Operating System Security Fundamentals – Kali Linux

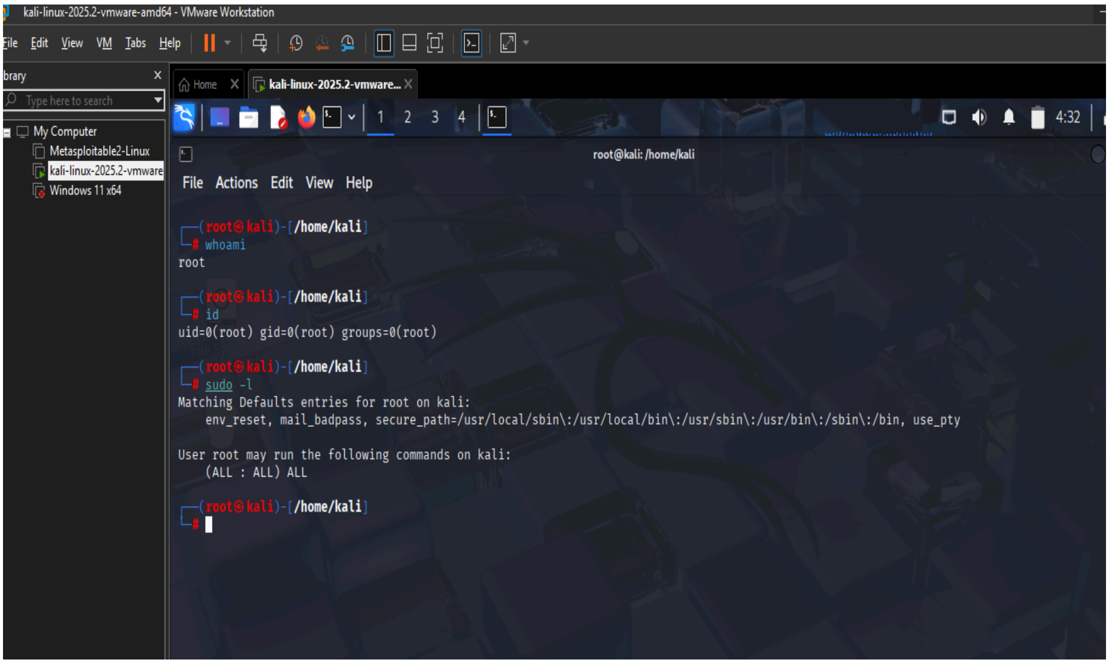
1.User Accounts and Privileges

Kali Linux uses a **non-root user by default**, which improves security.

Observations:

- Normal users have limited permissions.
- Administrative tasks are performed using `sudo`.
- Root user has full system control.

Commands used:


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
brary
Type here to search
My Computer
Metasploitable2-Linux
kali-linux-2025.2-vmware
Windows 11 x64
Home
kali-linux-2025.2-vmware...
1 2 3 4
4:32
root@kali: /home/kali
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/kali]
└─# whoami
root

┌──(root㉿kali)-[/home/kali]
└─# id
uid=0(root) gid=0(root) groups=0(root)

┌──(root㉿kali)-[/home/kali]
└─# sudo -l
Matching Defaults entries for root on kali:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User root may run the following commands on kali:
    (ALL : ALL) ALL

