Task 2: Operating System Security Fundamentals (Linux & Windows)

◆ Objective

The objective of this task is to understand operating system–level security, including user access control, file permissions, firewall configuration, process monitoring, service management, and OS hardening best practices using Linux and Windows.

◆ Tools Used

Primary OS: Kali Linux VM)

Virtualization Tool: VMare workstation

Windows Security Tool: Windows Defender Firewall

Commands Used: ls -l, chmod, chown, ufw, ps, systemctl

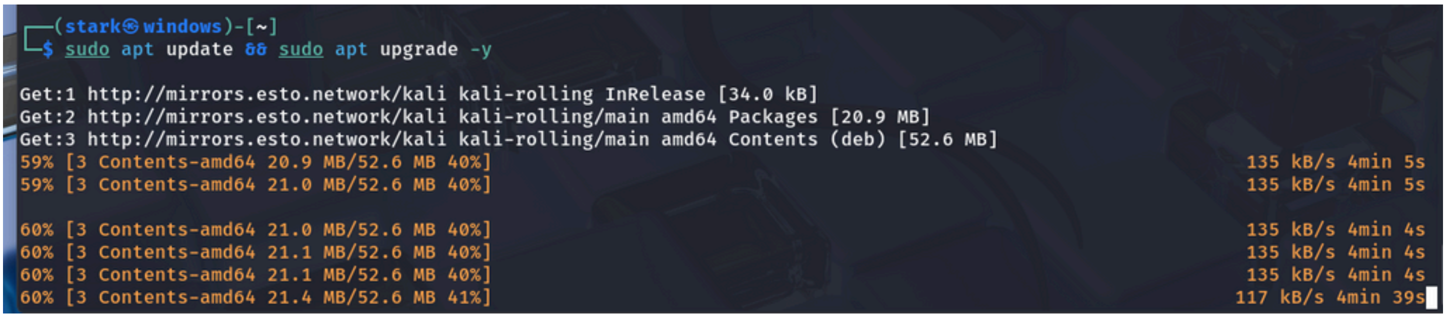
◆ Task Implementation

Installation of Kali Linux Virtual Machine

A Kali Linux virtual machine was installed using VMare workstation. The system was updated after installation to ensure the latest security patches were applied.

Command used:

sudo apt update && sudo apt upgrade -y



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

Get:1 http://mirrors.esto.network/kali kali-rolling InRelease [34.0 kB]
Get:2 http://mirrors.esto.network/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://mirrors.esto.network/kali kali-rolling/main amd64 Contents (deb) [52.6 MB]
59% [3 Contents-amd64 20.9 MB/52.6 MB 40%]                          135 kB/s 4min 5s
59% [3 Contents-amd64 21.0 MB/52.6 MB 40%]                          135 kB/s 4min 5s

