Computer Network Security

Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

Firewall Exploration Lab

Task 0: Get Familiar with the Lab Setup

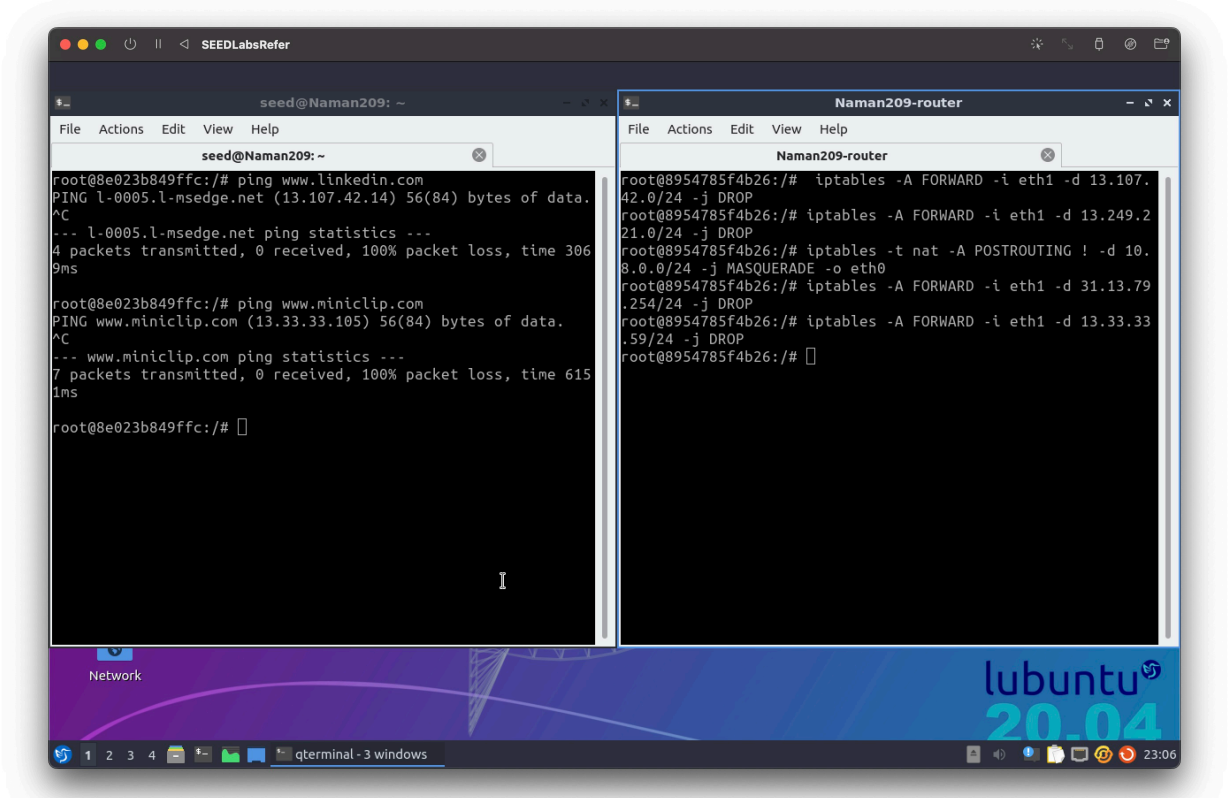
In router:

```bash
iptables -A FORWARD -i eth1 -d 13.107.42.0/24 -j DROP
 iptables -A FORWARD -i eth1 -d 13.33.33.59/24 -j DROP
```

Note `13.249.221.0/24` changed to `13.33.33.59/24` for relevant `miniclip.com` ip

In B/B1/B2:

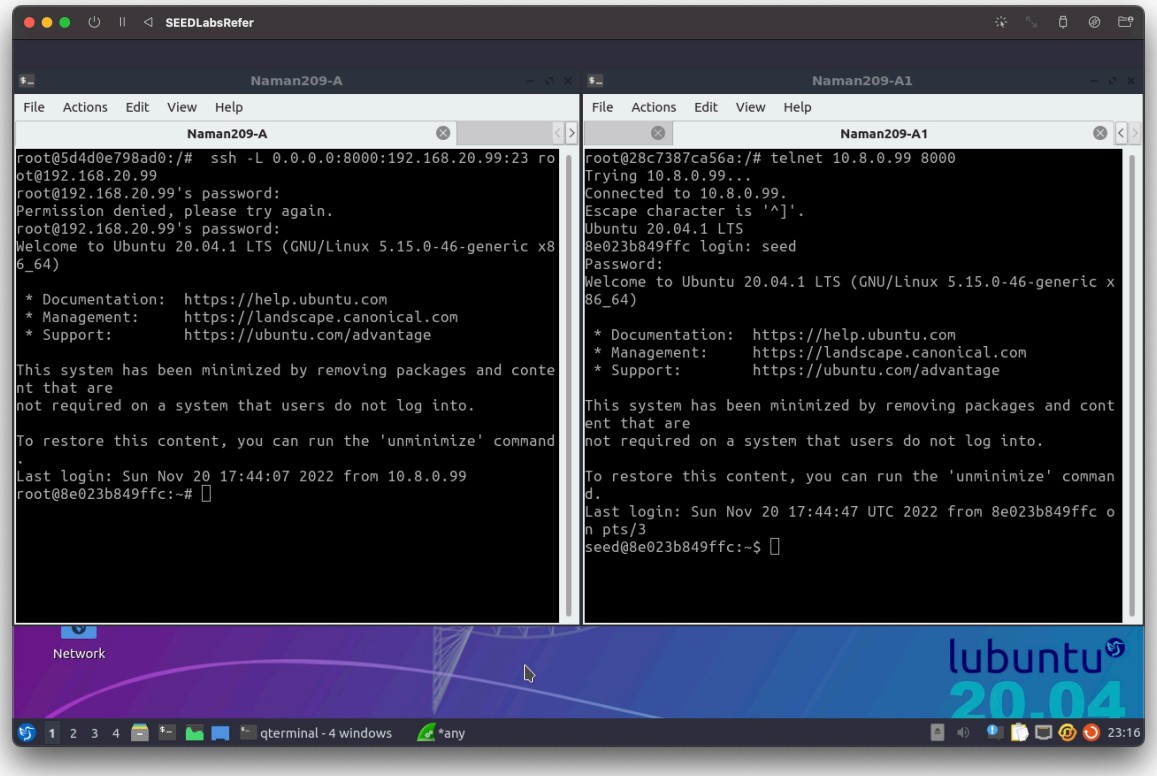
```bash
ping www.linkedin.com
ping www.miniclip.com
```



