Incident Response Report

Incident Response & Security Breach Simulation

Incident Summary

On **24 February 2026 at 11:17 AM**, multiple failed SSH login attempts were detected on the Kali Linux system.

The attempts were made using an **invalid username (wronguser)** via SSH service.

Detection

The incident was identified by analyzing the authentication logs located at:

```
/var/log/auth.log
```

Command used:

```
sudo cat /var/log/auth.log | grep "Failed password"
```

Log Evidence Collected

The following suspicious entries were found:

```
2026-02-24T11:17:37 Failed password for invalid user wronguser from ::1 port 55376 ssh2
2026-02-24T11:17:45 Failed password for invalid user wronguser from ::1 port 55376 ssh2
2026-02-24T11:17:58 Failed password for invalid user wronguser from ::1 port 55376 ssh2
2026-02-24T11:17:59 Connection closed by invalid user wronguser ::1 port 55376 [preauth]
```

Analysis

- Attack Type: SSH Brute Force Attempt
- Target Account: Invalid user "wronguser"
- Source IP Address: ::1 (IPv6 localhost)
- Port Used: 55376
- Service Targeted: SSH (Port 22)
- Number of Failed Attempts: 3

Important Observation:

The IP address ::1 represents **localhost (IPv6 loopback address)**.

This confirms the attack was **simulated internally for testing purposes**.

Incident Classification

- Category: Authentication Attack
- Sub-Type: Brute Force Attempt
- Severity Level: Low

Reason:

- No valid account compromised
- No successful login observed
- Attack originated from local system

Containment Actions Taken

- SSH logs were monitored
- No valid user accounts were compromised
- System verified for unauthorized access
- SSH service configuration reviewed

Eradication Steps

- Ensured no unknown users exist
- Verified SSH configuration file
- Confirmed no root login was successful

Optional hardening applied:

- Disable root login
- Enable strong password policy

Recovery

- SSH service confirmed operational
- No data loss observed
- System integrity verified

Root Cause Analysis

Root cause of incident:

The SSH service was accessible and allowed login attempts without rate limiting.

No brute-force protection mechanism like **Fail2Ban** was enabled.

🔟 Preventive Security Recommendations

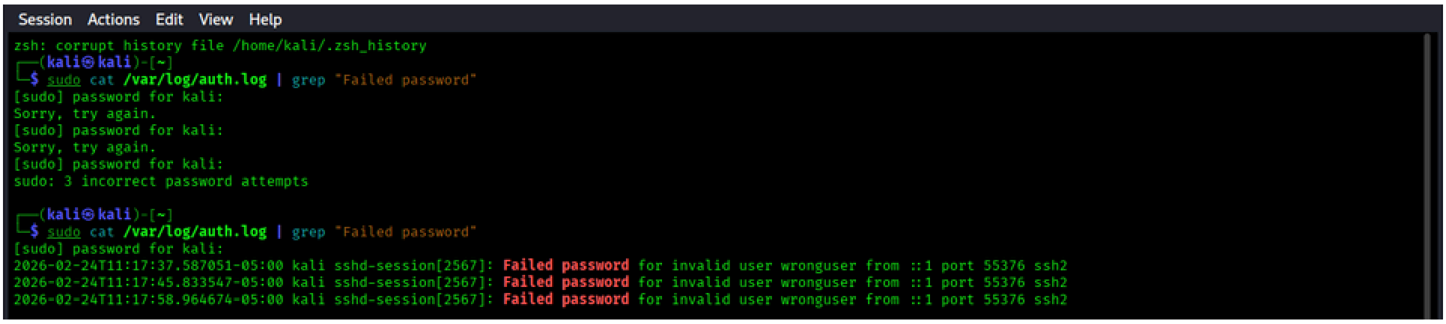
1. Install and configure Fail2Ban
2. Disable root SSH login
3. Implement SSH key-based authentication
4. Enable firewall rules