60% [3 Contents-amd64 21.0 MB/52.6 MB 40%]                          135 kB/s 4min 4s
60% [3 Contents-amd64 21.1 MB/52.6 MB 40%]                          135 kB/s 4min 4s
60% [3 Contents-amd64 21.1 MB/52.6 MB 40%]                          135 kB/s 4min 4s
60% [3 Contents-amd64 21.4 MB/52.6 MB 41%]                         117 kB/s 4min 39s
```

Kali Linux desktop running inside Vmare

Terminal showing successful update

User Accounts & Access Control

Linux uses user-based access control where each user has specific permissions.

Commands used:

whoami

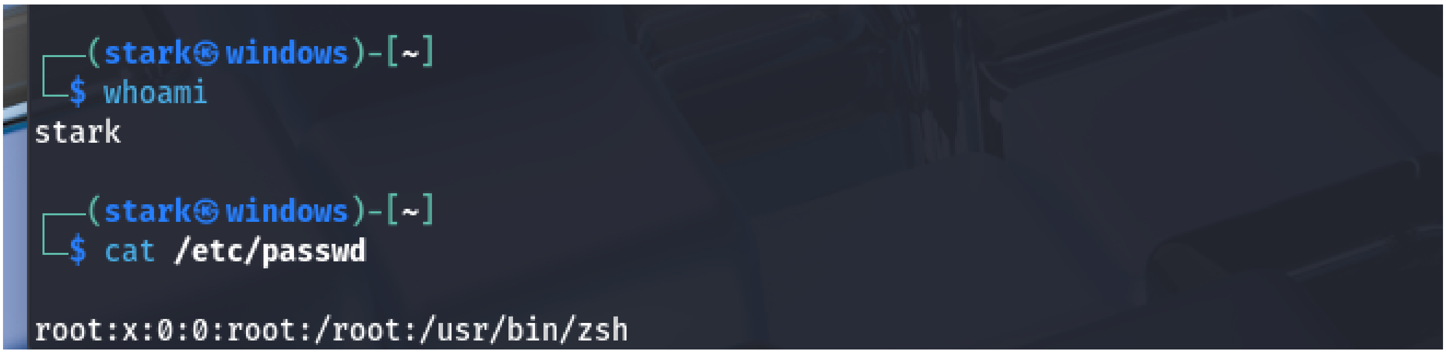
cat /etc/passwd

groups

root → administrator user

normal user → limited privileges

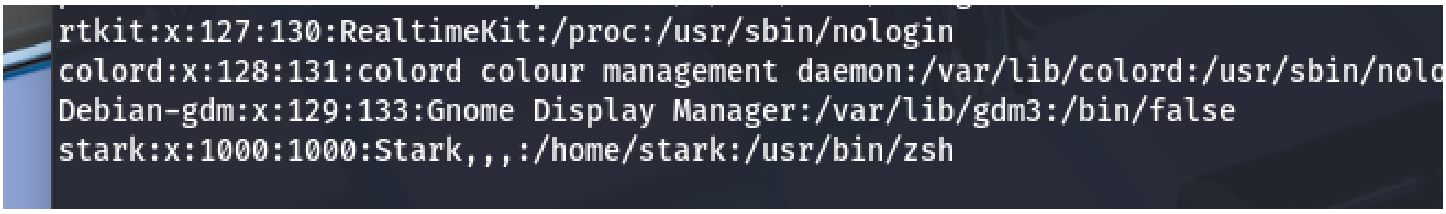
sudo → temporary administrative access



```
┌──(stark㉿windows)-[~]
└─$ whoami
stark

┌──(stark㉿windows)-[~]
└─$ cat /etc/passwd

root:x:0:0:root:/root:/usr/bin/zsh
```



```
rtkit:x:127:130:RealtimeKit:/proc:/usr/sbin/nologin
colord:x:128:131:colord colour management daemon:/var/lib/colord:/usr/sbin/nolo
Debian-gdm:x:129:133:Gnome Display Manager:/var/lib/gdm3:/bin/false
stark:x:1000:1000:Stark,,,:/home/stark:/usr/bin/zsh
```

File Permissions in Linux

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

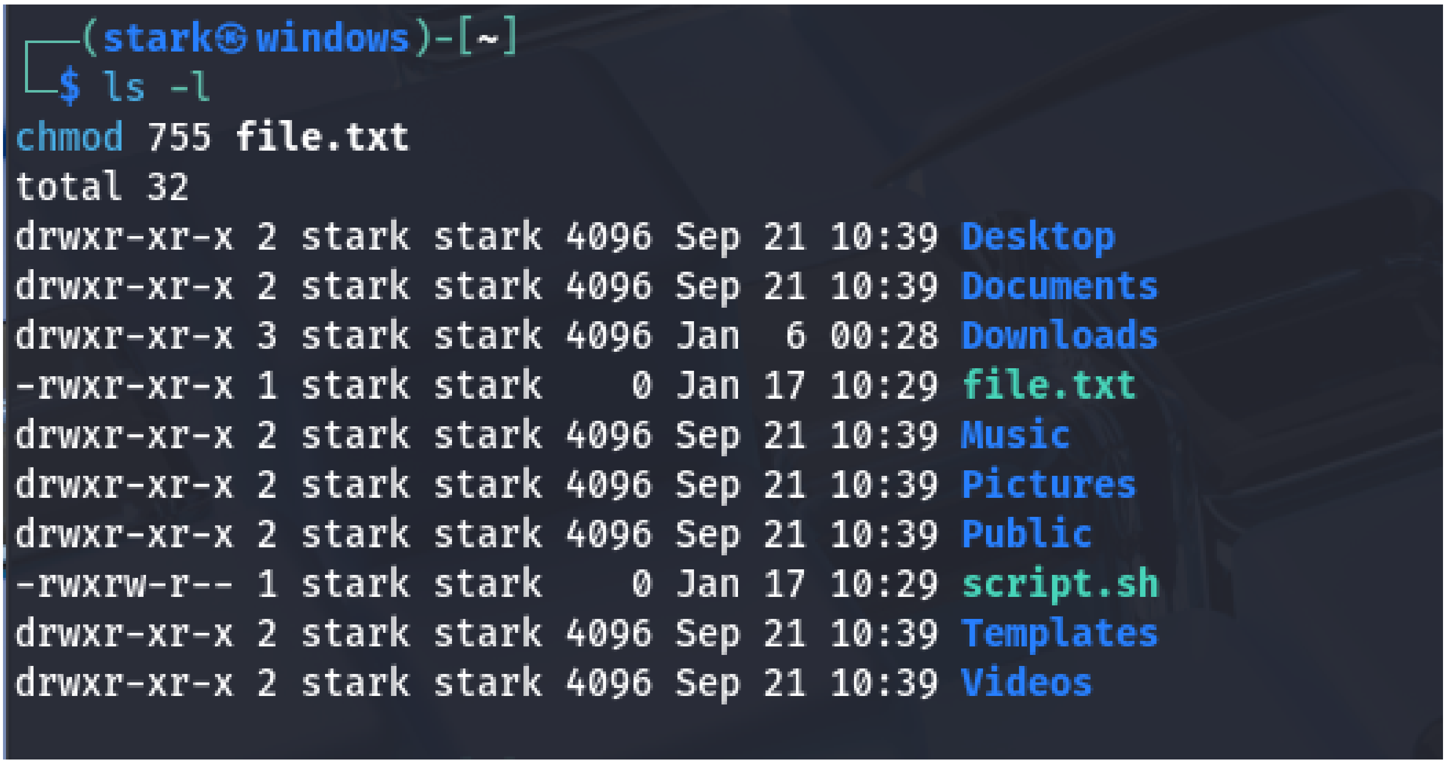
Commands used:

ls -l

chmod 755 file.txt

chmod u+x script.sh

chown user:user file.txt