Task 1: Static Port Forwarding

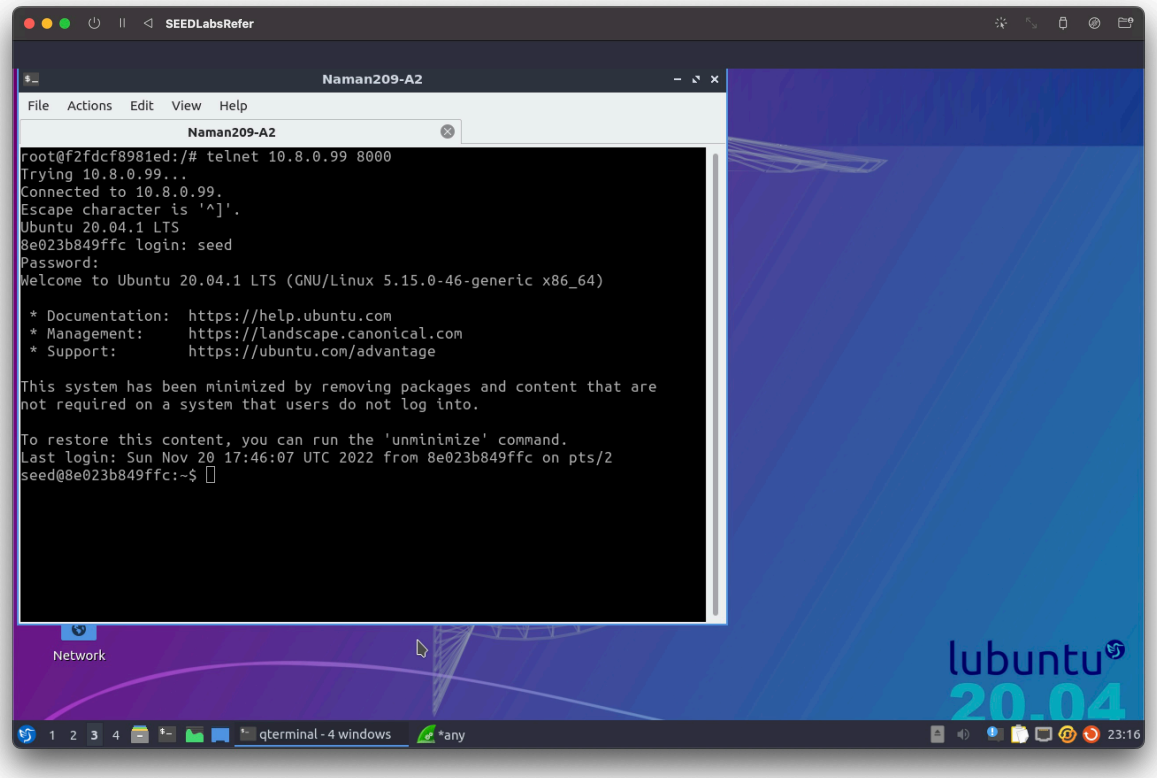
In Container A:

```bash
ssh -L 0.0.0.0:8000:192.168.20.99:23 root@192.168.20.99
```



