

I used Kali Linux virtual machine in VirtualBox

Normal users have limited access, while root/administrator has full system control

```
Session Actions Edit View Help

[(kali㉿kali)-[~]] $ ls -l demo.txt
-rwx----- 1 kali kali 0 Jan 18 09:22 demo.txt

[(kali㉿kali)-[~]] $ ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME COMMAND
root           1  0.1  0.5 24468 11924 ?      Ss  03:59  0:21 /sbin/init
root           2  0.0  0.0     0   0 ?      S  03:59  0:02 [kthreadd]
root           3  0.0  0.0     0   0 ?      S  03:59  0:00 [pool_wor
root           4  0.0  0.0     0   0 ?      I< 03:59  0:00 [kworker/
root           5  0.0  0.0     0   0 ?      I< 03:59  0:00 [kworker/
root           6  0.0  0.0     0   0 ?      I< 03:59  0:00 [kworker/
root           7  0.0  0.0     0   0 ?      I< 03:59  0:00 [kworker/
root           8  0.0  0.0     0   0 ?      I< 03:59  0:00 [kworker/
root          12  0.0  0.0     0   0 ?      I  03:59  0:00 [kworker/
root          13  0.0  0.0     0   0 ?      I< 03:59  0:00 [kworker/
root          14  0.0  0.0     0   0 ?      S  03:59  0:11 [ksoftirq
root          15  0.2  0.0     0   0 ?      I  03:59  0:40 [rcu_pree
root          16  0.0  0.0     0   0 ?      S  03:59  0:00 [rcu_exp_
root          17  0.0  0.0     0   0 ?      S  03:59  0:00 [rcu_exp_
root          18  0.0  0.0     0   0 ?      S  03:59  0:02 [migratio
root          19  0.0  0.0     0   0 ?      S  03:59  0:00 [idle_inj]
```

```
Session Actions Edit View Help

[(kali㉿kali)-[~]] $ whoami
kali

[(kali㉿kali)-[~]] $ id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25
nner,107(bluetooth),120(lpadmin),129(wireshark),130(kaboxer),131(vboxsf)

[(kali㉿kali)-[~]] $ ls -l
demo.py
Desktop
Documents
Downloads
hello.py
kalilinuxcourse
Music
Pictures
Public
rdp_lab
Templates
```

## File Permissions

```
Session Actions Edit View Help  
Videos  
└──(kali㉿kali)-[~]  
└─$ ls -l  
total 56  
-rw-rw-r-- 1 kali kali 39 Dec 26 02:04 demo.py  
drwxr-xr-x 2 kali kali 4096 Dec 25 13:27 Desktop  
drwxr-xr-x 2 kali kali 4096 Dec 26 11:20 Documents  
drwxr-xr-x 2 kali kali 4096 Dec 26 08:52 Downloads  
-rw-rw-r-- 1 kali kali 142 Dec 26 02:14 hello.py  
drwxrwxr-x 2 kali kali 4096 Dec 25 14:11 kalilinuxcourse  
drwxr-xr-x 2 kali kali 4096 Dec 25 13:27 Music  
drwxr-xr-x 2 kali kali 4096 Dec 26 08:56 Pictures  
drwxr-xr-x 2 kali kali 4096 Dec 25 13:27 Public  
drwxrwxr-x 2 kali kali 4096 Dec 26 07:19 rdp_lab  
drwxr-xr-x 2 kali kali 4096 Dec 25 13:27 Templates  
-rw-rw-r-- 1 kali kali 0 Dec 26 02:02 test1.  
-rw-rw-r-- 1 kali kali 32 Dec 26 01:59 test1.py  
-rw-rw-r-- 1 kali kali 0 Dec 26 09:25 testfile.txt  
-rw-rw-r-- 1 kali kali 1 Dec 26 01:57 test.py  
drwxr-xr-x 2 kali kali 4096 Dec 25 13:27 Videos  
└──(kali㉿kali)-[~]
```

