Tittle : The Case of the Knocking Neighbor and the Unlocked Door

Simulated Incident Report by Shewag Bhattarai.

19th June 2025

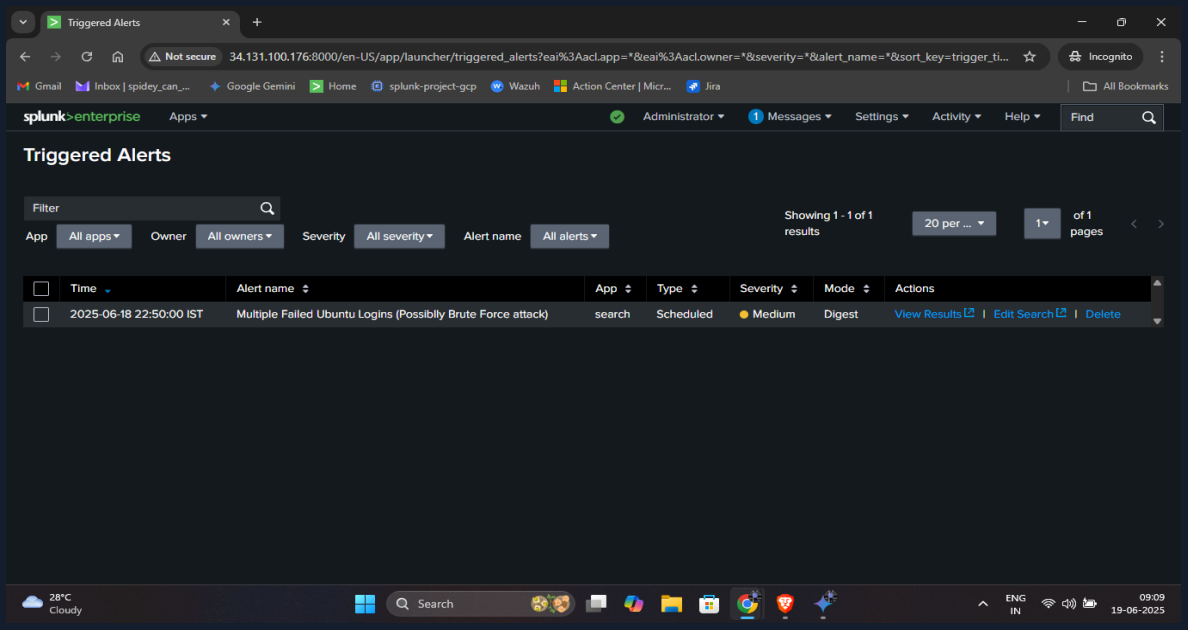
Important Disclaimer

This document represents a simulated cybersecurity incident report. All activities described herein, including the "attack," detection, investigation, and mitigation, were performed in a controlled personal lab environment specifically for educational and demonstration purposes. This is not a report of a real-world security breach or incident that occurred in a production environment. Any references to specific systems, users, or timelines are illustrative for the simulation and do not pertain to real-world operational infrastructure or events. The primary goal of this exercise and report is to showcase practical skills in cybersecurity incident response, detection engineering, and SIEM/HIDS utilization.

Index

Simulated Incident Report

Executive Summary



- Incident ID: INC-20250619-002
- Incident Severity: Medium (P3) - *Simulated Incident, High if Real*
- Incident Status: Contained & Remediated
- Incident Overview:On June 18, 2025, a scheduled alert from Splunk identified suspicious SSH activity suggestive of a brute-force attack targeting an Ubuntu virtual machine within the isolated Home SOC Lab. Subsequent investigation confirmed that the brute-force attempt was successful, resulting in unauthorized SSH access to the system. Further forensic analysis uncovered the creation of a new, unauthorized user account, indicating an effort by the attacker to establish persistence. This simulated incident underscores both the effectiveness of SIEM-based detection using Splunk and Wazuh, and the essential role of a structured incident response process in identifying, analyzing, and mitigating unauthorized access events.
- Key Findings:The incident analysis revealed that the SSH service running on the targeted Ubuntu virtual machine was successfully exploited by the

attacker. The root cause was identified as weak password hygiene on a legitimate user account, which allowed the attacker to gain access via a brute-force authentication attack. The exposed SSH service, accessible from the attacker’s Kali Linux VM without adequate network restrictions or rate limiting, further enabled these attempts. Log evidence confirmed numerous failed SSH login attempts preceding a successful authentication. Following the compromise, the attacker created a new unauthorized user account, indicating an intentional effort to establish persistence on the system. These findings highlight critical security gaps in access control, credential management, and network exposure.

