task 2

OS Security & Hardening Using **Kali Linux**

🔧 Tool Used

Primary OS: Kali Linux (Virtual Machine)

Virtualization: VirtualBox
Security Tools: Built-in Linux security tools

1️⃣ Install & Prepare Kali Linux

- Install Kali Linux as a **Virtual Machine**
- Login using a **standard user account** (not root)

Update the system: sudo apt update && sudo apt upgrade -y

2️⃣ User Accounts & Access Control

Check existing users:

```
cat /etc/passwd
```

Check currently logged-in users:

```
who
```

3️⃣ File Permissions & Ownership

Linux uses **Read (r), Write (w), Execute (x)** permissions.

View permissions:ls -l

4️⃣ Administrator vs Standard User

User Type	Description
Standard User	Limited privileges, safer
Root User	Full system control

5️⃣ Enable Firewall (UFW in Kali)

Install and enable UFW:

```
sudo apt install ufw -y sudo ufw enable sudo ufw status
```

Allow required services only:

```
sudo ufw allow ssh
```

6️⃣ Identify Running Processes & Services

View running processes:

```
ps aux
```

Real-time monitoring:

```
top
```

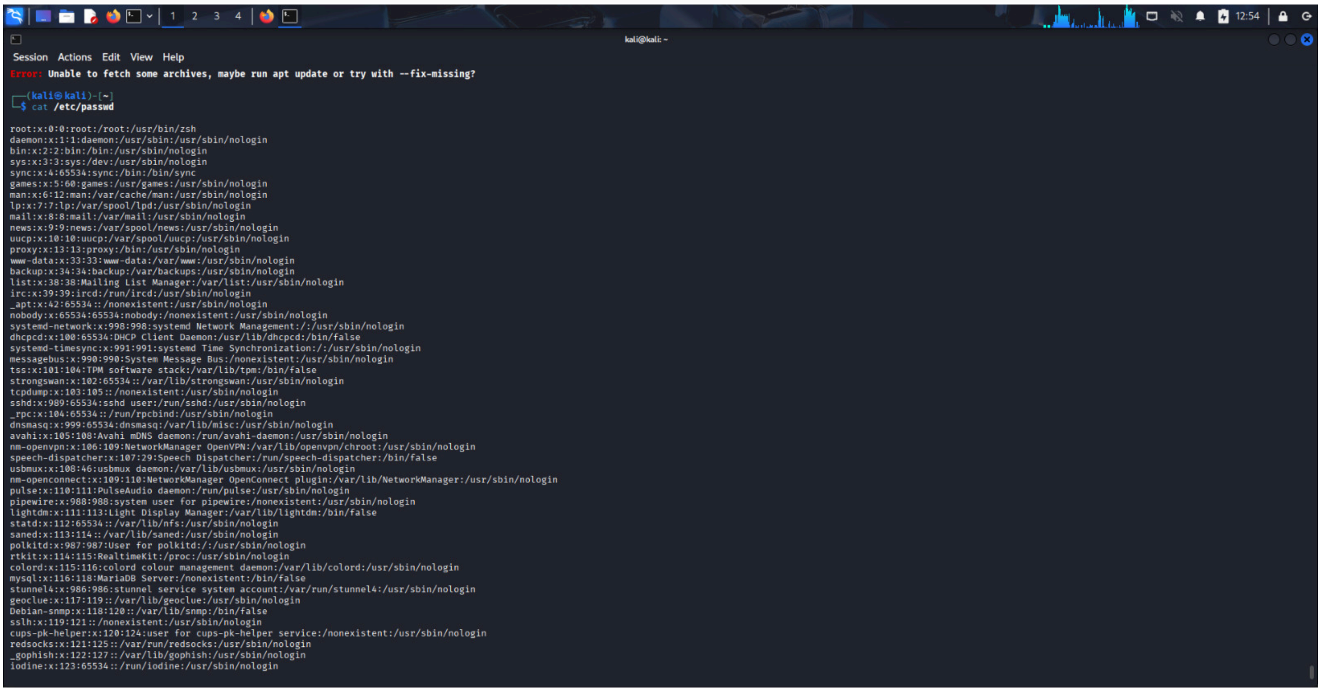
Check active services:

```
systemctl list-units --type=service
```