┌──(root㉿kali)-[/home/kali]
└─# 
```

Using a normal user instead of root reduces the risk of accidental system damage and security breaches.

2. File Permissions in Linux

Linux uses file permissions to control access to files and directories.

Permission Types:

- **Read (r)** – View file contents
- **Write (w)** – Modify file
- **Execute (x)** – Run file

Commands used: ls -l , chmod, chown

Proper file permissions prevent unauthorized access and protect sensitive system files.

3. Firewall Configuration

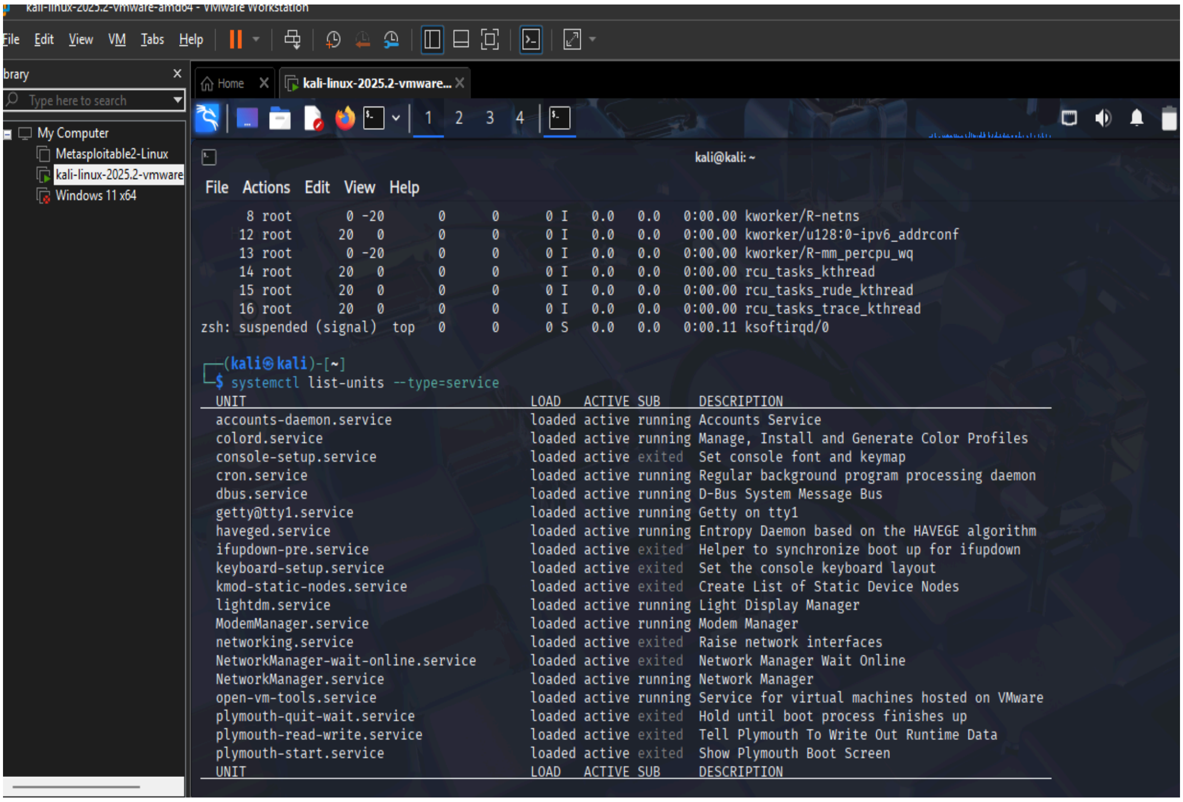
A firewall is used to control incoming and outgoing network traffic.

The firewall helps block unauthorized network connections and reduces exposure to attacks.

4. Running Processes and Services

Active processes and services were reviewed to identify unnecessary services.

Commands used: ps aux, top, systemctl list-units --type=service


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
brary
Type here to search
My Computer
Metasploitable2-Linux
kali-linux-2025.2-vmware
Windows 11 x64
Home
kali-linux-2025.2-vmware...
1 2 3 4
kali@kali: ~
File Actions Edit View Help

```
     8 root       0 -20       0       0      0 I   0.0   0.0   0:00.00 kworker/R-netns
    12 root      20   0       0       0      0 I   0.0   0.0   0:00.00 kworker/u128:0-ipv6_addrconf
    13 root       0 -20       0       0      0 I   0.0   0.0   0:00.00 kworker/R-mm_percpu_wq
    14 root      20   0       0       0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
    15 root      20   0       0       0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
    16 root      20   0       0       0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
zsh: suspended (signal)  top    0       0      0 S   0.0   0.0   0:00.11 ksoftirqd/0

