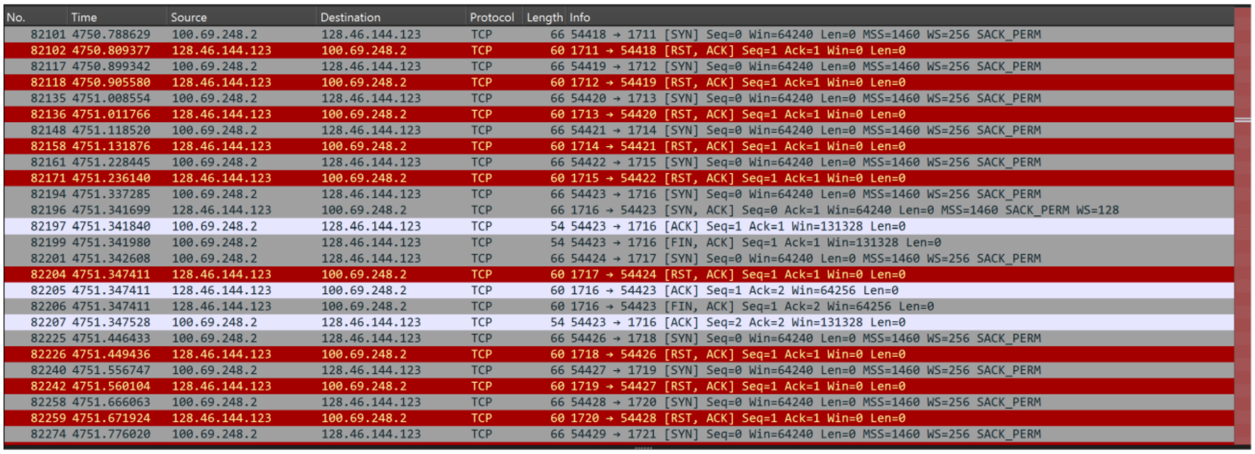
Homework Number: 8

Name: Andrew Wu

ECN Login: wu1795

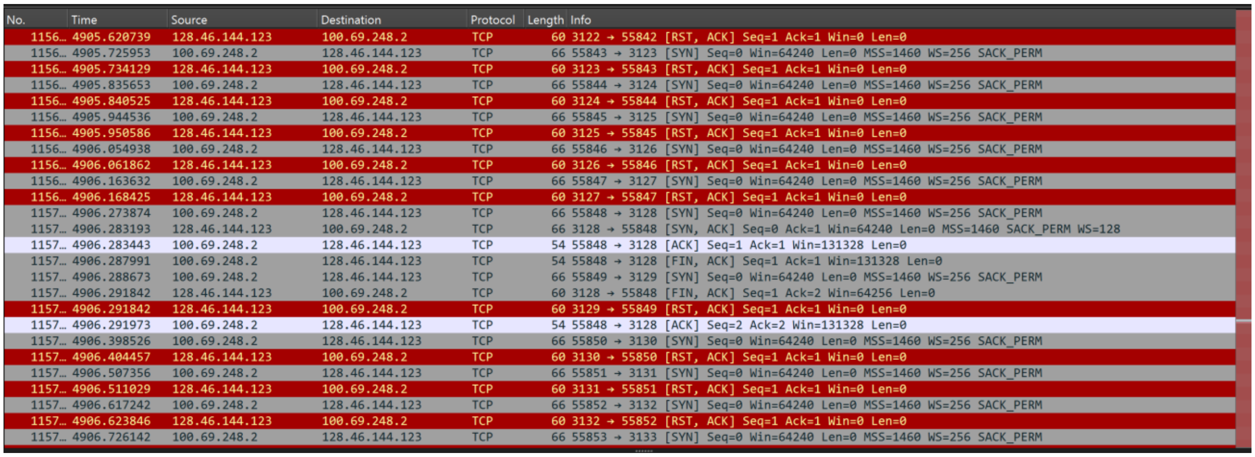
Due Date: 3/21/24



No.	Time	Source	Destination	Protocol	Length	Info
82101	4750.788629	100.69.248.2	128.46.144.123	TCP	66	54418 → 1711 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
82102	4750.809377	128.46.144.123	100.69.248.2	TCP	60	1711 → 54418 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82117	4750.899342	100.69.248.2	128.46.144.123	TCP	66	54419 → 1712 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
82118	4750.905580	128.46.144.123	100.69.248.2	TCP	60	1712 → 54419 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82135	4751.008554	100.69.248.2	128.46.144.123	TCP	66	54420 → 1713 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
82136	4751.011766	128.46.144.123	100.69.248.2	TCP	60	1713 → 54420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82148	4751.118520	100.69.248.2	128.46.144.123	TCP	66	54421 → 1714 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
82158	4751.131876	128.46.144.123	100.69.248.2	TCP	60	1714 → 54421 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82161	4751.228445	100.69.248.2	128.46.144.123	TCP	66	54422 → 1715 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
82171	4751.236140	128.46.144.123	100.69.248.2	TCP	60	1715 → 54422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82194	4751.337285	100.69.248.2	128.46.144.123	TCP	66	54423 → 1716 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
82196	4751.341699	128.46.144.123	100.69.248.2	TCP	66	1716 → 54423 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
82197	4751.341840	100.69.248.2	128.46.144.123	TCP	54	54423 → 1716 [ACK] Seq=1 Ack=1 Win=131328 Len=0
82199	4751.341980	100.69.248.2	128.46.144.123	TCP	54	54423 → 1716 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
82201	4751.342608	100.69.248.2	128.46.144.123	TCP	66	54424 → 1717 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
82204	4751.347411	128.46.144.123	100.69.248.2	TCP	60	1717 → 54424 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82205	4751.347411	128.46.144.123	100.69.248.2	TCP	60	1716 → 54423 [ACK] Seq=1 Ack=2 Win=64256 Len=0
82206	4751.347411	128.46.144.123	100.69.248.2	TCP	60	1716 → 54423 [FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0
82207	4751.347528	100.69.248.2	128.46.144.123	TCP	54	54423 → 1716 [ACK] Seq=2 Ack=2 Win=131328 Len=0
82225	4751.446433	100.69.248.2	128.46.144.123	TCP	66	54426 → 1718 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
82226	4751.449436	128.46.144.123	100.69.248.2	TCP	60	1718 → 54426 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82240	4751.556747	100.69.248.2	128.46.144.123	TCP	66	54427 → 1719 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
82242	4751.560104	128.46.144.123	100.69.248.2	TCP	60	1719 → 54427 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82258	4751.666063	100.69.248.2	128.46.144.123	TCP	66	54428 → 1720 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
82259	4751.671924	128.46.144.123	100.69.248.2	TCP	60	1720 → 54428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82274	4751.776020	100.69.248.2	128.46.144.123	TCP	66	54429 → 1721 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Figure 1: Snapshot of port 1716 communication and the 100 syn packets flooding the port

The block of grey in the middle of the snapshot that is highlighted is the communication between my computer and port 1716 of the moonshine network.



No.	Time	Source	Destination	Protocol	Length	Info