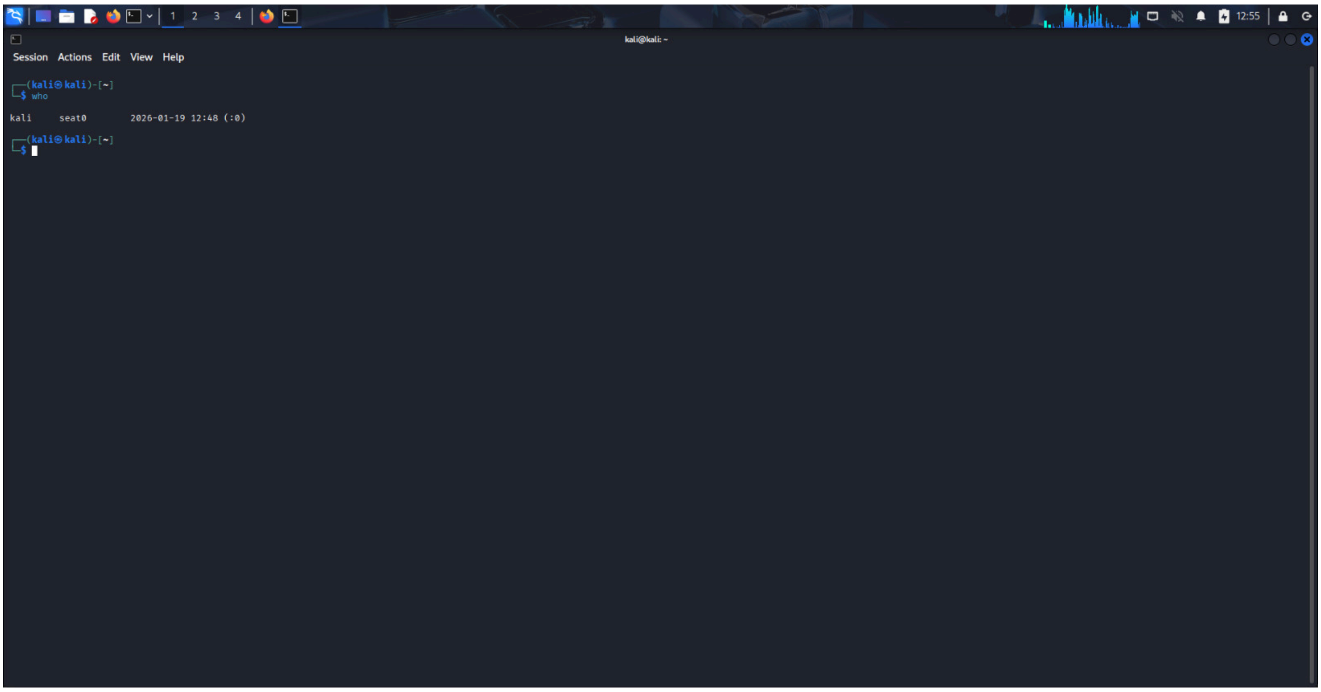
7️⃣ Disable Unnecessary Services

Stop unused services:

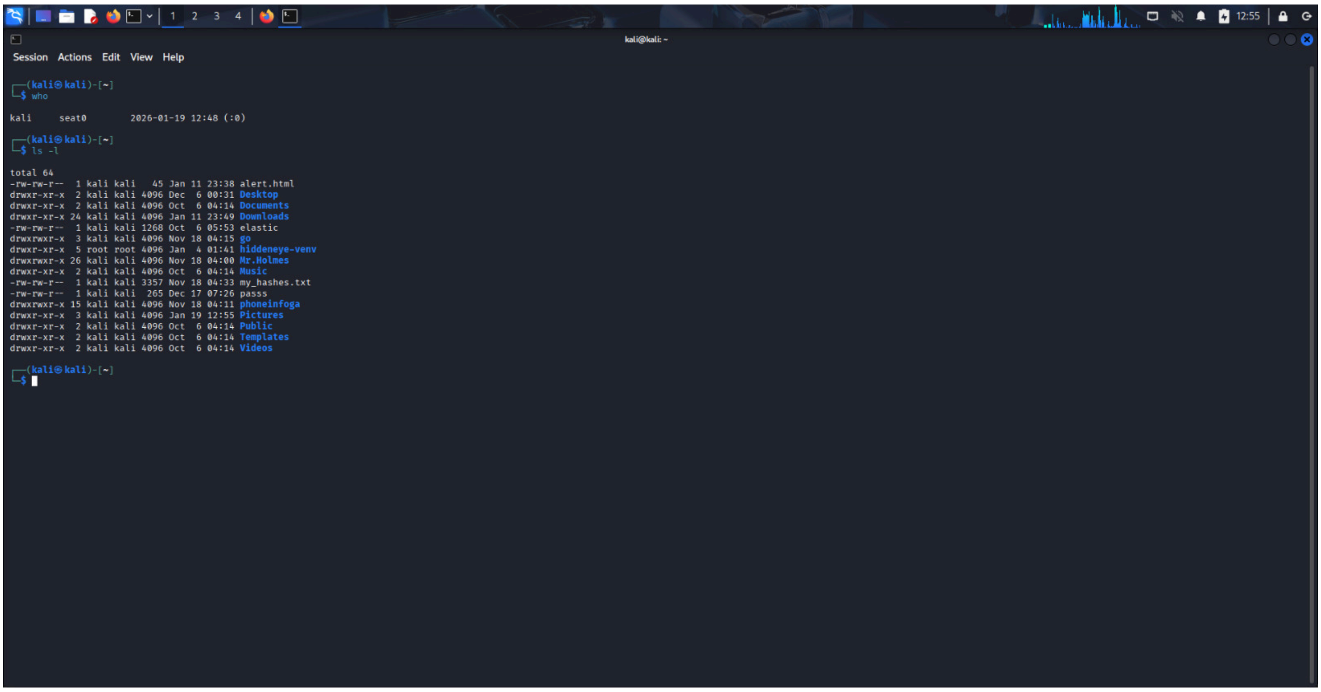
```
sudo systemctl stop service_name sudo systemctl disable service_name
```