In Container A1 and A2:

```bash
telnet 10.8.0.99 8000
```

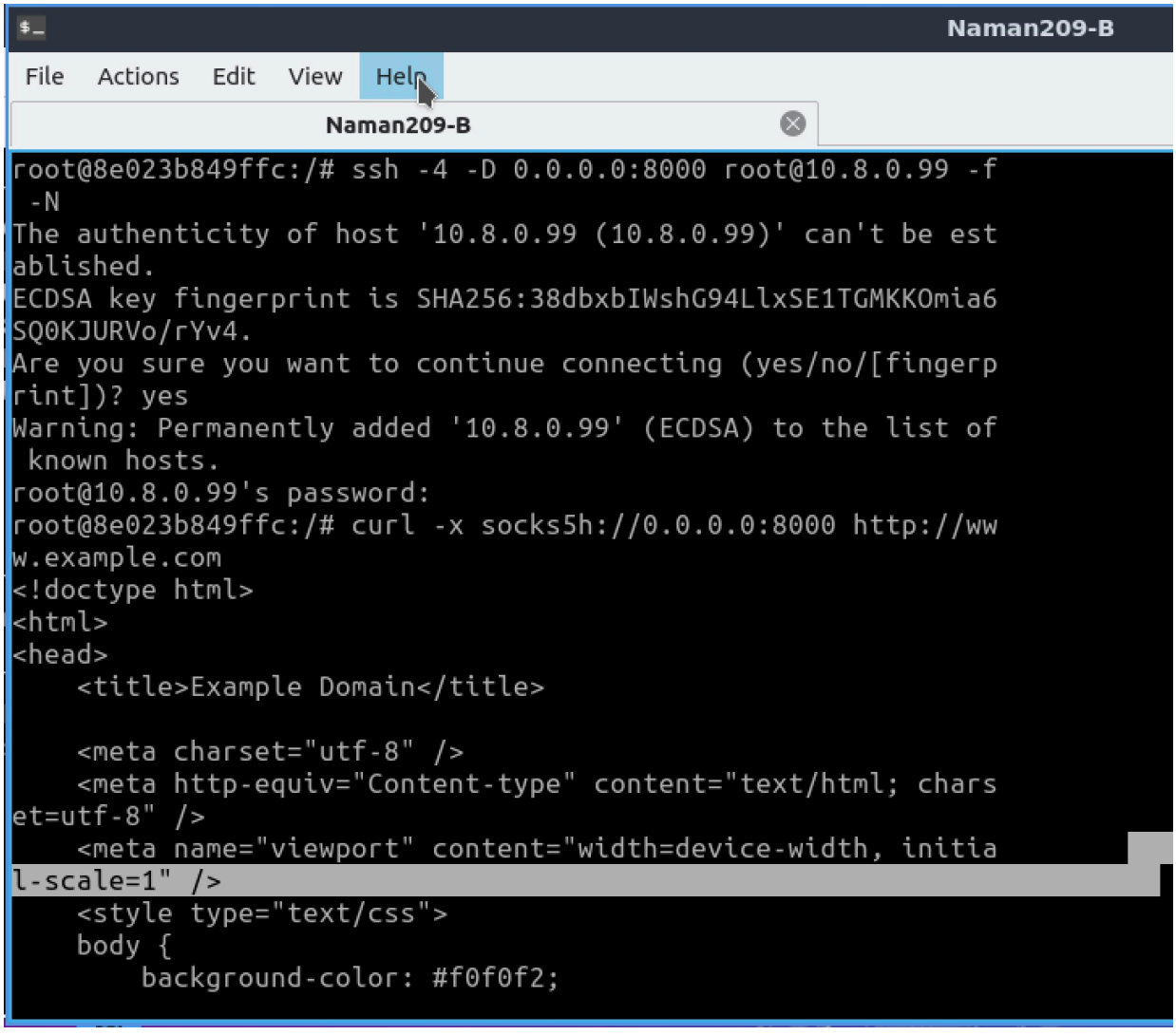


Task 2: Dynamic Port Forwarding

Task 2.1: Setting Up Dynamic Port Forwarding

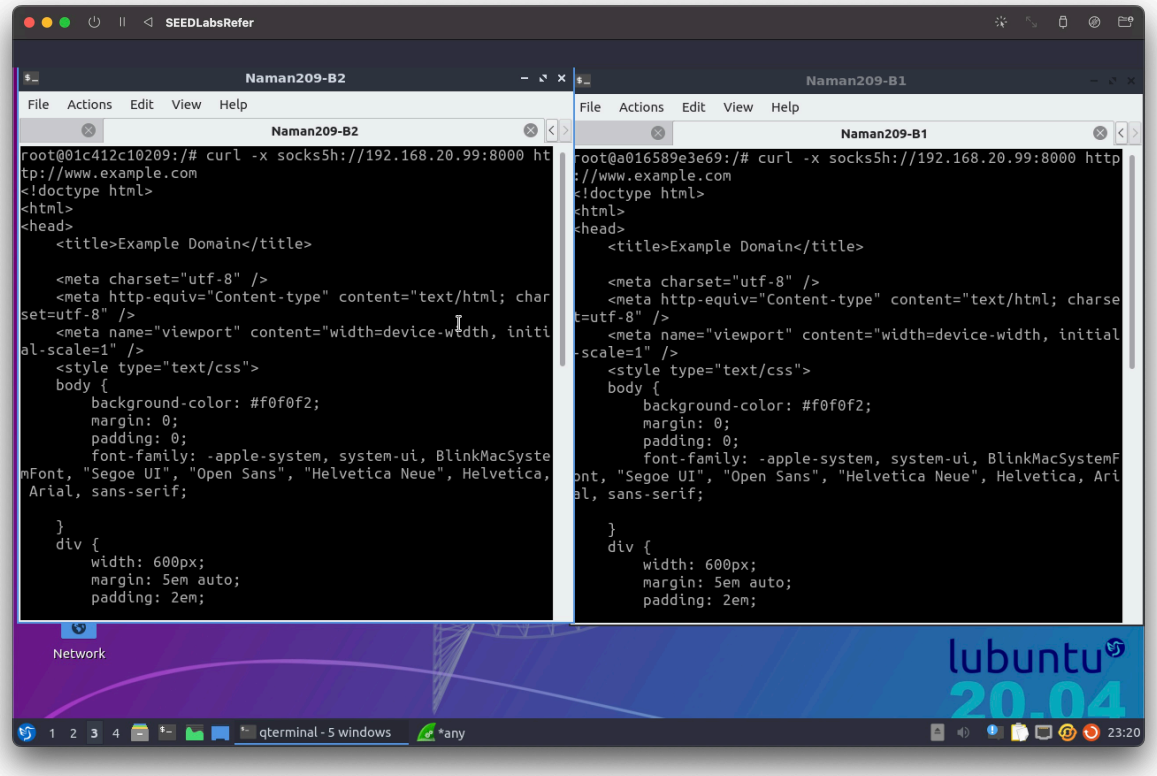
In B:

```bash
ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
curl -x socks5h://0.0.0.0:8000 http://www.example.com
```

