

Operating System Security Fundamentals

(Linux & Windows)

January 16, 2026

Contents

1	Installing a Linux Virtual Machine	2
2	User Accounts and Access Control	2
3	File Permissions in Linux	3
4	Administrator vs Standard User	4
5	Firewall Configuration	4
6	Running Processes and Services	5
7	Disabling Unnecessary Services	7
8	Operating System Hardening Best Practices	7
9	summary	7

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

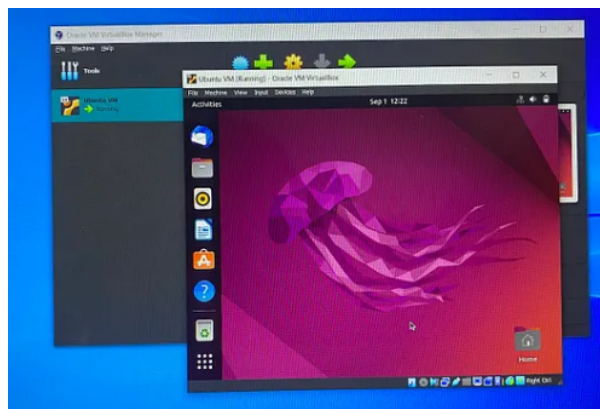


Figure 1: Linux VM Installation using VirtualBox

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
```

```

(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:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
tss:x:102:104:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:104:105::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:106:108:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
nm-openvpn:x:107:109:NetworkManager OpenVPN,,,:/var/lib/openvpn:/usr/sbin/nologin
speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/usr/sbin/nologin

(kali@kali)-[~]
$ whoami
kali

(kali@kali)-[~]
$ groups
kali adm dialout cdrom floppy sudo audio dip video plugdev users netdev bluetooth scanner lpadmin wireshark kaboxer

```

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

```

```

(root@kali)-[/home/kali]
# chmod 755 testfile.txt

(root@kali)-[/home/kali]
# ls -l testfile.txt
-rwxr-xr-x 1 root root 0 Jan 16 00:39 testfile.txt

(root@kali)-[/home/kali]
# sudo chown root:root testfile.txt

(root@kali)-[/home/kali]
# ls -l testfile.txt
-rwxr-xr-x 1 root root 0 Jan 16 00:39 testfile.txt

```

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
```

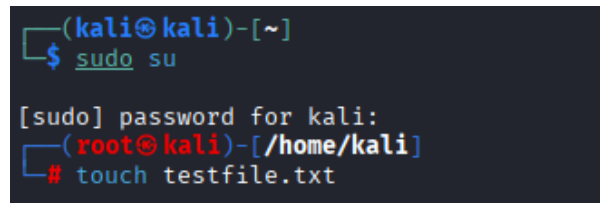
A terminal window with a dark background. The prompt is (kali@kali)-[~]. The user enters 'sudo su'. The prompt changes to [sudo] password for kali:. The user enters their password. The prompt changes to (root@kali)-[/home/kali]. The user enters 'touch testfile.txt'.

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
```

```

(root@kali)~[/home/kali]
# sudo apt install ufw
The following packages were automatically installed and are no longer
required:
  amass-common libgtksourceviewmm-3.0-0v5 libpython3.10-stdlib
  crackmapexec libgumbo2 libpython3.10-stdlib
  firebird3.0-common libbdf4-0-alt libpython3.10-stdlib
  firebird3.0-common-doc libbdf5-103-1t64 libqt5ct
  firmware-ti-connectivity libbdf5-hl-100t64 libqt5se
  icu-devtools libicu-dev libqt5we
  libbluray2 libjs-jquery-ui librav1e
  libbson-1.0-0t64 libjxl0.10 librsfr
  libcapstone4 liblbfgsb0 libsigse
  libconfig++9v5 libldap-2.5-0 libsoup-
  libconfig9 libmongoc-1.0-0t64 libsoup2
  libflac12t64 libmongocrypt0 libtag1v
  libgdal35 libmsgpack-0-1 libtag1v
  libgdal-common libnetcdf19t64 libtagc0
  libgdal22 libogdi4.1 libtheor
  libgeos3.13.0 libplacebo349 libudfre
  libglapi-mesa libpoppler140 libutemp
  libgtksourceview-3.0-1 libportmidi0 libvpx9
  libgtksourceview-3.0-common libpython3.12-dev libwebrt
Use 'sudo apt autoremove' to remove them.

Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1280
  Download size: 169 kB
  Space needed: 880 kB / 48.2 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.3
  Fetched 169 kB in 1s (129 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.

(root@kali)~[/home/kali]
# sudo ufw status
Status: inactive

(root@kali)~[/home/kali]
# sudo ufw enable
Firewall is active and enabled on system startup

(root@kali)~[/home/kali]
# sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

```

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 st
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 avail

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME
5401	root	20	0	2221484	743200	16660	S	379.1	9.2	36:33.34
917	root	20	0	393000	140780	52564	S	1.3	1.7	2:21.54
1315	kali	20	0	311192	64600	22636	S	0.7	0.8	1:32.77
575	root	20	0	113744	9356	7700	S	0.3	0.1	1:08.94
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	1:12.34
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	0:07.61
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	0:05.54
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	0:00.00
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	0:00.00
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	0:00.00
17	root	20	0	0	0	0	S	0.0	0.0	0:00.00
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
```

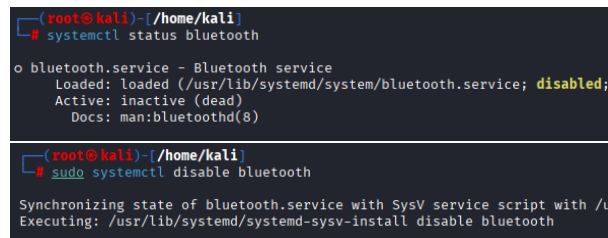
UNIT	LOAD
accounts-daemon.service	loaded
colord.service	loaded
console-setup.service	loaded
cron.service	loaded
dbus.service	loaded
getty@tty1.service	loaded
haveged.service	loaded
ifupdown-pre.service	loaded
keyboard-setup.service	loaded
kmod-static-nodes.service	loaded
lightdm.service	loaded
ModemManager.service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

7 Disabling Unnecessary Services

Disabling unused services reduces the system attack surface.

Command

```
sudo systemctl disable bluetooth
```



```
(root@kali)~/home/kali
# systemctl status bluetooth

o bluetooth.service - Bluetooth service
   Loaded: loaded (/usr/lib/systemd/system/bluetooth.service; disabled;
   Active: inactive (dead)
   Docs: man:bluetoothd(8)

---
(root@kali)~/home/kali
# sudo systemctl disable bluetooth

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