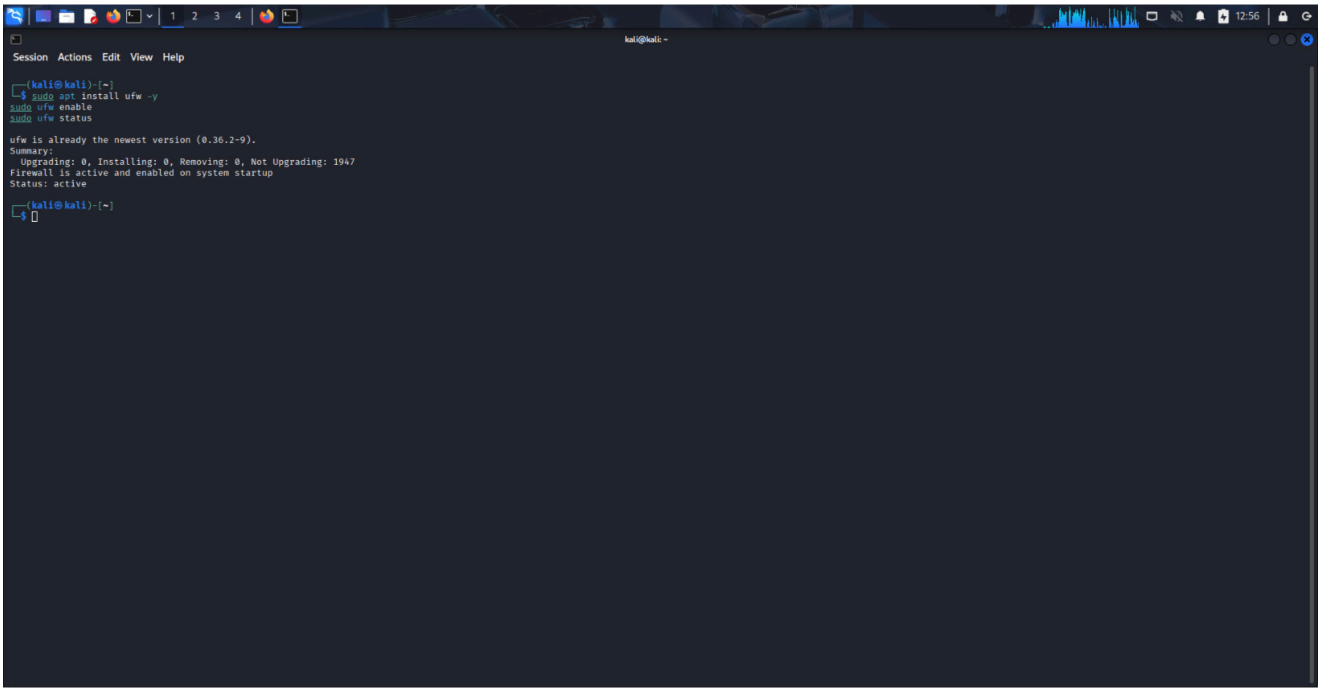
```
Error: Unable to fetch some archives, maybe run apt update or try with --fix-missing?

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

root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon:/usr/lib/dhcpcd:/bin/false
systemd-timesync:x:991:991:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:990:990:System Message Bus:/nonexistent:/usr/sbin/nologin
tss:x:101:104:TPM software stack:/var/lib/tpm:/bin/false
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:103:105::/nonexistent:/usr/sbin/nologin
sshd:x:989:65534:sshd user:/run/sshd:/usr/sbin/nologin
_rpc:x:104:65534::/run/rpcbind:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:105:108:Avahi mDNS daemon:/run/avahi-daemon:/usr/sbin/nologin
nm-openvpn:x:106:109:NetworkManager OpenVPN:/var/lib/openvpn/chroot:/usr/sbin/nologin
speech-dispatcher:x:107:29:Speech Dispatcher:/run/speech-dispatcher:/bin/false
usbmux:x:108:46:usbmux daemon:/var/lib/usbmux:/usr/sbin/nologin
nm-openconnect:x:109:110:NetworkManager OpenConnect plugin:/var/lib/NetworkManager:/usr/sbin/nologin
pulse:x:110:111:PulseAudio daemon:/run/pulse:/usr/sbin/nologin
pipewire:x:988:988:system user for pipewire:/nonexistent:/usr/sbin/nologin
lightdm:x:111:113:Light Display Manager:/var/lib/lightdm:/bin/false
statd:x:112:65534::/var/lib/nfs:/usr/sbin/nologin
saned:x:113:114::/var/lib/saned:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/:/usr/sbin/nologin
rtkit:x:114:115:RealtimeKit:/proc:/usr/sbin/nologin
colord:x:115:116:colord colour management daemon:/var/lib/colord:/usr/sbin/nologin
mysql:x:116:118:MariaDB Server:/nonexistent:/bin/false
stunnel4:x:986:986:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
geoclue:x:117:119::/var/lib/geoclue:/usr/sbin/nologin
Debian-snmp:x:118:120::/var/lib/snmp:/bin/false
sslh:x:119:121::/nonexistent:/usr/sbin/nologin
cups-pk-helper:x:120:124:user for cups-pk-helper service:/nonexistent:/usr/sbin/nologin
redsocks:x:121:125::/var/run/redsocks:/usr/sbin/nologin
_gophish:x:122:127::/var/lib/gophish:/usr/sbin/nologin
iodine:x:123:65534::/run/iodine:/usr/sbin/nologin
```