Immediate Actions:

Upon detection and initial confirmation of the successful brute-force and unauthorized access, immediate containment measures were initiated to limit the attacker's access and prevent further damage.

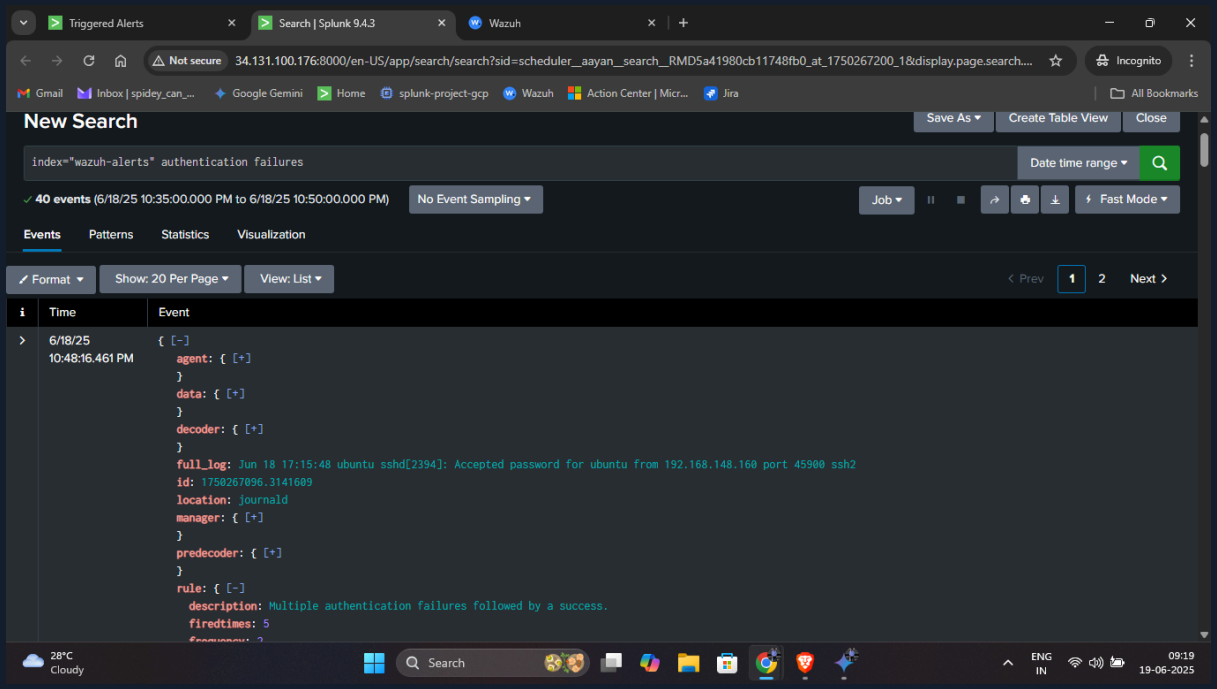
- **Compromised User Password Change:** The password for the compromised `ubuntu` user account was immediately changed to a strong, unique value.
- **Attacker IP Blocking:** The attacker's source IP address (`192.168.148.160`) was explicitly denied access to SSH (port 22) on the Ubuntu VM's firewall (UFW), effectively severing the current connection and preventing immediate re-entry from that IP.

Stakeholder Impact:

In the context of Cybersonick, this simulated incident carries several potential impacts on various stakeholders, emphasizing the importance of robust security measures and swift response.

