COMPUTER NETWORK SECURITY

LAB-7

FIREWALL EVASION LAB

NAME: VISHWAS M

SRN: PES2UG20CS390

SEC: F

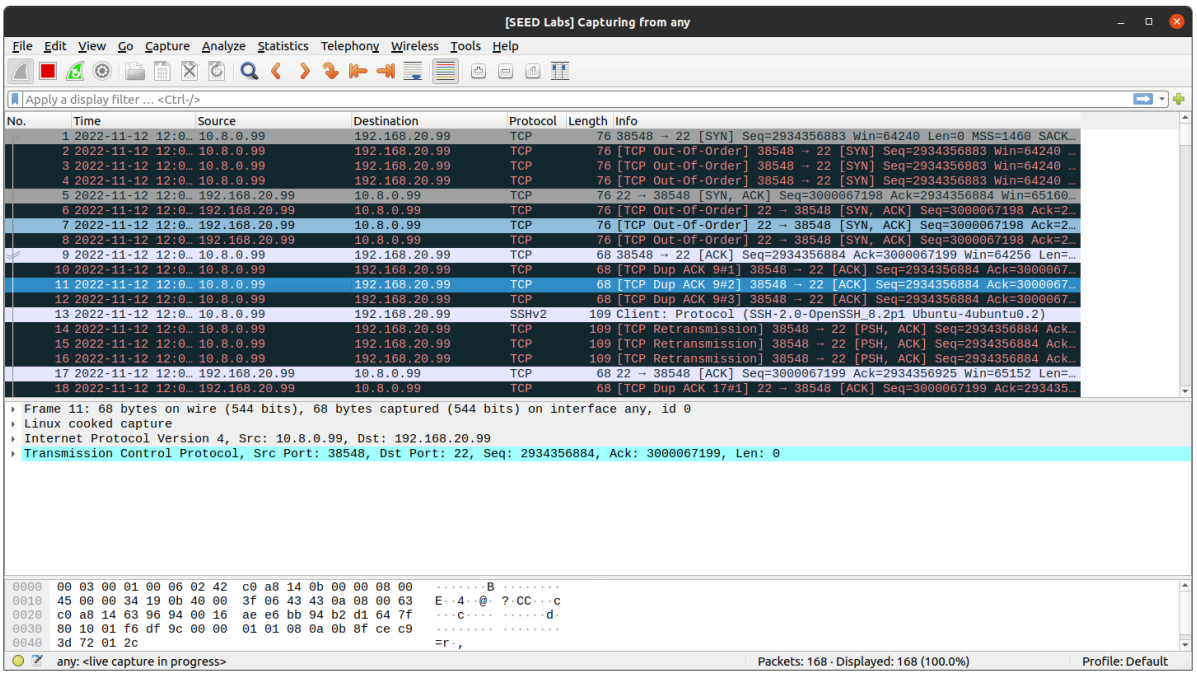
DATE:26/10/2022

Task 0: Get Familiar with The Lab Setup

```
root@router-firewall:PES2UG20CS390:Name:VishwasM$:/# iptables -A FORWARD -i eth1 -d 18.66
.53.41/24 -j DROP
root@router-firewall:PES2UG20CS390:Name:VishwasM$:/# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
DROP       tcp  --  anywhere             anywhere
DROP       all  --  anywhere             93.184.216.0/24
DROP       all  --  anywhere             13.107.42.0/24
DROP       all  --  anywhere             server-13-249-221-0.blr50.r.cloudfront.net/24
DROP       all  --  anywhere             server-18-66-53-0.bom78.r.cloudfront.net/24

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@router-firewall:PES2UG20CS390:Name:VishwasM$:/#
```