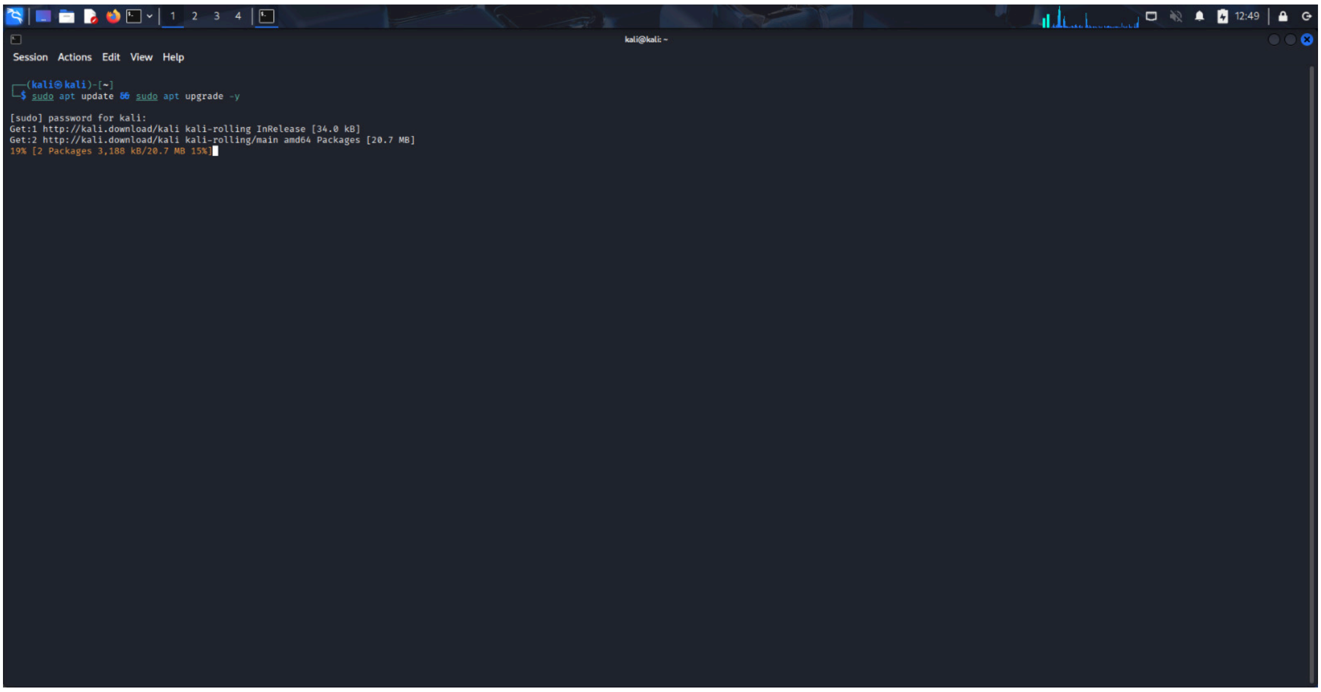
```
┌──(kali㉿kali)-[~]
└─$ who

kali     seat0        2026-01-19 12:48 (:0)

┌──(kali㉿kali)-[~]
└─$ 
```



