

Computer Network Security

Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

Firewall Exploration Lab

Task 0: Get Familiar with the Lab Setup

In router:

```
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
```

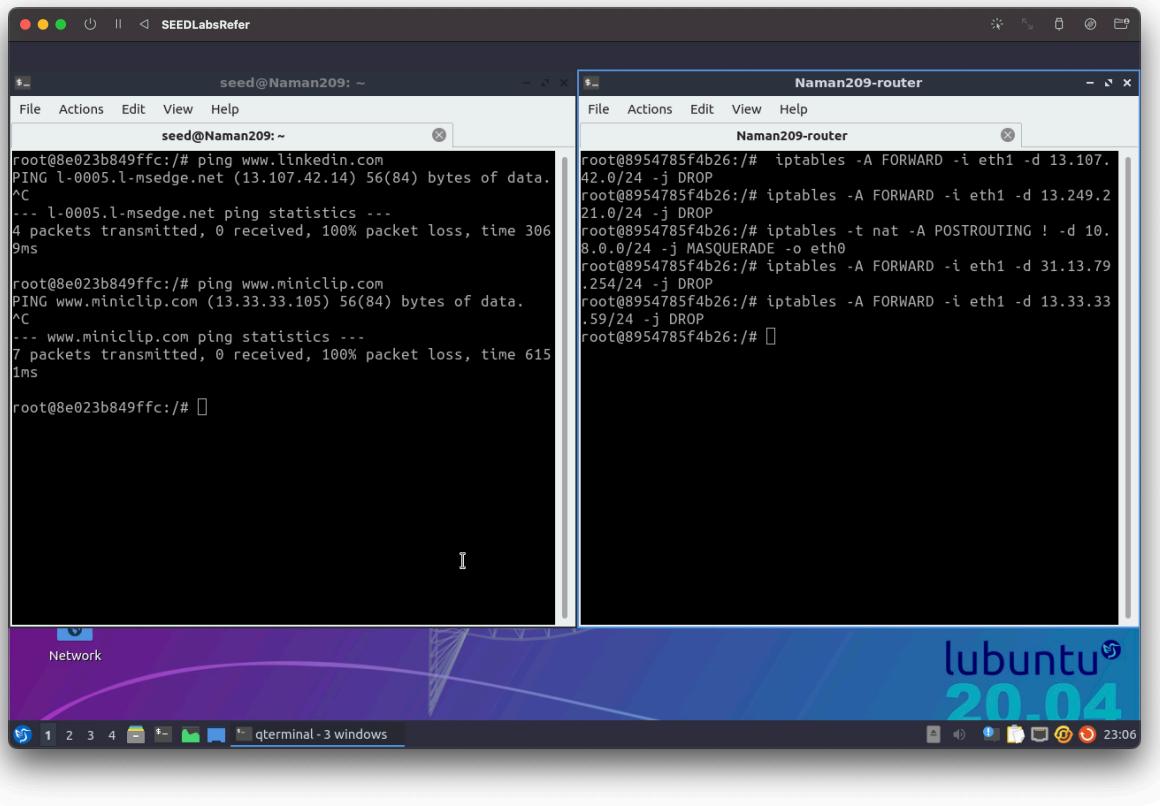
Bash

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

In B/B1/B2:

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

Bash

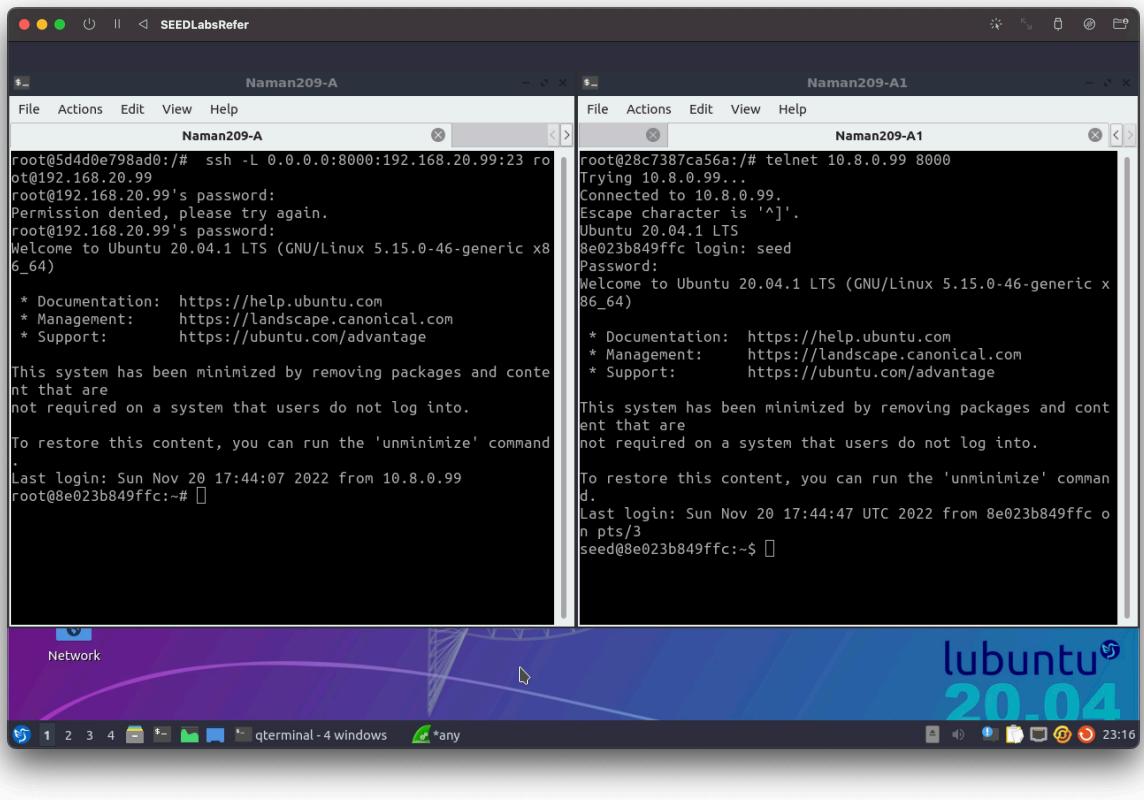


Task 1: Static Port Forwarding

In Container A:

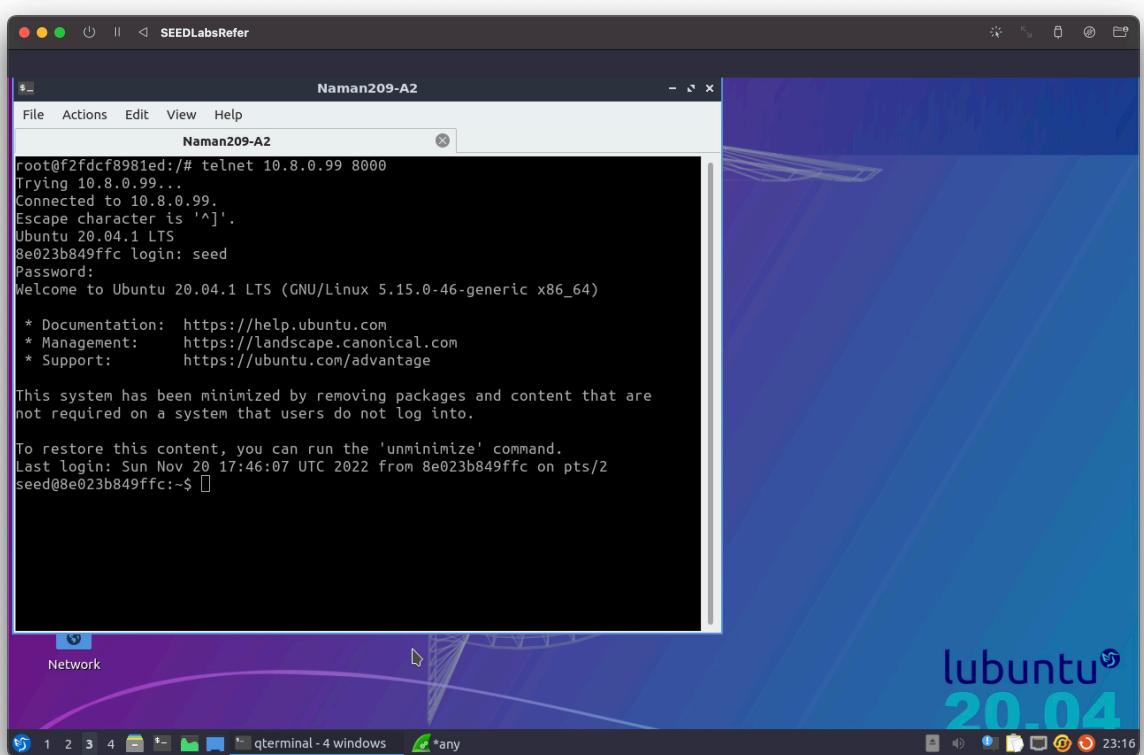
```
ssh -L 0.0.0.0:8000:192.168.20.99:23 root@192.168.20.99
```

