CYBER SECURITY INTERNSHIP

Ministry of MSME, Govt. of India

Task 16

INCIDENT RESPONSE & SECURITY BREACH SIMULATION

JASHMI KS

This task demonstrates a simulated security incident and the implementation of an Incident Response process on an Ubuntu virtual machine.

The objective was to simulate a security breach (failed login attack), analyze system logs to detect suspicious activity, classify the incident, contain the threat, remove the root cause, restore system security, and recommend preventive measures.

Objectives

- Simulate a security incident
- Identify suspicious activity using Linux logs
- Classify the incident based on severity
- Contain and remove the threat
- Restore system security
- Document the incident response timeline
- Recommend preventive security measures

Scope of the Simulation

- Environment: Ubuntu VM
- Platform: Oracle VM VirtualBox
- Incident Type: Repeated Failed Login Attempts (Brute Force Simulation)
- Log Source: /var/log/auth.log

The simulation was limited to the virtual lab environment and did not affect external systems.

Methodology

The incident response followed standard phases:

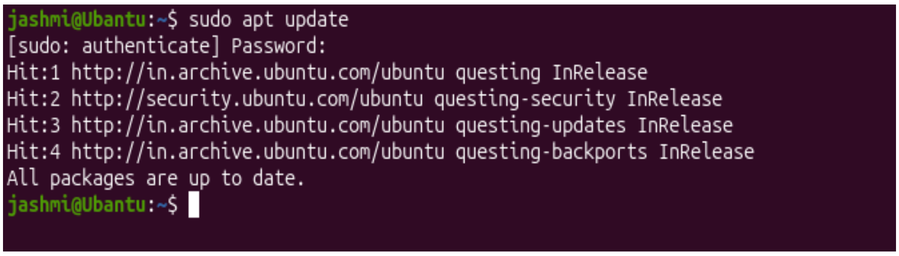
1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery

Incident Simulation & Response Steps

Step 1: Preparation

The Ubuntu system was updated before simulation.

Commands used: sudo apt update , sudo apt upgrade -y



```
jashmi@Ubantu:~$ sudo apt update
[sudo: authenticate] Password:
Hit:1 http://in.archive.ubuntu.com/ubuntu questing InRelease
Hit:2 http://security.ubuntu.com/ubuntu questing-security InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu questing-updates InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu questing-backports InRelease
All packages are up to date.
jashmi@Ubantu:~$
```

Step 2: Simulating the Security Incident

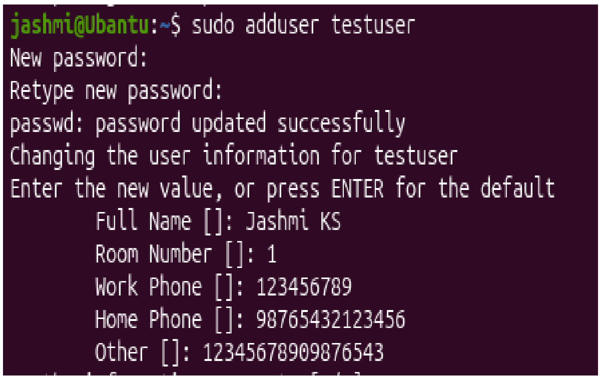
A test user account was created: sudo adduser testuser

A password was assigned: sudo passwd testuser

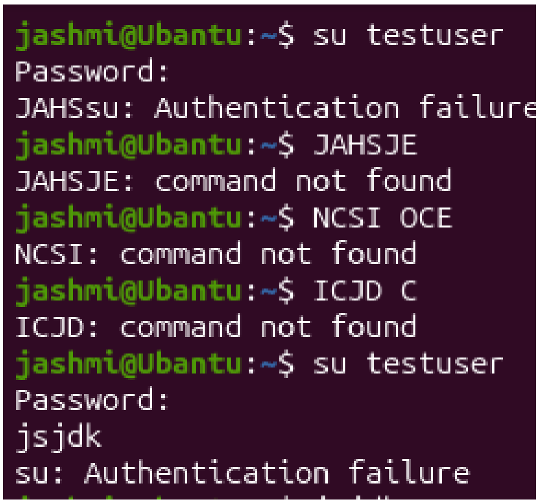
Now, multiple failed login attempts were intentionally performed: su testuser

Incorrect password was entered multiple times (5–6 attempts).