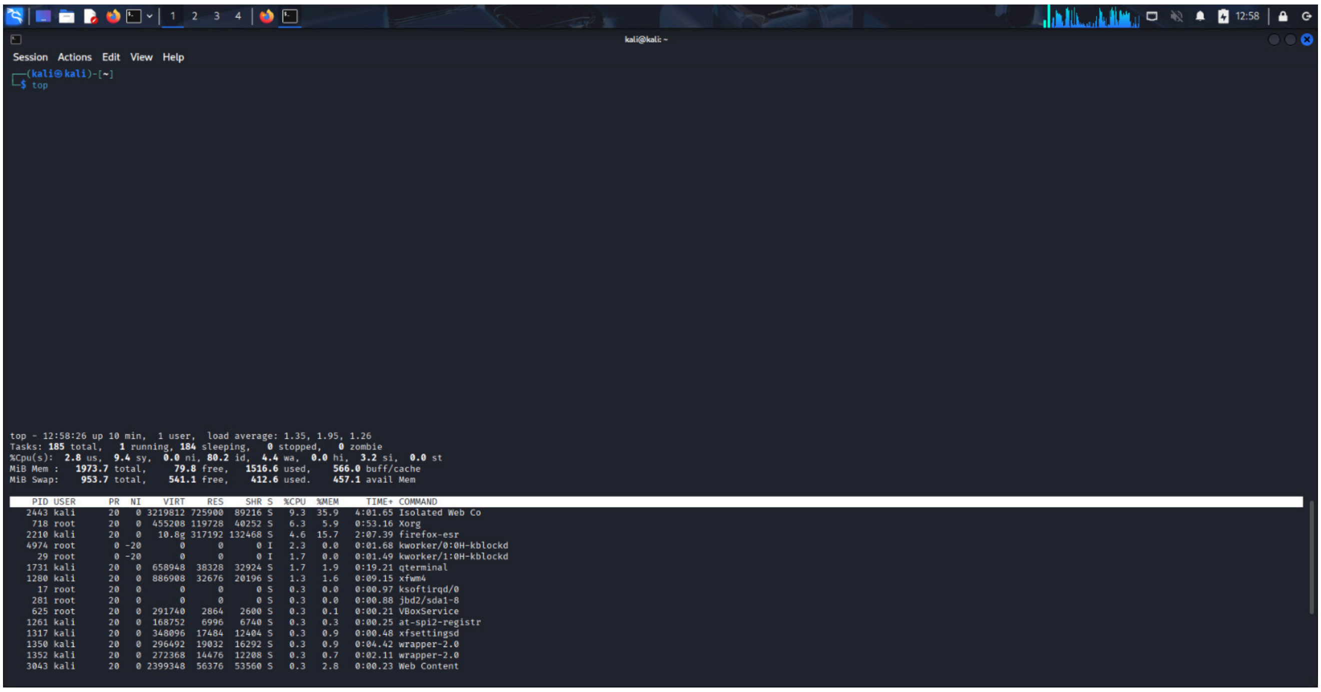
```
┌──(kali㉿kali)-[~]
└─$ who

kali     seat0        2026-01-19 12:48 (:0)

┌──(kali㉿kali)-[~]
└─$ ls -l

total 64
-rw-rw-r--  1 kali kali   45 Jan 11 23:38 alert.html
drwxr-xr-x  2 kali kali 4096 Dec  6 00:31 Desktop
drwxr-xr-x  2 kali kali 4096 Oct  6 04:14 Documents
drwxr-xr-x 24 kali kali 4096 Jan 11 23:49 Downloads
-rw-rw-r--  1 kali kali 1268 Oct  6 05:53 elastic
drwxrwxr-x  3 kali kali 4096 Nov 18 04:15 go
drwxr-xr-x  5 root root 4096 Jan  4 01:41 hiddeneye-venv
drwxrwxr-x 26 kali kali 4096 Nov 18 04:00 Mr.Holmes
drwxr-xr-x  2 kali kali 4096 Oct  6 04:14 Music
-rw-rw-r--  1 kali kali 3357 Nov 18 04:33 my_hashes.txt
-rw-rw-r--  1 kali kali  265 Dec 17 07:26 passs
drwxrwxr-x 15 kali kali 4096 Nov 18 04:11 phoneinfoga
drwxr-xr-x  3 kali kali 4096 Jan 19 12:55 Pictures
drwxr-xr-x  2 kali kali 4096 Oct  6 04:14 Public
drwxr-xr-x  2 kali kali 4096 Oct  6 04:14 Templates
drwxr-xr-x  2 kali kali 4096 Oct  6 04:14 Videos

┌──(kali㉿kali)-[~]
└─$ 
```



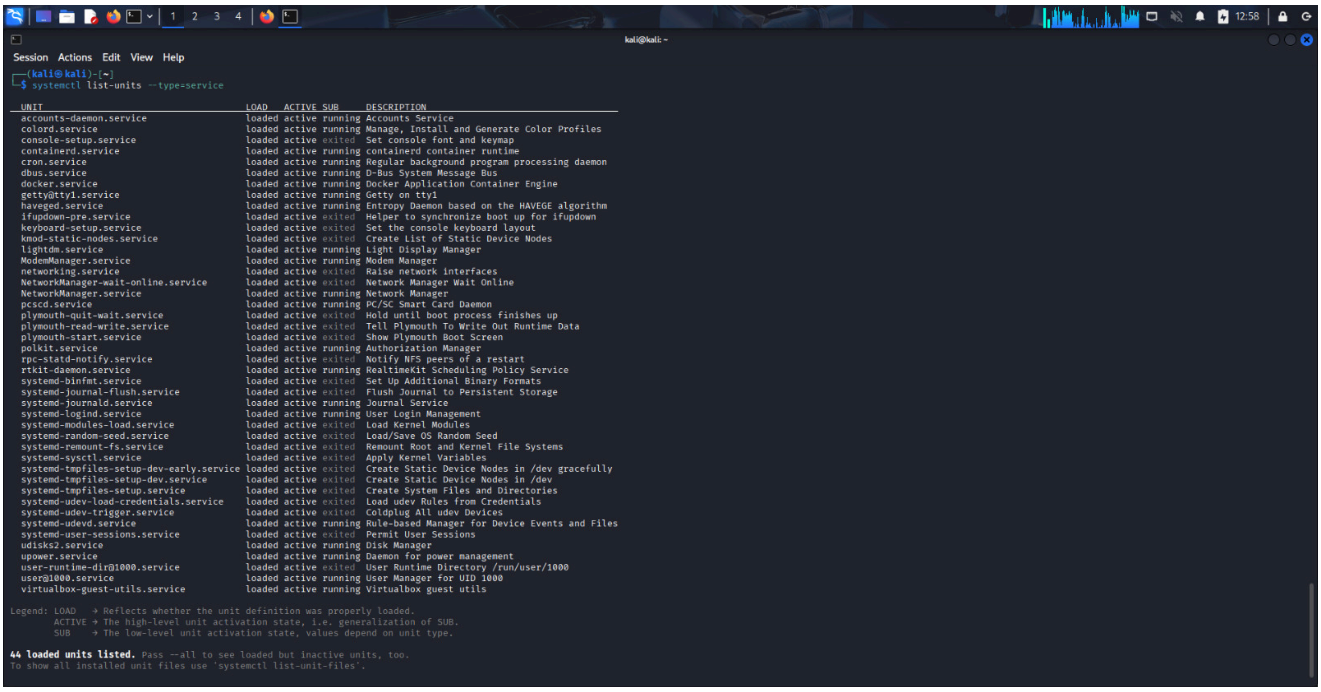
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install ufw -y
sudo ufw enable
sudo ufw status

ufw is already the newest version (0.36.2-9).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1947
Firewall is active and enabled on system startup
Status: active

