COMPUTER NETWORK SECURITY -08

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

Task 0 : Get Familiar with the Lab Setup

The two interfaces are checked to ensure that eth0 holds the 10.8.0.1 subnet and eth1 holds the 192.168.20.1 subnet. The following command is executed on the router/firewall and the resultant output is as shown below-

```
CS280_FIREWALL :/# ip -br address
lo               UNKNOWN        127.0.0.1/8
eth1@if25        UP             192.168.20.11/24
eth0@if27        UP             10.8.0.11/24
CS280_FIREWALL :/#


CS280_FIREWALL :/#
```

In order to verify if the routing tables at the router/firewall are working, we add two rules as shown below-

The rules drop those packets originating from the eth1 network that are to be forwarded by the router to the destined IP address (miniclip and linkedin in this case). The internal network in B connects to the Internet via the external network A.

```
CS280_FIREWALL :/# iptables -A FORWARD -i eth1 -d 13.107.42.0/24 -j DROP
CS280_FIREWALL :/# iptables -A FORWARD -i eth1 -d 13.249.221.0/24 -j DROP
CS280_FIREWALL :/#
```

When HostB in the internal network pings LinkedIn or Miniclip, the ICMP packets reach the router/firewall lying between eth0 and eth1's network. The firewall drops those packets pertaining to the rules mentioned above and therefore, the two pings are not successful.

```
CS280_B :/# ping www.linkedin.com
PING l-0005.l-msedge.net (13.107.42.14) 56(84) bytes of data.
^Z
[3]+  Stopped                 ping www.linkedin.com
CS280_B :/# ping www.miniclip.com
PING www.miniclip.com (13.249.221.22) 56(84) bytes of data.
^Z
[4]+  Stopped                 ping www.miniclip.com
CS280_B :/#
```

COMPUTER NETWORK SECURITY -08

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

Task 1 : Static Port Forwarding

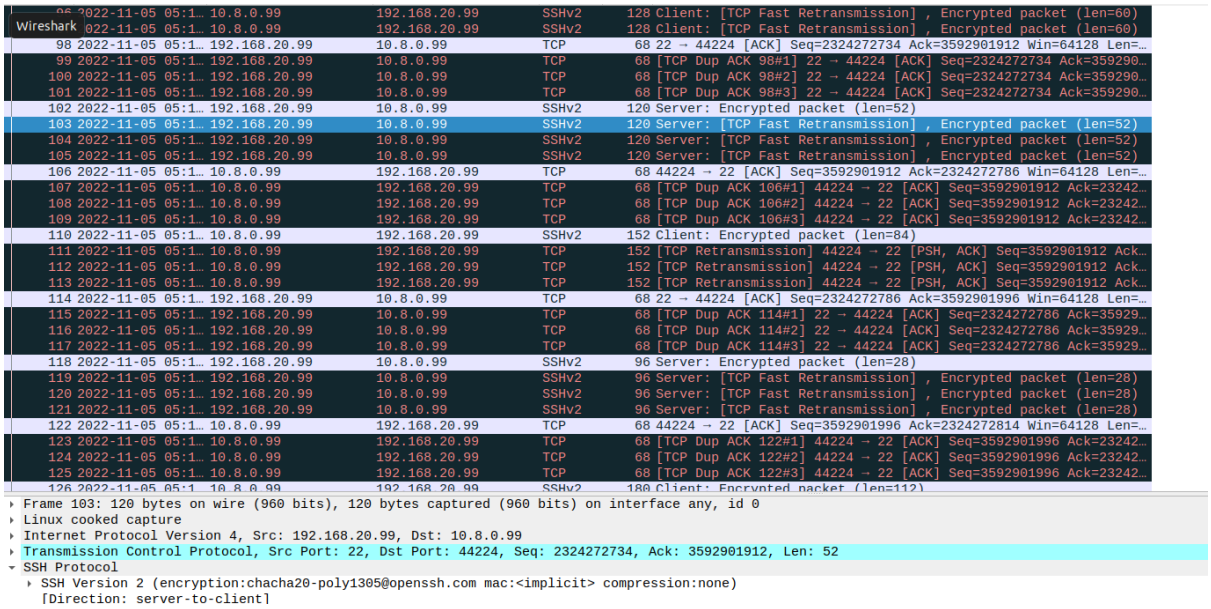
In this task an SSH connection is initiated between Host A in the eth1 network to HostB in the eth0 network. SSH connections are allowed b/w the two networks as the firewall does not drop those TCP packets directed to Port 22.