This simulates a **Brute Force Login Attempt**.



```
jashmi@Ubantu:~$ sudo adduser testuser
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for testuser
Enter the new value, or press ENTER for the default
        Full Name []: Jashmi KS
        Room Number []: 1
        Work Phone []: 123456789
        Home Phone []: 98765432123456
        Other []: 12345678909876543
```



```
jashmi@Ubantu:~$ su testuser
Password:
JAHSsu: Authentication failure
jashmi@Ubantu:~$ JAHSJE
JAHSJE: command not found
jashmi@Ubantu:~$ NCSI OCE
NCSI: command not found
jashmi@Ubantu:~$ ICJD C
ICJD: command not found
jashmi@Ubantu:~$ su testuser
Password:
jsjdk
su: Authentication failure
```

Step 3: Identifying Suspicious Activity (Log Analysis)

Authentication logs were analyzed using:

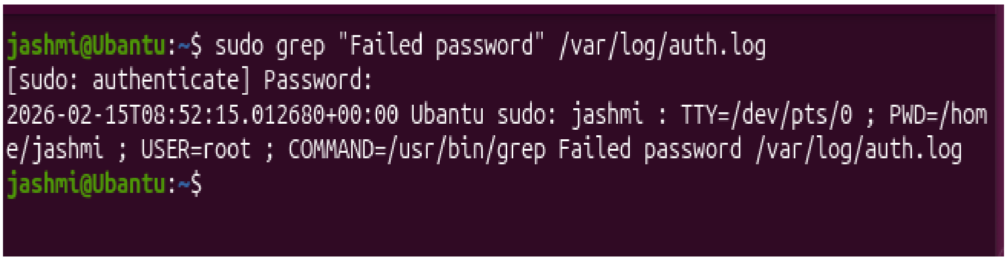
sudo cat /var/log/auth.log | grep "Failed password"

OR

sudo journalctl | grep "Failed password"

The system displayed repeated failed login attempts from the same user/IP.

This indicates unauthorized login attempts.



```
jashmi@Ubantu:~$ sudo grep "Failed password" /var/log/auth.log
[sudo: authenticate] Password:
2026-02-15T08:52:15.012680+00:00 Ubantu sudo: jashmi : TTY=/dev/pts/0 ; PWD=/hom
e/jashmi ; USER=root ; COMMAND=/usr/bin/grep Failed password /var/log/auth.log
jashmi@Ubantu:~$
```

Step 4: Incident Classification

Attack Type: Brute Force Attack

Target: User Authentication System

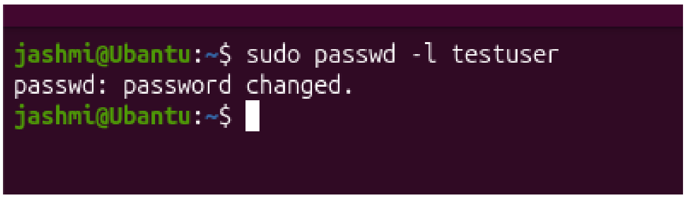
Severity Level: Medium (Local simulation)

If performed remotely on production systems, severity would be High.