```
┌──(stark㉿windows)-[~]
└─$ ls -l
chmod 755 file.txt
total 32
drwxr-xr-x 2 stark stark 4096 Sep 21 10:39 Desktop
drwxr-xr-x 2 stark stark 4096 Sep 21 10:39 Documents
drwxr-xr-x 3 stark stark 4096 Jan  6 00:28 Downloads
-rwxr-xr-x 1 stark stark    0 Jan 17 10:29 file.txt
drwxr-xr-x 2 stark stark 4096 Sep 21 10:39 Music
drwxr-xr-x 2 stark stark 4096 Sep 21 10:39 Pictures
drwxr-xr-x 2 stark stark 4096 Sep 21 10:39 Public
-rwxrw-r-- 1 stark stark    0 Jan 17 10:29 script.sh
drwxr-xr-x 2 stark stark 4096 Sep 21 10:39 Templates
drwxr-xr-x 2 stark stark 4096 Sep 21 10:39 Videos
```

Administrator vs Standard User

Root user: Full system control

Standard user: Restricted access

Best practice: Do not log in as root daily

Linux restricts direct root login to improve security.

Terminal showing denied root login attempt OR explanation note

Firewall Configuration

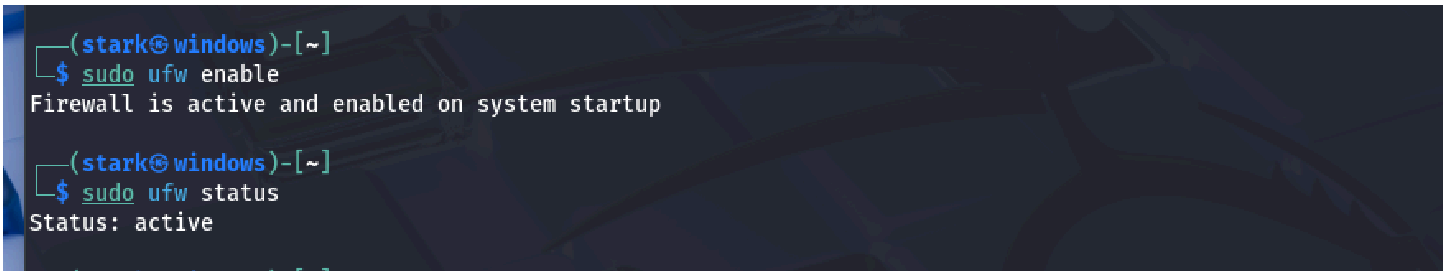
Linux (UFW)

sudo ufw enable

sudo ufw status

Windows

Windows Defender Firewall enabled via Control Panel



