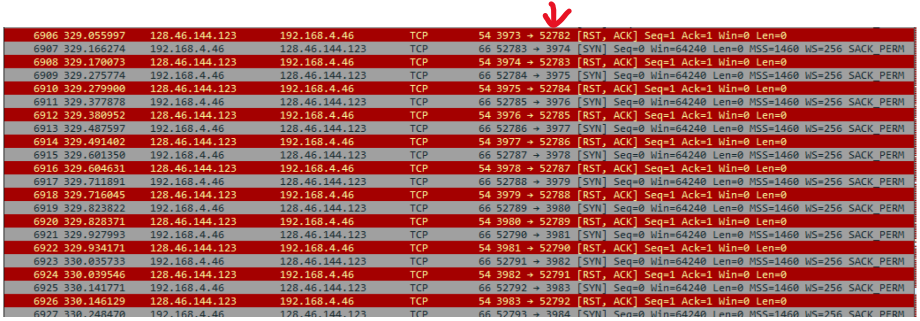
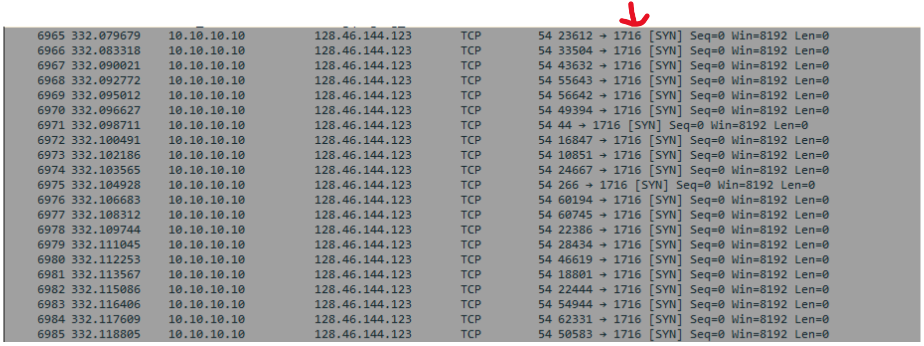
I have first put the spoofIP and targetIP in TcpAttack class in order to use in other functions, and then complete the scanTarget function according to Lecture 16 example code. In this function it scans all the port to see which port is open and the next function attackTarget is used to flood the port and I have also write function according to Lecture 16 code example, and return 1 if it perform a Dos attack.

Screenshot for port scanning:



```
6906 329.055997   128.46.144.123   192.168.4.46     TCP   54 3973 → 52782 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6907 329.166274   192.168.4.46     128.46.144.123   TCP   66 52783 → 3974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6908 329.170073   128.46.144.123   192.168.4.46     TCP   54 3974 → 52783 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6909 329.275774   192.168.4.46     128.46.144.123   TCP   66 52784 → 3975 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6910 329.279900   128.46.144.123   192.168.4.46     TCP   54 3975 → 52784 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6911 329.377878   192.168.4.46     128.46.144.123   TCP   66 52785 → 3976 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6912 329.380952   128.46.144.123   192.168.4.46     TCP   54 3976 → 52785 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6913 329.487597   192.168.4.46     128.46.144.123   TCP   66 52786 → 3977 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6914 329.491402   128.46.144.123   192.168.4.46     TCP   54 3977 → 52786 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6915 329.601350   192.168.4.46     128.46.144.123   TCP   66 52787 → 3978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6916 329.604631   128.46.144.123   192.168.4.46     TCP   54 3978 → 52787 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6917 329.711891   192.168.4.46     128.46.144.123   TCP   66 52788 → 3979 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6918 329.716045   128.46.144.123   192.168.4.46     TCP   54 3979 → 52788 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6919 329.823822   192.168.4.46     128.46.144.123   TCP   66 52789 → 3980 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6920 329.828371   128.46.144.123   192.168.4.46     TCP   54 3980 → 52789 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6921 329.927993   192.168.4.46     128.46.144.123   TCP   66 52790 → 3981 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6922 329.934171   128.46.144.123   192.168.4.46     TCP   54 3981 → 52790 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6923 330.035733   192.168.4.46     128.46.144.123   