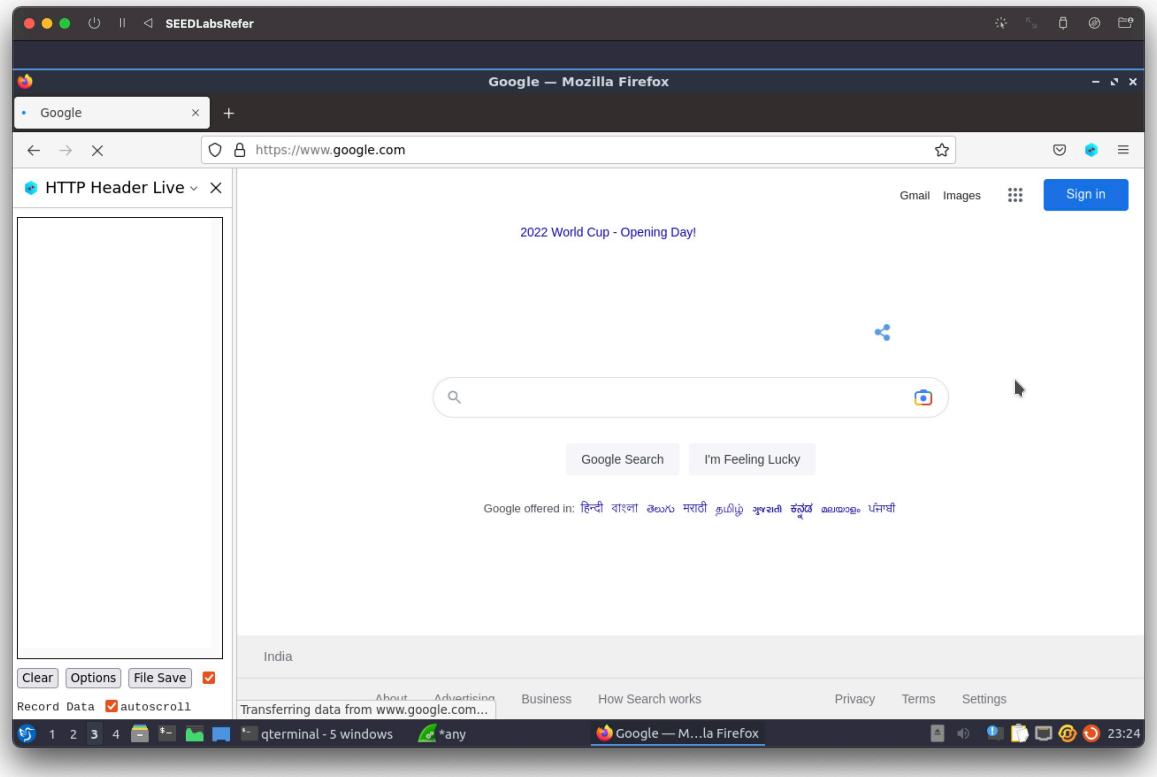


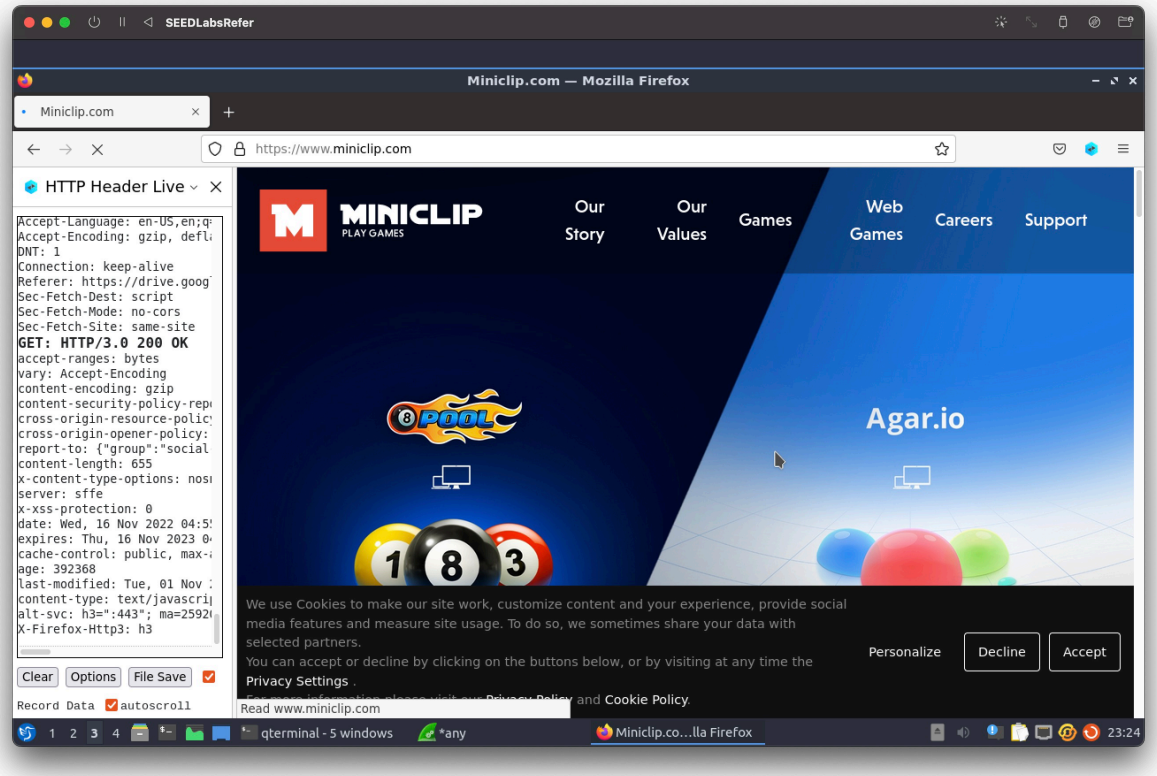
In B1 and B2:

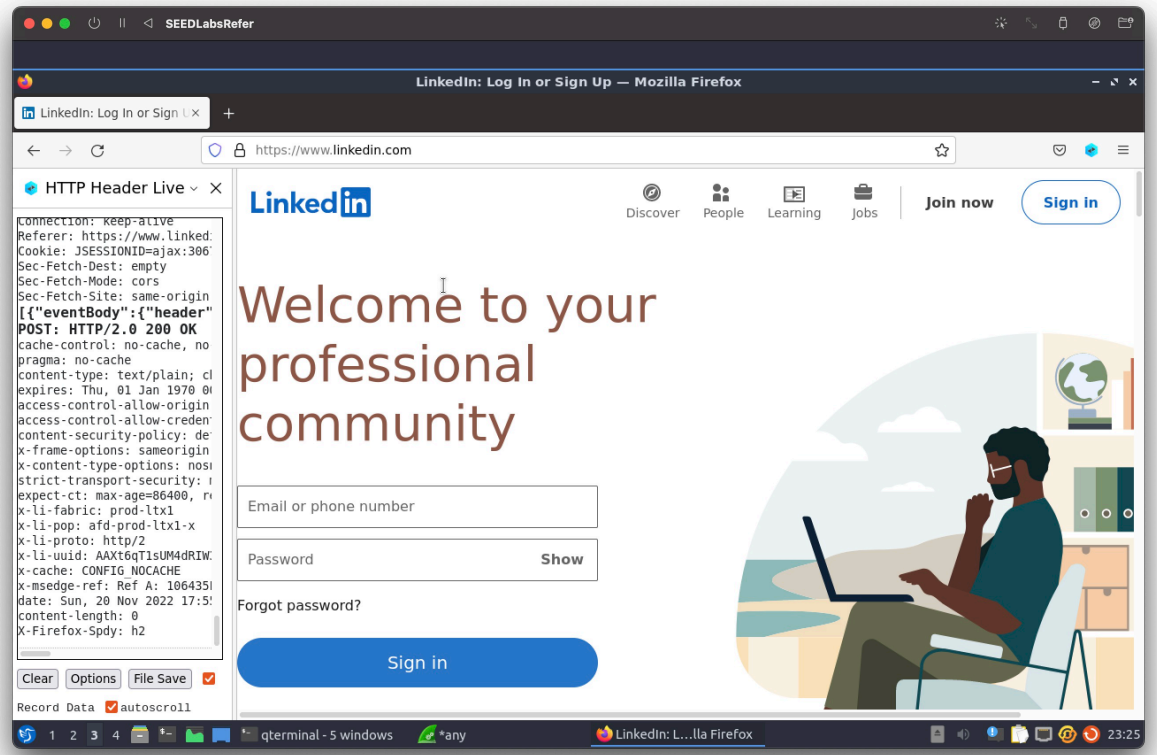
```bash
curl -x socks5h://192.168.20.99:8000 http://www.example.com
```



