Harsh Parihar - 111801015

Lab2

(a) Connect to host h1. Ensure that you are able to ping x.virtnet.com for all h ∈ {h2, h3, h4, h5}. Send 5 ping packets to each of these hosts and report the respective average round-trip time.

Setting up the virtual network.

```
harsh@harsh-Vostro-3578:~/Downloads/lab2_network$ ./setupVMs.sh
Copying VM configuration...
harsh@harsh-Vostro-3578:~/Downloads/lab2_network$ ./startVMs.sh
Starting the VMs...
Waiting for VM "r1" to power on...
VM "r1" has been successfully started.
Waiting for VM "r2" to power on...
VM "r2" has been successfully started.
Waiting for VM "r3" to power on...
VM "r3" has been successfully started.
Waiting for VM "h5" to power on...
VM "h5" has been successfully started.
Waiting for VM "h1" to power on...
VM "h1" has been successfully started.
Waiting for VM "h2" to power on...
VM "h2" has been successfully started.
Waiting for VM "h3" to power on...
VM "h3" has been successfully started.
Waiting for VM "h4" to power on...
VM "h4" has been successfully started.
harsh@harsh-Vostro-3578:~/Downloads/lab2_network$ ./connect.sh h1
spawn ssh -p 14501 -o StrictHostKeyChecking=no tc@localhost
tc@localhost's password:
   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

tc@h1:~$ ping h2.virtnet.com
```

Pinging h2:

```
tc@h1:~$ ping -c 5 h2.virtnet.com
PING h2.virtnet.com (192.168.1.3): 56 data bytes
64 bytes from 192.168.1.3: seq=0 ttl=64 time=1.457 ms
64 bytes from 192.168.1.3: seq=1 ttl=64 time=1.424 ms
64 bytes from 192.168.1.3: seq=2 ttl=64 time=1.419 ms
64 bytes from 192.168.1.3: seq=3 ttl=64 time=1.557 ms
64 bytes from 192.168.1.3: seq=4 ttl=64 time=1.464 ms

--- h2.virtnet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.419/1.464/1.557 ms
tc@h1:~$
```

Avg time= 1.464 ms

Pinging h3:

```
tc@h1:~$ ping -c 5 h3.virtnet.com
PING h3.virtnet.com (192.168.2.2): 56 data bytes
64 bytes from 192.168.2.2: seq=0 ttl=62 time=6.504 ms
64 bytes from 192.168.2.2: seq=1 ttl=62 time=3.116 ms
64 bytes from 192.168.2.2: seq=2 ttl=62 time=3.516 ms
64 bytes from 192.168.2.2: seq=3 ttl=62 time=3.212 ms
64 bytes from 192.168.2.2: seq=4 ttl=62 time=2.972 ms

--- h3.virtnet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.972/3.864/6.504 ms
tc@h1:~$
```

Avg time= 3.864 ms

Pinging h4:

```
tc@h1:~$ ping -c 5 h4.virtnet.com
PING h4.virtnet.com (192.168.2.3): 56 data bytes
64 bytes from 192.168.2.3: seq=0 ttl=62 time=3.262 ms
64 bytes from 192.168.2.3: seq=1 ttl=62 time=3.109 ms
64 bytes from 192.168.2.3: seq=2 ttl=62 time=2.990 ms
64 bytes from 192.168.2.3: seq=3 ttl=62 time=2.840 ms
64 bytes from 192.168.2.3: seq=4 ttl=62 time=2.970 ms

--- h4.virtnet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.840/3.034/3.262 ms
tc@h1:~$
```

Avg time= 3.034 ms

Pinging h5:

```
tc@h1:~$ ping -c 5 h5.virtnet.com
PING h5.virtnet.com (192.168.3.2): 56 data bytes
64 bytes from 192.168.3.2: seq=0 ttl=62 time=2.956 ms
64 bytes from 192.168.3.2: seq=1 ttl=62 time=3.022 ms
64 bytes from 192.168.3.2: seq=2 ttl=62 time=2.714 ms
64 bytes from 192.168.3.2: seq=3 ttl=62 time=2.414 ms
64 bytes from 192.168.3.2: seq=4 ttl=62 time=3.093 ms

--- h5.virtnet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.414/2.839/3.093 ms
tc@h1:~$
```

Avg time= 2.839 ms

(b) Host A is running a FTP server, whereas Host B is simultaneously running two HTTP servers on port numbers in the range 8000 to 9000. Identify hosts A and B. What are the incoming ports of the HTTP servers on host B?

By running host [domain_name] I got IP address of each of the virtual machines, then using nmap on each of IP address gives the services they are listening on.

```
tc@h1:~$ host h2.virtnet.com
h2.virtnet.com has address 192.168.1.3
tc@h1:~$
tc@h1:~$ nmap 192.168.1.3

Starting Nmap 6.40 ( http://nmap.org ) at 2021-09-02 07:32 UTC
Nmap scan report for h2.virtnet.com (192.168.1.3)
Host is up (0.00078s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
tc@h1:~$
```

So h2 is listening on ftp server, hence host A is h2.

```
tc@h1:~$ nmap h3.virtnet.com -p 8000-9000

Starting Nmap 6.40 ( http://nmap.org ) at 2021-09-02 14:19 UTC
Nmap scan report for h3.virtnet.com (192.168.2.2)
Host is up (0.0015s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
8143/tcp open  unknown
8534/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
tc@h1:~$
```

Only h3 had two services running between specified ports, hence host B is h3. The port numbers are: 8143 and 8534.

