Operating System Security Fundamentals
(Linux & Windows)

January 16, 2026

Contents

1 Installing a Linux Virtual Machine

A Linux virtual machine was installed using VirtualBox. Ubuntu Linux was selected due to its stability and security features.

Steps

- Download VirtualBox
- Create a new VM
- Assign RAM and storage
- Install Ubuntu OS

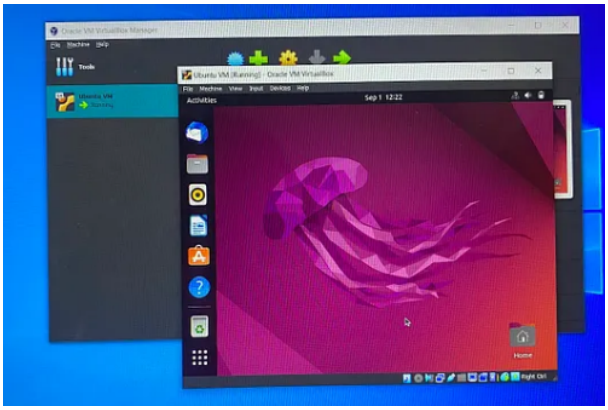

Figure 1: Linux VM Installation using VirtualBox

2 User Accounts and Access Control

Linux uses user accounts and groups to control access to system resources. Each user has a unique UID and belongs to one or more groups.

Commands Used

```
cat /etc/passwd
groups
whoami
```

Figure 2: User Accounts and Groups

3 File Permissions in Linux

Linux file permissions determine who can read, write, or execute a file.

Commands Used

```
ls -l
chmod 755 filename
chown user:group filename
```

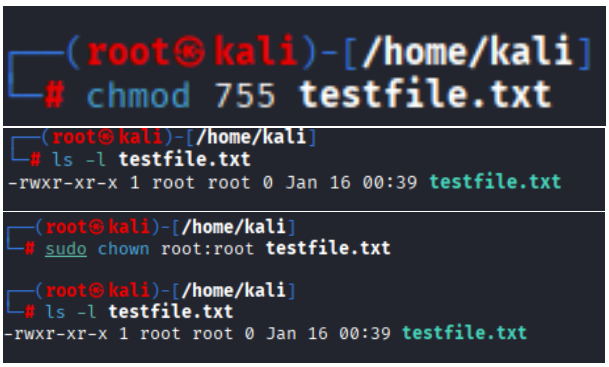

Figure 3: File Permissions using chmod and chown

4 Administrator vs Standard User

Administrator (root) users have full control over the system, while standard users have limited privileges.

Command

```
sudo su
```

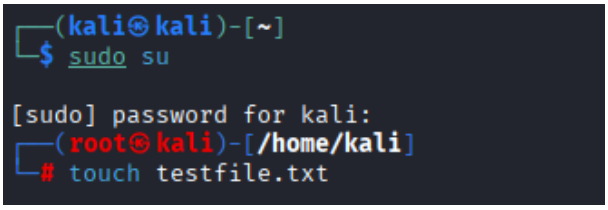

Figure 4: Administrator vs Standard User Privileges

5 Firewall Configuration

Firewalls help protect systems from unauthorized access.

