Sapience Edu Connect Pvt Ltd

NAME: DEVALLA JWALA NARSIMHA
DOMAIN: CYBER SECURITY

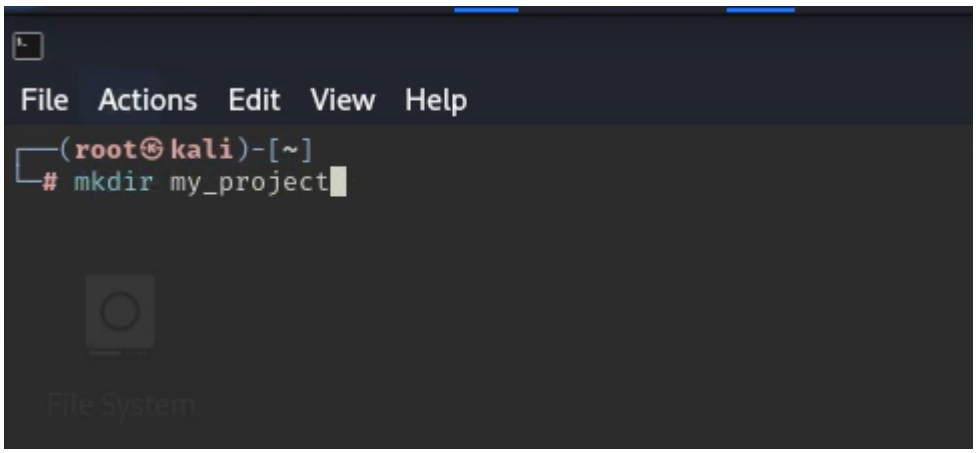
Week 2: Linux Fundamentals

Task 2

1. Create a directory named my_project and navigate into it

Step1:

mkdir my_project



Step2:

cd my_project

2. Inside my_project, create an empty file named notes.txt.

Step1:

touch notes.txt

3. Copy notes.txt to a new file named backup_notes.txt, then move it into a newly created subdirectory called backup.

Step1:

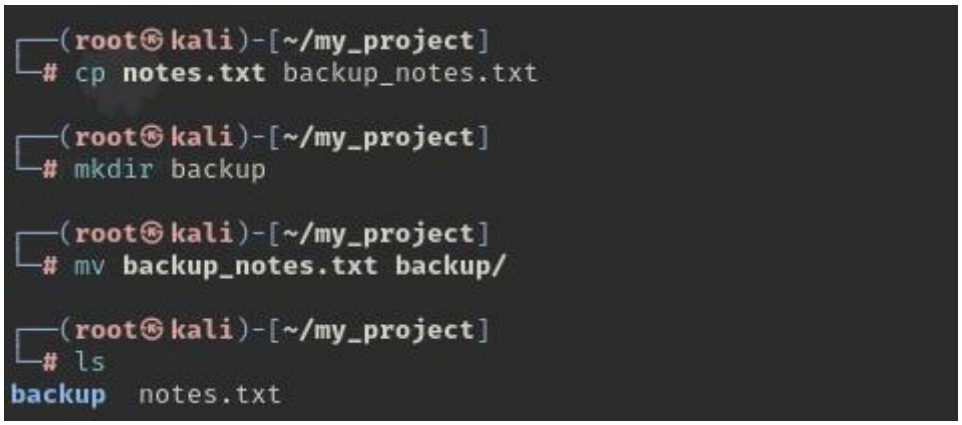
cp notes.txt backup_notes.txt

Step2:

mkdir backup

Step3:

mv backup_notes.txt backup/



4. Delete the backup directory along with its contents.

Step1:

rm -r backup

```
┌──(root㉿kali)-[~/my_project]
└─# rm -r backup

┌──(root㉿kali)-[~/my_project]
└─# ls
notes.txt
```

5. Create a file named script.sh, grant it executable permissions, and change its permissions so it is readable and executable only by the file owner.