5. Monitor authentication logs regularly
6. Use strong password policy
7. Implement multi-factor authentication

Incident Timeline Document

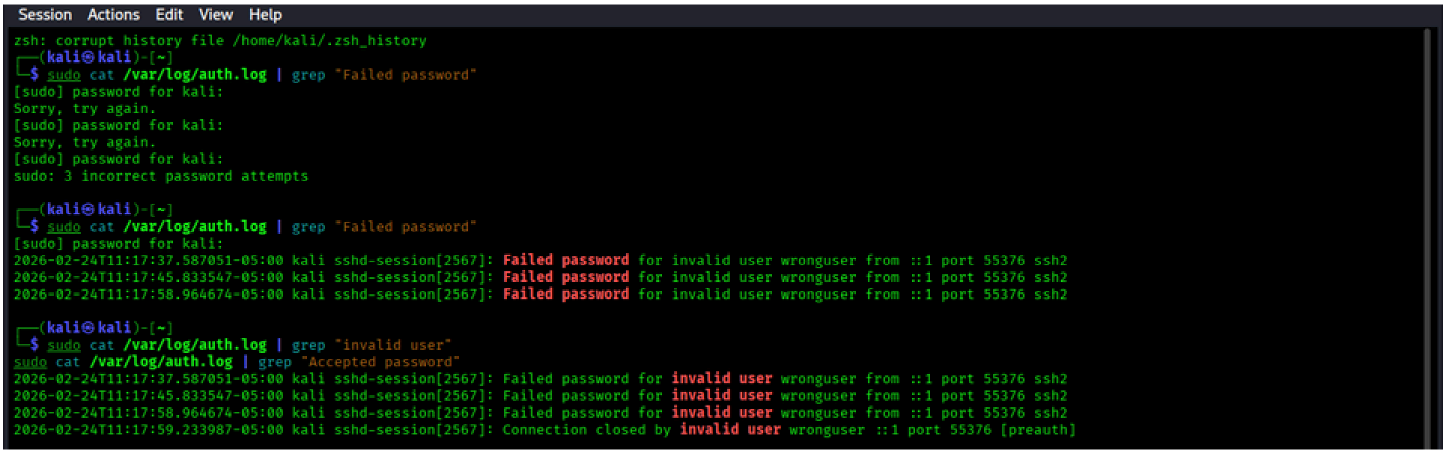
Incident Timeline – 24 February 2026

Time	Event
11:17:37	First failed login attempt detected
11:17:45	Second failed login attempt
11:17:58	Third failed login attempt
11:17:59	SSH connection closed
11:20:00	Logs analyzed
11:25:00	Incident classified
11:30:00	Security review completed



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/auth.log | grep "Failed password"
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
sudo: 3 incorrect password attempts

┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/auth.log | grep "Failed password"
[sudo] password for kali:
2026-02-24T11:17:37.587051-05:00 kali sshd-session[2567]: Failed password for invalid user wronguser from ::1 port 55376 ssh2
2026-02-24T11:17:45.833547-05:00 kali sshd-session[2567]: Failed password for invalid user wronguser from ::1 port 55376 ssh2
2026-02-24T11:17:58.964674-05:00 kali sshd-session[2567]: Failed password for invalid user wronguser from ::1 port 55376 ssh2
```



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/auth.log | grep "Failed password"
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
sudo: 3 incorrect password attempts

┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/auth.log | grep "Failed password"
[sudo] password for kali:
2026-02-24T11:17:37.587051-05:00 kali sshd-session[2567]: Failed password for invalid user wronguser from ::1 port 55376 ssh2
2026-02-24T11:17:45.833547-05:00 kali sshd-session[2567]: Failed password for invalid user wronguser from ::1 port 55376 ssh2
2026-02-24T11:17:58.964674-05:00 kali sshd-session[2567]: Failed password for invalid user wronguser from ::1 port 55376 ssh2

┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/auth.log | grep "invalid user"
sudo cat /var/log/auth.log | grep "Accepted password"
2026-02-24T11:17:37.587051-05:00 kali sshd-session[2567]: Failed password for invalid user wronguser from ::1 port 55376 ssh2
2026-02-24T11:17:45.833547-05:00 kali sshd-session[2567]: Failed password for invalid user wronguser from ::1 port 55376 ssh2
2026-02-24T11:17:58.964674-05:00 kali sshd-session[2567]: Failed password for invalid user wronguser from ::1 port 55376 ssh2
2026-02-24T11:17:59.233987-05:00 kali sshd-session[2567]: Connection closed by invalid user wronguser ::1 port 55376 [preauth]
```