## Task 16 – SSH Log Monitoring and Analysis

**Internship:** Cyber Security Internship
**Name:** Adil Firoz
**Date:** 13 February 2026
**Operating System:** Kali Linux
**Tools Used:** Linux Terminal, journalctl, SSH

### Objective

The objective of this task was to monitor and analyze SSH authentication logs in Kali Linux to identify failed and successful login attempts using system log analysis techniques.

### Procedure

### 1 Generate Failed SSH Login Attempts

Multiple failed login attempts were generated using an invalid username to create authentication failure logs.

Command used:

```
ssh fakeuser@localhost
```

An incorrect password was entered several times to simulate brute-force or unauthorized access attempts.

### 2 Generate Successful SSH Login

A valid SSH login was performed using the correct system username and password.

Command used:

```
ssh safe@localhost
```

This created a successful authentication log entry.

### 3 Analyze Failed Login Attempts

The following command was used to filter failed SSH login attempts:

```
sudo journalctl | grep "Failed password"
```

The logs showed multiple failed login attempts for an invalid user from localhost (::1).

### 4 Analyze Successful Login

The following command was used to identify successful SSH authentication:

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

The log confirmed a successful login for the valid user **safe**.

### Observations

#### Failed Login Attempts

- Multiple failed authentication attempts were detected.
- The username used was invalid.
- The source IP was localhost (::1).
- These logs indicate unauthorized access attempts.

#### Successful Login

- A successful login entry was recorded for the valid user.
- Authentication method: password
- Service: SSH

### Security Significance

Monitoring authentication logs helps in:

- Detecting brute-force attacks
- Identifying unauthorized access attempts
- Tracking legitimate user logins
- Strengthening system security monitoring

### Conclusion

The task was successfully completed. SSH authentication logs were monitored and analyzed to identify both failed and successful login attempts. This demonstrates how system logs can be used for security auditing and intrusion detection in a Linux environment