

## Task 16: Incident Response & Security Breach Simulation

**Target System:** Kali Linux (SSH Enabled)

**Log Monitoring Tool:** journalctl

**Service Monitored:** SSH

---

### 1 Objective

To detect and respond to a simulated brute-force SSH login attack by analyzing authentication logs, identifying the attacker IP, performing containment, and securing the system.

---

### 2 Start & Verify SSH Service

Command:

```
sudo systemctl status ssh
```

Result:

SSH service is active and running.

```
(stark@windows)-[~]
$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: disabled)
  Active: active (running) since Tue 2026-02-17 21:05:28 IST; 4min 28s ago
    Invocation: baca63f1493c4176ba07a2e760df8486
      Docs: man:sshd(8)
             man:sshd_config(5)
    Main PID: 4473 (sshd)
      Tasks: 1 (limit: 4500)
     Memory: 4.9M (peak: 9.4M)
        CPU: 266ms
      CGroup: /system.slice/ssh.service
              └─4473 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Feb 17 21:06:56 windows sshd-session[5298]: pam_unix(sshd:auth): check pass; user unknown
Feb 17 21:06:56 windows sshd-session[5298]: pam_winbind(sshd:auth): getting password (0x000
```

---

### 3 Simulate Failed Login Attempts

Command:

```
ssh wronguser@localhost
```

Enter incorrect password multiple times.

Result:

Permission denied messages displayed.

```
(stark@windows)-[~]
$ ssh wronguser@localhost

The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:27K7EuTSXKVmIPDgvhEusZ48Re9Fi13q2cY7h1nsWHI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
wronguser@localhost's password:
Permission denied, please try again.
wronguser@localhost's password:
Permission denied, please try again.
wronguser@localhost's password:
wronguser@localhost: Permission denied (publickey,password).  

(stark@windows)-[~]
```

### 4 Analyze Failed Login Logs

Command:

```
sudo journalctl -u ssh | grep "Failed"
```

Result:

```
(stark@windows)-[~]
$ sudo journalctl -u ssh | grep "Failed"

Feb 17 21:06:52 windows sshd-session[5298]: Failed password for invalid user wronguser from ::1 port 60522 ssh2
Feb 17 21:06:58 windows sshd-session[5298]: Failed password for invalid user wronguser from ::1 port 60522 ssh2
Feb 17 21:07:03 windows sshd-session[5298]: Failed password for invalid user wronguser from ::1 port 60522 ssh2  

(stark@windows)-[~]
```

## 5 Identify Attacker IP

Command:

```
sudo journalctl -u ssh | grep "Failed password"
```

Attacker IP Identified:

::1

```
(stark@windows)-[~]
$ sudo journalctl -u ssh | grep "Failed password"
Feb 17 21:06:52 windows sshd-session[5298]: Failed password for invalid user wronguser from ::1 port 60522 ssh2
Feb 17 21:06:58 windows sshd-session[5298]: Failed password for invalid user wronguser from ::1 port 60522 ssh2
Feb 17 21:07:03 windows sshd-session[5298]: Failed password for invalid user wronguser from ::1 port 60522 ssh2

(stark@windows)-[~]
```

---

## 6 Containment – Lock Suspicious Account

Command:

```
sudo passwd -l wronguser
```

Verify:

```
sudo passwd -S wronguser
```

Result:

Account locked successfully.

```
(stark@windows)-[~]
$ sudo useradd wronguser

(stark@windows)-[~]
$ sudo passwd -l wronguser
passwd: password changed.

(stark@windows)-[~]
$ sudo passwd -S wronguser
wronguser L 2026-02-17 0 99999 7 -1

(stark@windows)-[~]
```

## 7 Containment – Block Attacker IP

Command:

```
sudo ufw deny from ::1
```

Verify:

```
sudo ufw status
```

Result:

Firewall rule added.

```
(stark@windows)-[~]
$ sudo ufw deny from ::1
Rule added (v6)

(stark@windows)-[~]
$ sudo ufw status
Status: active

To                         Action      From
--                         -----      ---
Anywhere (v6)             DENY       ::1
```

---

## 8 Monitor Logs After Containment

Command:

```
sudo journalctl -u ssh -f
```

Result:

No further failed login attempts detected.

```
[stark@windows] ~
$ sudo journalctl -u ssh -f
Feb 17 21:06:56 windows sshd-session[5298]: pam_unix(sshd:auth): check pass; user unknown
Feb 17 21:06:56 windows sshd-session[5298]: pam_winbind(sshd:auth): getting password (0x00000388)
Feb 17 21:06:56 windows sshd-session[5298]: pam_winbind(sshd:auth): pam_get_item returned a password
Feb 17 21:06:58 windows sshd-session[5298]: Failed password for invalid user wronguser from ::1 port 60522 ssh2
Feb 17 21:07:01 windows sshd-session[5298]: pam_unix(sshd:auth): check pass; user unknown
Feb 17 21:07:01 windows sshd-session[5298]: pam_winbind(sshd:auth): getting password (0x00000388)
Feb 17 21:07:01 windows sshd-session[5298]: pam_winbind(sshd:auth): pam_get_item returned a password
Feb 17 21:07:03 windows sshd-session[5298]: Failed password for invalid user wronguser from ::1 port 60522 ssh2
Feb 17 21:07:03 windows sshd-session[5298]: Connection closed by invalid user wronguser ::1 port 60522 [preauth]
Feb 17 21:07:03 windows sshd-session[5298]: PAM 2 more authentication failures; logname= uid =0 euid=0 tty=ssh ruser= rhost=:1
^C
[stark@windows] ~
```

## 9 Incident Timeline

### Time Event

21:06 Failed login attempts detected

21:07 Log analysis performed

21:08 Attacker IP identified

21:09 Account locked

21:10 IP blocked

21:12 System secured

---

## 10 Final Outcome

- Brute-force SSH attack simulated
- Failed login attempts detected
- Attacker IP identified
- Account locked

- Firewall rule implemented
- System secured successfully