Security Incident Investigation Report

Prepared By: Vignesh

Role: Cybersecurity Analyst (Entry-Level)

Certification: Google Cybersecurity Professional Certificate

Date: 07 - DEC - 2025

1. Executive Summary:

- This report analyzes SSH authentication logs and identifies a brute-force attack that resulted in a successful root login.
- The attack originated from an external IP address, compromising system security.

2. Findings:

- Attacker IP: 45.67.89.12
- Attack Type: Brute-force login attempt
- Target Accounts: admin, test, root
- Success: Root access was successfully obtained

3. Evidence:

Jan 12 10:02:15 Failed password for invalid user admin from 45.67.89.12
Jan 12 10:02:22 Failed password for root from 45.67.89.12
Jan 12 10:02:25 Accepted password for root from 45.67.89.12

4. Impact:

- Attackers may have gained full control of the system, including access to sensitive files and services.

5. Recommendations:

1. Block attacker IP
2. Disable direct root login
3. Change all system passwords
4. Enable MFA
5. Limit SSH login attempts
6. Install fail2ban
7. Audit system for persistence

6. Conclusion:

A brute-force attack resulted in successful unauthorized system access. Immediate incident response actions are necessary to prevent further exploitation.