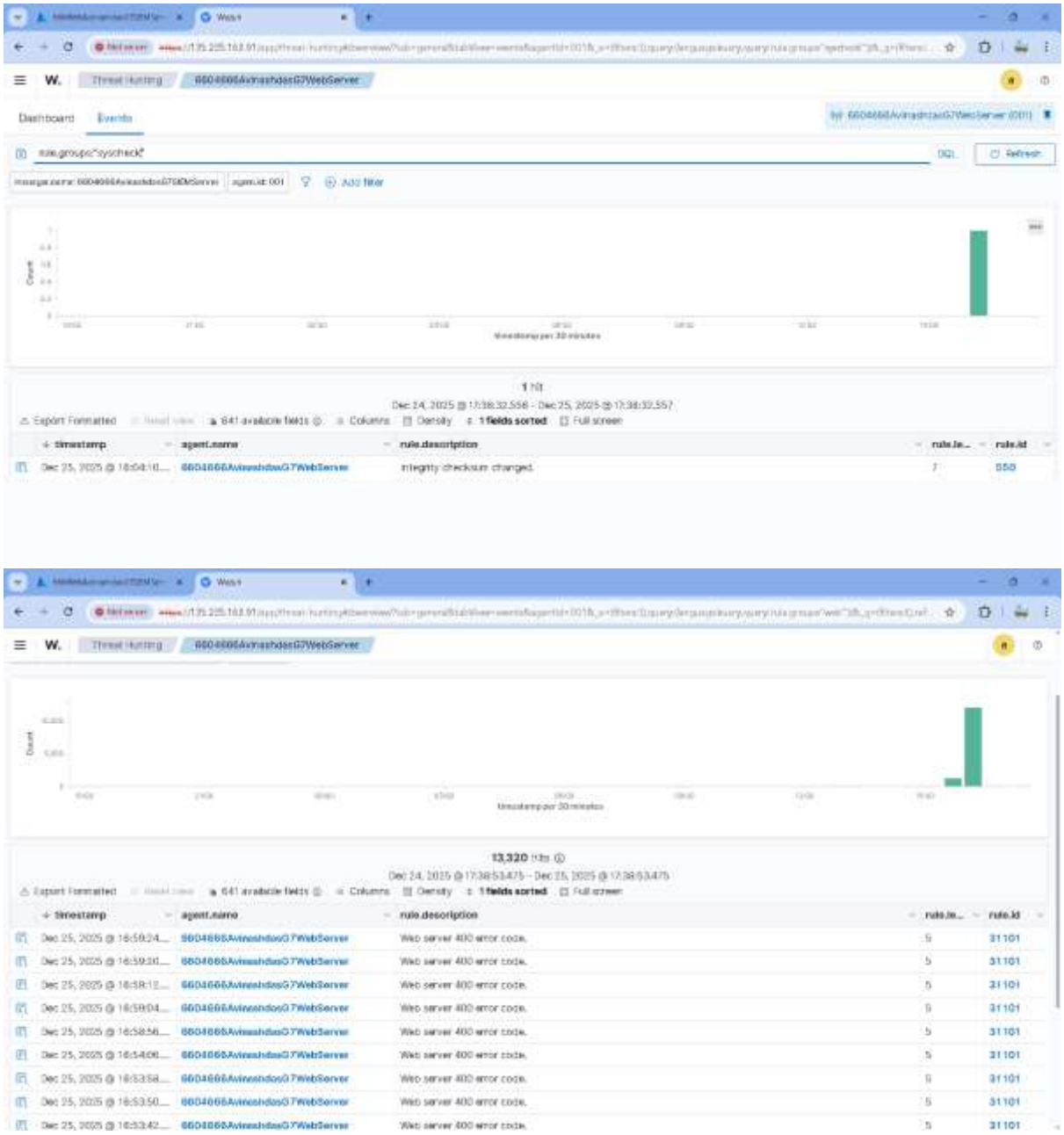


Logs were collected from all virtual machines and forwarded to the SIEM platform, including system logs, authentication logs, audit logs, and web server logs.

---

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