A connects to B; A1 and A2 tunnel into A and subsequently reach HostB.

When the below command is executed, HostA is able to connect to HostB via SSH.

```
CS280_A :/# ssh -L 0.0.0.0:8000:192.168.20.99:23 root@192.168.20.99
The authenticity of host '192.168.20.99 (192.168.20.99)' can't be established.
ECDSA key fingerprint is SHA256:n1b+aWRCO80F7lOi9dLj1tmdnSCCkYPm2TIg7SCqGoc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.20.99' (ECDSA) to the list of known hosts.
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.

The programs included with the Ubuntu system are free software;
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.

root@01bac72c5340:~# S
```

The corresponding Wireshark output can be seen below-



COMPUTER NETWORK SECURITY -08

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

TCP packets directed from 10.8.9.99 (HostA) reaches 192.168.20.99 (HostB) and vice versa.

When Hosta A1 and A2 telnet into 10.8.0.99(HostA), they connect to HostB via the SSH tunnel that is established when HostA connects to HostB.

Therefore, although A1 and A2 cannot directly telnet into HostB, they can telnet into B via A's SSH tunnel. This is static port forwarding. The port number (8000 is where the SSH tunnel is created on HostA) is also mentioned when the telnet command is used so that the tunnelling is possible.

```
CS280_A1 :/# telnet 10.8.0.99 8000
Trying 10.8.0.99...
Connected to 10.8.0.99.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
01bac72c5340 login: seed
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.

The programs included with the Ubuntu system are free software;
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.
```

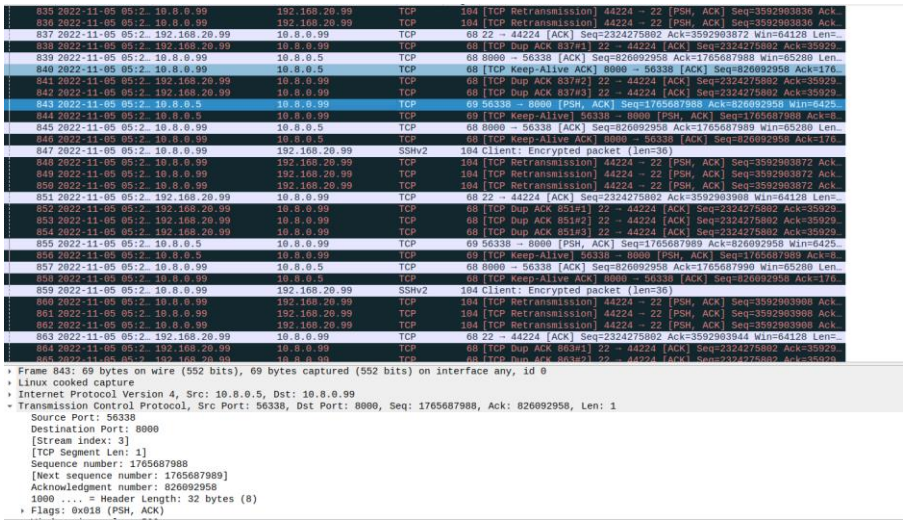
```
CS280_A2 :/# telnet 10.8.0.99 8000
Trying 10.8.0.99...
Connected to 10.8.0.99.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
01bac72c5340 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * 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  5 09:22:12 UTC 2022 from 01bac72c5340 on pts/3
```

The result of the same can be observed in the Wireshark outputs for both the telnets. The screenshots of the same are shown below-

