Computer Networks Final Project

Date: 2020-12-22

GitHub Repository: https://github.com/sell50/Network-Project

Group Members:

Abdul Arif

Ayokunle Olufemi Ayoola

Brett Robert Shepley

Katerina Pace

Required Work:

- Traceroute between one or more job seekers and any other node in the network and find the nearest job seeker(s) to the target node. **(COMPLETED)**
- Spy on your neighbours, the job creator could direct the job seekers to report the IP address and MAC address for every live host who shares the same LAN with the job seeker, the job creator should detect the job seekers that share the same LAN if any. **(COMPLETED)**
- Create a simple user-interface or config files to enable testing your project (including all the parts from the assignments and the new extension). **(COMPLETED)**
- If the job fails (e.g. the job seeker or creator crash), you should be able to resume from the crash point and not start/restart the entire job (Bonus 5%). **(COMPLETED)**

Deployment and Testing Instructions:

A demo video was also included in the GitHub Repo if any confusion arises

1. *Open Python Project in python ide (PyCharm)*
2. *Confirm all proper libraries have been installed*
3. *Run Server.py*
4. *Run Client.py*
5. *Run Client1.py* (Client1.py is a carbon copy of Client.py, used to simulate running a standalone .exe)
6. (Client.py) Enter “LOGIN Steven 123 JobCreator”
7. (Client.py) Enter “VIEWJOBS”
8. (Client.py) Enter “CREATEJOB Steven PortDetection 10 1.1.1.92 25565”
9. (Client.py) Enter “VIEWJOBS”
10. (Client1.py) Enter “LOGIN Brett 123 JobSeeker”
11. (Client1.py) Enter “VIEWJOBS”
12. (Client1.py) Enter “JOINJOB Steven PortDetection Brett”
13. (Client.py) Enter “STARTJOB Steven PortDetection”
14. (Client1.py) Enter “VIEWJOBS”
15. (Client1.py) Enter “COMPLETEJOB Steven PortDetection 1.1.1.92 25565”
16. *Check ClientOutput.txt for results*

Test Cases and Corresponding Output:

Figure 1.0: IP Detection

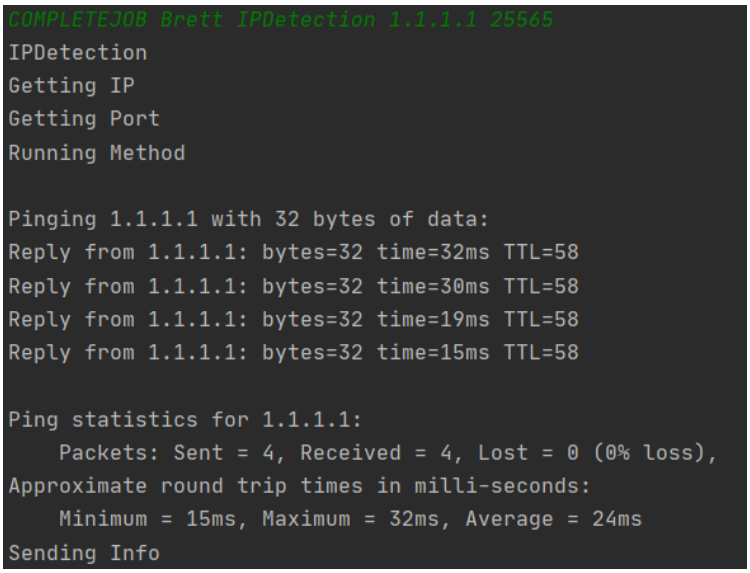

Figure 1.1: Port Detection

Figure 1.2: TCP Flood Attack

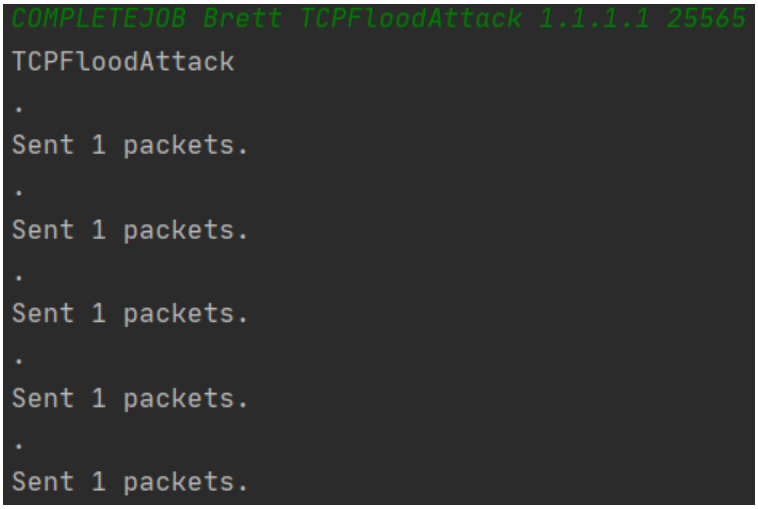

Figure 1.3: UDP Flood Attack

```
COMPLETEJOB Brett UDPFloodAttack 1.1.1.1 25565
UDPFloodAttack
Getting IP
Getting Port
Sending Info
Running Method
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

Figure 1.4: Node Location

```
COMPLETEJOB Brett NodeLocation 1.1.1.1 00
NodeLocation
Getting IP
Getting Port
Running Method
Find your IP Address at 'https://www.whatismyip.com/' Then Enter That Address
24.57.4.177
Sending Info
```

Figure 1.5: Node LAN Scan

```
COMPLETEJOB Brett NodeLANScan 00 00
NodeLANScan
IP Address: 192.168.86.1    MAC Address: ec:08:6b:ea:fc:e9
IP Address: 192.168.86.36   MAC Address: f8:94:c2:d1:57:86
IP Address: 192.168.86.25   MAC Address: d0:23:db:1f:27:8c
IP Address: 192.168.86.33   MAC Address: f6:6a:72:d8:dd:c5
IP Address: 192.168.86.37   MAC Address: 7c:b0:c2:b3:ad:f8
IP Address: 192.168.86.24   MAC Address: de:c8:03:7d:2c:5c
IP Address: 192.168.86.22   MAC Address: 04:e5:36:ca:9c:4c
IP Address: 192.168.86.47   MAC Address: d4:e6:b7:a5:93:d9
IP Address: 192.168.86.46   MAC Address: a6:5b:79:c1:d6:79
```

Figure 2.0: All Jobs Outputs

```
Target IP: 1.1.1.1 Online
Target IP Address: 1.1.1.1 Target Port: 25565:  Closed
Target IP: 1.1.1.1 Target Port: 25565 TCP Flood Attack
Target IP: 1.1.1.1 Target Port: 25565 UDP Flood Attack
Target IP: 1.1.1.1 Latitude: -33.8548157 Longitude: 151.2164539 Distance: 245.72545655670274
IP Address: 192.168.86.1    MAC Address: ec:08:6b:ea:fc:e9
IP Address: 192.168.86.36   MAC Address: f8:94:c2:d1:57:86
IP Address: 192.168.86.25   MAC Address: d0:23:db:1f:27:8c
IP Address: 192.168.86.33   MAC Address: f6:6a:72:d8:dd:c5
IP Address: 192.168.86.37   MAC Address: 7c:b0:c2:b3:ad:f8
IP Address: 192.168.86.24   MAC Address: de:c8:03:7d:2c:5c
IP Address: 192.168.86.22   MAC Address: 04:e5:36:ca:9c:4c
IP Address: 192.168.86.47   MAC Address: d4:e6:b7:a5:93:d9
IP Address: 192.168.86.46   MAC Address: a6:5b:79:c1:d6:79
```