

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$:/#
```



The screenshot shows a terminal window titled 'seed@VM: ~/.../Labsetup'. It contains the following text:

```
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
root@hostA:PES2UG20CS390:Name:VishwasM$:/# ssh -L 0.0.0.0:8000:192.168.20.99:23 root@192.168.20.99
root@192.168.20.99's password:
Permission denied, please try again.
root@192.168.20.99's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

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 06:27:04 2022 from 10.8.0.99
root@hostB:PES2UG20CS390:Name:VishwasM$::~#
```

[SEED Labs] Capturing from any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl>/

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-11-12 12:0...	10.8.0.99	192.168.20.99	TCP	76	38548 → 22 [SYN] Seq=2934356883 Win=64240 Len=0 MSS=1460 SACK...
2	2022-11-12 12:0...	10.8.0.99	192.168.20.99	TCP	76	[TCP Out-Of-Order] 38548 → 22 [SYN] Seq=2934356883 Win=64240 ...
3	2022-11-12 12:0...	10.8.0.99	192.168.20.99	TCP	76	[TCP Out-Of-Order] 38548 → 22 [SYN] Seq=2934356883 Win=64240 ...
4	2022-11-12 12:0...	10.8.0.99	192.168.20.99	TCP	76	[TCP Out-Of-Order] 38548 → 22 [SYN] Seq=2934356883 Win=64240 ...
5	2022-11-12 12:0...	192.168.20.99	10.8.0.99	TCP	76	22 → 38548 [SYN, ACK] Seq=3000067198 Ack=2934356884 Win=65160 ...
6	2022-11-12 12:0...	192.168.20.99	10.8.0.99	TCP	76	[TCP Out-Of-Order] 22 → 38548 [SYN, ACK] Seq=3000067198 Ack=2...
7	2022-11-12 12:0...	192.168.20.99	10.8.0.99	TCP	76	[TCP Out-Of-Order] 22 → 38548 [SYN, ACK] Seq=3000067198 Ack=2...
8	2022-11-12 12:0...	192.168.20.99	10.8.0.99	TCP	76	[TCP Out-Of-Order] 22 → 38548 [SYN, ACK] Seq=3000067198 Ack=2...
9	2022-11-12 12:0...	10.8.0.99	192.168.20.99	TCP	68	38548 → 22 [ACK] Seq=2934356884 Ack=3000067199 Win=64256 Len=...
10	2022-11-12 12:0...	10.8.0.99	192.168.20.99	TCP	68	[TCP Dup ACK 9#1] 38548 → 22 [ACK] Seq=2934356884 Ack=3000067...
11	2022-11-12 12:0...	10.8.0.99	192.168.20.99	TCP	68	[TCP Dup ACK 9#2] 38548 → 22 [ACK] Seq=2934356884 Ack=3000067...
12	2022-11-12 12:0...	10.8.0.99	192.168.20.99	TCP	68	[TCP Dup ACK 9#3] 38548 → 22 [ACK] Seq=2934356884 Ack=3000067...
13	2022-11-12 12:0...	10.8.0.99	192.168.20.99	SSHv2	109	Client: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.2)
14	2022-11-12 12:0...	10.8.0.99	192.168.20.99	TCP	109	[TCP Retransmission] 38548 → 22 [PSH, ACK] Seq=2934356884 Ack...
15	2022-11-12 12:0...	10.8.0.99	192.168.20.99	TCP	109	[TCP Retransmission] 38548 → 22 [PSH, ACK] Seq=2934356884 Ack...
16	2022-11-12 12:0...	10.8.0.99	192.168.20.99	TCP	109	[TCP Retransmission] 38548 → 22 [PSH, ACK] Seq=2934356884 Ack...
17	2022-11-12 12:0...	192.168.20.99	10.8.0.99	TCP	68	22 → 38548 [ACK] Seq=3000067199 Ack=2934356925 Win=65152 Len=...
18	2022-11-12 12:0...	192.168.20.99	10.8.0.99	TCP	68	[TCP Dup ACK 17#1] 22 → 38548 [ACK] Seq=3000067199 Ack=293435...

Frame 11: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.8.0.99, Dst: 192.168.20.99
Transmission Control Protocol, Src Port: 38548, Dst Port: 22, Seq: 2934356884, Ack: 3000067199, Len: 0

0000 00 03 00 01 00 06 02 42 c0 a8 14 0b 00 00 08 00B.....
0010 45 00 00 34 19 0b 40 00 3f 06 43 43 0a 08 00 63 E..4..@..?..CC...c
0020 c0 a8 14 03 96 94 00 16 ae e6 bb 94 b2 d1 64 7f ..C.....d..
0030 80 10 01 f6 df 9c 00 00 01 01 08 0a 0b 8f ce c9
0040 3d 72 01 2c =r.,

any: <live capture in progress> Packets: 168 · Displayed: 168 (100.0%) Profile: Default

```
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

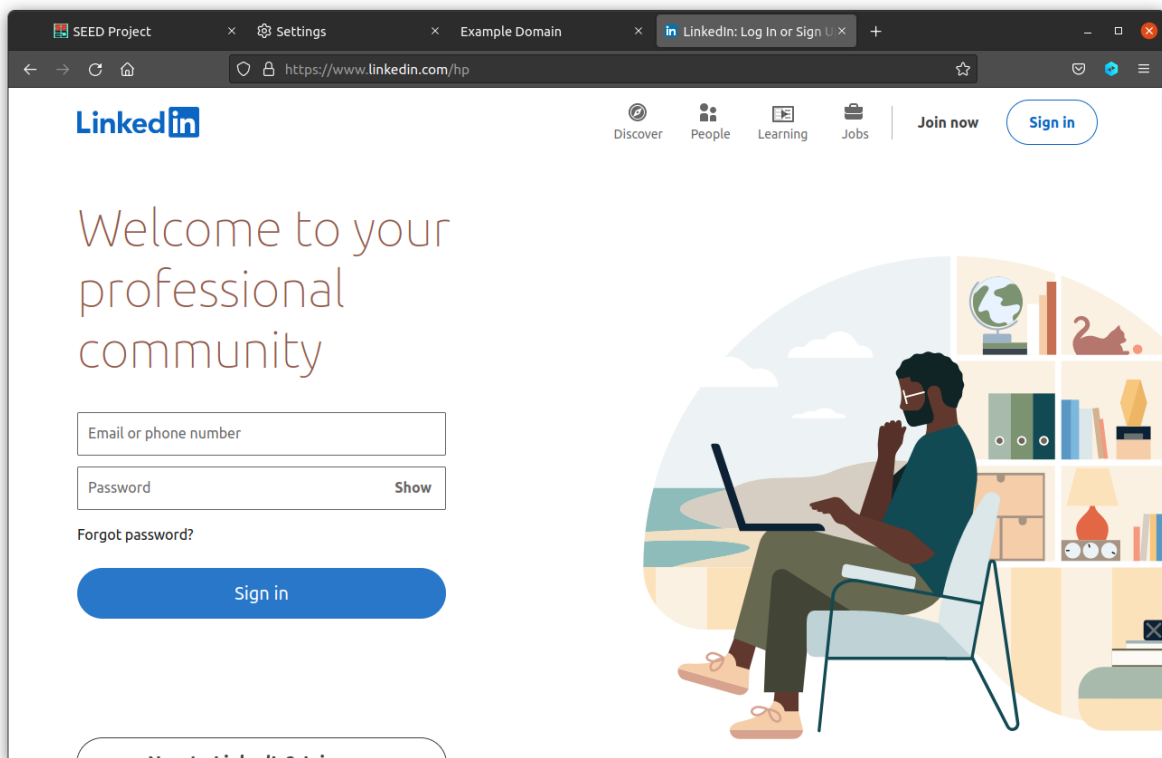
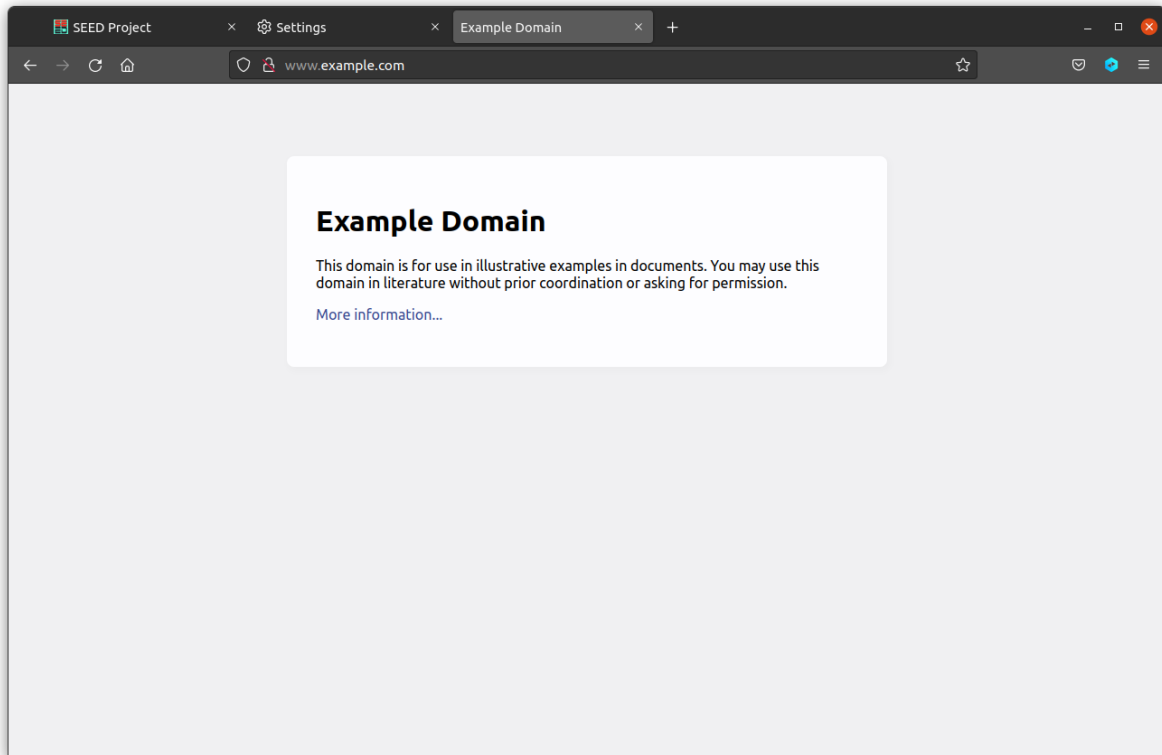
seed@hostB:PES2UG20CS390:Name:VishwasM$~$
```

Task 2.1: Setting Up Dynamic Port Forwarding

```
[11/18/22]seed@VM: ~/.../Labsetup$ docksh 15
root@hostB:PES2UG20CS390:Name:VishwasMS:/# 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+XWlRi3dDYFSUxTZt86VpVo9fjdDWVsI.
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:VishwasMS:/# 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 rgba(0,0,0,0.02);
        }
    </style>
</head>
<body>
    <div>
        <p>Hello World!</p>
    </div>
</body>
</html>
```

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

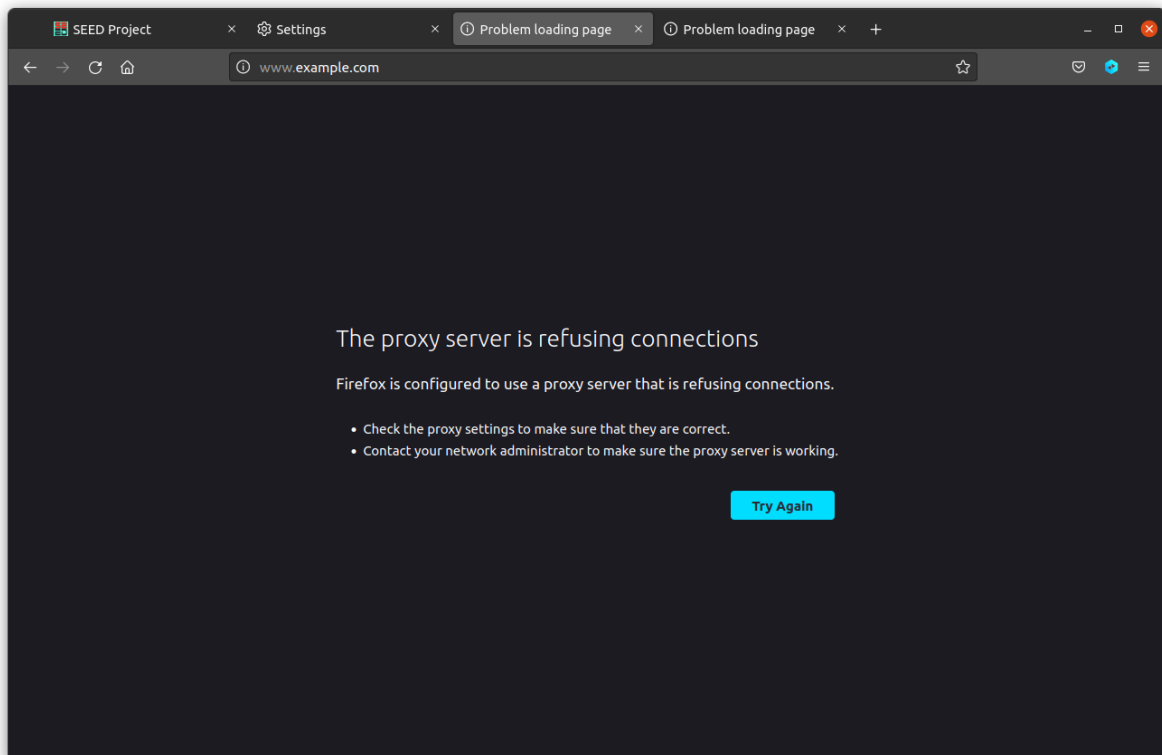
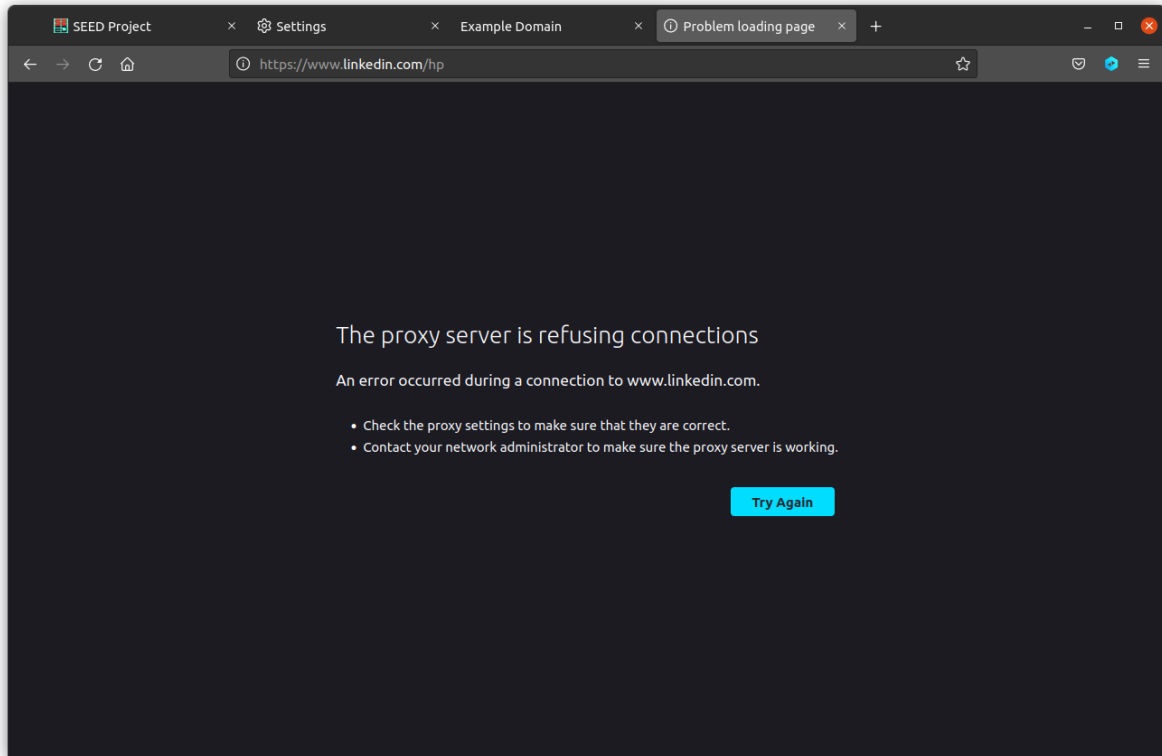
<script src="https://static-expl.licdn.com/aero-v1/sc/h/avzjesp0yrbz0c8qa81r63x7m" async></script>
>

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

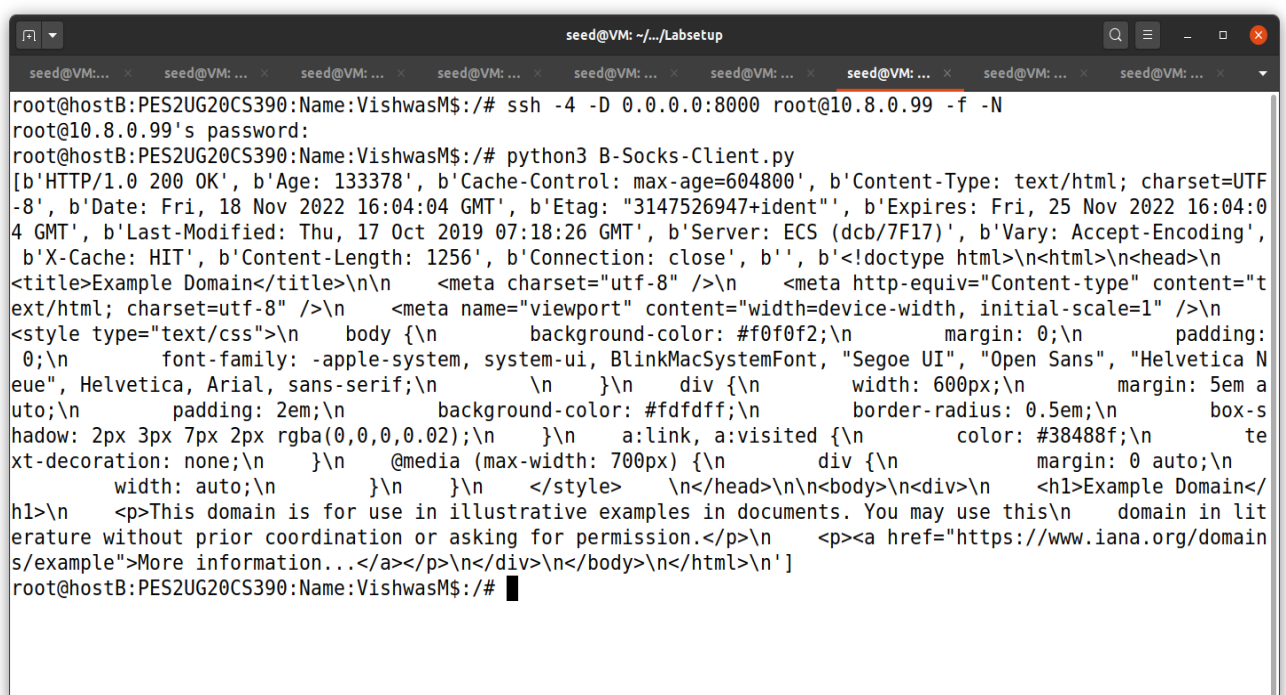
We are killing the ssh tunnel and checking whether we are able to reach the websites in the next task.

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 16:04:04 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="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\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 domain in literature 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 16:05:09 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="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  }\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<div>\n  <h1>Example Domain</h1>\n  <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>\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 16:05:47 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="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  }\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<div>\n  <h1>Example Domain</h1>\n  <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>\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$:/#
```

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