- **Internal Security Teams (Cybersonick SOC):**
  - **Workload Increase:** Immediate increase in workload for the SOC team for detection, investigation, and response.
  - **Skill Validation:** Provided a critical hands-on opportunity to validate skills in SIEM analysis (Splunk, Wazuh), incident correlation, and executing containment/eradication procedures.
  - **Process Improvement:** Highlighted areas for potential improvement in detection rules and response playbooks for SSH-based attacks.
- **System Owners/Administrators:**
  - **System Integrity:** Direct impact on the integrity of the Ubuntu VM's user management system due to the creation of an unauthorized user.
  - **Vulnerability Remediation:** Required immediate action to patch vulnerabilities (weak password, open SSH configuration) and strengthen system security.
  - **Downtime (Potential):** In a real scenario, could lead to a temporary isolation or shutdown of the affected VM for forensic analysis, impacting service availability.
- **Users (e.g., `ubuntu` user):**
  - **Account Compromise:** The `ubuntu` user account was compromised, necessitating an immediate password change and potential review of its privileges.
  - **Security Awareness:** Underscored the importance of strong password practices and vigilance against social engineering/phishing.
- **Cybersonick's Overall Security Posture:**
  - **Validated Controls:** Demonstrated that the deployed SIEM and HIDS solutions are effective in detecting critical unauthorized access and persistence events.
  - **Identified Gaps:** Highlighted areas where security controls (e.g., automated brute-force prevention, stronger password policies) could be enhanced to reduce the attack surface.
  - **Reputation (Simulated):** If this were a real production environment, it would pose a significant reputational risk to Cybersonick, impacting trust from clients and partners.

Technical Analysis



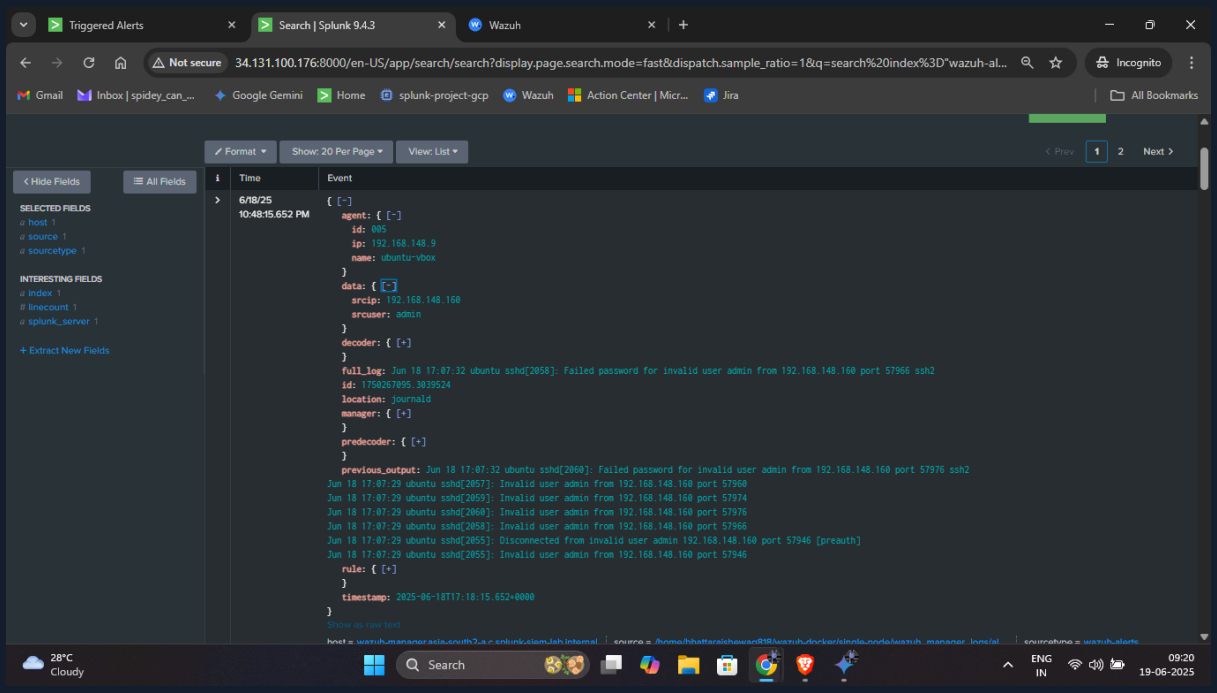
Affected Systems & Data

The primary affected system was the **Ubuntu VM**, acting as the target host within the isolated Home SOC Lab. This virtual machine's SSH service was the direct target of the attack, and its user management system was compromised to establish persistence.