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup   seed@VM: ~/.../Labsetup   seed@VM: ~/.../Labsetup   seed@VM: ~/.../Labsetup
root@hostB1:PES2UG20CS390:Name:VishwasM$:/# ping www.linkedin.com
PING www.linkedin.com (13.107.42.14) 56(84) bytes of data.
^C
--- www.linkedin.com ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4121ms

root@hostB1:PES2UG20CS390:Name:VishwasM$:/# ping www.miniclip.com
PING www.miniclip.com (18.66.53.41) 56(84) bytes of data.
^C
--- www.miniclip.com ping statistics ---
12 packets transmitted, 0 received, 100% packet loss, time 11249ms

root@hostB1:PES2UG20CS390:Name:VishwasM$:/#
```

Task1: Static Port Forwarding



```
seed@VM: ~/.../Labsetup
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@hostB:PES2UG20CS390:Name:VishwasM$:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.20.99  netmask 255.255.255.0  broadcast 192.168.20.255
        ether 02:42:c0:a8:14:63  txqueuelen 0  (Ethernet)
        RX packets 317  bytes 36588 (36.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 170  bytes 26439 (26.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 183  bytes 12093 (12.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 183  bytes 12093 (12.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

seed@hostB:PES2UG20CS390:Name:VishwasM$:~$
```

```
seed@VM: ~/.../Labsetup

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Nov 12 06:34:16 UTC 2022 from hostB:PES2UG20CS390:Name:VishwasM$ on pts/3
seed@hostB:PES2UG20CS390:Name:VishwasM$:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.20.99  netmask 255.255.255.0  broadcast 192.168.20.255
        ether 02:42:c0:a8:14:63  txqueuelen 0  (Ethernet)
        RX packets 295  bytes 34812 (34.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 157  bytes 24297 (24.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 146  bytes 9342 (9.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 146  bytes 9342 (9.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