(c) Let us call the HTTP servers running on host B as S1 and S2. On each of these servers there are two text files (within some directory). Download these files. Hint: directory listing is enabled on these servers. Each of these files contains one half of the password needed to log into the FTP server on host A. Write down this password.

```
tc@h1:~$ wget h3.virtnet.com:8143
Connecting to h3.virtnet.com:8143 (192.168.2.2:8143)
index.html           100% |*******************************************************************
tc@h1:~$
tc@h1:~$ cat index.html
Explore the folder t32 on this web server
tc@h1:~$
tc@h1:~$ wget h3.virtnet.com:8143/t32
Connecting to h3.virtnet.com:8143 (192.168.2.2:8143)
Connecting to h3.virtnet.com:8143 (192.168.2.2:8143)
t32                  100% |*******************************************************************
tc@h1:~$
tc@h1:~$ cat t32
<!DOCTYPE html>
<html>
<head>
<title>Index of /t32/</title>
<style type="text/css">
a, a:active {text-decoration: none; color: blue;}
a:visited {color: #48468F;}
a:hover, a:focus {text-decoration: underline; color: red;}
body {background-color: #F5F5F5;}
h2 {margin-bottom: 12px;}
table {margin-left: 12px;}
th, td { font: 90% monospace; text-align: left;}
th { font-weight: bold; padding-right: 14px; padding-bottom: 3px;}
td {padding-right: 14px;}
td.s, th.s {text-align: right;}
div.list { background-color: white; border-top: 1px solid #646464; border-bottom: 1px solid #6
div.foot { font: 90% monospace; color: #787878; padding-top: 4px;}
</style>
</head>
<body>
<h2>Index of /t32/</h2>
<div class="list">
<table summary="Directory Listing" cellpadding="0" cellspacing="0">
<thead><tr><th class="n">Name</th><th class="m">Last Modified</th><th class="s">Size</th><th c
```

In this file, there is a mention of key.txt file. Lets see can we download it.

```
tc@h1:~$ wget h3.virtnet.com:8143/t32/key.txt
Connecting to h3.virtnet.com:8143 (192.168.2.2:8143)
key.txt              100% |*******************************
tc@h1:~$ cat key.txt
The first half of the password is use
tc@h1:~$
```

Hence the first half of the pass word is use.
Similarly following the above process with another port gives the second half of the password as r@487. Hence the password is user@487.

(d) One of the HTTP server on host B runs HTTP/1.0 and the other runs HTTP/1.1. Match the port number of the servers to corresponding HTTP versions.

```
tc@h1:~$ wget -S h3.virtnet.com:8143
Connecting to h3.virtnet.com:8143 (192.168.2.2:8143)
  HTTP/1.0 200 OK
  Content-Type: text/html
  Accept-Ranges: bytes
  ETag: "3519008462"
  Last-Modified: Fri, 02 Aug 2019 08:14:13 GMT
  Content-Length: 42
  Connection: close
  Date: Thu, 02 Sep 2021 14:54:02 GMT
  Server: lighttpd/1.4.54

wget: can't open 'index.html': File exists
tc@h1:~$
tc@h1:~$
tc@h1:~$ wget -S h3.virtnet.com:8534
Connecting to h3.virtnet.com:8534 (192.168.2.2:8534)
  HTTP/1.1 200 OK
  Content-Type: text/html
  Accept-Ranges: bytes
  ETag: "3518972526"
  Last-Modified: Fri, 02 Aug 2019 08:15:26 GMT
  Content-Length: 42
  Connection: close
  Date: Thu, 02 Sep 2021 14:54:28 GMT
  Server: lighttpd/1.4.54

wget: can't open 'index.html': File exists
tc@h1:~$
```

Hence port 8143 runs on HTTP/1.0 and the other runs on HTTP/1.1.

(e) Using command lftp, FTP into host A using username "tc" and the password obtained in step (c). There is a file called "sol.txt" (within a directory) on this machine. Download it and look at its contents. This file contains the password for user "tc" on host h5. Write down this password.

```
tc@h1:~$
tc@h1:~$
tc@h1:~$ lftp h2.virtnet.com -u tc
Password:
lftp tc@h2.virtnet.com:~> cd msg
cd ok, cwd=/msg
lftp tc@h2.virtnet.com:/msg> get sol.txt
32 bytes transferred
lftp tc@h2.virtnet.com:/msg> cat sol.txt
The password for h5 is user@324
33 bytes transferred
lftp tc@h2.virtnet.com:/msg>
```

Hence the password is user@324.

f) SSH into host h5 using username "tc" and the password obtained in the previous step. There is file with the extension ".pcapng" in the home directory of user "tc". What is the name of this file?

```
tc@h1:~$
tc@h1:~$ ssh tc@h5.virtnet.com
The authenticity of host 'h5.virtnet.com (192.168.3.2)' can't
be established.
ECDSA key fingerprint is SHA256:UTHWKQ7ZOcnnXJFeX3JboQ4wSdRUA2
UGd1b01923oJo.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added 'h5.virtnet.com,192.168.3.2' (ECDSA
) to the list of known hosts.
tc@h5.virtnet.com's password:
   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

tc@h5:~$ ls
my_capture.pcapng
tc@h5:~$
```

Hence the name of the file is my_capture.

g) Download this file to your physical host machine (Hint: host h5 can be accessed via SSH on port 14505 on the loopback IP address of the physical host) and open it with wireshark.

```
harsh@harsh-Vostro-3578:~/Downloads/lab2_network$ scp -P 14505 tc@localhost:/home/tc/my_capture.pcapng /home/harsh/Desktop/
tc@localhost's password:
my_capture.pcapng
harsh@harsh-Vostro-3578:~/Downloads/lab2_network$ cd /home/harsh/Desktop/
harsh@harsh-Vostro-3578:~/Desktop$ ls
my_capture.pcapng
harsh@harsh-Vostro-3578:~/Desktop$
```