- **Target Host:** Ubuntu VM
  - **IP Address:** `192.168.148.9` (Confirmed at time of attack, though subject to DHCP changes in a non-static lab setup).
  - **Hostname:** `ubuntu` (as identified in logs)
  - **Compromised Service:** SSH (Port 22/TCP)
  - **Compromised User Account:** `ubuntu` (default user on the VM)
- **Attacker Host:** Kali Linux VM
  - **IP Address:** `192.168.148.160` (Source IP of attack activities)
- **Data Impacted:** User authentication data, system user accounts. No evidence of data exfiltration was observed or performed in this simulated

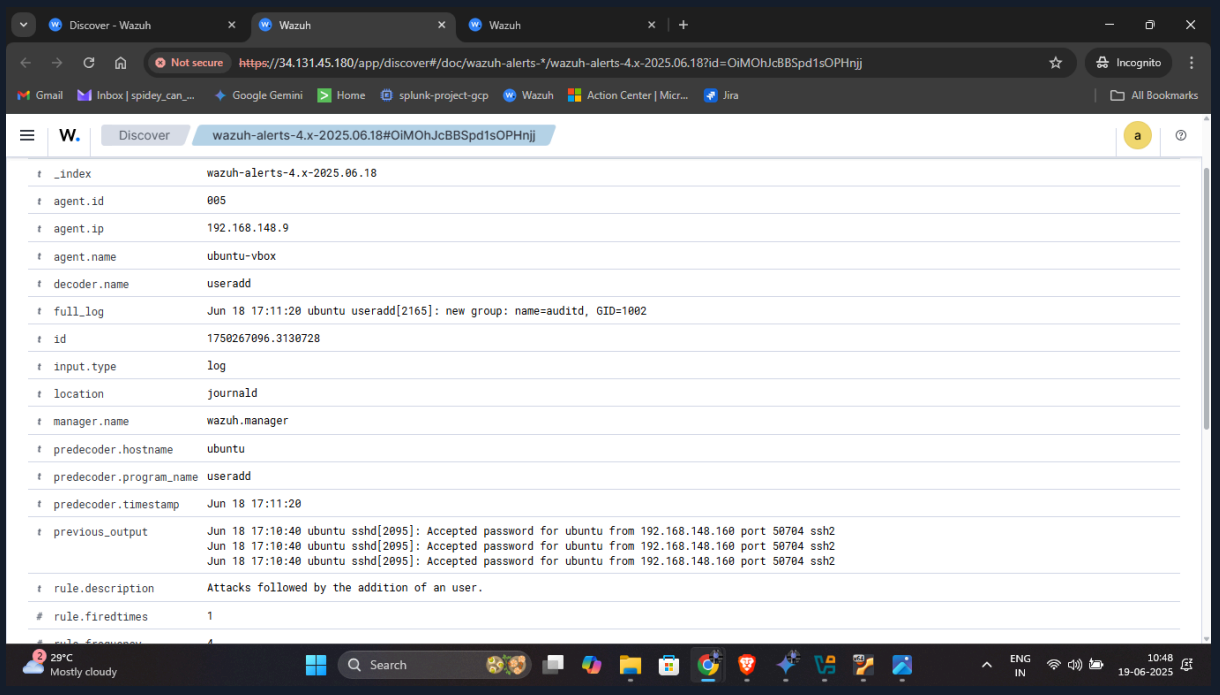
scenario, however, the capability for such an action was present post-compromise.

- **Evidence Sources & Analysis**



The investigation relied heavily on logs and alerts generated by the Security Information and Event Management (SIEM) systems, Splunk Enterprise and Wazuh HIDS, deployed within the Home SOC Lab.

- **Splunk Enterprise (SIEM):**
  - **Alert Triggered:** `Multiple Failed Ubuntu Logins (Possibly Brute Force attack)`
    - **Timestamp:** `2025-06-18 22:50:00 IST`
    - **Severity:** Medium (as configured)
    - **Type:** Scheduled Search
  - **Log Data Source:** `index="ubuntu_vbox" sourcetype=linux:syslog`
  - **Key Splunk Findings:**
    - Numerous log entries indicating "Failed password for" attempts originating from `192.168.148.160`.

        - A critical log entry confirming "Accepted password for ubuntu from 192.168.148.160" at `Jun 18 17:10:40` (Ubuntu VM time, correlation to IST was performed for report).
        - A subsequent log entry indicating `useradd` activity for the user `auditd` at `Jun 18 17:11:20` (Ubuntu VM time).
- **Wazuh HIDS:**
    - 

    - **Agent on Ubuntu VM:** `agent.name: ubuntu-vbox` (`agent.id: 005`)
    - **Manager:** `wazuh.manager`
    - **Key Wazuh Alerts/Rules Triggered:**
        - `rule.id: 5710` (sshd: Attempt to login using a non-existent user / Multiple authentication failures) - triggered repeatedly.
        - `rule.id: 100001` (Custom SSH brute force alert) - triggered by high volume of failed logins.
        - `rule.id: 5712` (sshd: Authentication success) - triggered upon successful login.
        - `rule.id: 5901` (User added to the system) - triggered for the creation of the `auditd` user.