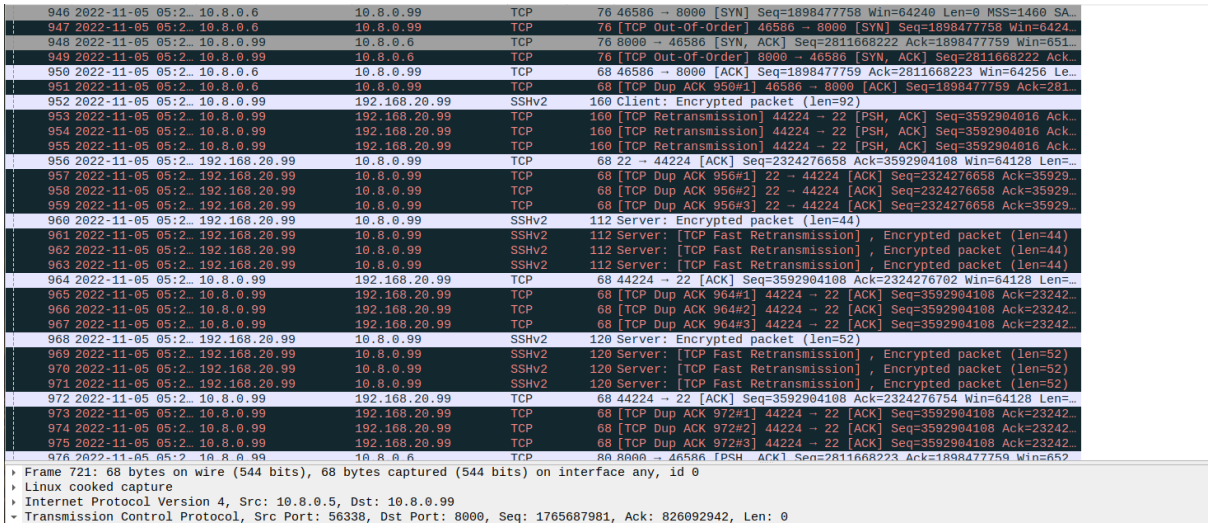
COMPUTER NETWORK SECURITY -08

Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section



for A1



For A2

As seen above, TCP packets are first sent from the respective hosts (A1 and A2) to HostA. Via SSH tunnelling, those packets are tunnelled and forwarded via the SSH tunnel to HostB (past the firewall). The ACK packets for every TCP packet received are sent back from HostB to HostA and eventually to HostA1/HostA2.

(1) How many TCP connections are involved in this entire process. You should run Wireshark or Tcpdump to capture the network traffic, and then point out all the involved TCP connections from the captured traffic.

Soln: As explained above, two TCP connections are involved in the process. The first connection is between the host (HostA1 or HostA2) and Host A. This can be inferred from the communication seen on Wireshark. The second TCP connection is between Host A and HostB.

COMPUTER NETWORK SECURITY -08

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

(2) Why can this tunnel successfully help users evade the firewall rule specified in the lab setup?

Soln: The firewall allows SSH connection/session between the hosts of the two networks (eth0 and eth1) and blocks any telnet connections b/w them. HostA's SSH connection with B is allowed. HostA1 telnets to HostA, from which it tunnels to HostB via the SSH tunnel. Therefore, there is no direct violation of the router firewall rules, so the firewall does not drop any packets, thereby making this attack/access successful.

COMPUTER NETWORK SECURITY -08

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

Task 2: Dynamic Port Forwarding

Task 2.1: Setting Up Dynamic Port Forwarding

In the previous task, we used static port forwarding to create an SSH tunnel. A static port tunnel can help several hosts on one side of the firewall tunnel into one specific server (at a specific port) on the other end of it. If the user intends to connect to multiple servers at the other end, then dynamic port forwarding is used.

