Day 2 cybersecurity internship

Os security checklist

Environment used : Linux WSL (Debian)

2. Explored user accounts from ashik to root using : sudo su command

Changed permissions and learned about control mechanics

```
root@ASHIK:/home/ashik# whoami
root
root@ASHIK:/home/ashik# id
uid=0(root) gid=0(root) groups=0(root)
root@ASHIK:/home/ashik#
```

```
root@ASHIK:/home/ashik# ls -l
total 952
drw-r----- 2 ashik ashik   4096 Nov 30 16:01 ashikkk.txt
-rw-r--r-- 1 ashik ashik    160 Dec 27 06:41 ashikkk.txt.zip
drwxr-xr-x 2 ashik ashik   4096 Dec  5 17:22 ashok1.txt
-rw-r--r-- 1 ashik ashik    174 Dec  1 16:06 file.zip
drwxr-xr-x 3 ashik ashik   4096 Dec 27 06:15 home
-rw-r--r-- 1 ashik ashik 223269 Nov 30 15:52 kali-ferrofluid.jpg
-rw-r--r-- 1 ashik ashik 715087 Nov 27 22:05 kali-ferrofluid.jpg.1
-rw-r--r-- 1 ashik ashik    114 Jan  8 17:35 sample2.tar
-rw-r--r-- 1 ashik ashik    114 Dec 27 07:09 sample.tar
drwxr-xr-x 2 ashik ashik   4096 Dec 27 07:17 scripts
root@ASHIK:/home/ashik# chmod 755 ashikkk.txt
root@ASHIK:/home/ashik# ls -l
total 952
drwxr-xr-x 2 ashik ashik   4096 Nov 30 16:01 ashikkk.txt
-rw-r--r-- 1 ashik ashik    160 Dec 27 06:41 ashikkk.txt.zip
drwxr-xr-x 2 ashik ashik   4096 Dec  5 17:22 ashok1.txt
-rw-r--r-- 1 ashik ashik    174 Dec  1 16:06 file.zip
drwxr-xr-x 3 ashik ashik   4096 Dec 27 06:15 home
-rw-r--r-- 1 ashik ashik 223269 Nov 30 15:52 kali-ferrofluid.jpg
-rw-r--r-- 1 ashik ashik 715087 Nov 27 22:05 kali-ferrofluid.jpg.1
-rw-r--r-- 1 ashik ashik    114 Jan  8 17:35 sample2.tar
-rw-r--r-- 1 ashik ashik    114 Dec 27 07:09 sample.tar
drwxr-xr-x 2 ashik ashik   4096 Dec 27 07:17 scripts
root@ASHIK:/home/ashik#
```

3. Learn file permissions using chmod, chown and ls -l

```
root@ASHIK:/home/ashik# ls -l
total 952
drw-r----- 2 ashik ashik   4096 Nov 30 16:01 ashikkk.txt
-rw-r--r-- 1 ashik ashik    160 Dec 27 06:41 ashikkk.txt.zip
drwxr-xr-x 2 ashik ashik   4096 Dec  5 17:22 ashok1.txt
-rw-r--r-- 1 ashik ashik    174 Dec  1 16:06 file.zip
drwxr-xr-x 3 ashik ashik   4096 Dec 27 06:15 home
-rw-r--r-- 1 ashik ashik 223269 Nov 30 15:52 kali-ferrofluid.jpg
-rw-r--r-- 1 ashik ashik 715087 Nov 27 22:05 kali-ferrofluid.jpg.1
-rw-r--r-- 1 ashik ashik    114 Jan  8 17:35 sample2.tar
-rw-r--r-- 1 ashik ashik    114 Dec 27 07:09 sample.tar
drwxr-xr-x 2 ashik ashik   4096 Dec 27 07:17 scripts
root@ASHIK:/home/ashik# chmod 755 ashikkk.txt
root@ASHIK:/home/ashik# ls -l
total 952
drwxr-xr-x 2 ashik ashik   4096 Nov 30 16:01 ashikkk.txt
-rw-r--r-- 1 ashik ashik    160 Dec 27 06:41 ashikkk.txt.zip
drwxr-xr-x 2 ashik ashik   4096 Dec  5 17:22 ashok1.txt
-rw-r--r-- 1 ashik ashik    174 Dec  1 16:06 file.zip
drwxr-xr-x 3 ashik ashik   4096 Dec 27 06:15 home
-rw-r--r-- 1 ashik ashik 223269 Nov 30 15:52 kali-ferrofluid.jpg
-rw-r--r-- 1 ashik ashik 715087 Nov 27 22:05 kali-ferrofluid.jpg.1
-rw-r--r-- 1 ashik ashik    114 Jan  8 17:35 sample2.tar
-rw-r--r-- 1 ashik ashik    114 Dec 27 07:09 sample.tar
drwxr-xr-x 2 ashik ashik   4096 Dec 27 07:17 scripts
root@ASHIK:/home/ashik# chown 640 ashikkk.txt
root@ASHIK:/home/ashik# ls -l
total 952
```

