INCIDENT RESPONSE REPORT

Subject: SSH Brute Force Attack Analysis

Incident ID: IR-2025-1207-SSH

PREPARED BY:

Vignesh K.

SOC Analyst / Security Researcher

CERTIFICATIONS: Google Cybersecurity Professional

REPORT DATE: December 7, 2025

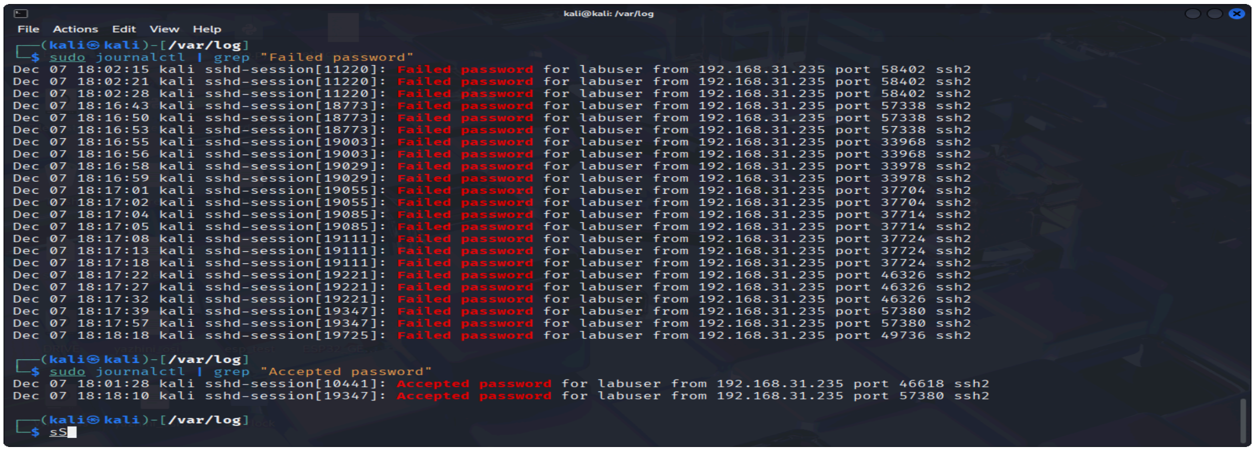
Incident ID	IR-2025-1207-SSH
Date	December 7, 2025
Severity	Critical
Status	Closed (Lab Simulation)

1. Executive Summary:

- On December 7, the host `kali` was subjected to a brute-force attack targeting the SSH service (Port 22). The attacker utilized the IP `192.168.31.235` to target the user account `labuser`.
- The attack was successful, resulting in unauthorized access at 18:18:10. This report documents the detection, analysis, and remediation steps for this portfolio scenario.

2. Detection & Analysis:

- **Trigger:** Manual log review using `journalctl`.
- **Command:** `sudo journalctl | grep "Failed password"`
- **Observation:** Logs indicated a high frequency of failed login attempts typical of automated tools (e.g., Hydra), originating from a single internal IP address.



```
┌──(kali㉿kali)-[/var/log]
└─$ sudo journalctl | grep "Failed password"
Dec 07 18:02:15 kali sshd-session[11220]: Failed password for labuser from 192.168.31.235 port 58402 ssh2
Dec 07 18:02:21 kali sshd-session[11220]: Failed password for labuser from 192.168.31.235 port 58402 ssh2
Dec 07 18:02:28 kali sshd-session[11220]: Failed password for labuser from 192.168.31.235 port 58402 ssh2
Dec 07 18:16:43 kali sshd-session[18773]: Failed password for labuser from 192.168.31.235 port 57338 ssh2
Dec 07 18:16:50 kali sshd-session[18773]: Failed password for labuser from 192.168.31.235 port 57338 ssh2
Dec 07 18:16:53 kali sshd-session[18773]: Failed password for labuser from 192.168.31.235 port 57338 ssh2
Dec 07 18:16:55 kali sshd-session[19003]: Failed password for labuser from 192.168.31.235 port 33968 ssh2
Dec 07 18:16:56 kali sshd-session[19003]: Failed password for labuser from 192.168.31.235 port 33968 ssh2
Dec 07 18:16:58 kali sshd-session[19029]: Failed password for labuser from 192.168.31.235 port 33978 ssh2
Dec 07 18:16:59 kali sshd-session[19029]: Failed password for labuser from 192.168.31.235 port 33978 ssh2
Dec 07 18:17:01 kali sshd-session[19055]: Failed password for labuser from 192.168.31.235 port 37704 ssh2
Dec 07 18:17:02 kali sshd-session[19055]: Failed password for labuser from 192.168.31.235 port 37704 ssh2
Dec 07 18:17:04 kali sshd-session[19085]: Failed password for labuser from 192.168.31.235 port 37714 ssh2
Dec 07 18:17:05 kali sshd-session[19085]: Failed password for labuser from 192.168.31.235 port 37714 ssh2
Dec 07 18:17:08 kali sshd-session[19111]: Failed password for labuser from 192.168.31.235 port 37724 ssh2
Dec 07 18:17:13 kali sshd-session[19111]: Failed password for labuser from 192.168.31.235 port 37724 ssh2
Dec 07 18:17:18 kali sshd-session[19111]: Failed password for labuser from 192.168.31.235 port 37724 ssh2
Dec 07 18:17:22 kali sshd-session[19221]: Failed password for labuser from 192.168.31.235 port 46326 ssh2
Dec 07 18:17:27 kali sshd-session[19221]: Failed password for labuser from 192.168.31.235 port 46326 ssh2
Dec 07 18:17:32 kali sshd-session[19221]: Failed password for labuser from 192.168.31.235 port 46326 ssh2
Dec 07 18:17:39 kali sshd-session[19347]: Failed password for labuser from 192.168.31.235 port 57380 ssh2
Dec 07 18:17:57 kali sshd-session[19347]: Failed password for labuser from 192.168.31.235 port 57380 ssh2
Dec 07 18:18:18 kali sshd-session[19725]: Failed password for labuser from 192.168.31.235 port 49736 ssh2

┌──(kali㉿kali)-[/var/log]
└─$ sudo journalctl | grep "Accepted password"
Dec 07 18:01:28 kali sshd-session[10441]: Accepted password for labuser from 192.168.31.235 port 46618 ssh2
Dec 07 18:18:10 kali sshd-session[19347]: Accepted password for labuser from 192.168.31.235 port 57380 ssh2

┌──(kali㉿kali)-[/var/log]
└─$ sS
```

3. Key Observables (IOCs):

- **Attacker IP:** `192.168.31.235`
- **Target User:** `labuser`
- **Compromise Time:** 18:18:10 (Source Port 57380)

4. Remediation & Hardening:

- **Immediate Action:** Blocked attacker IP via firewall.
- **Recovery:** Reset compromised user credentials.
- **Prevention:** Disabled password authentication in `/etc/ssh/sshd_config` and implemented Key-Based Authentication.