Indicators of Compromise (IoCs)

The following Indicators of Compromise (IoCs) were identified during the investigation:

- **Source IP Address:** `192.168.148.160` (Attacker's Kali Linux VM)
- **Compromised Account:** `ubuntu` (on the target VM)
- **Unauthorized User Account:** `auditd` (created by attacker for persistence)
- **Malicious Activity:** SSH brute-force attempts.
- **Post-Exploitation Activity:** New user creation via `useradd` command.

Root Cause Analysis

The root cause of this incident was a combination of weak security configurations and insufficient authentication policies.

- **Primary Root Cause: Weak password hygiene** for the `ubuntu` user account. This allowed the brute-force attack to eventually succeed despite multiple failed attempts.
- **Contributing Factor 1: SSH service exposed to the attacker's network segment** (or broadly accessible from `192.168.148.160`) without robust rate-limiting or IP-based access controls (beyond basic firewall blocking implemented post-attack). This facilitated the sustained brute-force attempt.
- **Contributing Factor 2:** Lack of immediate account lockout policies for failed login attempts, which would have automatically disabled the `ubuntu` account after a certain number of incorrect password attempts, mitigating the brute-force attack.

Nature of the Attack

This incident represents a **credential stuffing/brute-force attack** followed by **unauthorized access and persistence establishment.**

- **Phase 1: Reconnaissance (Simulated):** The attacker (Kali VM) performed initial scans to identify the SSH service (port 22) on the Ubuntu VM.

- **Phase 2: Brute Force:** A dictionary-based brute-force attack was launched against the SSH service using `Hydra`, targeting common usernames including `ubuntu`.
- **Phase 3: Unauthorized Access:** The brute-force attack successfully compromised the `ubuntu` user's credentials, allowing the attacker to establish an unauthorized SSH session.
- **Phase 4: Persistence:** Immediately following unauthorized access, the attacker created a new system user named `auditd` (`sudo useradd -m -s /bin/bash auditd`). This action aimed to establish a backdoor for continued access, even if the primary compromised account's password was changed or if the attacker was logged out.

Impact Analysis

The impact of this incident is significant, moving beyond mere detection of an attack attempt to confirmed compromise and persistence.

- **Confidentiality:** Compromised authentication credentials and the creation of a new user account could lead to unauthorized access to sensitive data on the Ubuntu VM. The attacker had full access to the system.
- **Integrity:** The creation of a new user (`auditd`) directly altered the integrity of the system's user management and security posture. Other system configurations or data could have been altered had the attack progressed further.
- **Availability:** While direct denial-of-service was not observed, a compromised system could be used to launch attacks against other internal or external systems, potentially impacting network availability. Resources could also be consumed by malicious processes.

- **Reputation/Compliance (Simulated):** In a real-world scenario, such a breach would carry significant reputational damage and potential compliance violations depending on the data stored on the system.
- **Control over System:** The attacker gained full control over the Ubuntu VM, with root privileges acquired via `sudo` from the `ubuntu` user, enabling them to create new users and potentially execute arbitrary commands.

Response and Recovery Analysis

Immediate Response Action

Upon detection and initial confirmation of the successful brute-force and unauthorized access, immediate containment measures were initiated to limit the attacker's access and prevent further damage.

- **Compromised User Password Change:** The password for the compromised `ubuntu` user account was immediately changed to a strong, unique value.
- **Attacker IP Blocking:** The attacker's source IP address (`192.168.148.160`) was explicitly denied access to SSH (port 22) on the Ubuntu VM's firewall (UFW), effectively severing the current connection and preventing immediate re-entry from that IP.

Eradication Measures

Following containment, comprehensive eradication steps were performed to remove all traces of the attacker and their malicious artifacts from the compromised system.

- **Unauthorized User Deletion:** The newly created, unauthorized user account, `auditd`, was immediately and permanently deleted from the system, including its home directory (`sudo userdel -r auditd`).
- **Persistence Mechanism Audit:** Thorough checks were performed for other persistence mechanisms, including suspicious cron jobs, unauthorized services, and unusual SSH keys. No additional unauthorized persistence mechanisms were found beyond the `auditd` user.
- **Log Integrity Review (Conceptual):** While not actively tampered with in this simulation, in a real scenario, logs would be reviewed for any signs of attacker attempts to clear or modify them to hide their tracks.