chmod and chown practice

```
Session Actions Edit View Help  
└──(kali㉿kali)-[~]  
└─$ touch demo.txt  
└──(kali㉿kali)-[~]  
└─$ ls -l  
total 56  
-rw-rw-r-- 1 kali kali 39 Dec 26 02:04 demo.py  
-rw-rw-r-- 1 kali kali 0 Jan 18 09:22 demo.txt  
drwxr-xr-x 2 kali kali 4096 Dec 25 13:27 Desktop  
drwxr-xr-x 2 kali kali 4096 Dec 26 11:20 Documents  
drwxr-xr-x 2 kali kali 4096 Dec 26 08:52 Downloads  
-rw-rw-r-- 1 kali kali 142 Dec 26 02:14 hello.py  
drwxrwxr-x 2 kali kali 4096 Dec 25 14:11 kalilinuxcourse  
drwxr-xr-x 2 kali kali 4096 Dec 25 13:27 Music  
drwxr-xr-x 2 kali kali 4096 Dec 26 08:56 Pictures  
drwxr-xr-x 2 kali kali 4096 Dec 25 13:27 Public  
drwxrwxr-x 2 kali kali 4096 Dec 26 07:19 rdp_lab  
drwxr-xr-x 2 kali kali 4096 Dec 25 13:27 Templates  
-rw-rw-r-- 1 kali kali 0 Dec 26 02:02 test1.
```

```
Session Actions Edit view Help

[(kali㉿kali)-[~]]$ chmod 700 demo.txt

[(kali㉿kali)-[~]]$ ls -l
total 56
-rw-rw-r-- 1 kali kali 39 Dec 26 02:04 demo.py
-rwx----- 1 kali kali 0 Jan 18 09:22 demo.txt
drwxr-xr-x 2 kali kali 4096 Dec 25 13:27 Desktop
drwxr-xr-x 2 kali kali 4096 Dec 26 11:20 Documents
drwxr-xr-x 2 kali kali 4096 Dec 26 08:52 Downloads
drwxr-xr-x 2 kali kali 142 Dec 26 02:14 hello.py
-rw-rw-r-- 1 kali kali 4096 Dec 25 14:11 kalilinuxcourse
drwxrwxr-x 2 kali kali 4096 Dec 25 13:27 Music
drwxr-xr-x 2 kali kali 4096 Dec 26 08:56 Pictures
drwxr-xr-x 2 kali kali 4096 Dec 25 13:27 Public
drwxrwxr-x 2 kali kali 4096 Dec 26 07:19 Up_lab
drwxrwxr-x 2 kali kali 4096 Dec 25 13:27 Templates
drwxr-xr-x 2 kali kali 0 Dec 26 02:02 test1.
```

chmod is used to change file permissions and chown is used to change file ownership