seed@hostB:PES2UG20CS390:Name:VishwasM$:~$
```

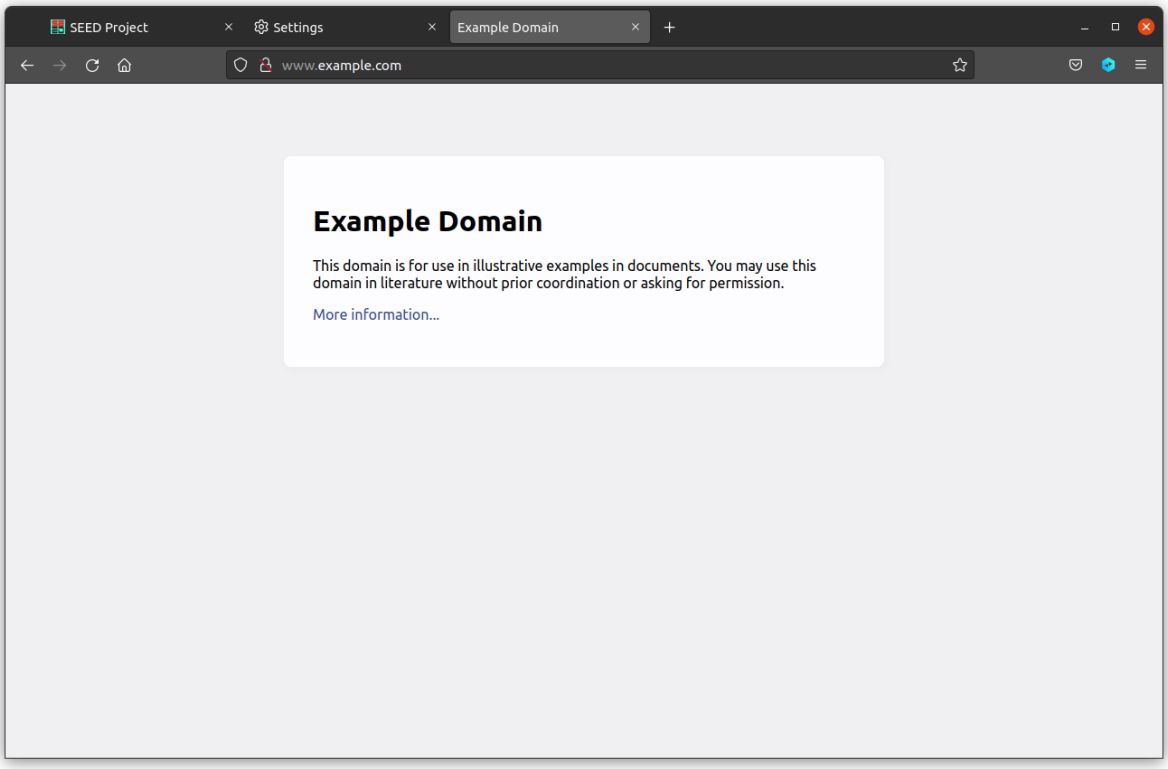
Task 2: Dynamic Port Forwarding

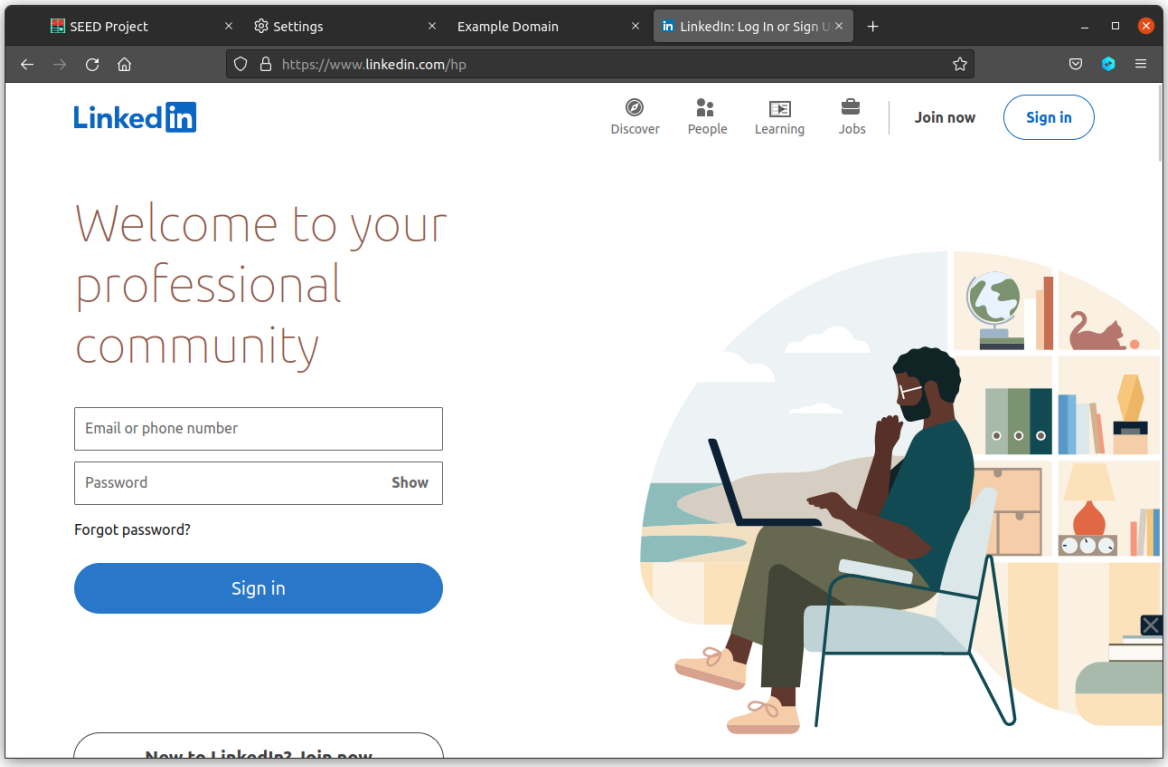
Task 2.1: Setting Up Dynamic Port Forwarding