Linux Firewall (UFW)

```
sudo ufw enable
sudo ufw status
```

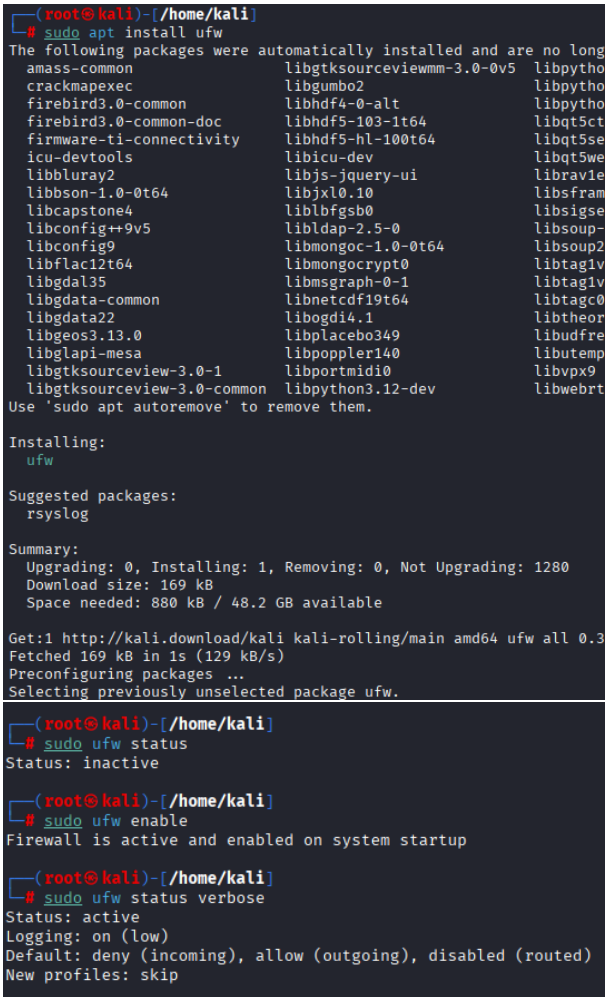

Figure 5: UFW Firewall Enabled

6 Running Processes and Services

Processes and services running on a system can be viewed using system commands.