## Administrator VS Standard User

administrator can make system-wide changes, standard users cannot

### Firewall enable

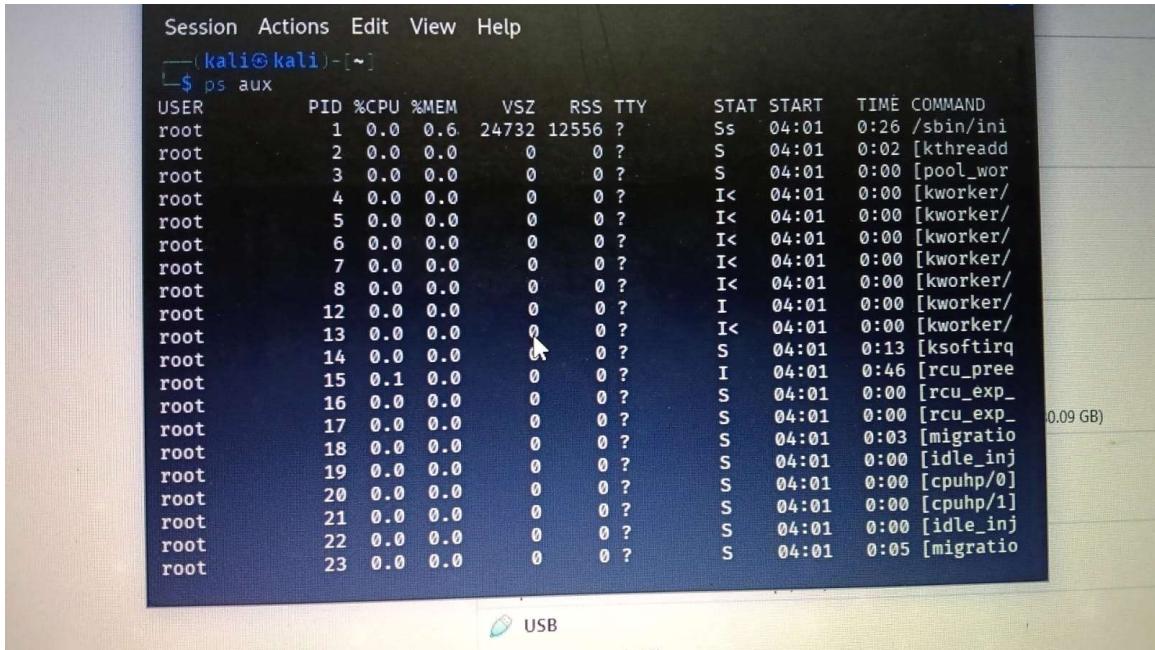
```
(Reading database ... 422160 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-9_all.deb ...
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...
Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
update-rc.d: It looks like a non-network service, we enable it.
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' →
'/usr/lib/systemd/system/ufw.service'.
Processing triggers for kali-menu (2025.4.3) ...
Processing triggers for man-db (2.13.1-1) ...

[(kali㉿kali)-[~]]$ sudo ufw enable
Firewall is active and enabled on system startup

[(kali㉿kali)-[~]]$ sudo ufw status
Status: active
```