```
┌──(stark㉿windows)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

┌──(stark㉿windows)-[~]
└─$ sudo ufw status
Status: active
```

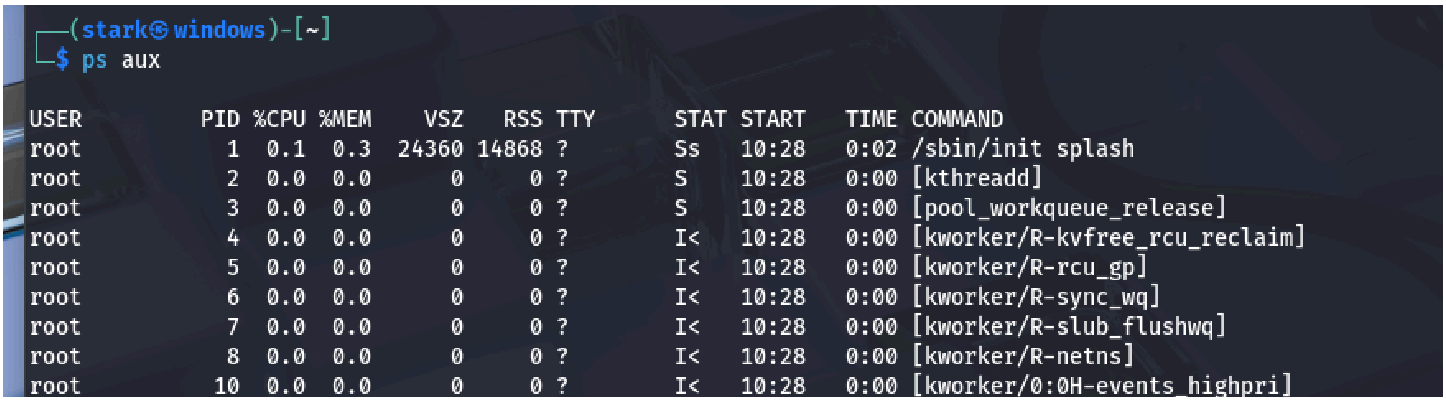
ufw status showing active

Windows Defender Firewall ON screen (if using Windows)

Identifying Running Processes & Services

Commands used:

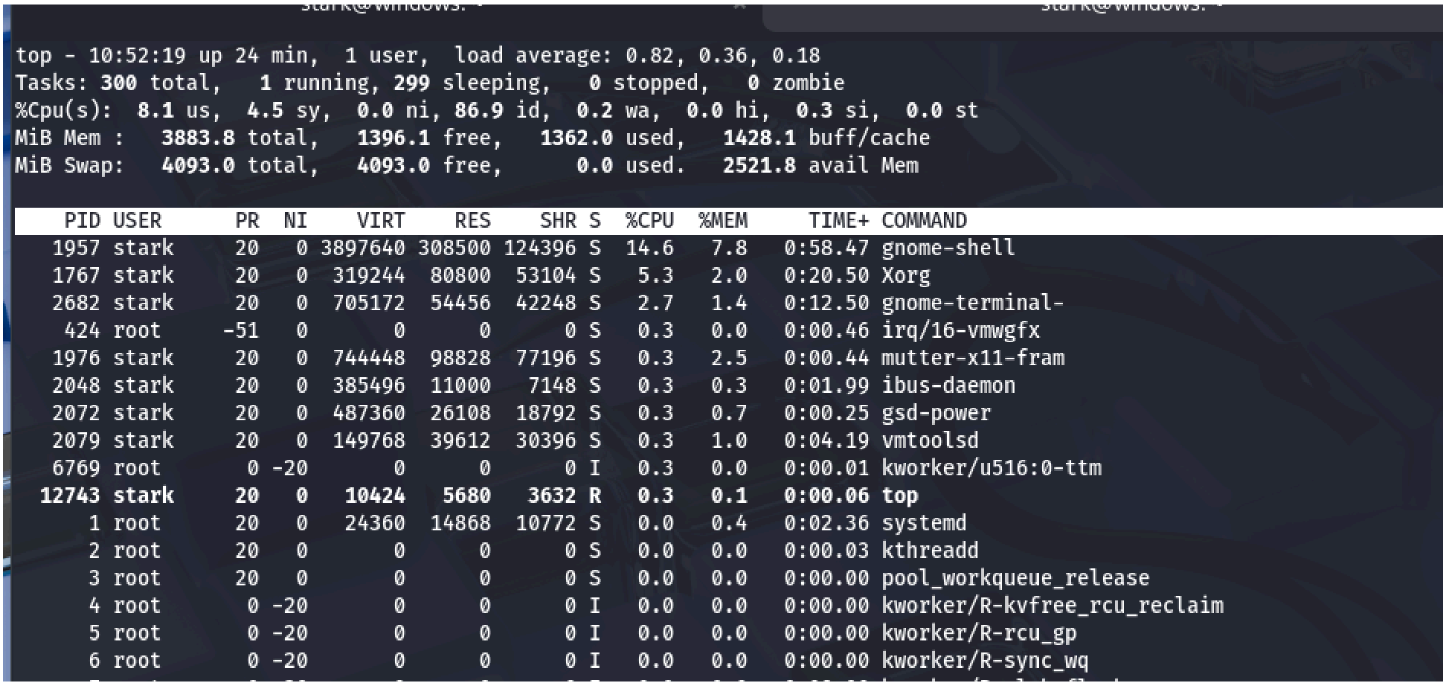
ps aux