Bash



In Container A1 and A2:

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
```

The screenshot shows a terminal window titled "Naman209-B". The window has a menu bar with "File", "Actions", "Edit", "View", and "Help". The "Help" option is currently selected. The main area of the terminal displays the following command and its output:

```
root@8e023b849ffc:/# ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
The authenticity of host '10.8.0.99 (10.8.0.99)' can't be established.
ECDSA key fingerprint is SHA256:38dbxbIWshG94LlxSE1TGMKK0mia6
SQ0KJURVo/rYv4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.8.0.99' (ECDSA) to the list of
known hosts.
root@10.8.0.99's password:
root@8e023b849ffc:/# curl -x socks5h://0.0.0.0:8000 http://www.example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>
    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
        body {
            background-color: #f0f0f2;
```

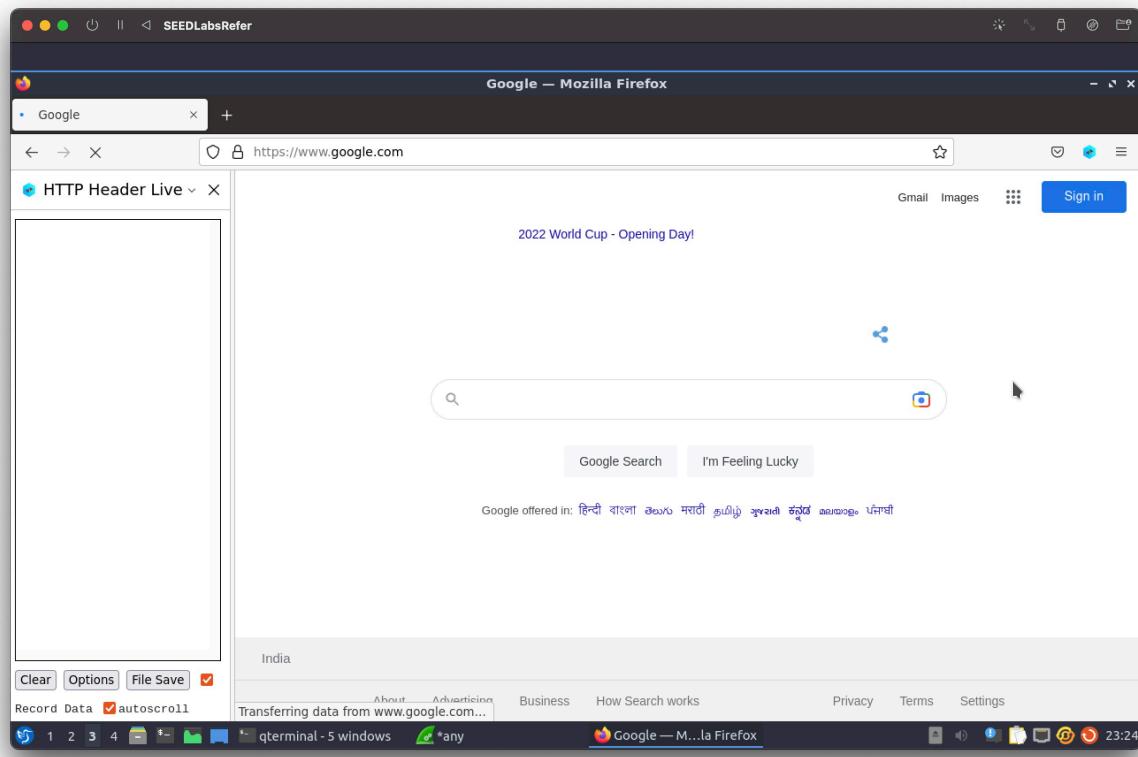
In B1 and B2:

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