1156…	4905.620739	128.46.144.123	100.69.248.2	TCP	60	3122 → 55842 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1156…	4905.725953	100.69.248.2	128.46.144.123	TCP	66	55843 → 3123 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1156…	4905.734129	128.46.144.123	100.69.248.2	TCP	60	3123 → 55843 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1156…	4905.835653	100.69.248.2	128.46.144.123	TCP	66	55844 → 3124 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1156…	4905.840525	128.46.144.123	100.69.248.2	TCP	60	3124 → 55844 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1156…	4905.944536	100.69.248.2	128.46.144.123	TCP	66	55845 → 3125 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1156…	4905.950586	128.46.144.123	100.69.248.2	TCP	60	3125 → 55845 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1156…	4906.054938	100.69.248.2	128.46.144.123	TCP	66	55846 → 3126 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1156…	4906.061862	128.46.144.123	100.69.248.2	TCP	60	3126 → 55846 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1156…	4906.163632	100.69.248.2	128.46.144.123	TCP	66	55847 → 3127 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1156…	4906.168425	128.46.144.123	100.69.248.2	TCP	60	3127 → 55847 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1157…	4906.273874	100.69.248.2	128.46.144.123	TCP	66	55848 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1157…	4906.283193	128.46.144.123	100.69.248.2	TCP	66	3128 → 55848 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
1157…	4906.283443	100.69.248.2	128.46.144.123	TCP	54	55848 → 3128 [ACK] Seq=1 Ack=1 Win=131328 Len=0
1157…	4906.287991	100.69.248.2	128.46.144.123	TCP	54	55848 → 3128 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
1157…	4906.288673	100.69.248.2	128.46.144.123	TCP	66	55849 → 3129 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1157…	4906.291842	128.46.144.123	100.69.248.2	TCP	60	3128 → 55848 [FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0
1157…	4906.291842	128.46.144.123	100.69.248.2	TCP	60	3129 → 55849 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1157…	4906.291973	100.69.248.2	128.46.144.123	TCP	54	55848 → 3128 [ACK] Seq=2 Ack=2 Win=131328 Len=0
1157…	4906.398526	100.69.248.2	128.46.144.123	TCP	66	55850 → 3130 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1157…	4906.404457	128.46.144.123	100.69.248.2	TCP	60	3130 → 55850 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1157…	4906.507356	100.69.248.2	128.46.144.123	TCP	66	55851 → 3131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1157…	4906.511029	128.46.144.123	100.69.248.2	TCP	60	3131 → 55851 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1157…	4906.617242	100.69.248.2	128.46.144.123	TCP	66	55852 → 3132 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1157…	4906.623846	128.46.144.123	100.69.248.2	TCP	60	3132 → 55852 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1157…	4906.726142	100.69.248.2	128.46.144.123	TCP	66	55853 → 3133 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Figure 2: Snapshot of port 3128 communication and the 100 syn packets flooding the port

The block of grey in the middle of the snapshot that is highlighted is the communication between my computer and port 3128 of the moonshine network.

In my code, for scanTarget, I first initialized a list to contain the port numbers referencing the ports that are open. I then test each port between the rangeStart and rangeEnd values, create a socket for each port to send packets through, and set the timeout for the socket to 0.1. I then try to connect to the port, if successful, add the port number to the open list. If unsuccessful, pass and continue onto the next port. To confirm which ports are open, I print the port numbers to the terminal if there are ports open, and “No open ports in specified range” if there are no open ports in the range. I then write the open ports to the output file. For attackTarget, I use scapy to create a IP header, TCP header, and a packet specified for the open port. From there, I send the packets to the open port, return 0 if there is an exception and 1 if there isn’t an exception and the DoS attack goes through.