```
┌──(stark㉿windows)-[~]
└─$ ps aux

USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.1  0.3  24360 14868 ?        Ss   10:28   0:02 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    10:28   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    10:28   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   10:28   0:00 [kworker/R-kvfree_rcu_reclaim]
root           5  0.0  0.0      0     0 ?        I<   10:28   0:00 [kworker/R-rcu_gp]
root           6  0.0  0.0      0     0 ?        I<   10:28   0:00 [kworker/R-sync_wq]
root           7  0.0  0.0      0     0 ?        I<   10:28   0:00 [kworker/R-slub_flushwq]
root           8  0.0  0.0      0     0 ?        I<   10:28   0:00 [kworker/R-netns]
root          10  0.0  0.0      0     0 ?        I<   10:28   0:00 [kworker/0:0H-events_highpri]
```

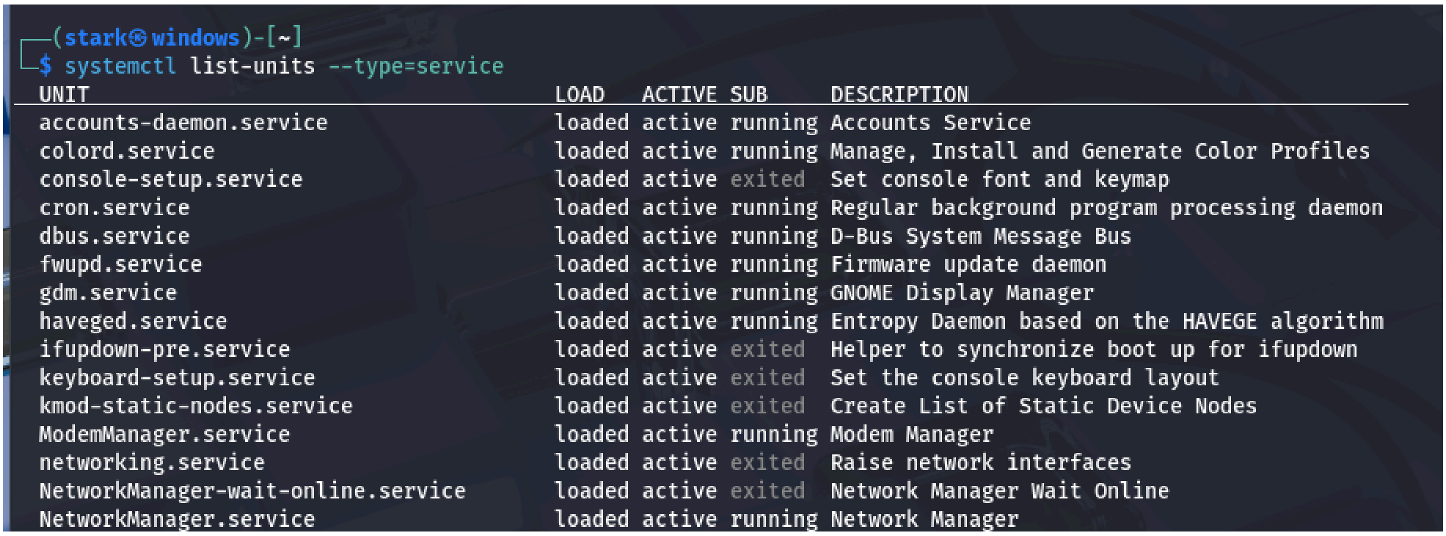
top