```
root@01c412c10209:/# curl -x socks5h://192.168.20.99:8000 http://www.example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
        body {
            background-color: #f0f0f2;
            margin: 0;
            padding: 0;
            font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;
        }
        div {
            width: 600px;
            margin: 5em auto;
            padding: 2em;
        }
    </style>
</head>
<body>
    <div>
        <h1>Example Domain</h1>
        <p>The domain hasIPv4 address 192.168.20.99</p>
        <p>The domain hasIPv6 address fe80::501:1ff:fe00:1</p>
    </div>
</body>
</html>
```

Task 2.2: Testing the Tunnel Using Browser



SEEDLabsRefer

Miniclip.com — Mozilla Firefox

Miniclip.com

https://www.miniclip.com

HTTP Header Live

```
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Referer: https://drive.google.com
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-site
GET: HTTP/3.0 200 OK
accept-ranges: bytes
vary: Accept-Encoding
content-encoding: gzip
content-security-policy: report-only
cross-origin-resource-policies: cross-origin-opener-policy
report-to: {"group": "social"
content-length: 655
x-content-type-options: nosniff
server: sffe
x-xss-protection: 0
date: Wed, 16 Nov 2022 04:51:43
expires: Thu, 16 Nov 2023 04:51:43
cache-control: public, max-age: 392368
last-modified: Tue, 01 Nov 2022 04:51:43
content-type: text/javascript
alt-svc: h3=":443"; ma=2592
X-Firefox-Http3: h3

```

Clear Options File Save

Record Data autoscroll

Our Story Our Values Games Web Games Careers Support

MINICLIP PLAY GAMES

Agar.io

8 POOL

We use Cookies to make our site work, customize content and your experience, provide social media features and measure site usage. To do so, we sometimes share your data with selected partners.

You can accept or decline by clicking on the buttons below, or by visiting at any time the Privacy Settings.

Personalize Decline Accept

Read www.miniclip.com

terminal - 5 windows Miniclip.co...lla Firefox 23:24

SEEDLabsRefer

LinkedIn: Log In or Sign Up — Mozilla Firefox

LinkedIn: Log In or Sign Up

https://www.linkedin.com

HTTP Header Live