┌──(kali㉿kali)-[~]
└─$ 
```



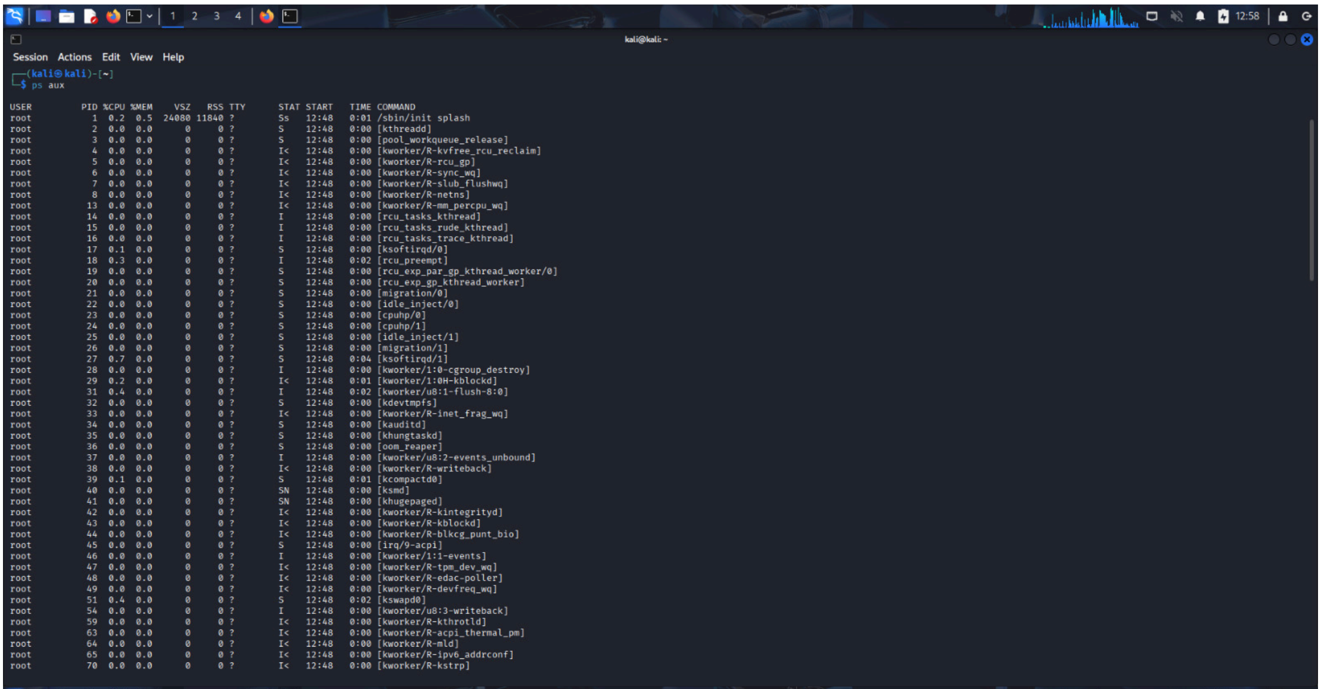
```
┌──(kali㉿kali)-[~]
└─$ sudo apt update && sudo apt upgrade -y

