ECE 404 Homework 8

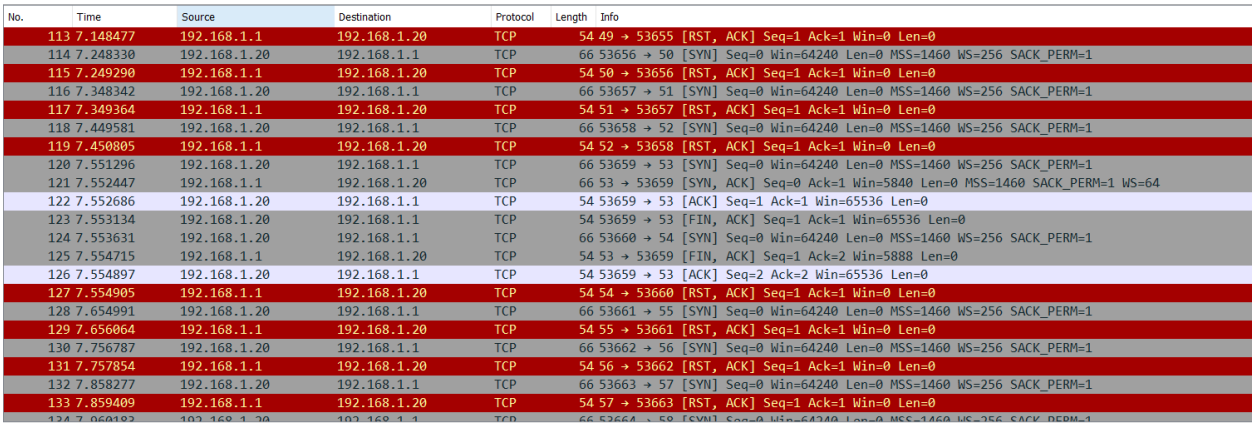
Elias Talcott

March 26, 2020

Contents

1 Port Scanning

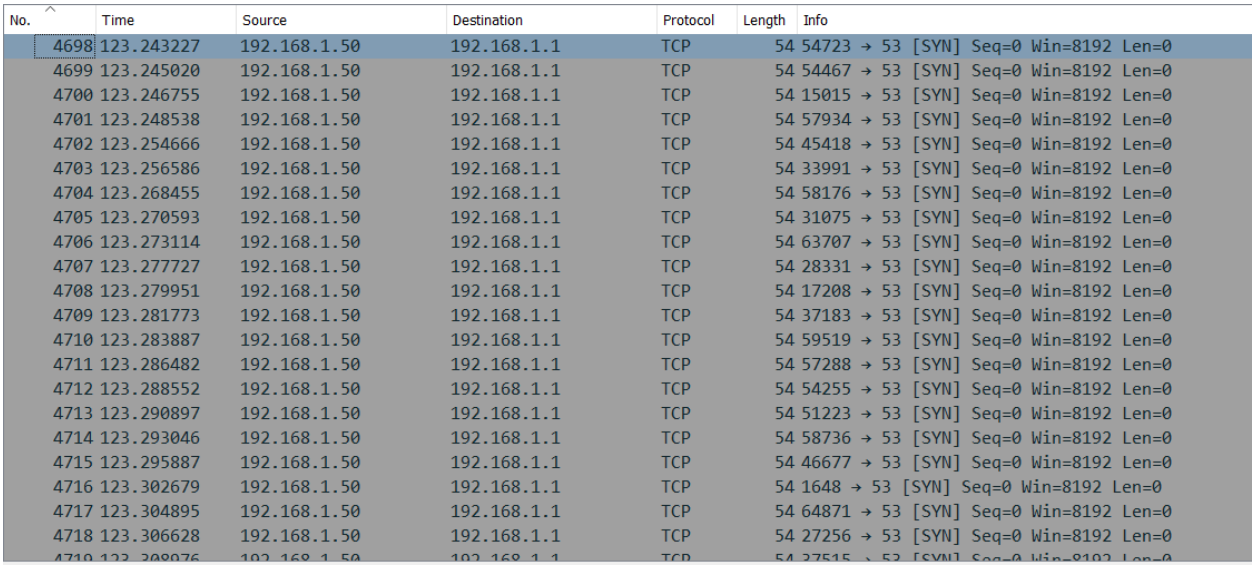
This image shows a portion of the result when port scanning was performed on IP address 192.168.1.1 using IP address 192.168.1.20. Most ports shown in this image are closed, but port 53 is detected to be open. The port scan from port 0 to port 1000 took approximately a minute and a half.