Recovery Steps

Recovery efforts focused on hardening the system against future similar attacks and restoring its security posture to a state stronger than before the incident.

- **SSH Configuration Hardening:** The SSH daemon configuration (`/etc/ssh/sshd_config`) on the Ubuntu VM was hardened. Key changes implemented included:
    - Setting `PermitRootLogin no` to prevent direct root logins.
    - Reducing `MaxAuthTries` to `3` to limit brute-force attempts.
    - Ensuring `PasswordAuthentication` is set to `no` (if SSH key authentication is enforced in the lab) or reviewing other authentication settings.

- **System Updates:** The Ubuntu VM was fully updated to ensure all operating system packages and dependencies were patched to their latest stable versions (`sudo apt update && sudo apt upgrade -y`), addressing any known vulnerabilities.

Post-Incident Actions

The post-incident phase focused on analyzing lessons learned and formulating recommendations to enhance security posture and prevent recurrence.

Lessons Learned

- **Effectiveness of SIEM Detection:** The integration of Wazuh with Splunk proved highly effective in detecting the SSH brute-force, successful login, and unauthorized user creation in a timely manner. The custom Splunk alert was crucial for aggregate visibility, complemented by detailed Wazuh rule triggers.
- **Importance of Strong Authentication:** The successful brute-force attack underscored the critical importance of strong, complex passwords and the necessity of multi-factor authentication (MFA) for all user accounts, especially those exposed to network services.
- **Vigilance Against Persistence:** The attacker's immediate creation of the `auditd` user highlighted the need for rapid eradication of persistence mechanisms and thorough post-compromise integrity checks.
- **Layered Security:** This incident demonstrated the value of a layered security approach, where the firewall (UFW) provided host-level containment after initial detection by the SIEM/HIDS.
- **Incident Response Process Validation:** The simulation provided practical experience in following the Incident Response Life Cycle, from initial detection and triage through containment, eradication, and recovery.

Recommendations for Improvement

- **Implement Multi-Factor Authentication (MFA) for SSH:** Mandate MFA for all SSH access to critical systems, including the Ubuntu VM. This would

significantly reduce the risk of successful credential-based attacks, even with weak passwords.

- **Enforce Strong Password Policies:** Implement and enforce a robust password policy that requires complexity, length, and regular rotation for all user accounts.
- **Deploy Automated Brute-Force Prevention (e.g., `fail2ban`):** Configure and deploy automated tools like `fail2ban` on the Ubuntu VM to automatically block malicious IP addresses after a configurable number of failed login attempts, providing an immediate, proactive layer of defense.
- **Migrate to SSH Key-Based Authentication:** Transition SSH authentication from passwords to cryptographic keys, disabling password authentication entirely on critical systems. This provides a much stronger authentication mechanism.
- **Implement Least Privilege Principle:** Continuously review and enforce the principle of least privilege for all user accounts, ensuring users only have the minimum necessary permissions to perform their duties.
- **Enhance Custom Detection Rules:** Review and refine existing Splunk and Wazuh rules to improve the fidelity and speed of alerts for SSH brute-force attempts, successful logins from unusual sources, and user account creation outside of standard provisioning processes. Consider adding behavioral analytics for unusual user activity.
- **Conduct Regular Vulnerability Assessments:** Periodically scan systems for open ports, misconfigurations, and known vulnerabilities that could be exploited.
- **Security Awareness Training:** Conduct ongoing security awareness training for all users, emphasizing the importance of password security and identifying suspicious activities.

Guidance and Learning Assistance (Gemini AI)

This report was compiled with the direct guidance and assistance of Gemini AI. Gemini AI provided structured prompts, technical explanations, and report content generation based on the user's input and lab observations. This collaboration

demonstrates how AI tools can be leveraged in a Security Operations Center (SOC) environment to:

- **Streamline Documentation:** Automate the writing of detailed incident reports, saving valuable analyst time.
- **Structure Response:** Provide a framework for incident response activities, ensuring all critical steps are covered.
- **Enhance Learning:** Offer real-time guidance and explanations on cybersecurity concepts, tools, and best practices.

The successful execution and documentation of this simulated incident, from attack to full recovery, highlights the practical application of theoretical cybersecurity knowledge within a hands-on lab environment, further enhanced by AI-driven assistance.