drwxr-xr-x 2 640 ashik 4096 Nov 30 16:01 ashikkk.txt

-rw-r--r-- 1 ashik ashik 160 Dec 27 06:41 ashikkk.txt.zip

drwxr-xr-x 2 ashik ashik 4096 Dec 5 17:22 ashok1.txt

-rw-r--r-- 1 ashik ashik 174 Dec 1 16:06 file.zip

drwxr-xr-x 3 ashik ashik 4096 Dec 27 06:15 home

-rw-r--r-- 1 ashik ashik 223269 Nov 30 15:52 kali-ferrofluid.jpg

-rw-r--r-- 1 ashik ashik 715087 Nov 27 22:05 kali-ferrofluid.jpg.1

-rw-r--r-- 1 ashik ashik 114 Jan 8 17:35 sample2.tar

-rw-r--r-- 1 ashik ashik 114 Dec 27 07:09 sample.tar

drwxr-xr-x 2 ashik ashik 4096 Dec 27 07:17 scripts

root@ASHIK:/home/ashik# chown ashik ashikkk.txt

4. Understanding administrator vs standard user privileges

Admin accounts have full control over installing softwares to manage users and have most privilege compared to standard users whereas Standard users operate within a restricted environment

Eg: root user can change ownerships and file permissions, but standard user can't do it.

5.Enabled Firewall in Linux (Debian WSL)

Command used : sudo apt install ufw –y

root@ASHIK:/home/ashik# sudo ufw allow ssh

Rules updated

Rules updated (v6)

root@ASHIK:/home/ashik# sudo ufw status

Status: inactive

root@ASHIK:/home/ashik# sudo ufw enable

Firewall is active and enabled on system startup

root@ASHIK:/home/ashik# sudo ufw status

Status: active

To	Action	From
22/tcp	ALLOW	Anywhere
22/tcp (v6)	ALLOW	Anywhere (v6)

6.Identifying running process and services

Command used:

ps aux (for viewing running processes)

top (for real time monitoring)

htop(for color coded monitoring same as top)

These are used to identify what are the services running in our system and check for a specific service.

7. Disable unnecessary services to reduce attack surface

root@ASHIK:/home/ashik# systemctl list-units --type=service --state=running

UNIT	LOAD	ACTIVE	SUB	DESCRIPTION
console-getty.service	loaded	active	running	Console Getty
cron.service	loaded	active	running	Regular background program>
dbus.service	loaded	active	running	D-Bus System Message Bus
getty@tty1.service	loaded	active	running	Getty on tty1
systemd-journald.service	loaded	active	running	Journal Service
systemd-logind.service	loaded	active	running	User Login Management
systemd-udevd.service	loaded	active	running	Rule-based Manager for Dev>

user@0.service loaded active running User Manager for UID 0

user@1000.service loaded active running User Manager for UID 1000

Legend: LOAD → Reflects whether the unit definition was properly loaded.

ACTIVE → The high-level unit activation state, i.e. generalization >

SUB → The low-level unit activation state, values depend on unit>

9 loaded units listed.

lines 1-16/16 (END)

LIST SERVICES ENABLED AT BOOT (grep)

root@ASHIK:/home/ashik# systemctl list-unit-files --type=service | grep enabled

console-getty.service enabled-runtime disabled

cron.service enabled enabled

cryptdisks-early.service masked enabled

cryptdisks.service masked enabled

e2scrub_reap.service enabled enabled

getty@.service enabled enabled

hwclock.service masked enabled

ifupdown-wait-online.service disabled enabled

networking.service enabled enabled

nftables.service disabled enabled

serial-getty@.service disabled enabled

sudo.service masked enabled

systemd-confext.service disabled enabled

systemd-network-generator.service disabled enabled

systemd-networkd-wait-online.service disabled enabled

systemd-networkd-wait-online@.service disabled enabled

systemd-networkd.service disabled enabled

systemd-pcrlock-file-system.service disabled enabled

systemd-pcrlock-firmware-code.service disabled enabled

systemd-pcrlock-firmware-config.service disabled enabled

systemd-pcrlock-machine-id.service disabled enabled

systemd-pcrlock-make-policy.service disabled enabled

systemd-pcrlock-secureboot-authority.service disabled enabled

systemd-pcrlock-secureboot-policy.service disabled enabled

systemd-pstore.service enabled enabled

systemd-remount-fs.service enabled-runtime enabled

systemd-sysext.service disabled enabled

systemd-udev-load-credentials.service disabled enabled

ufw.service enabled enabled

x11-common.service masked enabled

root@ASHIK:/home/ashik#

EXPOSED PORT SERVICES

root@ASHIK:/home/ashik# ss -tulnp

Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

udp UNCONN 0 0 127.0.0.1:323 0.0.0.0:*

udp UNCONN 0 0 10.255.255.254:53 0.0.0.0:*

udp UNCONN 0 0 [::1]:323 [::]:*

tcp LISTEN 0 1000 10.255.255.254:53 0.0.0.0:*

root@ASHIK:/home/ashik#

8. BEST OS HARDERNING PRACTICES :

Least privilege

Strong Authentication

Use UAC on windows

Use correct file permissions

Setup a Firewall

Disable unnecessary services

Monitor logs

Take regular backups

Use SSH keys