[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 [20.7 MB]
19% [2 Packages 3,188 kB/20.7 MB 15%]
```



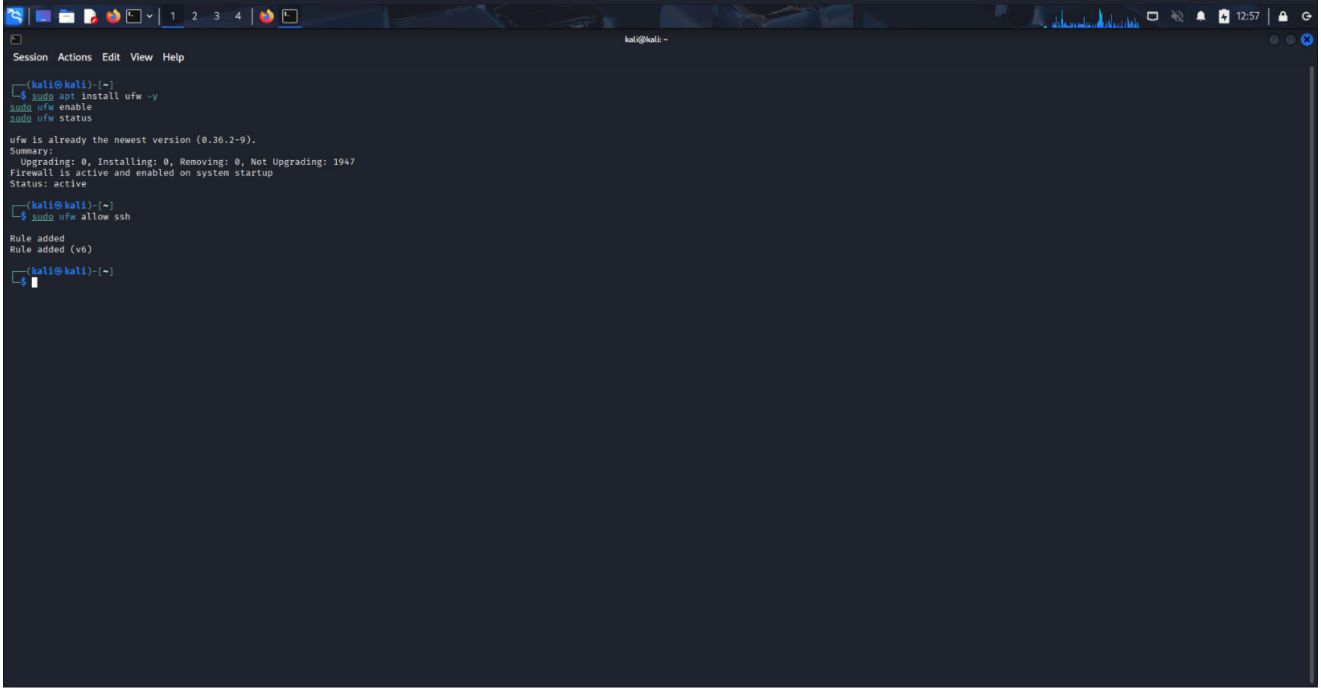
```
┌──(kali㉿kali)-[~]
└─$ top

top - 12:58:26 up 10 min,  1 user,  load average: 1.35, 1.95, 1.26
Tasks: 185 total,   1 running, 184 sleeping,   0 stopped,   0 zombie
%Cpu(s):  2.8 us,  9.4 sy,  0.0 ni, 80.2 id,  4.4 wa,  0.0 hi,  3.2 si,  0.0 st
MiB Mem :   1973.7 total,     79.8 free,   1516.6 used,    566.0 buff/cache
MiB Swap:    953.7 total,    541.1 free,    412.6 used.    457.1 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   2443 kali      20   0 3219812 725900  89216 S   9.3  35.9   4:01.65 Isolated Web Co
    718 root      20   0  455208 119728  40252 S   6.3   5.9   0:53.16 Xorg
   2210 kali      20   0   10.8g 317192 132468 S   4.6  15.7   2:07.39 firefox-esr
   4974 root       0 -20       0      0      0 I   2.3   0.0   0:01.68 kworker/0:0H-kblockd
     29 root       0 -20       0      0      0 I   1.7   0.0   0:01.49 kworker/1:0H-kblockd
   1731 kali      20   0  658948  38328  32924 S   1.7   1.9   0:19.21 qterminal
   1280 kali      20   0  886908  32676  20196 S   1.3   1.6   0:09.15 xfwm4
     17 root      20   0       0      0      0 S   0.3   0.0   0:00.97 ksoftirqd/0
    281 root      20   0       0      0      0 S   0.3   0.0   0:00.88 jbd2/sda1-8
    625 root      20   0  291740   2864   2600 S   0.3   0.1   0:00.21 VBoxService
   1261 kali      20   0  168752   6996   6740 S   0.3   0.3   0:00.25 at-spi2-registr
   1317 kali      20   0  348096  17484  12404 S   0.3   0.9   0:00.48 xfsettingsd
   1350 kali      20   0  296492  19032  16292 S   0.3   0.9   0:04.42 wrapper-2.0
   1352 kali      20   0  272368  14476  12208 S   0.3   0.7   0:02.11 wrapper-2.0
   3043 kali      20   0 2399348  56376  53560 S   0.3   2.8   0:00.23 Web Content
```



```
┌──(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
  containerd.service                       loaded active running containerd container runtime
  cron.service                             loaded active running Regular background program processing daemon
  dbus.service                             loaded active running D-Bus System Message Bus
  docker.service                           loaded active running Docker Application Container Engine
  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
  pcscd.service                            loaded active running PC/SC Smart Card Daemon
  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
  polkit.service                           loaded active running Authorization Manager
  rpc-statd-notify.service                 loaded active exited  Notify NFS peers of a restart
  rtkit-daemon.service                     loaded active running RealtimeKit Scheduling Policy Service
  systemd-binfmt.service                   loaded active exited  Set Up Additional Binary Formats
  systemd-journal-flush.service            loaded active exited  Flush Journal to Persistent Storage
  systemd-journald.service                 loaded active running Journal Service
  systemd-logind.service                   loaded active running User Login Management
  systemd-modules-load.service             loaded active exited  Load Kernel Modules
  systemd-random-seed.service              loaded active exited  Load/Save OS Random Seed
  systemd-remount-fs.service               loaded active exited  Remount Root and Kernel File Systems
  systemd-sysctl.service                   loaded active exited  Apply Kernel Variables
  systemd-tmpfiles-setup-dev-early.service loaded active exited  Create Static Device Nodes in /dev gracefully
  systemd-tmpfiles-setup-dev.service       loaded active exited  Create Static Device Nodes in /dev
  systemd-tmpfiles-setup.service           loaded active exited  Create System Files and Directories
  systemd-udev-load-credentials.service    loaded active exited  Load udev Rules from Credentials
  systemd-udev-trigger.service             loaded active exited  Coldplug All udev Devices
  systemd-udevd.service                    loaded active running Rule-based Manager for Device Events and Files
  systemd-user-sessions.service            loaded active exited  Permit User Sessions
  udisks2.service                          loaded active running Disk Manager
  upower.service                           loaded active running Daemon for power management
  user-runtime-dir@1000.service            loaded active exited  User Runtime Directory /run/user/1000
  user@1000.service                        loaded active running User Manager for UID 1000
  virtualbox-guest-utils.service           loaded active running Virtualbox guest utils