An SSH session/tunnel (allowing for dynamic port forwarding) is established from HostB to HostA in this case.

```
CS280_B :/# 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:n1b+aWRCO80F7lOi9dLj1tmdnSCCkYPm2TIg7SCqGoc.
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:
CS280_B :/#
```

When curl is executed on HostB and details of example.com (which is blocked by the firewall) are sought, the result is as shown below-

```
CS280_B :/# 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);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
    </style>
</head>

<body>
<div>
    <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>
</div>
</body>
</html>
CS280_B :/#
```

The corresponding HTML page of that site is directed back to the HostB. In this port forwarding, the destination port is not explicitly specified as the port no. can vary for different websites. The source port at which the tunnel exists is however specified.

COMPUTER NETWORK SECURITY -08

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

B1 cannot access example.com on its own because of the firewall filtering. However, when it tunnels into HostB it connects to HostA which in turn connects to the Internet and sends across the request, response packets. B acts as an intermediary to the HTTP requests made by B1 and therefore, B is acting as the proxy in this case.

The result is the same for B2 as can be shown below→

B1:

```
CS280_B1 :/# 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;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
```

B2:

```
    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);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
    </style>
</head>

<body>
<div>
    <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>
</div>
</body>
</html>
CS280_B2 :/#
```

(3) Which computer establishes the actual connection with the intended web server?

Soln: HostA establishes the actual connection with the intended server. HostB connects to HostA and HostB1/B2 connects to HostB.

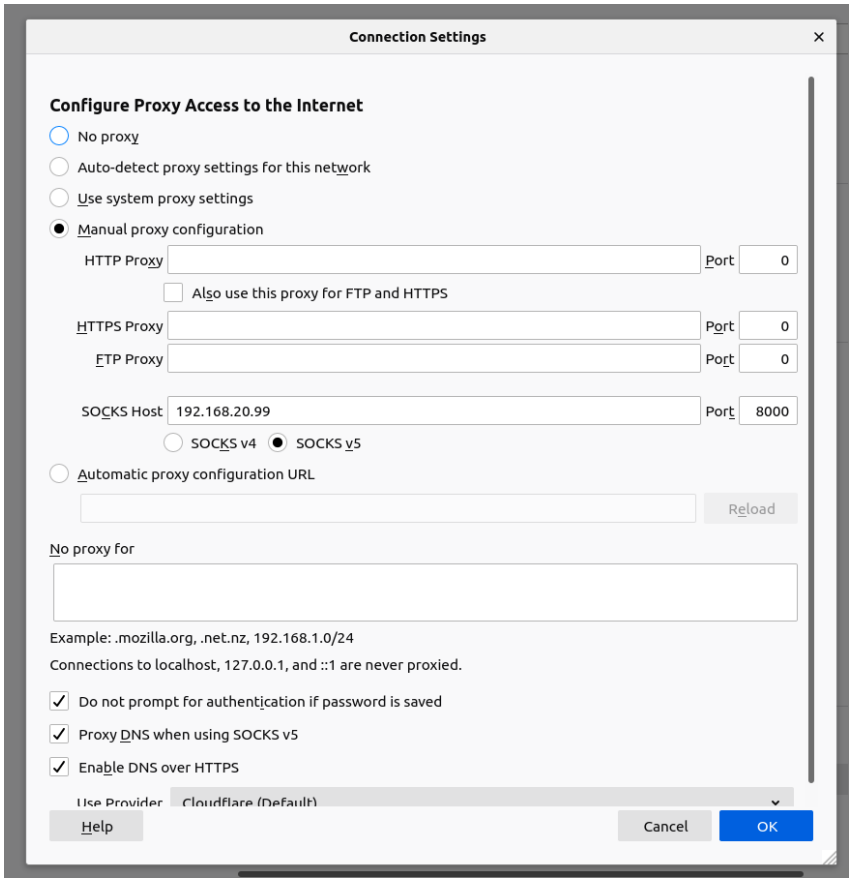
(4) How does this computer know which server it should connect to?

Soln: HTTP requests sent in turn have the destination IP address and the port number that the packet is intended to. When HostA receives this packet via the tunnel, it sends

this packet out to the Internet, realising that this packet is not meant for any host systems inside its local network.

Task 2.2: Testing the Tunnel Using Browser

The PROXY settings of the web browser on HostVM are changed. By allowing custom configurations, the SSH tunnel that was previously connected is used as the tunnel to allow hosts to connect to servers on the Internet. The result of the action is shown below-



When https://www.google.com is entered on the URL, the resultant traffic data seen on the router/firewall is displayed by tcpdump. The result is as shown below-

```
CS280_FIREWALL :/# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
09:57:53.574809 IP B-192.168.20.99.net-192.168.20.0.44070 > A-10.8.0.99.net-10.8.0.0.ssh: Flags [P.], seq 2134695642:2134695814, ack 2275249146, win 11394, options [nop,nop,TS val 1241148511 ecr 1528815920], length 172
09:57:53.574898 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.44070: Flags [.], ack 172, win 2489, options [nop,nop,TS val 1528818076 ecr 1241148511], length 0
09:57:53.608516 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.44070: Flags [P.], seq 1:157, ack 172, win 2489, options [nop,nop,TS val 1528818110 ecr 1241148511], length 156
09:57:53.608587 IP B-192.168.20.99.net-192.168.20.0.44070 > A-10.8.0.99.net-10.8.0.0.ssh: Flags [.], ack 157, win 11394, options [nop,nop,TS val 1241148545 ecr 1528818110], length 0
09:57:53.608829 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.44070: Flags [P.], seq 157:3053, ack 172, win 2489, options [nop,nop,TS val 1528818110 ecr 1241148545], length 2896
09:57:53.608844 IP B-192.168.20.99.net-192.168.20.0.44070 > A-10.8.0.99.net-10.8.0.0.ssh: Flags [.], ack 3053, win 11384, options [nop,nop,TS val 1241148545 ecr 1528818110], length 0
09:57:53.608850 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.44070: Flags [P.], seq 3053:5949, ack 172, win 2489, options [nop,nop,TS val 1528818110 ecr 1241148545], length 2896
09:57:53.608859 IP B-192.168.20.99.net-192.168.20.0.44070 > A-10.8.0.99.net-10.8.0.0.ssh: Flags [.], ack 5949, win 11373, options [nop,nop,TS val 1241148545 ecr 1528818110], length 0
09:57:53.608862 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.44070: Flags [P.], seq 5949:7497, ack 172, win 2489, options [nop,nop,TS val 1528818110 ecr 1241148545], length 1548
09:57:53.608869 IP B-192.168.20.99.net-192.168.20.0.44070 > A-10.8.0.99.net-10.8.0.0.ssh: Flags [.], ack 7497, win 11367, options [nop,nop,TS val 1241148545 ecr 1528818110], length 0
```

COMPUTER NETWORK SECURITY -08

Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section

```
09:58:04.408055 IP B-192.168.20.99.net-192.168.20.0.44070 > A-10.8.0.99.net-10.8.0.0.ssh: Flags [P.], seq 27276:28232, ack 942849, win 11394,
 options [nop,nop,TS val 1241159344 ecr 1528828909], length 956
09:58:04.408061 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.44070: Flags [.], ack 28232, win 2484, options [nop,nop,TS
 val 1528828909 ecr 1241159344], length 0
09:58:04.408074 IP B-192.168.20.99.net-192.168.20.0.44070 > A-10.8.0.99.net-10.8.0.0.ssh: Flags [P.], seq 28232:28372, ack 942849, win 11394,
 options [nop,nop,TS val 1241159344 ecr 1528828909], length 140
09:58:04.408078 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.44070: Flags [.], ack 28372, win 2483, options [nop,nop,TS
 val 1528828909 ecr 1241159344], length 0
09:58:04.466173 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.44070: Flags [P.], seq 942849:943093, ack 28372, win 2489,
 options [nop,nop,TS val 1528828967 ecr 1241159344], length 244
09:58:04.466234 IP B-192.168.20.99.net-192.168.20.0.44070 > A-10.8.0.99.net-10.8.0.0.ssh: Flags [.], ack 943093, win 11394, options [nop,nop,
TS val 1241159402 ecr 1528828967], length 0
09:58:04.470226 IP B-192.168.20.99.net-192.168.20.0.44070 > A-10.8.0.99.net-10.8.0.0.ssh: Flags [P.], seq 28372:28448, ack 943093, win 11394,
 options [nop,nop,TS val 1241159406 ecr 1528828967], length 76
09:58:04.470267 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.44070: Flags [.], ack 28448, win 2489, options [nop,nop,TS
 val 1528828971 ecr 1241159406], length 0
09:58:04.503987 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.44070: Flags [P.], seq 943093:943337, ack 28448, win 2489,
 options [nop,nop,TS val 1528829005 ecr 1241159406], length 244
09:58:04.504897 IP B-192.168.20.99.net-192.168.20.0.44070 > A-10.8.0.99.net-10.8.0.0.ssh: Flags [P.], seq 28448:28524, ack 943337, win 11394,
 options [nop,nop,TS val 1241159441 ecr 1528829005], length 76
09:58:04.504916 IP A-10.8.0.99.net-10.8.0.0.ssh > B-192.168.20.99.net-192.168.20.0.44070: Flags [.], ack 28524, win 2489, options [nop,nop,TS
 val 1528829006 ecr 1241159441], length 0
^Z
[2]+  Stopped                 tcpdump
CS280_FIREWALL :/#
```

We see the tunneling from HostB in the internal network to HostA in the external network. After the tunneling, Host B is able to connect to the web server (google.com) in our case. The resultant output is redirected back to A which is then redirected back to HostB with the ACK. The ACK packets we see above are directed from B to A.

googlee.com screen is not shown as it is considered moot when compared to the data revealed by tcpdump. It is of belief that those reviewing the document will not consider this a cause for penalization.

The SSH connection that is established between the two hosts must be removed. In order to do so, the following cleanup commands are used to remove all existing SSH connections that exist b/w the two systems.

```
S280_B :/# ps -eaf | grep "ssh"
oot          41       1  0 08:56 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
oot         148       1  0 09:31 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
oot         151       1  0 09:37 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
oot         153       1  0 09:37 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
```

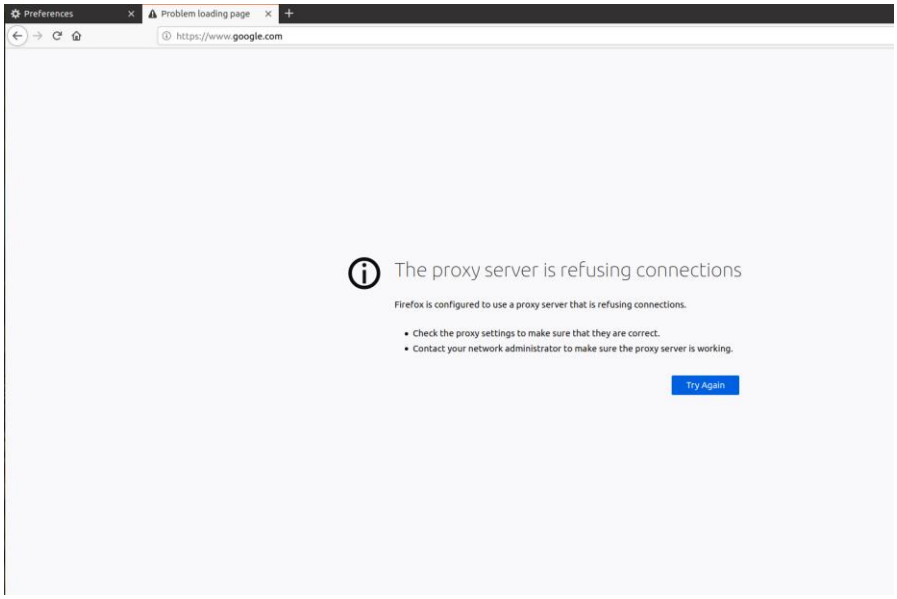
```
CS280_B :/# kill 148
CS280_B :/# ps -eaf | grep "ssh"
root          41       1  0 08:56 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root         148       1  0 09:31 ?        00:00:00 [ssh] <defunct>
root         151       1  0 09:37 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root         153       1  0 09:37 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
```

```
CS280_B :/# kill 151
CS280_B :/# kill 153
CS280_B :/# kill 158
CS280_B :/# ps -eaf | grep "ssh"
root          41       1  0 08:56 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root         148       1  0 09:31 ?        00:00:00 [ssh] <defunct>
root         151       1  0 09:37 ?        00:00:00 [ssh] <defunct>
root         153       1  0 09:37 ?        00:00:00 [ssh] <defunct>
```

Once the kill command is completed, the SSH connection is closed. Now when the user tries to access google.com from the internal network, the follwing output is displayed on the browser-

COMPUTER NETWORK SECURITY -08

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section



The proxy is closed i.e the SSH connection is terminated and therefore, there is no tunneling across the router/firewall. Therefore, no output is observed on tcpdump (no traffic).

```
CS280_FIREWALL :/# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^Z
[3]+  Stopped                 tcpdump
CS280_FIREWALL :/#
```

Task 2.3: Writing a SOCKS Client Using Python

An SSH tunnel/connection is restablished again. The same command used earlier is used to establish such a connection between the two hosts.

```
CS280_B :/# 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:n1b+aWRCO80F7lOi9dLj1tmdnSCCkYPm2TIg7SCqGoc.
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:
CS280_B :/#
```

The first python file B-Socks-Client.py is used to first create a proxy and specify the hostname and the portnumber to which the packets must route to. It also states the HTTP action (GET,POST etc.) to be taken during the HTTP request. Details of what should be done of the response generated (stored in the buffer) is also mentioned in this file.

COMPUTER NETWORK SECURITY -08

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

When executed on B, the response obtained (HTTP OK and headers followed by the page itself) is dispayed on the screen. The SSH tunnel from B to A is used for the same.

```
CS280_B :/# python3 B-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Age: 81852', b'Cache-Control: max-age=604800', b'Content-Type: text/html; charset=UTF-8', b'Date: Sat, 05 Nov 2022 09:
51:41 GMT', b'Etag: "3147526947+ident"', b'Expires: Sat, 12 Nov 2022 09:51:41 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b'Server
: ECS (oxr/8315)', 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=ut
f-8" />\n    <meta name="viewport" content="width=device-width, initial-scale=1" />\n    <style type="text/css">\n    body {\n        backgro
und-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        d
iv {\n            margin: 0 auto;\n            width: auto;\n        }\n    }\n    </style>    \n</head>\n\n<body>\n<div>\n    <h1>Example Do
main</h1>\n    <p>This domain is for use in illustrative examples in documents. You may use this\n    domain in literature without prior coor
dination or asking for permission.</p>\n    <p><a href="https://www.iana.org/domains/example">More information...</a></p>\n</div>\n</body>\n<
```

The same python program holds true for B1-B2-Socks-Client.py. The only exception is that the proxy detail is mentioned as B here, so that B1 and B2 can connect to B and in turn to A (and eventually the website).

The two python files in turn send HTTP Request packets to example.com from hosts on the internal network and the resultant responses are displayed on screen.

Output on B1

```
CS280_B1 :/# python3 B1-B2-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Age: 341789', b'Cache-Control: max-age=604800', b'Content-Type: text/html; charset=UTF-8', b'Date: Sat, 05 Nov 2022 09
:52:05 GMT', b'Etag: "3147526947+ident"', b'Expires: Sat, 12 Nov 2022 09:52:05 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b'Serve
r: ECS (oxr/831A)', 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=u
tf-8" />\n    <meta name="viewport" content="width=device-width, initial-scale=1" />\n    <style type="text/css">\n    body {\n        backgr
ound-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\n<body>\n<div>\n    <h1>Example D
omain</h1>\n    <p>This domain is for use in illustrative examples in documents. You may use this\n    domain in literature without prior coo
rdination or asking for permission.</p>\n    <p><a href="https://www.iana.org/domains/example">More information...</a></p>\n</div>\n</body>\n
</html>\n']
```