Task 2.2: Testing the Tunnel Using Browser

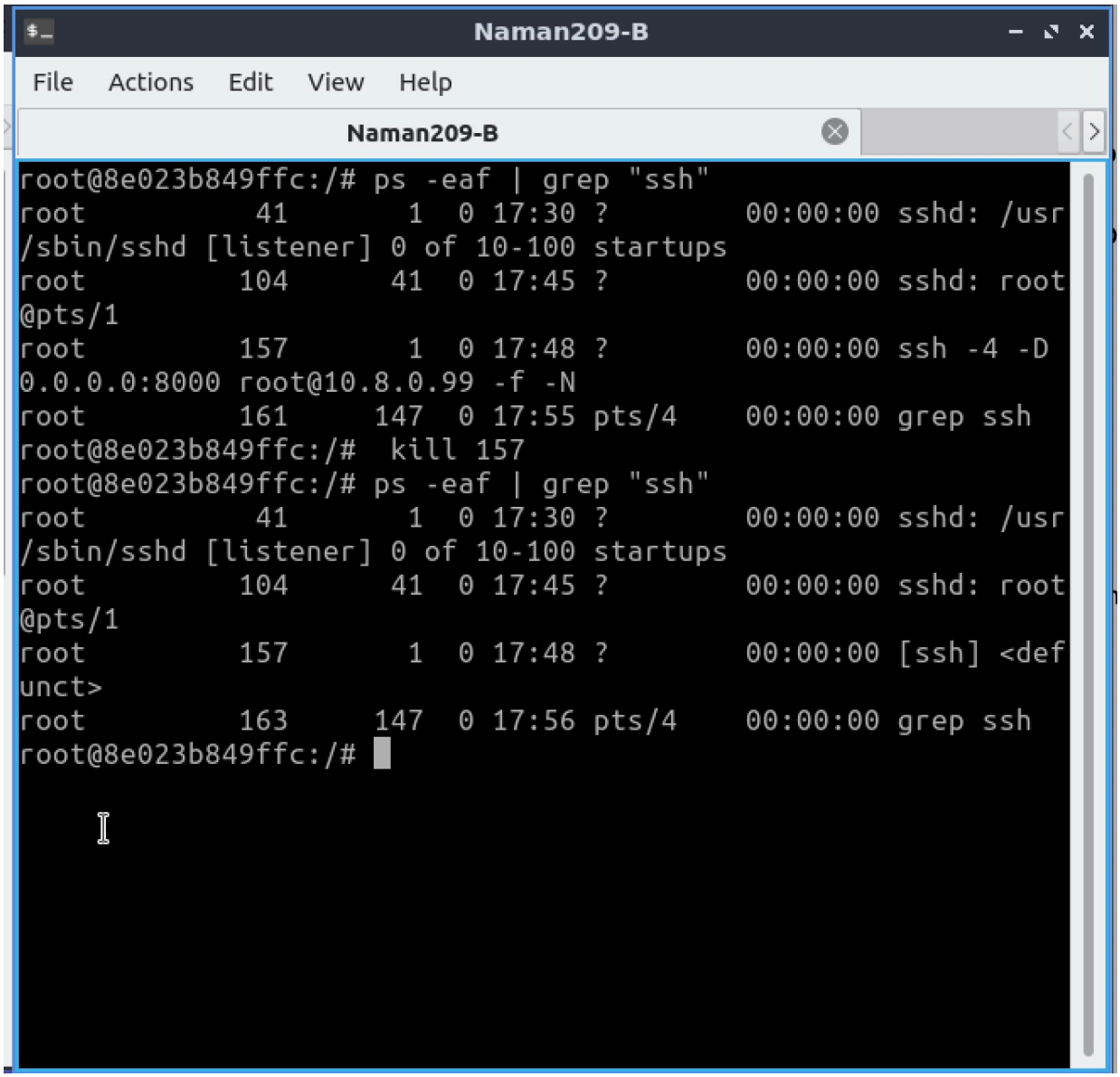


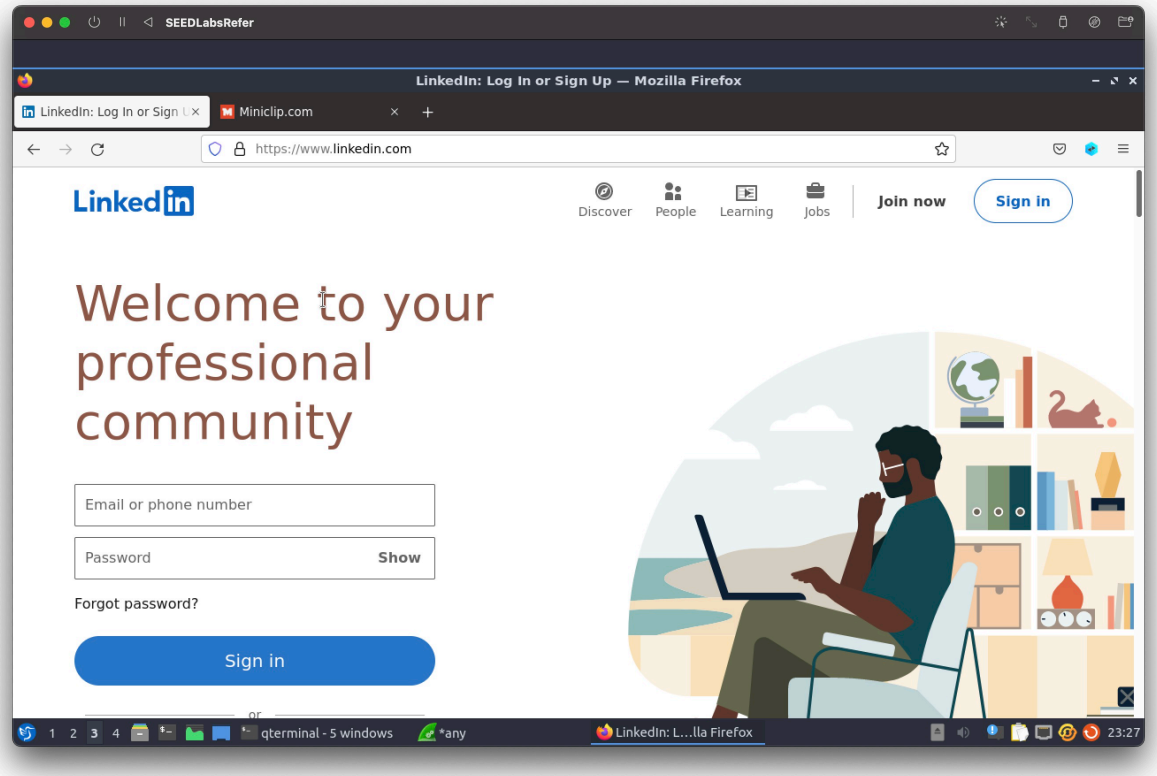


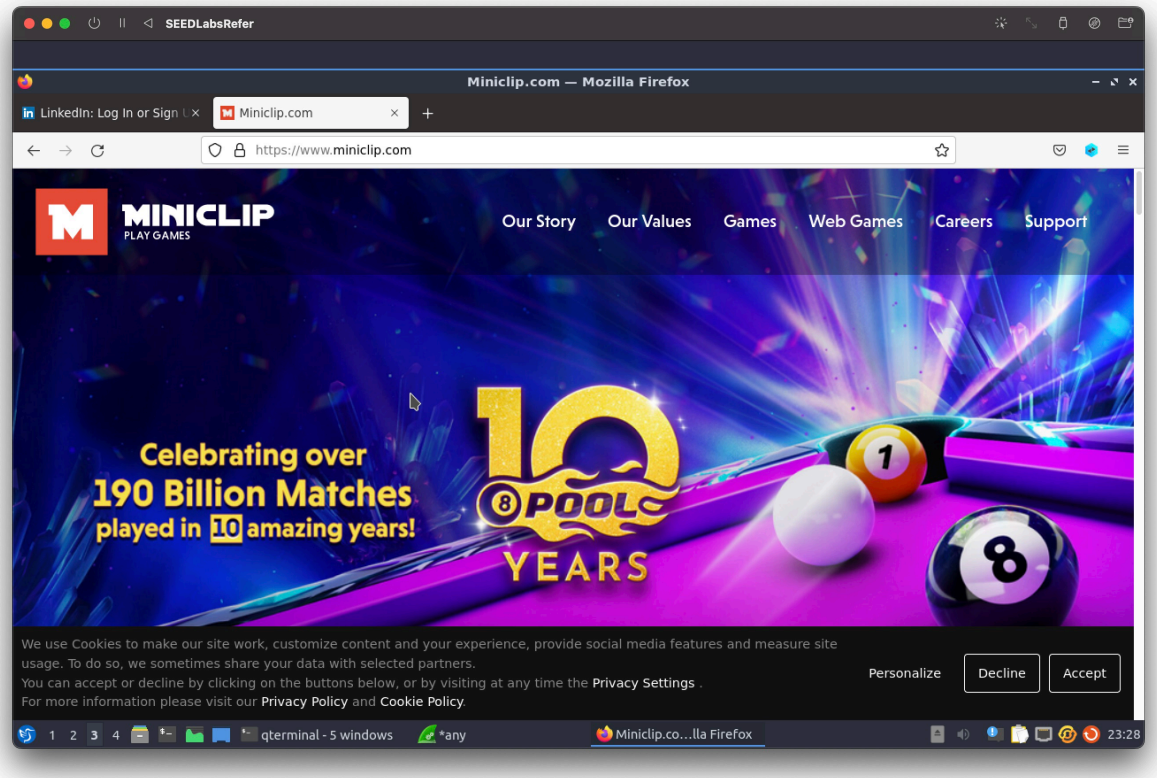


Bash

```
ps -eaf | grep "ssh"
```


Naman209-B
File Actions Edit View Help
Naman209-B
root@8e023b849ffc:/# ps -eaf | grep "ssh"
root 41 1 0 17:30 ? 00:00:00 sshd: /usr
/sbin/sshd [listener] 0 of 10-100 startups
root 104 41 0 17:45 ? 00:00:00 sshd: root
@pts/1
root 157 1 0 17:48 ? 00:00:00 ssh -4 -D
0.0.0.0:8000 root@10.8.0.99 -f -N
root 161 147 0 17:55 pts/4 00:00:00 grep ssh
root@8e023b849ffc:/# kill 157
root@8e023b849ffc:/# ps -eaf | grep "ssh"
root 41 1 0 17:30 ? 00:00:00 sshd: /usr
/sbin/sshd [listener] 0 of 10-100 startups
root 104 41 0 17:45 ? 00:00:00 sshd: root
@pts/1
root 157 1 0 17:48 ? 00:00:00 [ssh] <def
unct>
root 163 147 0 17:56 pts/4 00:00:00 grep ssh
root@8e023b849ffc:/#



