Incident Response Report

Incident Title: Repeated Failed Login Attempts (Possible Brute Force Attack)
Date: 13 February 2026
Tools Used:

- Linux: /var/log/auth.log
- Windows: Windows Event Viewer
- Alternative (optional): TheHive

1️⃣ Incident Description (Simulation)

A simulated attack was performed involving:

- Multiple failed login attempts (20+ attempts in 5 minutes)
- Target account: admin
- Source IP: 192.168.1.50
- System: Ubuntu Server / Windows 10 test machine

This indicates a **Brute Force Attack Attempt**.

2️⃣ Detection & Log Analysis

🔎 Linux Log Analysis

Command used:

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

Observed:

Failed password for admin from 192.168.1.50 port 53422 ssh2

Failed password for admin from 192.168.1.50 port 53423 ssh2

Indicators:

- Repeated failures
- Same source IP

- Short time interval

🔎 Windows Log Analysis

Open:
Event Viewer → Windows Logs → Security

Filter by:

- Event ID **4625** (Failed login)

Findings:

- Multiple 4625 events
- Same source network address
- Target account: Administrator

3️⃣ Incident Classification

Category	Value
Attack Type	Brute Force
Severity	Medium–High
Impact	Unauthorized access attempt
Status	Contained

4️⃣ Containment Actions

Immediate steps taken:

- 🔒 Locked affected account
- 🔥 Blocked attacker IP using firewall:

sudo ufw deny from 192.168.1.50

- Enabled account lockout policy

- Disabled SSH root login

Containment is important because:

- Prevents attacker from gaining access
- Stops lateral movement
- Reduces damage

5️⃣ Eradication (Remove Threat)

- Verified no successful login occurred
- Checked for unknown users:

cat /etc/passwd

- Reset passwords
- Updated system patches:

sudo apt update && sudo apt upgrade

6️⃣ Recovery

- Re-enabled legitimate user access
- Monitored logs for 24 hours
- Confirmed no further suspicious attempts

System restored to secure operational state.

7️⃣ Root Cause Analysis (RCA)

Root Cause:

- Weak password policy
- No account lockout configuration
- SSH exposed to internal network

Corrective Actions:

- Enforced strong password policy
- Enabled 2FA for admin accounts
- Limited SSH access using firewall rules

🗓️ **Incident Timeline Document**

Time Event

09:00 Multiple failed login attempts detected

09:05 Log analysis started

09:10 Source IP identified

09:12 Firewall rule applied

09:20 Password reset

09:30 Monitoring initiated

10:30 Incident closed

🛡 **Preventive Security Improvements**

1. Enable Multi-Factor Authentication (MFA)
2. Configure Account Lockout Policy
3. Implement Fail2Ban (Linux)
4. Deploy IDS/IPS
5. Centralized logging with SIEM
6. Regular log monitoring
7. Disable unused services
8. Use strong password policies (12+ characters)

🎯 **Final Outcome**

- Attack detected early
- No unauthorized access achieved
- Systems secured
- Preventive measures implemented
- Practical understanding of Incident Response lifecycle achieved