Legend: LOAD   → Reflects whether the unit definition was properly loaded.
        ACTIVE → The high-level unit activation state, i.e. generalization of SUB.
        SUB    → The low-level unit activation state, values depend on unit type.

44 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
```



```
┌──(kali㉿kali)-[~]
└─$ ps aux

USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.2  0.5  24080 11840 ?        Ss   12:48   0:01 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    12:48   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    12:48   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-kvfree_rcu_reclaim]
root           5  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-rcu_gp]
root           6  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-sync_wq]
root           7  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-slub_flushwq]
root           8  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-netns]
root          13  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-mm_percpu_wq]
root          14  0.0  0.0      0     0 ?        I    12:48   0:00 [rcu_tasks_kthread]
root          15  0.0  0.0      0     0 ?        I    12:48   0:00 [rcu_tasks_rude_kthread]
root          16  0.0  0.0      0     0 ?        I    12:48   0:00 [rcu_tasks_trace_kthread]
root          17  0.1  0.0      0     0 ?        S    12:48   0:00 [ksoftirqd/0]
root          18  0.3  0.0      0     0 ?        I    12:48   0:02 [rcu_preempt]
root          19  0.0  0.0      0     0 ?        S    12:48   0:00 [rcu_exp_par_gp_kthread_worker/0]
root          20  0.0  0.0      0     0 ?        S    12:48   0:00 [rcu_exp_gp_kthread_worker]
root          21  0.0  0.0      0     0 ?        S    12:48   0:00 [migration/0]
root          22  0.0  0.0      0     0 ?        S    12:48   0:00 [idle_inject/0]
root          23  0.0  0.0      0     0 ?        S    12:48   0:00 [cpuhp/0]
root          24  0.0  0.0      0     0 ?        S    12:48   0:00 [cpuhp/1]
root          25  0.0  0.0      0     0 ?        S    12:48   0:00 [idle_inject/1]
root          26  0.0  0.0      0     0 ?        S    12:48   0:00 [migration/1]
root          27  0.7  0.0      0     0 ?        S    12:48   0:04 [ksoftirqd/1]
root          28  0.0  0.0      0     0 ?        I    12:48   0:00 [kworker/1:0-cgroup_destroy]
root          29  0.2  0.0      0     0 ?        I<   12:48   0:01 [kworker/1:0H-kblockd]
root          31  0.4  0.0      0     0 ?        I    12:48   0:02 [kworker/u8:1-flush-8:0]
root          32  0.0  0.0      0     0 ?        S    12:48   0:00 [kdevtmpfs]
root          33  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-inet_frag_wq]
root          34  0.0  0.0      0     0 ?        S    12:48   0:00 [kauditd]
root          35  0.0  0.0      0     0 ?        S    12:48   0:00 [khungtaskd]
root          36  0.0  0.0      0     0 ?        S    12:48   0:00 [oom_reaper]
root          37  0.0  0.0      0     0 ?        I    12:48   0:00 [kworker/u8:2-events_unbound]
root          38  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-writeback]
root          39  0.1  0.0      0     0 ?        S    12:48   0:01 [kcompactd0]
root          40  0.0  0.0      0     0 ?        SN   12:48   0:00 [ksmd]
root          41  0.0  0.0      0     0 ?        SN   12:48   0:00 [khugepaged]
root          42  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-kintegrityd]
root          43  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-kblockd]
root          44  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-blkcg_punt_bio]
root          45  0.0  0.0      0     0 ?        S    12:48   0:00 [irq/9-acpi]
root          46  0.0  0.0      0     0 ?        I    12:48   0:00 [kworker/1:1-events]
root          47  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-tpm_dev_wq]
root          48  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-edac-poller]
root          49  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-devfreq_wq]
root          51  0.4  0.0      0     0 ?        S    12:48   0:02 [kswapd0]
root          54  0.0  0.0      0     0 ?        I    12:48   0:00 [kworker/u8:3-writeback]
root          59  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-kthrotld]
root          63  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-acpi_thermal_pm]
root          64  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-mld]
root          65  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-ipv6_addrconf]
root          70  0.0  0.0      0     0 ?        I<   12:48   0:00 [kworker/R-kstrp]
```



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

ufw is already the newest version (0.36.2-9).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1947
Firewall is active and enabled on system startup
Status: active

┌──(kali㉿kali)-[~]
└─$ sudo ufw allow ssh

Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ 
```