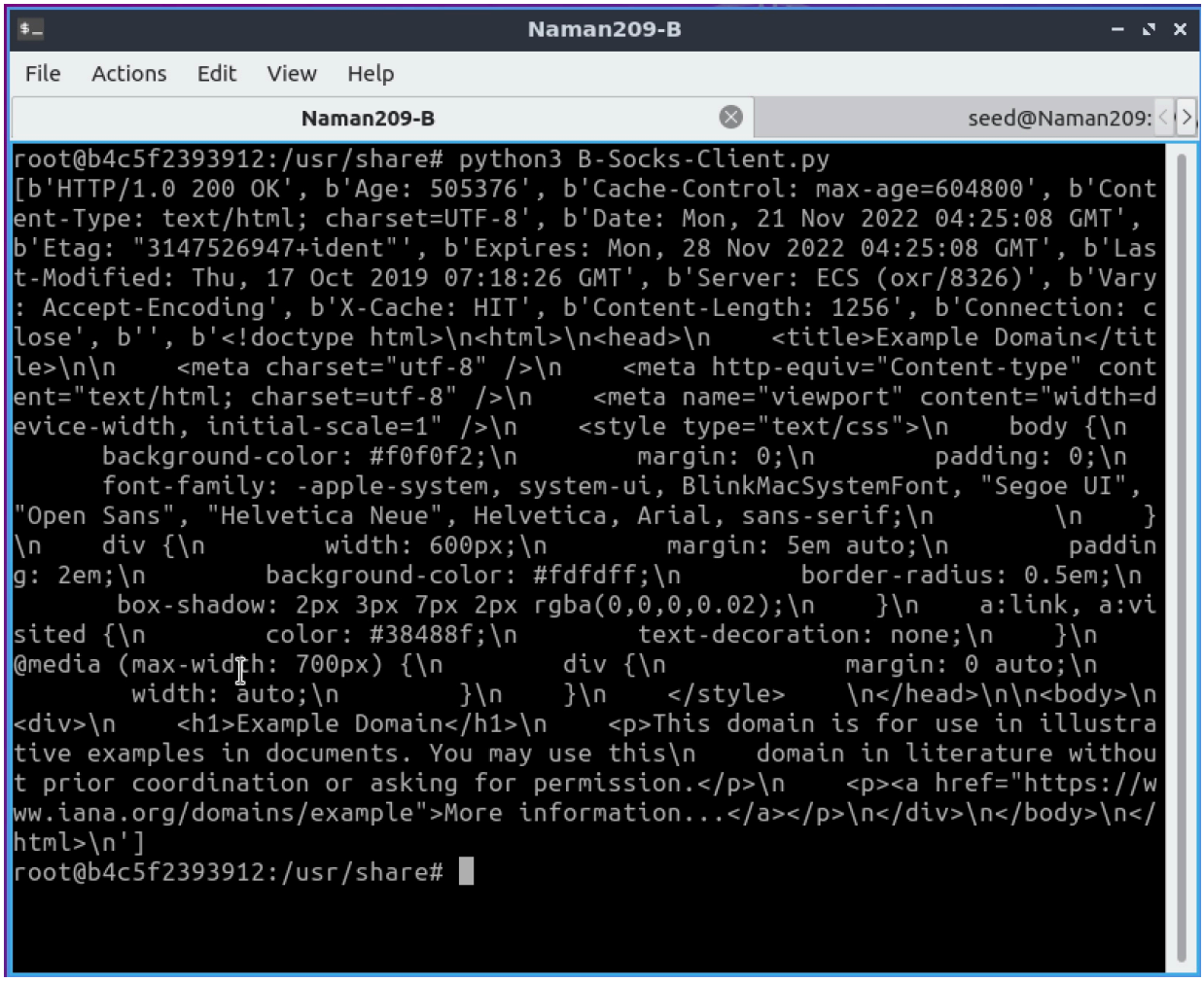


Observation: Inspite of firewall being active, we were successful in accessing the website due to evasion

Task 2.3: Writing a SOCKS Client Using Python

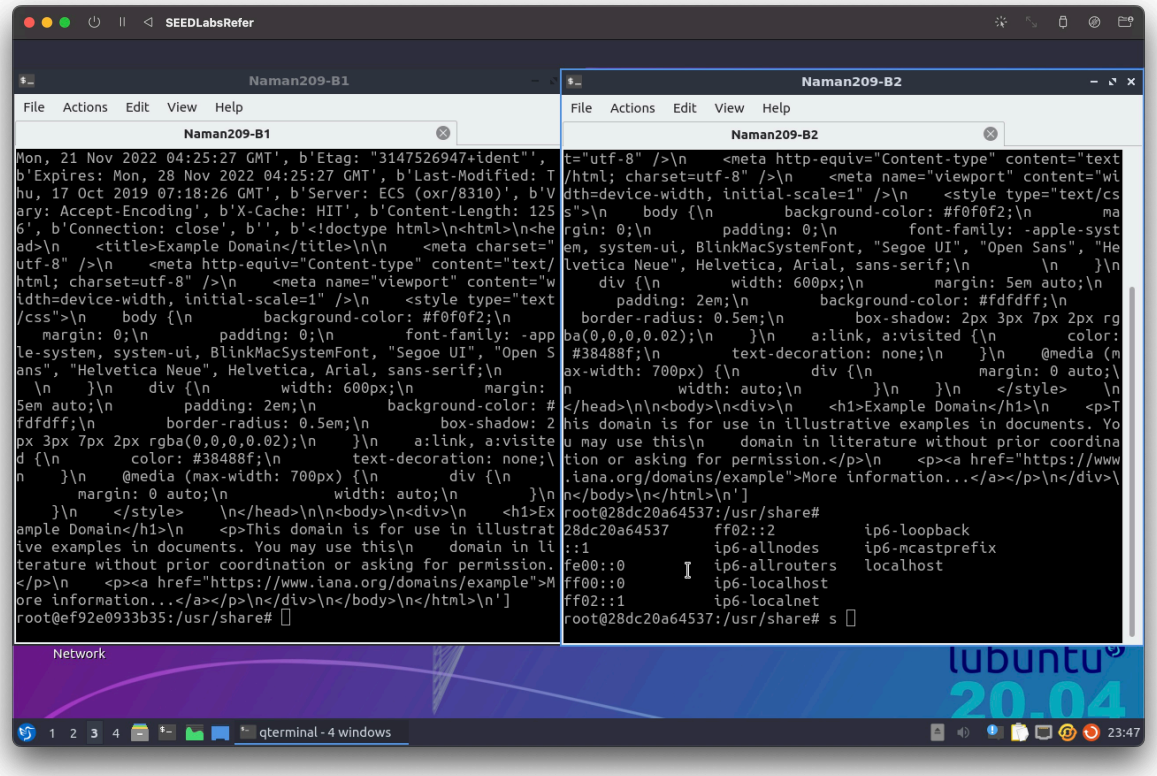
In B:

```bash
ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
python3 B-Socks-Client.py
```



In B1 and B2:

```bash
python3 B1-B2-Socks-Client.py
ps -eaf | grep "ssh"
kill
```



Task 3: Comparing SOCKS5 Proxy and VPN

Question: Both SOCKS5 proxy (dynamic port forwarding) and VPN are commonly used in creating tunnels to bypass firewalls, as well as to protect communications. Many VPN service providers provide both types of services. Sometimes, when a VPN service provider tells you that it provides the VPN service, but in reality, it is just a SOCKS5 proxy. Although both technologies can be used to solve the same problem, they do have significant differences. Please compare these two technologies, describing their differences, pros and cons.

Answer:

SOCKS5	**VPN**
PROS	
Masks User IP address	
Hides user identity for torrent clients	Provides data encryption
Faster than VPN	
Cons	
Third parties can still monitor download activity	
Differences	
Does not have its own software	Has its own software
Less costly	More costly
Works at app level	Works at system level
Used for web traffic (HTTP)	Used for all kinds of traffic