### **Task 6: Log Analysis & Intrusion Detection**

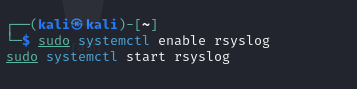
## **1. Setup: Enabling System Logging**

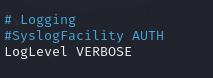
To analyze SSH login attempts, ensure that system logging is enabled.

### **Check Logs:**

* journalctl -u sshd → View SSH-related logs.
* cat /var/log/auth.log | grep "sshd" → Check authentication logs (for Debian-based systems).
* cat /var/log/secure | grep "sshd" → For RHEL-based systems.

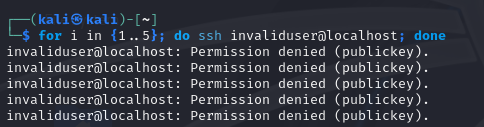
### **Enable Logging (if not enabled):**

Ensure rsyslog is installed and running:  
  


Ensure SSH logging is configured:  
  
  
  
  


## **2. Simulating Multiple Failed SSH Login Attempts**

Use the following command to simulate brute-force attempts:



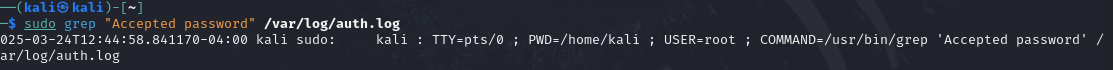
This will create multiple failed login attempts in /var/log/auth.log.

## **3. Exploit: Analyzing Logs**

### **Check for Failed SSH Logins**

Find failed login attempts:  


Count attempts per IP:  


Identify brute-force attacks (too many failed attempts from the same IP):  
 

### **Check for Successful Logins**

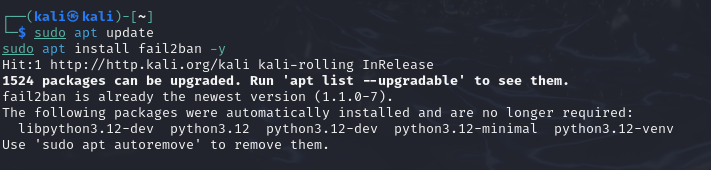
sudo grep "Accepted password" /var/log/auth.log

## **4. Mitigation: Preventing Brute-Force Attacks**

### **Install and Configure fail2ban**

sudo apt update

sudo apt install fail2ban -y



### **Enable SSH Protection in fail2ban**

Edit the jail configuration:  
 sudo nano /etc/fail2ban/jail.local

Add:  
 [sshd]

enabled = true

port = ssh

filter = sshd

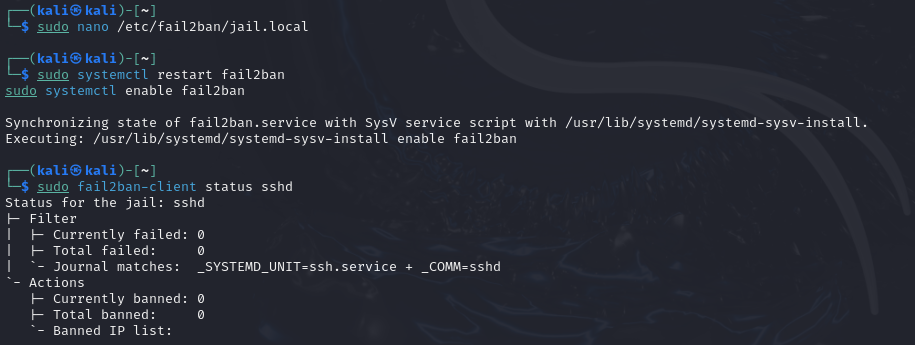
logpath = /var/log/auth.log

maxretry = 3

bantime = 600

Save and restart fail2ban:  
 sudo systemctl restart fail2ban

sudo systemctl enable fail2ban



### **Check if fail2ban is Working**

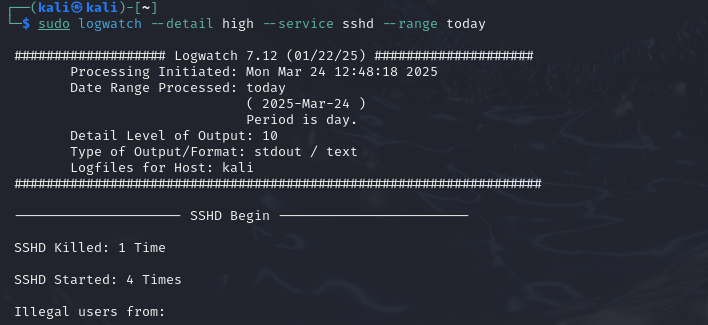
sudo fail2ban-client status sshd

## **5. Automate Log Monitoring**

### **Using logwatch**



Run logwatch manually:

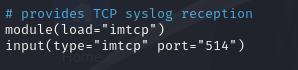


### **Using rsyslog for Centralized Logging**

Edit config:



Uncomment:



Restart rsyslog:

