Group 22 : El Paso
Pranchal
Liam

1. What were the Linux accounts that were present on the Raspberry Pi?

```
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
gnats
nobody
_apt
postfix
sshd
systemd-network
systemd-resolve
messagebus
systemd-timesync
systemd-coredump
tcpdump
pi
brown.j
smith.a
```

and only three users have an associated home directory

```
pi
brown.j
smith.a
```

3. What are the network settings of the Raspberry Pi (hostname, DNS, routes)? What are its IPv4 and IPv6 addresses?

Hostname :

> raspberry

DNS :

> search ep.int.e-netsec.org

Routes:

Destination	Gateway	Genmask	Flags
0.0.0.0	10.10.92.1	0.0.0.0	UG
10.10.92.0	0.0.0.0	255.255.255.0	U

ipv4 address :

> 10.10.92.10

Global ipv6 address :

> 2001:470:8cc5:3201:ba27:ebff:fe32:67

Local ipv6 address :

> fe80::ba27:ebff:fe32:67

Mac address:

> b8:27:eb:32:00:67

2. What is the purpose of the sudo(8) command? What advantages does it have over the su(1) command? Why is “root” disabled by default?

sudo allows users to execute a command as another user (which is almost always root). On the other hand, su allows you to switch your priveledges to that of another user, which may not be desired for security reasons if you only want to run a single command with elevated priveledges.

Root may be disabled by default to prevent any security breaches from giving attackers access to root priveledges.

4. Provide the output of your manual run of OpenVPN, your VPN tunnel IP address, and the ping output.

4.1 OpenVPN run

```
sudo openvpn net-sec.ovpn
```

```
2024-01-22 18:49:44 OpenVPN 2.6.8 [git:makepkg/3b0d9489cc423da3+] x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO] built on Nov 17 2023
2024-01-22 18:49:44 library versions: OpenSSL 3.2.0 23 Nov 2023, LZO 2.10
2024-01-22 18:49:44 DCO version: N/A
Enter Auth Username:
Enter Auth Password: •••••••••••••••
2024-01-22 18:49:50 TCP/UDP: Preserving recently used remote address: [AF_INET]129.10.112.35:1194
2024-01-22 18:49:50 UDPv4 link local: (not bound)
2024-01-22 18:49:50 UDPv4 link remote: [AF_INET]129.10.112.35:1194
2024-01-22 18:49:50 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2024-01-22 18:49:52 [Net-Sec CA] Peer Connection Initiated with [AF_INET]129.10.112.35:1194
2024-01-22 18:49:53 TUN/TAP device tun0 opened
2024-01-22 18:49:53 net_iface_mtu_set: mtu 1500 for tun0
2024-01-22 18:49:53 net_iface_up: set tun0 up
2024-01-22 18:49:53 net_addr_v4_add: 10.10.222.1/18 dev tun0
2024-01-22 18:49:53 sitnl_send: rtnl: generic error (-17): File exists
2024-01-22 18:49:53 sitnl_send: rtnl: generic error (-17): File exists
2024-01-22 18:49:53 Initialization Sequence Completed
```

4.2 VPN Tunnel Info

`ifconfig tun0`

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.222.1  netmask 255.255.192.0  destination 10.10.222.1
        inet6 fe80::92cf:a054:5052:8fa6  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 26  bytes 4000 (3.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 52  bytes 6806 (6.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Local addresses:

> IPv4 = 10.10.222.1

> IPv6 = fe80::92cf:a054:5052:8fa6

4.3 Ping output

`ping 10.10.1.`

```
PING 10.10.1.1 (10.10.1.1) 56(84) bytes of data.
64 bytes from 10.10.1.1: icmp_seq=1 ttl=64 time=11.5 ms
64 bytes from 10.10.1.1: icmp_seq=2 ttl=64 time=14.4 ms
64 bytes from 10.10.1.1: icmp_seq=3 ttl=64 time=25.5 ms
64 bytes from 10.10.1.1: icmp_seq=4 ttl=64 time=25.9 ms
64 bytes from 10.10.1.1: icmp_seq=5 ttl=64 time=15.9 ms
64 bytes from 10.10.1.1: icmp_seq=6 ttl=64 time=20.2 ms
64 bytes from 10.10.1.1: icmp_seq=7 ttl=64 time=13.0 ms
64 bytes from 10.10.1.1: icmp_seq=8 ttl=64 time=15.3 ms
64 bytes from 10.10.1.1: icmp_seq=9 ttl=64 time=16.2 ms
^C
--- 10.10.1.1 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8010ms
rtt min/avg/max/mdev = 11.525/17.546/25.882/4.903 ms```
```