┌──(kali㉿kali)-[~]
└─$ systemctl list-units --type=service
  UNIT                                 LOAD   ACTIVE SUB     DESCRIPTION
  accounts-daemon.service              loaded active running Accounts Service
  colord.service                       loaded active running Manage, Install and Generate Color Profiles
  console-setup.service                loaded active exited  Set console font and keymap
  cron.service                         loaded active running Regular background program processing daemon
  dbus.service                         loaded active running D-Bus System Message Bus
  getty@tty1.service                   loaded active running Getty on tty1
  haveged.service                      loaded active running Entropy Daemon based on the HAVEGE algorithm
  ifupdown-pre.service                 loaded active exited  Helper to synchronize boot up for ifupdown
  keyboard-setup.service               loaded active exited  Set the console keyboard layout
  kmod-static-nodes.service            loaded active exited  Create List of Static Device Nodes
  lightdm.service                      loaded active running Light Display Manager
  ModemManager.service                 loaded active running Modem Manager
  networking.service                   loaded active exited  Raise network interfaces
  NetworkManager-wait-online.service   loaded active exited  Network Manager Wait Online
  NetworkManager.service               loaded active running Network Manager
  open-vm-tools.service                loaded active running Service for virtual machines hosted on VMware
  plymouth-quit-wait.service           loaded active exited  Hold until boot process finishes up
  plymouth-read-write.service          loaded active exited  Tell Plymouth To Write Out Runtime Data
  plymouth-start.service               loaded active exited  Show Plymouth Boot Screen
  UNIT                                 LOAD   ACTIVE SUB     DESCRIPTION
```

5. Disabled Service

sudo systemctl stop bluetooth

sudo systemctl disable Bluetooth

Disabling unused services reduces the attack surface and improves system security.

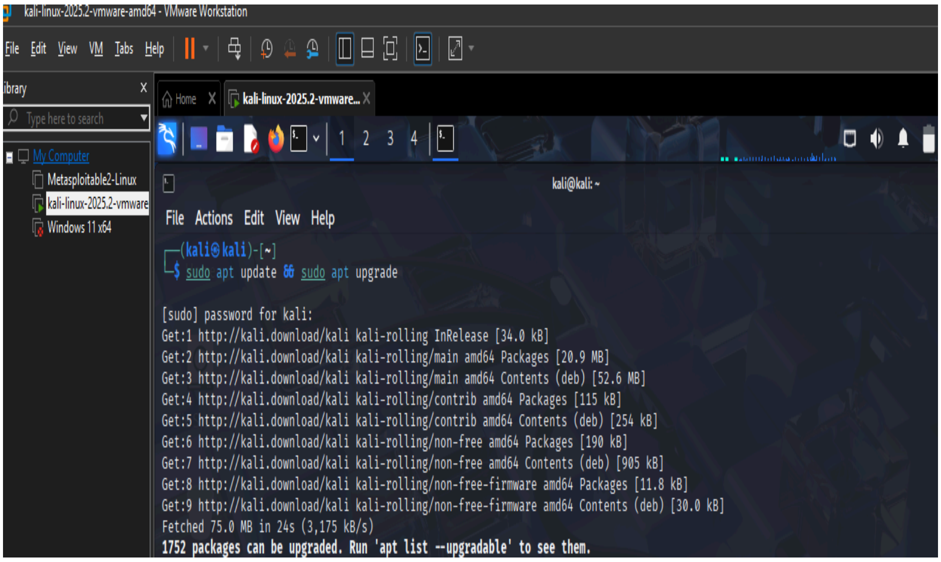
6. OS Hardening Best Practices

The following OS hardening practices were identified and applied:

- Use non-root user accounts
- Apply least privilege principle
- Enable firewall
- Disable unnecessary services
- Keep the system updated
- Use strong passwords
- Regularly monitor system logs

□ OS Security Checklist

Security Control	Status	Remarks
Non-root user enabled	✔	Default Kali setting
sudo access configured	✔	Used for admin tasks
File permissions checked	✔	chmod, chown
Firewall enabled	✔	UFW
Unnecessary services disabled	✔	Bluetooth
System updated	✔	apt update
Least privilege applied	✔	sudo usage



```
┌──(kali㉿kali)-[~]
└─$ sudo apt update && sudo apt upgrade

[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.6 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [254 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [190 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [905 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [11.8 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [30.0 kB]
Fetched 75.0 MB in 24s (3,175 kB/s)
1752 packages can be upgraded. Run 'apt list --upgradable' to see them.
```