Commands

```
ps aux
top
systemctl list-units --type=service
```

```
┌──(root㉿kali)-[/home/kali]
└─# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME
root           1  0.0  0.1  24540 14600 ?        Ss   Jan15   0:03
root           2  0.0  0.0      0     0 ?        S    Jan15   0:00
root           3  0.0  0.0      0     0 ?        S    Jan15   0:00
root           4  0.0  0.0      0     0 ?        I<   Jan15   0:00
root           5  0.0  0.0      0     0 ?        I<   Jan15   0:00
root           6  0.0  0.0      0     0 ?        I<   Jan15   0:00
root           7  0.0  0.0      0     0 ?        I<   Jan15   0:00
root           8  0.0  0.0      0     0 ?        I<   Jan15   0:00
root          12  0.0  0.0      0     0 ?        I    Jan15   0:00
root          13  0.0  0.0      0     0 ?        I<   Jan15   0:00
root          14  0.0  0.0      0     0 ?        S    Jan15   0:00
root          15  0.0  0.0      0     0 ?        I    Jan15   0:04
root          16  0.0  0.0      0     0 ?        S    Jan15   0:00
root          17  0.0  0.0      0     0 ?        S    Jan15   0:00
root          18  0.0  0.0      0     0 ?        S    Jan15   0:00
root          19  0.0  0.0      0     0 ?        S    Jan15   0:00
root          20  0.0  0.0      0     0 ?        S    Jan15   0:00
root          21  0.0  0.0      0     0 ?        S    Jan15   0:00
root          22  0.0  0.0      0     0 ?        S    Jan15   0:00
root          23  0.0  0.0      0     0 ?        S    Jan15   0:00
root          24  0.0  0.0      0     0 ?        S    Jan15   0:00
root          27  0.0  0.0      0     0 ?        S    Jan15   0:00
root          28  0.0  0.0      0     0 ?        S    Jan15   0:00
root          29  0.0  0.0      0     0 ?        S    Jan15   0:00
root          30  0.0  0.0      0     0 ?        S    Jan15   0:00
root          32  0.0  0.0      0     0 ?        I<   Jan15   0:04
root          33  0.0  0.0      0     0 ?        S    Jan15   0:00
root          34  0.0  0.0      0     0 ?        S    Jan15   0:00
root          35  0.0  0.0      0     0 ?        S    Jan15   0:00
root          36  0.0  0.0      0     0 ?        S    Jan15   0:00
root          38  0.0  0.0      0     0 ?        I<   Jan15   0:00
root          39  0.0  0.0      0     0 ?        I    Jan15   0:09
root          44  0.0  0.0      0     0 ?        I    Jan15   0:06
root          45  0.0  0.0      0     0 ?        S    Jan15   0:00
```

```
┌──(root㉿kali)-[/home/kali]
└─# top
top - 00:52:08 up  4:42,  1 user,  load average: 5.14, 4.13, 2.35
Tasks: 227 total,   1 running, 225 sleeping,   0 stopped,   1 zombie
%Cpu(s): 93.8 us,  2.1 sy,  0.0 ni,  0.2 id,  3.8 wa,  0.0 hi,  0.2 s
MiB Mem :   7909.3 total,    139.8 free,   2088.5 used,   5997.2 buff
MiB Swap:   1024.0 total,   1024.0 free,      0.0 used.   5820.8 avai

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+
   5401 root      20   0 2221484 743200  16660 S 379.1   9.2  36:33.39
    917 root      20   0  393000 140780  52564 S   1.3   1.7   2:21.58
   1315 kali      20   0  311192  64600  22636 S   0.7   0.8   1:32.73
    575 root      20   0  113744   9356   7700 S   0.3   0.1   1:08.99
   1253 kali      20   0 1183892 114624  72164 S   0.3   1.4   1:16.24
   1374 kali      20   0  370248  39376  29772 S   0.3   0.5   1:12.30
   1593 kali      20   0  389912   8300   7068 S   0.3   0.1   0:01.72
   5463 root      20   0       0      0      0 I   0.3   0.0   0:07.67
   6601 root      20   0       0      0      0 I   0.3   0.0   0:06.74
   7435 root      20   0       0      0      0 I   0.3   0.0   0:05.56
   8711 root      20   0   10472   5992   3816 R   0.3   0.1   0:00.54
      1 root      20   0   24540  14600  10168 S   0.0   0.2   0:03.04
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.02
      3 root      20   0       0      0      0 S   0.0   0.0   0:00.00
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00
      7 root       0 -20       0      0      0 I   0.0   0.0   0:00.00
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00
     12 root      20   0       0      0      0 I   0.0   0.0   0:00.00
     13 root       0 -20       0      0      0 I   0.0   0.0   0:00.09
     14 root      20   0       0      0      0 S   0.0   0.0   0:00.74
     15 root      20   0       0      0      0 I   0.0   0.0   0:04.58
     16 root      20   0       0      0      0 S   0.0   0.0   0:00.03
     17 root      20   0       0      0      0 S   0.0   0.0   0:00.01
     18 root      rt   0       0      0      0 S   0.0   0.0   0:00.24
     19 root     -51   0       0      0      0 S   0.0   0.0   0:00.00
     20 root      20   0       0      0      0 S   0.0   0.0   0:00.00
     21 root      20   0       0      0      0 S   0.0   0.0   0:00.00
     22 root     -51   0       0      0      0 S   0.0   0.0   0:00.00
```

```
┌──(root㉿kali)-[/home/kali]
└─# systemctl list-units --type=service

  UNIT                                      LOAD
  accounts-daemon.service                   loade
  colord.service                            loade
  console-setup.service                     loade
  cron.service                              loade
  dbus.service                              loade
  getty@tty1.service                        loade
  haveged.service                           loade
  ifupdown-pre.service                      loade
  keyboard-setup.service                    loade
  kmod-static-nodes.service                 loade
  lightdm.service                           loade
  ModemManager.service                      loade
  nessusd.service                           loade
  networking.service                        loade
  NetworkManager-wait-online.service        loade
  NetworkManager.service                    loade
  open-vm-tools.service                     loade
  plymouth-quit-wait.service                loade
  plymouth-read-write.service               loade
  plymouth-start.service                    loade
  polkit.service                            loade
  rpc-statd-notify.service                  loade
  rtkit-daemon.service                      loade
  systemd-binfmt.service                    loade
  systemd-journal-flush.service             loade
```

7 Disabling Unnecessary Services

Disabling unused services reduces the system attack surface.

Command

```
sudo systemctl disable bluetooth
```

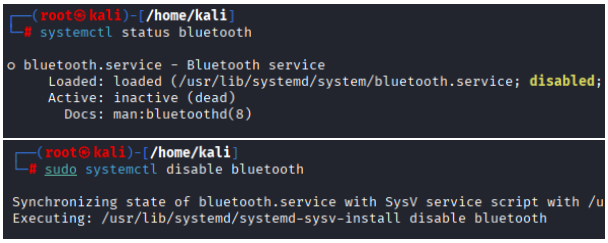

Figure 7: Disabling Unnecessary Services

8 Operating System Hardening Best Practices

- Use strong passwords
- Keep the OS updated
- Enable firewall
- Disable unused services
- Apply least privilege principle
- Monitor logs regularly

9 summary

Operating system security is essential to protect systems from threats. Proper configuration, user management, and hardening techniques significantly reduce security risks.