Step 5: Containment

To prevent further login attempts, the affected account was locked:
sudo passwd -l testuser

This disables the user account temporarily.



```
jashmi@Ubantu:~$ sudo passwd -l testuser
passwd: password changed.
jashmi@Ubantu:~$ 
```

Step 6: Eradication

The root cause (weak password & repeated attempts) was addressed by:

1. Changing password:

sudo passwd testuser

2. Removing unnecessary user:

sudo deluser testuser

3. Blocking suspicious IP (if remote attack):

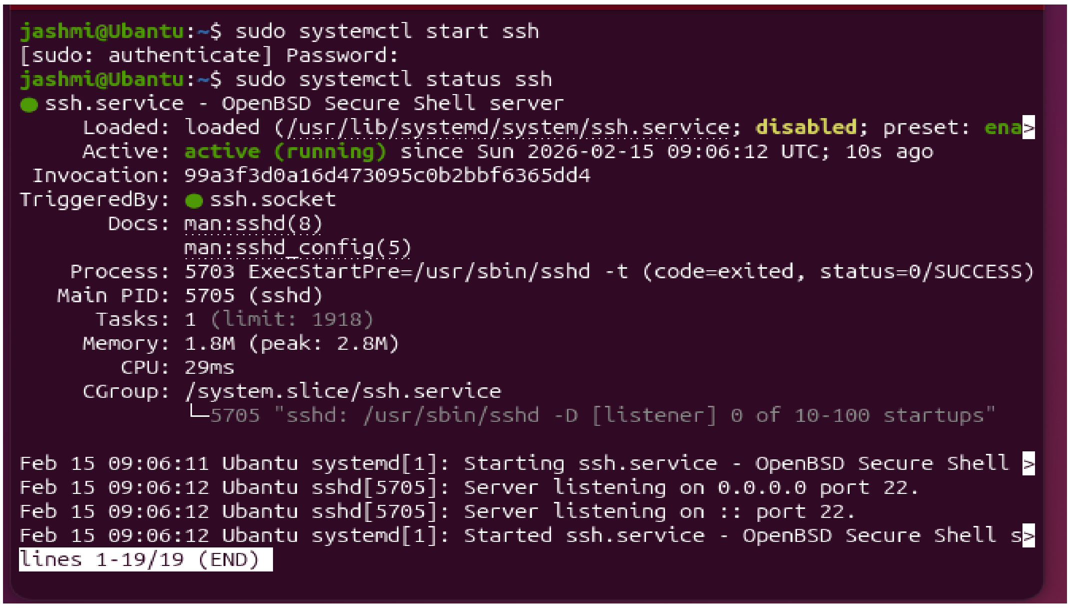
sudo ufw deny <IP_address>

Step 7: Recovery

System integrity was verified:
sudo systemctl status ssh

Passwords were reset, and firewall was enabled:
sudo ufw enable

System returned to secure operational state.



```
jashmi@Ubantu:~$ sudo systemctl start ssh
[sudo: authenticate] Password:
jashmi@Ubantu:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: ena>
     Active: active (running) since Sun 2026-02-15 09:06:12 UTC; 10s ago
 Invocation: 99a3f3d0a16d473095c0b2bbf6365dd4
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 5703 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 5705 (sshd)
      Tasks: 1 (limit: 1918)
     Memory: 1.8M (peak: 2.8M)
        CPU: 29ms
     CGroup: /system.slice/ssh.service
             └─5705 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Feb 15 09:06:11 Ubantu systemd[1]: Starting ssh.service - OpenBSD Secure Shell >
Feb 15 09:06:12 Ubantu sshd[5705]: Server listening on 0.0.0.0 port 22.
Feb 15 09:06:12 Ubantu sshd[5705]: Server listening on :: port 22.
Feb 15 09:06:12 Ubantu systemd[1]: Started ssh.service - OpenBSD Secure Shell s>
lines 1-19/19 (END)
```

Root Cause Analysis

- Weak password policy
- No account lockout mechanism
- No intrusion detection system

Preventive Security Improvements

- Enforce strong password policy
- Enable account lockout policy
- Install and configure Fail2Ban
- Enable firewall (UFW)
- Disable root SSH login
- Regular log monitoring
- Enable multi-factor authentication (MFA)

Conclusion

The simulated incident demonstrated how repeated failed login attempts can be detected through system log analysis. By following structured incident response procedures — identification, containment, eradication, and recovery — the threat was effectively mitigated.

This task provided practical understanding of real-world incident response processes and log analysis techniques in Linux environments.