No.	Time	Source	Destination	Protocol	Length	Info
113	7.148477	192.168.1.1	192.168.1.20	TCP	54	49 → 53655 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
114	7.248330	192.168.1.20	192.168.1.1	TCP	66	53656 → 50 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
115	7.249290	192.168.1.1	192.168.1.20	TCP	54	50 → 53656 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116	7.348342	192.168.1.20	192.168.1.1	TCP	66	53657 → 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
117	7.349364	192.168.1.1	192.168.1.20	TCP	54	51 → 53657 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
118	7.449581	192.168.1.20	192.168.1.1	TCP	66	53658 → 52 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
119	7.450805	192.168.1.1	192.168.1.20	TCP	54	52 → 53658 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120	7.551296	192.168.1.20	192.168.1.1	TCP	66	53659 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
121	7.552447	192.168.1.1	192.168.1.20	TCP	66	53 → 53659 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=64
122	7.552686	192.168.1.20	192.168.1.1	TCP	54	53659 → 53 [ACK] Seq=1 Ack=1 Win=65536 Len=0
123	7.553134	192.168.1.20	192.168.1.1	TCP	54	53659 → 53 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0
124	7.553631	192.168.1.20	192.168.1.1	TCP	66	53660 → 54 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
125	7.554715	192.168.1.1	192.168.1.20	TCP	54	53 → 53659 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0
126	7.554897	192.168.1.20	192.168.1.1	TCP	54	53659 → 53 [ACK] Seq=2 Ack=2 Win=65536 Len=0
127	7.554905	192.168.1.1	192.168.1.20	TCP	54	54 → 53660 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128	7.654991	192.168.1.20	192.168.1.1	TCP	66	53661 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
129	7.656064	192.168.1.1	192.168.1.20	TCP	54	55 → 53661 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
130	7.756787	192.168.1.20	192.168.1.1	TCP	66	53662 → 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
131	7.757854	192.168.1.1	192.168.1.20	TCP	54	56 → 53662 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132	7.858277	192.168.1.20	192.168.1.1	TCP	66	53663 → 57 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
133	7.859409	192.168.1.1	192.168.1.20	TCP	54	57 → 53663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

2 SYN Flood Attack

This image shows a portion of the result of a SYN flood attack performed on IP address 192.168.1.1 using the spoof IP address 192.168.1.50. The source port is a randomly generated integer between 1024 and 65536 (non-"well-known" ports) and the destination port and number of SYN packets sent are as specified in the method call.



No.	Time	Source	Destination	Protocol	Length	Info
4698	123.243227	192.168.1.50	192.168.1.1	TCP	54	54723 → 53 [SYN] Seq=0 Win=8192 Len=0
4699	123.245020	192.168.1.50	192.168.1.1	TCP	54	54467 → 53 [SYN] Seq=0 Win=8192 Len=0
4700	123.246755	192.168.1.50	192.168.1.1	TCP	54	15015 → 53 [SYN] Seq=0 Win=8192 Len=0
4701	123.248538	192.168.1.50	192.168.1.1	TCP	54	57934 → 53 [SYN] Seq=0 Win=8192 Len=0
4702	123.254666	192.168.1.50	192.168.1.1	TCP	54	45418 → 53 [SYN] Seq=0 Win=8192 Len=0
4703	123.256586	192.168.1.50	192.168.1.1	TCP	54	33991 → 53 [SYN] Seq=0 Win=8192 Len=0
4704	123.268455	192.168.1.50	192.168.1.1	TCP	54	58176 → 53 [SYN] Seq=0 Win=8192 Len=0
4705	123.270593	192.168.1.50	192.168.1.1	TCP	54	31075 → 53 [SYN] Seq=0 Win=8192 Len=0
4706	123.273114	192.168.1.50	192.168.1.1	TCP	54	63707 → 53 [SYN] Seq=0 Win=8192 Len=0
4707	123.277727	192.168.1.50	192.168.1.1	TCP	54	28331 → 53 [SYN] Seq=0 Win=8192 Len=0
4708	123.279951	192.168.1.50	192.168.1.1	TCP	54	17208 → 53 [SYN] Seq=0 Win=8192 Len=0
4709	123.281773	192.168.1.50	192.168.1.1	TCP	54	37183 → 53 [SYN] Seq=0 Win=8192 Len=0
4710	123.283887	192.168.1.50	192.168.1.1	TCP	54	59519 → 53 [SYN] Seq=0 Win=8192 Len=0
4711	123.286482	192.168.1.50	192.168.1.1	TCP	54	57288 → 53 [SYN] Seq=0 Win=8192 Len=0
4712	123.288552	192.168.1.50	192.168.1.1	TCP	54	54255 → 53 [SYN] Seq=0 Win=8192 Len=0
4713	123.290897	192.168.1.50	192.168.1.1	TCP	54	51223 → 53 [SYN] Seq=0 Win=8192 Len=0
4714	123.293046	192.168.1.50	192.168.1.1	TCP	54	58736 → 53 [SYN] Seq=0 Win=8192 Len=0
4715	123.295887	192.168.1.50	192.168.1.1	TCP	54	46677 → 53 [SYN] Seq=0 Win=8192 Len=0
4716	123.302679	192.168.1.50	192.168.1.1	TCP	54	1648 → 53 [SYN] Seq=0 Win=8192 Len=0
4717	123.304895	192.168.1.50	192.168.1.1	TCP	54	64871 → 53 [SYN] Seq=0 Win=8192 Len=0
4718	123.306628	192.168.1.50	192.168.1.1	TCP	54	27256 → 53 [SYN] Seq=0 Win=8192 Len=0