```
Connection: keep-alive
Referer: https://www.linkedin.com
Cookie: JSESSIONID=ajax:306
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
[{"eventBody": {"header": "POST: HTTP/2.0 200 OK
cache-control: no-cache, no-pragma
content-type: text/plain; cl
expires: Thu, 01 Jan 1970 00:00:00
access-control-allow-origin: *
access-control-allow-credentials: true
content-security-policy: default-src 'self'; frame-ancestors 'none'; strict-transport-security: 1; upgrade-insecure-requests: 1
x-frame-options: sameorigin
x-content-type-options: nosniff
strict-transport-security: 1
expect-ct: max-age=86400, report-uri=/-/csp/report-uri
x-li-fabric: prod-ltx1
x-li-pop: afd-prod-ltx1-x
x-li-proto: http/2
x-li-uuid: AAxt6GJlsUM4dRIW
x-cache: CONFIG NOCACHE
x-msedge-ref: Ref A: 106435
date: Sun, 20 Nov 2022 17:51:43
content-length: 0
X-Firefox-Spdy: h2

```

Clear Options File Save

Record Data autoscroll

Discover People Learning Jobs Join now Sign in

Welcome to your professional community

Email or phone number

Password Show

Forgot password?

Sign in



terminal - 5 windows Miniclip.co...lla Firefox 23:24

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

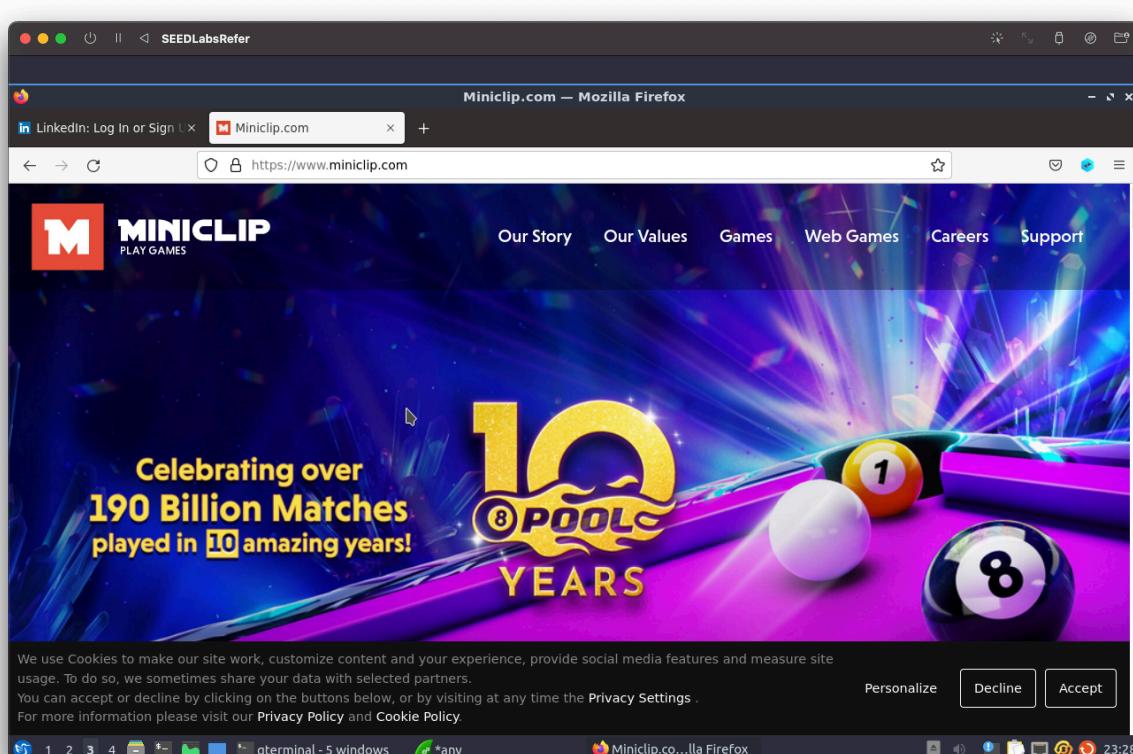
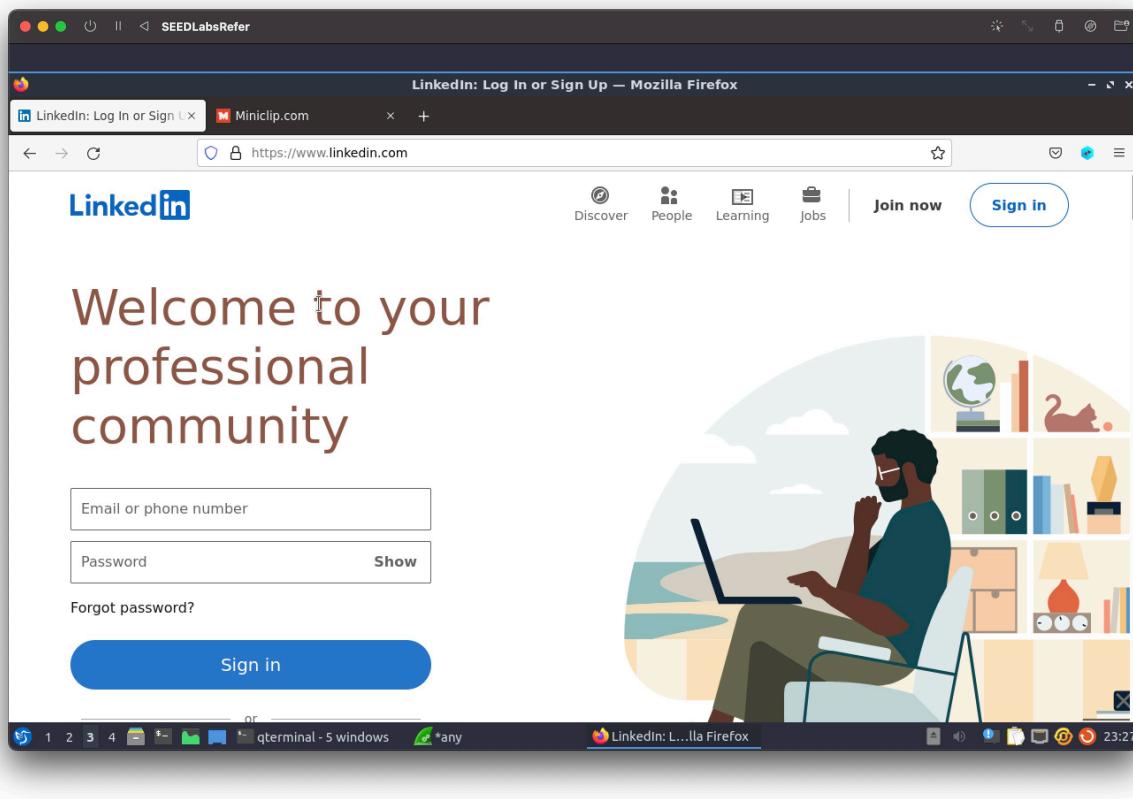
Bash

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:

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

Bash