firewall blocks unauthorized network access

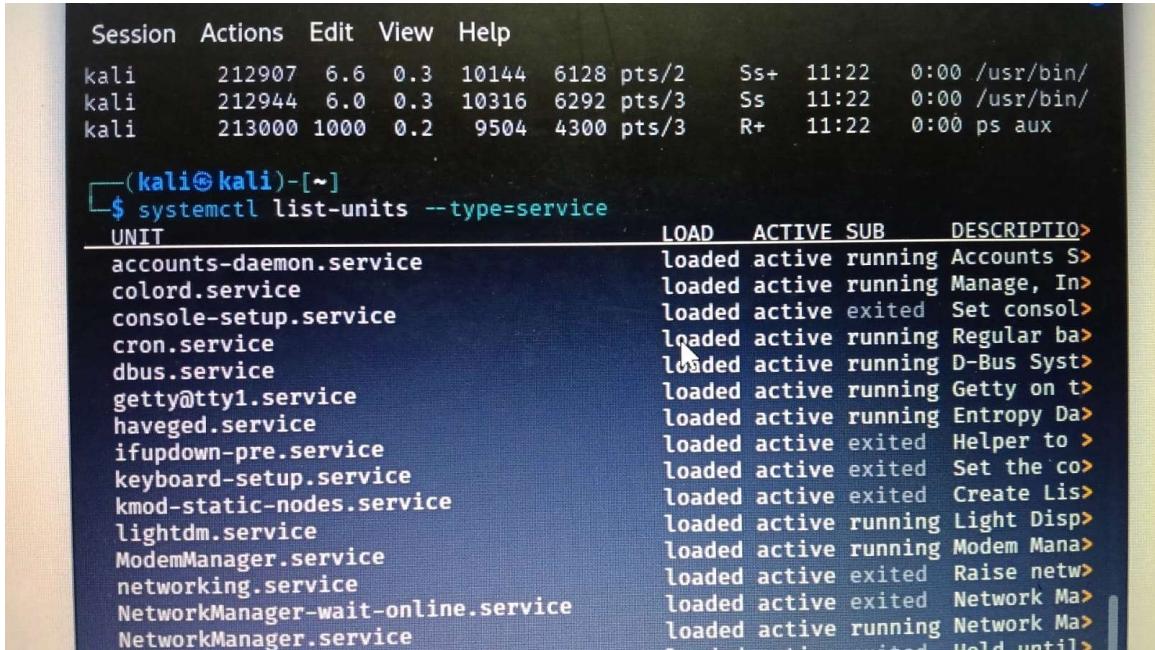
## Running processes



```
Session Actions Edit View Help
└─(kali㉿kali)-[~]
└─$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME COMMAND
root      1  0.0  0.6  24732 12556 ?      Ss  04:01  0:26 /sbin/init
root      2  0.0  0.0      0     0 ?      S  04:01  0:02 [kthreadd
root      3  0.0  0.0      0     0 ?      S  04:01  0:00 [pool_wor
root      4  0.0  0.0      0     0 ?      I<  04:01  0:00 [kworker/
root      5  0.0  0.0      0     0 ?      I<  04:01  0:00 [kworker/
root      6  0.0  0.0      0     0 ?      I<  04:01  0:00 [kworker/
root      7  0.0  0.0      0     0 ?      I<  04:01  0:00 [kworker/
root      8  0.0  0.0      0     0 ?      I<  04:01  0:00 [kworker/
root     12  0.0  0.0      0     0 ?      I  04:01  0:00 [kworker/
root     13  0.0  0.0      0     0 ?      I<  04:01  0:00 [kworker/
root     14  0.0  0.0      0     0 ?      S  04:01  0:13 [ksoftirq
root     15  0.1  0.0      0     0 ?      I  04:01  0:46 [rcu_pree
root     16  0.0  0.0      0     0 ?      S  04:01  0:00 [rcu_exp_
root     17  0.0  0.0      0     0 ?      S  04:01  0:00 [rcu_exp_
root     18  0.0  0.0      0     0 ?      S  04:01  0:03 [migratio
root     19  0.0  0.0      0     0 ?      S  04:01  0:00 [idle_inj
root     20  0.0  0.0      0     0 ?      S  04:01  0:00 [cpuhp/0]
root     21  0.0  0.0      0     0 ?      S  04:01  0:00 [cpuhp/1]
root     22  0.0  0.0      0     0 ?      S  04:01  0:00 [idle_inj
root     23  0.0  0.0      0     0 ?      S  04:01  0:05 [migratio
0.09 GB
```

running processes show active programs in the system

## Disable unnecessary services



UNIT	LOAD	ACTIVE	SUB	DESCRIPTION
accounts-daemon.service	loaded	active	running	Accounts S>
colord.service	loaded	active	running	Manage, In>
console-setup.service	loaded	active	exited	Set consol>
cron.service	loaded	active	running	Regular ba>
dbus.service	loaded	active	running	D-Bus Syst>
getty@tty1.service	loaded	active	running	Getty on t>
haveged.service	loaded	active	running	Entropy Da>
ifupdown-pre.service	loaded	active	exited	Helper to >
keyboard-setup.service	loaded	active	exited	Set the co>
kmod-static-nodes.service	loaded	active	exited	Create Lis>
lightdm.service	loaded	active	running	Light Disp>
ModemManager.service	loaded	active	running	Modem Mana>
networking.service	loaded	active	exited	Raise netw>
NetworkManager-wait-online.service	loaded	active	exited	Network Ma>
NetworkManager.service	loaded	active	running	Network Ma>

**sudo systemctl disable bluetooth**

disabling unused services reduces the attack surface