```
top - 10:52:19 up 24 min,  1 user,  load average: 0.82, 0.36, 0.18
Tasks: 300 total,   1 running, 299 sleeping,   0 stopped,   0 zombie
%Cpu(s):  8.1 us,  4.5 sy,  0.0 ni, 86.9 id,  0.2 wa,  0.0 hi,  0.3 si,  0.0 st
MiB Mem :   3883.8 total,   1396.1 free,   1362.0 used,   1428.1 buff/cache
MiB Swap:   4093.0 total,   4093.0 free,      0.0 used.   2521.8 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   1957 stark     20   0 3897640 308500 124396 S  14.6   7.8   0:58.47 gnome-shell
   1767 stark     20   0  319244  80800  53104 S   5.3   2.0   0:20.50 Xorg
   2682 stark     20   0  705172  54456  42248 S   2.7   1.4   0:12.50 gnome-terminal-
    424 root     -51   0       0      0      0 S   0.3   0.0   0:00.46 irq/16-vmwgfx
   1976 stark     20   0  744448  98828  77196 S   0.3   2.5   0:00.44 mutter-x11-fram
   2048 stark     20   0  385496  11000   7148 S   0.3   0.3   0:01.99 ibus-daemon
   2072 stark     20   0  487360  26108  18792 S   0.3   0.7   0:00.25 gsd-power
   2079 stark     20   0  149768  39612  30396 S   0.3   1.0   0:04.19 vmtoolsd
   6769 root       0 -20       0      0      0 I   0.3   0.0   0:00.01 kworker/u516:0-ttm
  12743 stark     20   0   10424   5680   3632 R   0.3   0.1   0:00.06 top
      1 root      20   0   24360  14868  10772 S   0.0   0.4   0:02.36 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.03 kthreadd
      3 root      20   0       0      0      0 S   0.0   0.0   0:00.00 pool_workqueue_release
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-kvfree_rcu_reclaim
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-rcu_gp
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-sync_wq
```

systemctl list-units --type=service



```
┌──(stark㉿windows)-[~]
└─$ 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
  fwupd.service                          loaded active running Firmware update daemon
  gdm.service                            loaded active running GNOME Display Manager
  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
  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
```

This helps identify unnecessary or suspicious services.

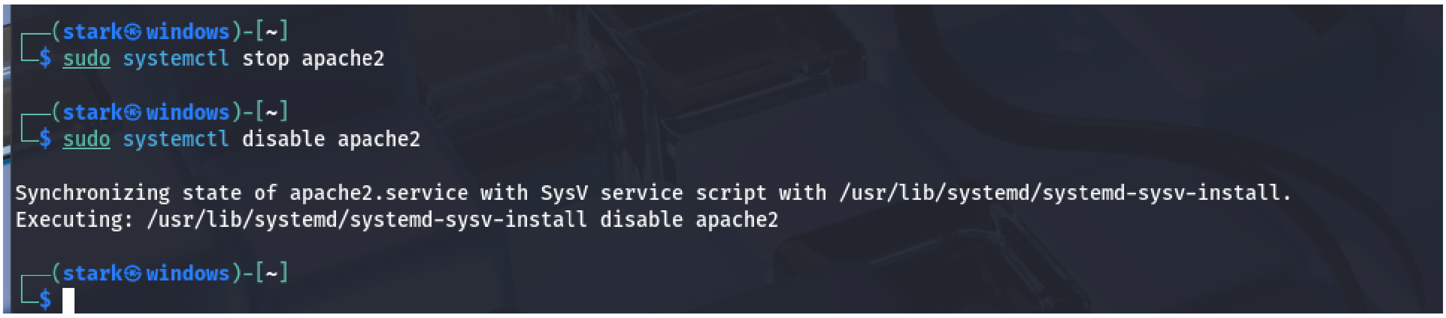
Disabling Unnecessary Services

Unused services increase attack surface and should be disabled.

Commands used:

sudo systemctl stop apache2

sudo systemctl disable apache2



```
┌──(stark㉿windows)-[~]
└─$ sudo systemctl stop apache2

┌──(stark㉿windows)-[~]
└─$ sudo systemctl disable apache2

Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable apache2

┌──(stark㉿windows)-[~]
└─$ 
```

Service stopped/disabled output

OS Hardening Best Practices

Linux Hardening

Use strong passwords

Disable root login

Use sudo

Enable firewall

Keep system updated

Remove unused packages

Restrict file permissions

Monitor logs

Windows Hardening

Enable Windows Defender

Enable Firewall

Use standard user account

Disable unused services

Enable BitLocker (if available)