Step1:

touch script.sh

Step2:

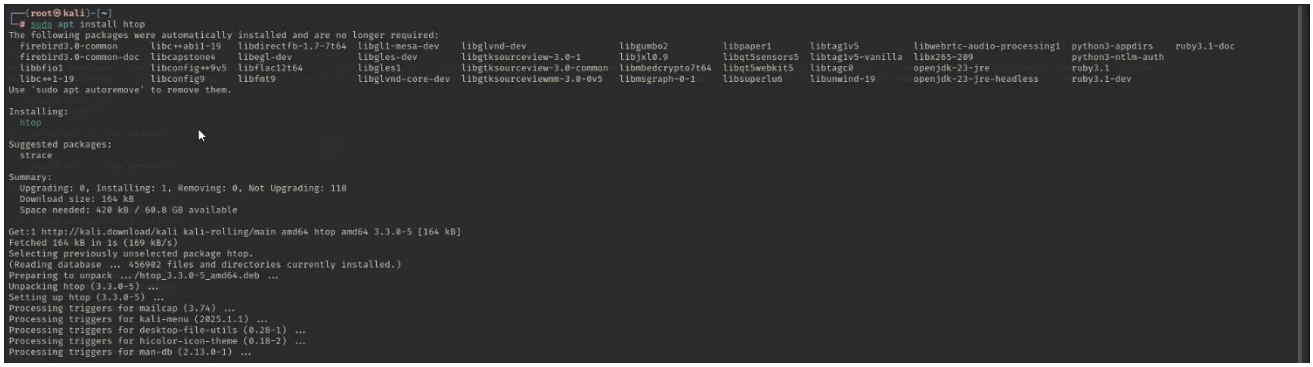
chmod 700 script.sh

```
┌──(root㉿kali)-[~/my_project]
└─# touch script.sh

┌──(root㉿kali)-[~/my_project]
└─# chmod 700 script.sh

┌──(root㉿kali)-[~/my_project]
└─# ls
notes.txt  script.sh
```

6. Update your package manager's repository list, install the htop package, verify its installation, and then uninstall it.

Step1:

sudo apt install htop

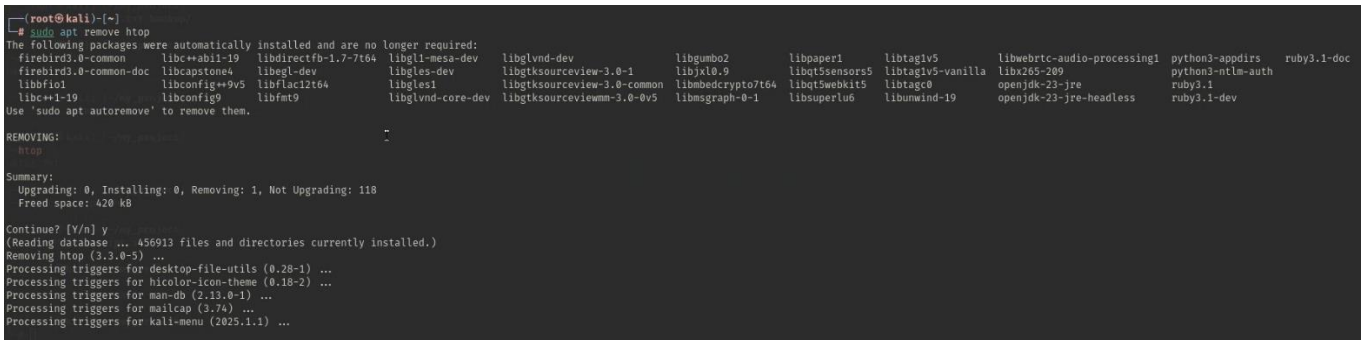


Step2:

htop –version

Step1:

sudo apt remove htop



7. Check all running processes, identify the PID of a specific process (e.g., sleep if running), and terminate it using the kill command.

Step1:

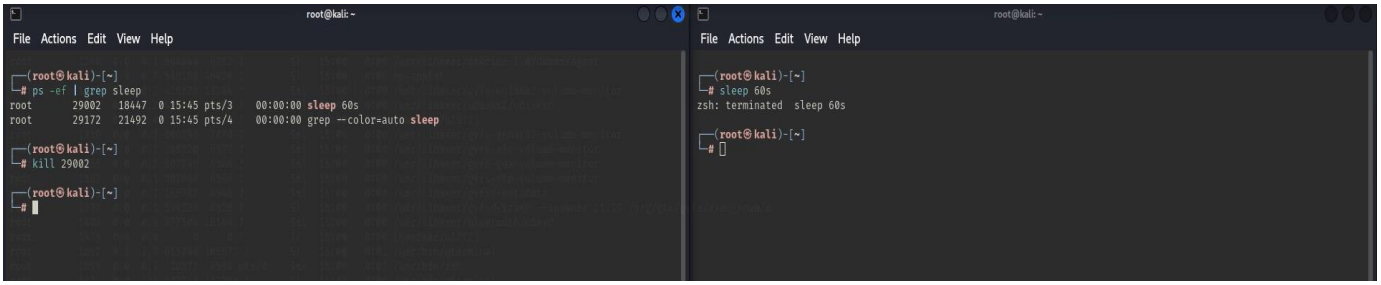
Sleep 60s

Sleep2:

ps aux | grep sleep

step3:

kill <PID>



8. Display your machine's IP address, ping google.com to verify connectivity, and list all active network connections.

Step1:
hostname -I

```
┌──(root㉿kali)-[~]
└─# hostname -I
192.168.1.35 2401:4900:8fcf:2661:bbc0:80e3:7ee5:1bb6
```

Step2:
ping -c 4 google.com

```
┌──(root㉿kali)-[~]
└─# ping -c 4 google.com
PING google.com (2404:6800:4007:818::200e) 56 data bytes
64 bytes from maa05s17-in-x0e.1e100.net (2404:6800:4007:818::200e): icmp_seq=1 ttl=58 time=45.7 ms
64 bytes from maa05s17-in-x0e.1e100.net (2404:6800:4007:818::200e): icmp_seq=2 ttl=58 time=51.5 ms
64 bytes from maa05s17-in-x0e.1e100.net (2404:6800:4007:818::200e): icmp_seq=3 ttl=58 time=49.1 ms
64 bytes from maa05s17-in-x0e.1e100.net (2404:6800:4007:818::200e): icmp_seq=4 ttl=58 time=46.7 ms

── google.com ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 45.708/48.258/51.521/2.241 ms
```

step3:
netstat -tuln

```
┌──(root㉿kali)-[~]
└─# netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp6       0      0 fe80::88dd:2cd5:fab:546 :::*
```

9. Addanewuser named testuser, switch to this user, and grant them sudo privileges.

Step1:

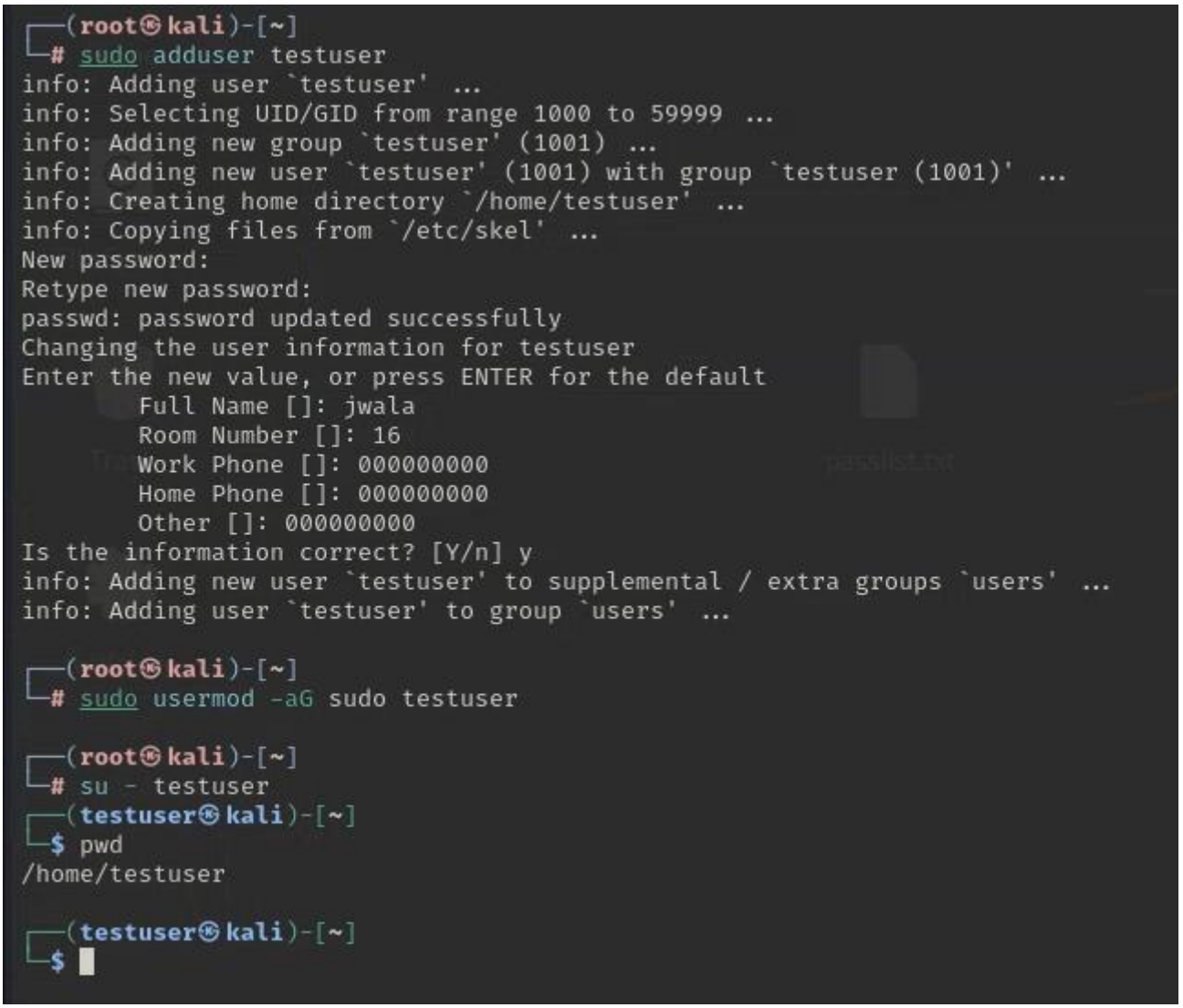
sudo adduser testuser

step2:

sudo usermod -aG sudo testuser

step3:

su – testuser



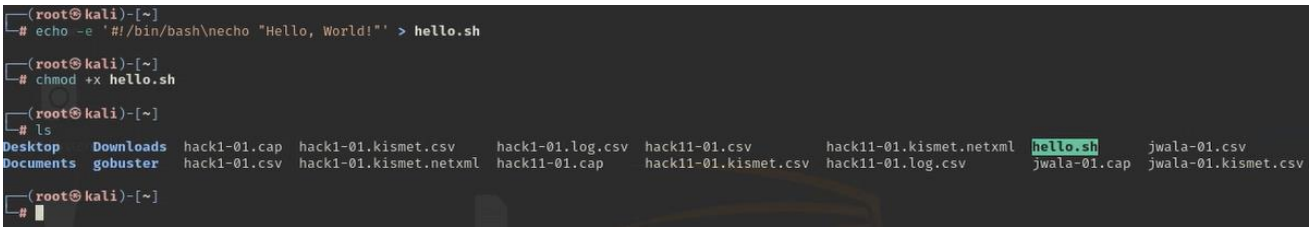
10. Write a shell script named hello.sh that outputs "Hello, World!" when executed.

Step1:

echo -e '#!/bin/bash\necho "Hello, World!"' > hello.sh

step2:

chmod +x hello.sh



11. Create a tarball of the my_project directory, extract its contents, and compress the tarball using gzip.

Step1:

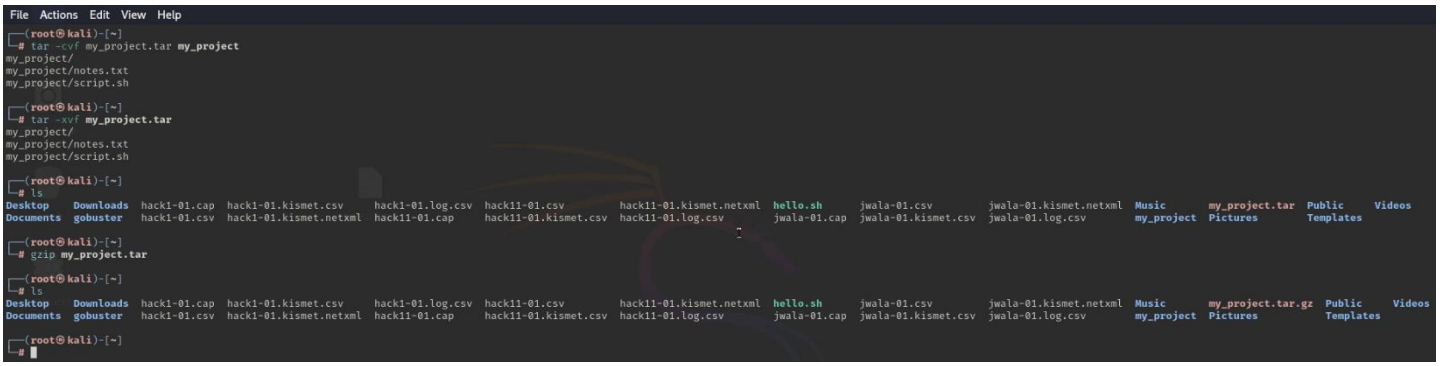
tar -cvf my_project.tar my_project

step2:

tar -xvf my_project.tar

step3:

gzip my_project.tar



12. Check the disk usage, memory usage, and CPU information of your system.

Step1:

df -h

```
┌──(root㉿kali)-[~]
└─# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            2.9G     0  2.9G   0% /dev
tmpfs           589M  976K  588M   1% /run
/dev/sda1        79G   18G   57G  24% /
tmpfs           2.9G  4.0K  2.9G   1% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-journald.service
tmpfs           2.9G   56K  2.9G   1% /tmp
tmpfs           1.0M     0  1.0M   0% /run/credentials/getty@tty1.service
tmpfs           589M  124K  589M   1% /run/user/0
```

step2:

```
┌──(root㉿kali)-[~]
└─# free -h
               total        used        free      shared  buff/cache   available
Mem:           5.7Gi       1.1Gi       4.3Gi        38Mi       676Mi       4.7Gi
Swap:          1.0Gi          0B       1.0Gi
```

free -h

step3:

lscpu

```
┌──(root㉿kali)-[~]
└─# lscpu
Architecture:             x86_64
  CPU op-mode(s):         32-bit, 64-bit
  Address sizes:          39 bits physical, 48 bits virtual
  Byte Order:             Little Endian
CPU(s):                   2
  On-line CPU(s) list:    0,1
Vendor ID:                GenuineIntel
  Model name:             11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz
    CPU family:           6
    Model:                141
    Thread(s) per core:   1
    Core(s) per socket:   2
    Socket(s):            1
    Stepping:             1
    BogoMIPS:             4608.00
    Flags:                fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx rdtscp lm constant_tsc rep_good nopl xtopology nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse
                          3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti fsgsbase bmi1 avx2 bmi2 invpcid rdseed adx clflushopt sha_ni arat md_clear flush_l1d arch_cap
                          abilities
Virtualization features:
  Hypervisor vendor:      KVM
  Virtualization type:    full
Caches (sum of all):
  L1d:                    96 KiB (2 instances)
  L1i:                    64 KiB (2 instances)
  L2:                     2.5 MiB (2 instances)
  L3:                     48 MiB (2 instances)
NUMA:
  NUMA node(s):           1
  NUMA node0 CPU(s):      0,1
Vulnerabilities:
  Gather data sampling:   Unknown: Dependent on hypervisor status
  Itlb multihit:          KVM: Mitigation: VMX unsupported
  L1tf:                   Mitigation; PTE Inversion
  Mds:                    Mitigation; Clear CPU buffers; SMT Host state unknown
  Meltdown:               Mitigation; PTI
  Mmio stale data:        Not affected
  Reg file data sampling: Not affected
  Retbleed:               Not affected
  Spec rstack overflow:   Not affected
  Spec store bypass:      Vulnerable
  Spectre v1:             Mitigation; usercopy/swapgs barriers and __user pointer sanitization
  Spectre v2:             Mitigation; Retpolines; STIBP disabled; RSB filling; PBRSB-eIBRS Not affected; BHI Retpoline
  Srbds:                  Not affected
  Tsx async abort:        Not affected
```

THANK YOU!