Task 6

Log Analysis & Intrusion Detection

Setup

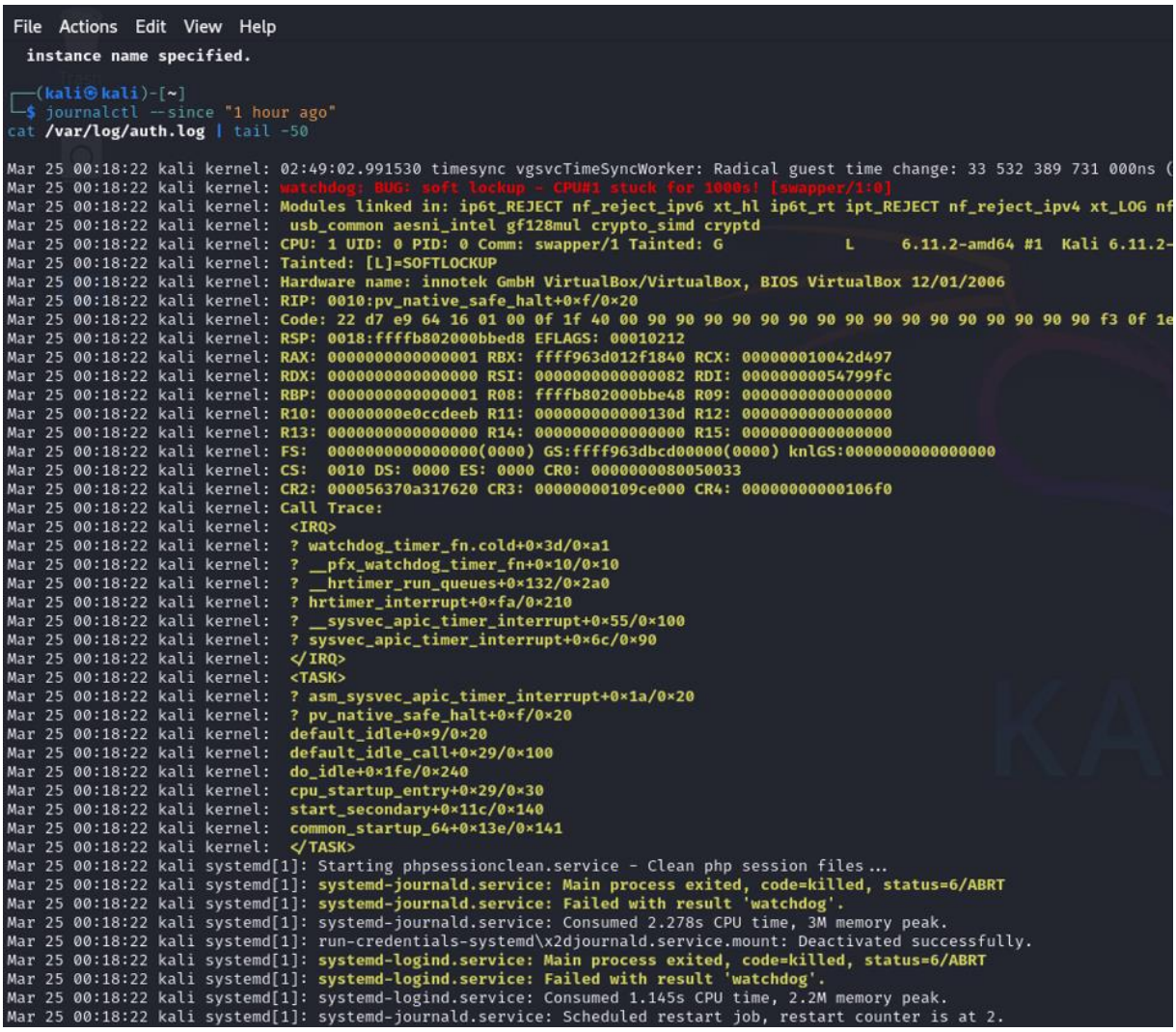
1. Before analyzing logs, we need to ensure that system logging is active.

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

The unit files have no installation config (WantedBy=, RequiredBy=, UpheldBy=,
Also=, or Alias= settings in the [Install] section, and DefaultInstance= for
template units). This means they are not meant to be enabled or disabled using systemctl.

Possible reasons for having these kinds of units are:
• A unit may be statically enabled by being symlinked from another unit's
  .wants/, .requires/, or .upholds/ directory.
• A unit's purpose may be to act as a helper for some other unit which has
  a requirement dependency on it.
• A unit may be started when needed via activation (socket, path, timer,
  D-Bus, udev, scripted systemctl call, ...).
• In case of template units, the unit is meant to be enabled with some
  instance name specified.
```

2. Check logs:



Exploit

1. **Analyze Logs for Failed SSH Logins:** Find failed attempts:

2. Count occurrences per IP:

Identify Brute-Force Attempts & Unauthorized Access:

- Check repeated failed attempts from the same IP.
- Review timestamps for patterns.
- Validate against legitimate access logs:

```
┌──(kali㉿kali)-[~]
└─$ grep "Failed password" /var/log/auth.log

2025-03-25T01:04:13.359237-04:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log

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

      1 COMMAND=/usr/bin/grep

┌──(kali㉿kali)-[~]
└─$ grep "Accepted password" /var/log/auth.log
```

Mitigation

1. Implement Fail2Ban to Block Repeated Failed Attempts:

Install Fail2Ban

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install fail2ban -y
```

Configure SSH protection:

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

```
  GNU nano 8.2
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 600
```

Restart Fail2Ban

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart fail2ban
sudo fail2ban-client status sshd

2025-03-25 01:08:43,696 fail2ban             [165701]: ERROR   Failed to access socket path: /var/run/fail2ban/fail2ban.sock. Is fail2ban running?
```

2. Set Up Log Monitoring Automation:

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install logwatch -y

Installing:
  logwatch

Suggested packages:
  libsys-cpu-perl  libsys-meminfo-perl

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1558
  Download size: 390 kB
  Space needed: 2,451 kB / 62.7 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 logwatch all 7.12-3 [390 kB]
Fetched 390 kB in 23s (16.8 kB/s)
Selecting previously unselected package logwatch.
(Reading database ... 403562 files and directories currently installed.)
Preparing to unpack .../logwatch_7.12-3_all.deb ...
Unpacking logwatch (7.12-3) ...
Setting up logwatch (7.12-3) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
```

Generate a security report

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

 ################### Logwatch 7.12 (01/22/25) ####################
        Processing Initiated: Tue Mar 25 01:09:56 2025
        Date Range Processed: today
                              ( 2025-Mar-25 )
                              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: 2 Times

 Illegal users from:
    ::1 (localhost): 1 Time
       invalid_user: 1 Time

 ---------------------- SSHD End -------------------------


 ###################### Logwatch End #########################
```

Configure rsyslog for centralized logging

Ensure remote logging is enabled if needed.

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

Conclusion

In this task, we successfully analyzed SSH login attempts, identified unauthorized access, and implemented security measures. By using system logs (journalctl or /var/log/auth.log), we detected failed login attempts and potential brute-force attacks. Fail2Ban was configured to block repeated failed logins, enhancing system security. Additionally, log monitoring automation was set up using logwatch to ensure continuous threat detection.