```
seed@VM: ~/.../Labsetup
[11/18/22]seed@VM:~/.../Labsetup$ docksh 15
root@hostB:PES2UG20CS390:Name:VishwasM$:/# ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
The authenticity of host '10.8.0.99 (10.8.0.99)' can't be established.
ECDSA key fingerprint is SHA256:SAlHsnwHSrJ+xW1Ri3dDYFSUxTZt86VpVo9fjdDWVsI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.8.0.99' (ECDSA) to the list of known hosts.
root@10.8.0.99's password:
root@hostB:PES2UG20CS390:Name:VishwasM$:/# 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;
        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;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
```

```
seed@VM: ~/.../Labsetup
          <span class="language-selector__label-text mr-0.5 break-words">
            Language
          </span>
          <icon class="language-selector__label-chevron w-2 h-2 absolute top-0 right-0" data-delayed-url="https://static-exp1.licdn.com/aero-
v1/sc/h/cyolgscd0imw2ldqppkrb84vo"></icon>
        </button>

    </div>


  </li>

      </ul>

<!---->    </footer>


        <script src="https://static-exp1.licdn.com/aero-v1/sc/h/d8vx878ytdex6www299utgupr" async defer></script>

<!---->          <script data-delayed-url="https://static-exp1.licdn.com/aero-v1/sc/h/etkd25e7kzp2lrg1w9y0kixlu" data-module-id="google-sign-
in-lib"></script>
          <script data-delayed-url="https://static-exp1.licdn.com/aero-v1/sc/h/98lptr8kagfxge22q7k1fps8" data-module-id="google-one-tap-lib">
</script>


            <script src="https://static-exp1.licdn.com/aero-v1/sc/h/avzjesp0yrbz0c8qa81r63x7m" async></script>

      </body>
    </html>

  root@hostB:PES2UG20CS390:Name:VishwasM$:/#
```

We created a ssh tunnelling between the servers to extract the websites that are blocked by the firewall.



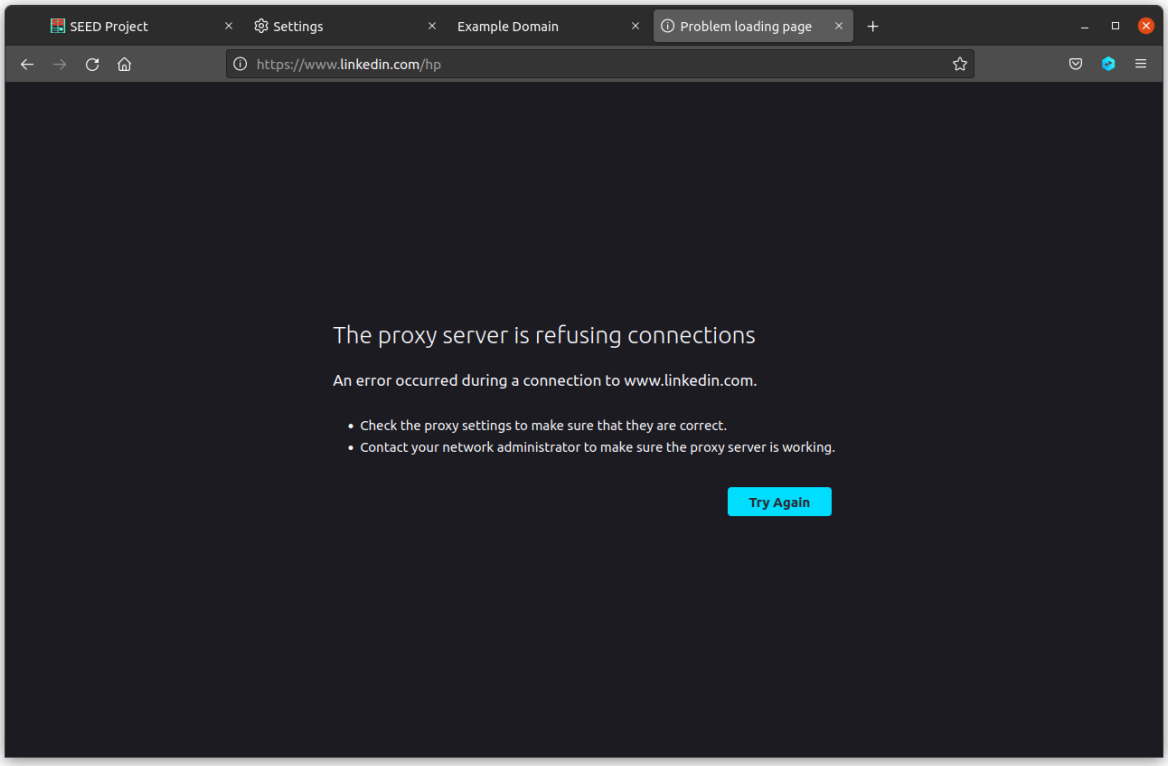


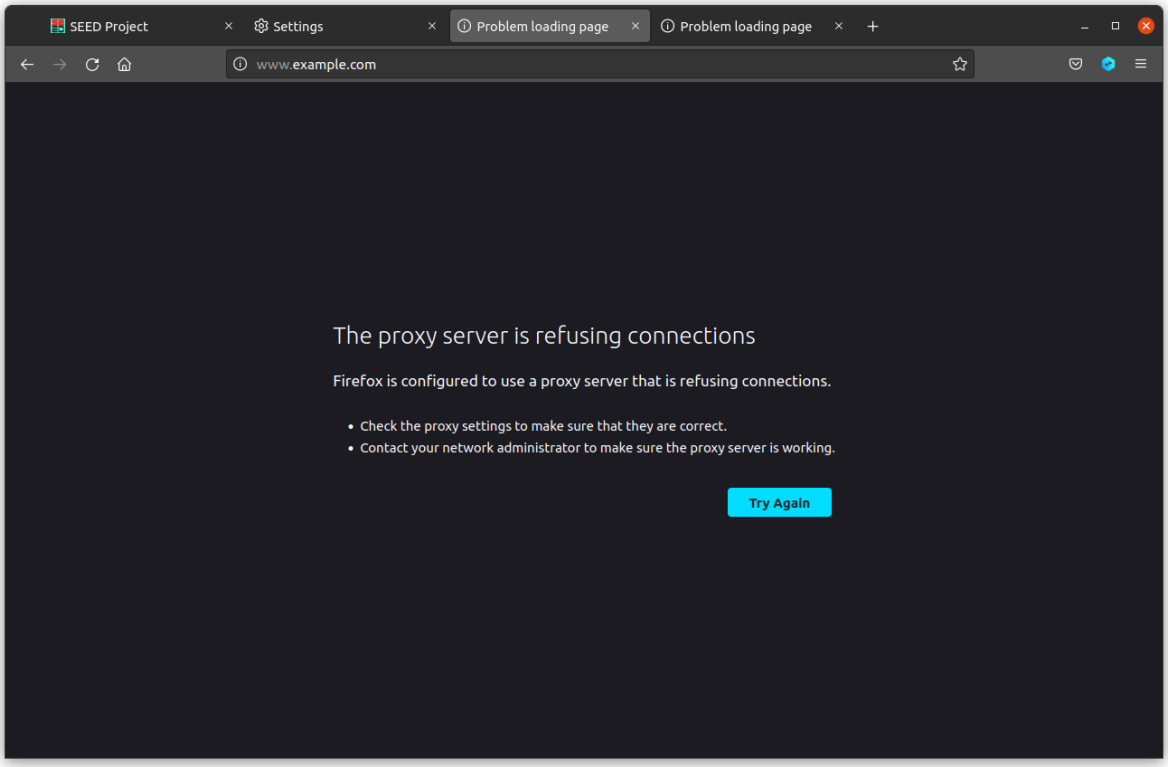
As we can see, the websites are available and are able to reach by the help of ssh tunnelling

```
seed@VM: ~/.../Labsetup
pt>

<!---->          <script data-delayed-url="https://static-exp1.licdn.com/aero-v1/sc/h/etkd25e7kzp2lrg1w9y0kix
lu" data-module-id="google-sign-in-lib"></script>
          <script data-delayed-url="https://static-exp1.licdn.com/aero-v1/sc/h/98lptr8kagfxge22q7k1fps8" data
-module-id="google-one-tap-lib"></script>


            <script src="https://static-exp1.licdn.com/aero-v1/sc/h/avzjesp0yrbz0c8qa81r63x7m" async></script
>

      </body>
    </html>

root@hostB:PES2UG20CS390:Name:VishwasM$:/# ps -eaf | grep ssh
root          38       1  0 13:05 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root          48       1  0 13:41 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root          54      40  0 15:54 pts/1    00:00:00 grep ssh
root@hostB:PES2UG20CS390:Name:VishwasM$:/# kill 48
root@hostB:PES2UG20CS390:Name:VishwasM$:/# ps -eaf | grep ssh
root          38       1  0 13:05 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root          48       1  0 13:41 ?        00:00:00 [ssh] <defunct>
root          56      40  0 15:56 pts/1    00:00:00 grep ssh
root@hostB:PES2UG20CS390:Name:VishwasM$:/#
```

We are killing the ssh tunnel and checking whether we ae able to reach the websites in the next task.

Task 2.2: Testing the Tunnel Using Browser





As we can see here we cannot reach the websites as we have removed the ssh tunnelling.

Task 2.3: Writing a SOCKS Client Using Python

```
seed@VM: ~/.../Labsetup
root@hostB:PES2UG20CS390:Name:VishwasM$:/# ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root@10.8.0.99's password:
root@hostB:PES2UG20CS390:Name:VishwasM$:/# python3 B-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Age: 133378', b'Cache-Control: max-age=604800', b'Content-Type: text/html; charset=UTF
-8', b'Date: Fri, 18 Nov 2022 16:04:04 GMT', b'Etag: "3147526947+ident"', b'Expires: Fri, 25 Nov 2022 16:04:0
4 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b'Server: ECS (dcb/7F17)', 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\n    <meta charset="utf-8" />\n    <meta http-equiv="Content-type" content="t
ext/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 N
eue", Helvetica, Arial, sans-serif;\n        \n    }\n    div {\n        width: 600px;\n        margin: 5em a
uto;\n        padding: 2em;\n        background-color: #fdfdff;\n        border-radius: 0.5em;\n        box-s
hadow: 2px 3px 7px 2px rgba(0,0,0,0.02);\n    }\n    a:link, a:visited {\n        color: #38488f;\n        te
xt-decoration: none;\n    }\n    @media (max-width: 700px) {\n        div {\n            margin: 0 auto;\n
        width: auto;\n        }\n    }\n    </style>    \n</head>\n\n<body>\n<div>\n    <h1>Example Domain</
h1>\n    <p>This domain is for use in illustrative examples in documents. You may use this\n    domain in lit
erature without prior coordination or asking for permission.</p>\n    <p><a href="https://www.iana.org/domain
s/example">More information...</a></p>\n</div>\n</body>\n</html>\n']
root@hostB:PES2UG20CS390:Name:VishwasM$:/#
```

```
seed@VM: ~/.../Labsetup
root@hostB1:PES2UG20CS390:Name:VishwasM$:/# nano B1-B2-Socks-Client.py
root@hostB1:PES2UG20CS390:Name:VishwasM$:/# python3 B1-B2-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Age: 345747', b'Cache-Control: max-age=604800', b'Content-Type: text/html; charset=UTF
-8', b'Date: Fri, 18 Nov 2022 16:05:09 GMT', b'Etag: "3147526947+ident"', b'Expires: Fri, 25 Nov 2022 16:05:0
9 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b'Server: ECS (dcb/7EA2)', 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\n    <meta charset="utf-8" />\n    <meta http-equiv="Content-type" content="t
ext/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 N
eue", Helvetica, Arial, sans-serif;\n        \n    }\n    div {\n        width: 600px;\n        margin: 5em a
uto;\n        padding: 2em;\n        background-color: #fdfdff;\n        border-radius: 0.5em;\n        box-s
hadow: 2px 3px 7px 2px rgba(0,0,0,0.02);\n    }\n    a:link, a:visited {\n        color: #38488f;\n        te
xt-decoration: none;\n    }\n    @media (max-width: 700px) {\n        div {\n            margin: 0 auto;\n
        width: auto;\n        }\n    }\n    </style>    \n</head>\n\n<body>\n<div>\n    <h1>Example Domain</
h1>\n    <p>This domain is for use in illustrative examples in documents. You may use this\n    domain in lit
erature without prior coordination or asking for permission.</p>\n    <p><a href="https://www.iana.org/domain
s/example">More information...</a></p>\n</div>\n</body>\n</html>\n']
root@hostB1:PES2UG20CS390:Name:VishwasM$:/#
```

```
seed@VM: ~/.../Labsetup
root@hostB2:PES2UG20CS390:Name:VishwasM$:/# nano B1-B2-Socks-Client.py
root@hostB2:PES2UG20CS390:Name:VishwasM$:/# python3 B1-B2-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Age: 390863', b'Cache-Control: max-age=604800', b'Content-Type: text/html; charset=UTF
-8', b'Date: Fri, 18 Nov 2022 16:05:47 GMT', b'Etag: "3147526947+ident"', b'Expires: Fri, 25 Nov 2022 16:05:4
7 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b'Server: ECS (dcb/7EA7)', 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\n    <meta charset="utf-8" />\n    <meta http-equiv="Content-type" content="t
ext/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 N
eue", Helvetica, Arial, sans-serif;\n        \n    }\n    div {\n        width: 600px;\n        margin: 5em a
uto;\n        padding: 2em;\n        background-color: #fdfdff;\n        border-radius: 0.5em;\n        box-s
hadow: 2px 3px 7px 2px rgba(0,0,0,0.02);\n    }\n    a:link, a:visited {\n        color: #38488f;\n        te
xt-decoration: none;\n    }\n    @media (max-width: 700px) {\n        div {\n            margin: 0 auto;\n
        width: auto;\n        }\n    }\n    </style>    \n</head>\n\n<body>\n<div>\n    <h1>Example Domain</
h1>\n    <p>This domain is for use in illustrative examples in documents. You may use this\n    domain in lit
erature without prior coordination or asking for permission.</p>\n    <p><a href="https://www.iana.org/domain
s/example">More information...</a></p>\n</div>\n</body>\n</html>\n']
root@hostB2:PES2UG20CS390:Name:VishwasM$:/#
```

```
root@hostB:PES2UG20CS390:Name:VishwasM$:/# ps -eaf | grep ssh
root          38       1  0 13:05 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root          48       1  0 13:41 ?        00:00:00 [ssh] <defunct>
root          62       1  0 16:03 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root          66      40  0 16:07 pts/1    00:00:00 grep ssh
root@hostB:PES2UG20CS390:Name:VishwasM$:/# kill 62
root@hostB:PES2UG20CS390:Name:VishwasM$:/# ps -eaf | grep ssh
root          38       1  0 13:05 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root          48       1  0 13:41 ?        00:00:00 [ssh] <defunct>
root          62       1  0 16:03 ?        00:00:00 [ssh] <defunct>
root          68      40  0 16:07 pts/1    00:00:00 grep ssh
root@hostB:PES2UG20CS390:Name:VishwasM$:/#
```

Task3: Comparing SOCKS5 Proxy and VPN:

SOCKS5 and VPN do a similar job in computer networking system. They are used to bypass the security and go pass through it reach the servers which are not meant to be visited. SSH tunnelling is little bit faster than VPN. Firewalls usually block some of the websites. These websites can be reached with the help of SSH Tunnelling and VPN.