```
root@b4c5f2393912:/usr/share# python3 B-Socks-Client.py  
[b'HTTP/1.0 200 OK', b'Age: 505376', b'Cache-Control: max-age=604800', b'Content-Type: text/html; charset=UTF-8', b'Date: Mon, 21 Nov 2022 04:25:08 GMT', b'Etag: "3147526947+ident"', b'Expires: Mon, 28 Nov 2022 04:25:08 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b'Server: ECS (oxr/8326)', b'Vary: Accept-Encoding', b'X-Cache: HIT', b'Content-Length: 1256', b'Connection: close', b'', b'<!doctype html>\n<html>\n<head>\n    <title>Example Domain</title>\n    <meta charset="utf-8" />\n    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />\n    <meta name="viewport" content="width=device-width, initial-scale=1" />\n    <style type="text/css">\n        body {\n            background-color: #f0f0f2;\n            margin: 0;\n            padding: 0;\n            font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;\n        }\n        div {\n            width: 600px;\n            margin: 5em auto;\n            padding: 2em;\n            background-color: #fdfdff;\n            border-radius: 0.5em;\n            box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);\n        }\n        a:link, a:visited {\n            color: #38488f;\n            text-decoration: none;\n        }\n        @media (max-width: 700px) {\n            div {\n                margin: 0 auto;\n                width: auto;\n            }\n        }\n    </style>\n</head>\n<body>\n    <h1>Example Domain</h1>\n    <p>This domain is for use in illustrative examples in documents. You may use this\n    domain in literature without prior coordination or asking for permission.</p>\n    <p><a href="https://www.iana.org/domains/example">More information...</a></p>\n</body>\n</html>\n']  
root@b4c5f2393912:/usr/share#
```

In B1 and B2:

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

Bash

```

Mon, 21 Nov 2022 04:25:27 GMT', b'ETag: "3147526947+ident"',  

b'Expires: Mon, 28 Nov 2022 04:25:27 GMT', b'Last-Modified: T  

hu, 17 Oct 2019 07:18:26 GMT', b'Server: ECS (oxr/8310)', b'V  

ary: Accept-Encoding', b'X-Cache: HIT', b'Content-Length: 125  

6', b'Connection: close', b'', b'<!doctype html><html><he  

ad><title>Example Domain</title><meta charset="utf-8" /><meta http-equiv="Content-type" content="text/html; charset=utf-8" /><meta name="viewport" content="width=device-width, initial-scale=1" /><style type="text/css"></head><body><h1>Example Domain</h1><p>This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.</p><p><a href="https://www.iana.org/domains/example">More information...</a></p></body></html>'</pre>
t="utf-8" />\n    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />\n    <meta name="viewport" content="width=device-width, initial-scale=1" />\n    <style type="text/css">\n        body {\n            background-color: #f0f0f2;\n            margin: 0;\n            padding: 0;\n            font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;\n        }\n        div {\n            width: 600px;\n            margin: 5em auto;\n            padding: 2em;\n            background-color: #fdfdff;\n            border-radius: 0.5em;\n            box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);\n        }\n        a:link, a:visited {\n            color: #38488f;\n            text-decoration: none;\n        }\n        @media (max-width: 700px) {\n            div {\n                margin: 0 auto;\n                width: auto;\n            }\n        }\n    </style>\n</head><body><h1>Example Domain</h1><p>This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.</p><p><a href="https://www.iana.org/domains/example">More information...</a></p></body></html>'</pre>
root@f92e0933b35:/usr/share# 
```

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