TCP   66 52791 → 3982 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6924 330.039546   128.46.144.123   192.168.4.46     TCP   54 3982 → 52791 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6925 330.141771   192.168.4.46     128.46.144.123   TCP   66 52792 → 3983 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6926 330.146129   128.46.144.123   192.168.4.46     TCP   54 3983 → 52792 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6927 330.248470   192.168.4.46     128.46.144.123   TCP   66 52793 → 3984 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
```

Sreenshot for SYN flood attack on port 1716



```
6965 332.079679   10.10.10.10     128.46.144.123   TCP   54 23612 → 1716 [SYN] Seq=0 Win=8192 Len=0
6966 332.083318   10.10.10.10     128.46.144.123   TCP   54 33504 → 1716 [SYN] Seq=0 Win=8192 Len=0
6967 332.090021   10.10.10.10     128.46.144.123   TCP   54 43632 → 1716 [SYN] Seq=0 Win=8192 Len=0
6968 332.092772   10.10.10.10     128.46.144.123   TCP   54 55643 → 1716 [SYN] Seq=0 Win=8192 Len=0
6969 332.095012   10.10.10.10     128.46.144.123   TCP   54 56642 → 1716 [SYN] Seq=0 Win=8192 Len=0
6970 332.096627   10.10.10.10     128.46.144.123   TCP   54 49394 → 1716 [SYN] Seq=0 Win=8192 Len=0
6971 332.098711   10.10.10.10     128.46.144.123   TCP   54 44 → 1716 [SYN] Seq=0 Win=8192 Len=0
6972 332.100491   10.10.10.10     128.46.144.123   TCP   54 16847 → 1716 [SYN] Seq=0 Win=8192 Len=0
6973 332.102186   10.10.10.10     128.46.144.123   TCP   54 10851 → 1716 [SYN] Seq=0 Win=8192 Len=0
6974 332.103565   10.10.10.10     128.46.144.123   TCP   54 24667 → 1716 [SYN] Seq=0 Win=8192 Len=0
6975 332.104928   10.10.10.10     128.46.144.123   TCP   54 266 → 1716 [SYN] Seq=0 Win=8192 Len=0
6976 332.106683   10.10.10.10     128.46.144.123   TCP   54 60194 → 1716 [SYN] Seq=0 Win=8192 Len=0
6977 332.108312   10.10.10.10     128.46.144.123   TCP   54 60745 → 1716 [SYN] Seq=0 Win=8192 Len=0
6978 332.109744   10.10.10.10     128.46.144.123   TCP   54 22386 → 1716 [SYN] Seq=0 Win=8192 Len=0
6979 332.111045   10.10.10.10     128.46.144.123   TCP   54 28434 → 1716 [SYN] Seq=0 Win=8192 Len=0
6980 332.112253   10.10.10.10     128.46.144.123   TCP   54 46619 → 1716 [SYN] Seq=0 Win=8192 Len=0
6981 332.113567   10.10.10.10     128.46.144.123   TCP   54 18801 → 1716 [SYN] Seq=0 Win=8192 Len=0
6982 332.115086   10.10.10.10     128.46.144.123   TCP   54 22444 → 1716 [SYN] Seq=0 Win=8192 Len=0
6983 332.116406   10.10.10.10     128.46.144.123   TCP   54 54944 → 1716 [SYN] Seq=0 Win=8192 Len=0
6984 332.117609   10.10.10.10     128.46.144.123   TCP   54 62331 → 1716 [SYN] Seq=0 Win=8192 Len=0
6985 332.118805   10.10.10.10     128.46.144.123   TCP   54 50583 → 1716 [SYN] Seq=0 Win=8192 Len=0
```