Output on B2:

```
CS280_B2 :/# python3 B1-B2-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Age: 405964', b'Cache-Control: max-age=604800', b'Content-Type: text/html; charset=UTF-8', b'Date: Sat, 05 Nov 2022 09
:52:20 GMT', b'Etag: "3147526947+ident"', b'Expires: Sat, 12 Nov 2022 09:52:20 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b'Serve
r: ECS (oxr/8310)', 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=u
tf-8" />\n    <meta name="viewport" content="width=device-width, initial-scale=1" />\n    <style type="text/css">\n    body {\n        backgr
ound-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\n<body>\n<div>\n    <h1>Example D
omain</h1>\n    <p>This domain is for use in illustrative examples in documents. You may use this\n    domain in literature without prior coo
rdination or asking for permission.</p>\n    <p><a href="https://www.iana.org/domains/example">More information...</a></p>\n</div>\n</body>\n
</html>\n']
```

The SSH connection that is established between the two hosts must be removed. In order to do so, the following cleanup commands are used to remove all existing SSH connections that exist b/w the two systems.

COMPUTER NETWORK SECURITY -08

Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section

```
S280_B :/# ps -eaf | grep "ssh"
oot          41       1  0 08:56 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
oot         148       1  0 09:31 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
oot         151       1  0 09:37 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
oot         153       1  0 09:37 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
```

```
CS280_B :/# kill 148
CS280_B :/# ps -eaf | grep "ssh"
root          41       1  0 08:56 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root         148       1  0 09:31 ?        00:00:00 [ssh] <defunct>
root         151       1  0 09:37 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root         153       1  0 09:37 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
```

```
CS280_B :/# kill 151
CS280_B :/# kill 153
CS280_B :/# kill 158
CS280_B :/# ps -eaf | grep "ssh"
root          41       1  0 08:56 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root         148       1  0 09:31 ?        00:00:00 [ssh] <defunct>
root         151       1  0 09:37 ?        00:00:00 [ssh] <defunct>
root         153       1  0 09:37 ?        00:00:00 [ssh] <defunct>
```

Task3: SOCKS5PROXY VS VPN

SOCKS5 PROXY	VPN
1. SOCK5 uses the SSH protocol to create a tunnel b/w the user and the server. There is no additional encryption added like in VPN, thereby making this more susceptible to attack if the attacker gains access to the server details. 2. These are relatively faster as there is no added burden of encryption (less security, but higher speed). 3. Proxy servers hold log information of the user. If attackers are able to access this information, then user privacy is compromised. Adding malware and viruses is easier in proxy servers. 4. SOCK5 Proxy allows for location spoofing i.e the users can fake their location i.e masquerade their IP address. 5. SOCK5 transfers small data packets and is therefore well suited for P2P environments. 6. SOCK5 proxy is application specific – one needs to ensure that all the relevant servers have the same SOCKS	1. A secure tunnel is created between the host/user and the private server – one that hackers,the ISP cannot snoop into. All packets that are exchanged b/w the user and the VPN are encypted. 2. VPNS are relatively slower as several encryption decryption schemes have to be implemented at different endpoints of the tunnel. 3. VPN is a better option to choose when getting past firewalls. If the agenda is to protect one's online presence regardless of their online activity, then VPNs are better suited. 4. VPNS provide for more stable connections. A VPN hides the user's IP address by connecting the user to an encypted, private server. 5. Preferred for use when foreign content across the world needs to be used, 6. VPN masks and encrypts all kinds of traffic.

server defined to obtain consistent results. 7. Proxy providers will give you the necessary input information for your browser, like the IP address name and port number. Once you enter the information into the system, you will connect to the proxy and browse anonymously. 8. Used in applications where more bandwidth is required.	7. A user must download the VPN software and create an account before accessing VPN services.