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:

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable rsyslog
sudo systemctl start rsyslog
```

Ensure SSH logging is configured:

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ssh/sshd_config
```

```
# Logging
#SyslogFacility AUTH
LogLevel VERBOSE
```

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart sshd
```

---

2. Simulating Multiple Failed SSH Login Attempts

Use the following command to simulate brute-force attempts:

```
┌──(kali㉿kali)-[~]
└─$ for i in {1..5}; do ssh invaliduser@localhost; done
invaliduser@localhost: Permission denied (publickey).
invaliduser@localhost: Permission denied (publickey).
invaliduser@localhost: Permission denied (publickey).
invaliduser@localhost: Permission denied (publickey).
invaliduser@localhost: Permission denied (publickey).
```

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:

```
┌──(kali㉿kali)-[~]
└─$ sudo grep "Failed password" /var/log/auth.log
2025-03-24T12:41:37.811578-04:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'F
ailed password' /var/log/auth.log
```

Count attempts per IP:

```
┌──(kali㉿kali)-[~]
└─$ sudo grep "Failed password" /var/log/auth.log | awk '{print $(NF-3)}' | sort | uniq -c | sort -nr
      2 COMMAND=/usr/bin/grep
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo grep "Accepted password" /var/log/auth.log
2025-03-24T12:44:58.841170-04:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Accepted password' /
var/log/auth.log
```

-

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

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
sudo apt install fail2ban -y
Hit:1 http://http.kali.org/kali kali-rolling InRelease
1524 packages can be upgraded. Run 'apt list --upgradable' to see them.
fail2ban is already the newest version (1.1.0-7).
The following packages were automatically installed and are no longer required:
  libpython3.12-dev  python3.12  python3.12-dev  python3.12-minimal  python3.12-venv
Use 'sudo apt autoremove' to remove them.
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/fail2ban/jail.local

┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart fail2ban
sudo systemctl enable fail2ban

Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban

┌──(kali㉿kali)-[~]
└─$ sudo fail2ban-client status sshd
Status for the jail: sshd
├─ Filter
│  ├─ Currently failed: 0
│  ├─ Total failed:     0
│  └─ Journal matches:  _SYSTEMD_UNIT=ssh.service + _COMM=sshd
└─ Actions
   ├─ Currently banned: 0
   ├─ Total banned:     0
   └─ Banned IP list:
```

Check if fail2ban is Working

sudo fail2ban-client status sshd

---

5. Automate Log Monitoring

Using logwatch

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install logwatch -y
The following packages were automatically installed and are no longer required:
  libpython3.12-dev  python3.12  python3.12-dev  python3.12-minimal  python3.12-venv
Use 'sudo apt autoremove' to remove them.
```

Run logwatch manually:

```
┌──(kali㉿kali)-[~]
└─$ sudo logwatch --detail high --service sshd --range today

 ################### Logwatch 7.12 (01/22/25) ####################
        Processing Initiated: Mon Mar 24 12:48:18 2025
        Date Range Processed: today
                              ( 2025-Mar-24 )
                              Period is day.
        Detail Level of Output: 10
        Type of Output/Format: stdout / text
        Logfiles for Host: kali
 ##################################################################

 ---------------------- SSHD Begin -----------------------

 SSHD Killed: 1 Time

 SSHD Started: 4 Times

 Illegal users from:
```

Using rsyslog for Centralized Logging

Edit config:

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/rsyslog.conf
```

Uncomment:

```
# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

Restart rsyslog:


(kali㉿kali)-[~]
$ sudo systemctl restart rsyslog