

Ethan James
Epjames
33378430

HW08

The image shows a Wireshark packet capture of a SYN flood attack. The filter is 'ip.addr==128.46.144.123'. The packet list shows a continuous stream of SYN packets from various source IP addresses to the destination IP 128.46.144.123 on port 1716. The packet details pane shows the TCP header with the SYN flag set. The packet bytes pane shows the raw data of the SYN packet.

No.	Time	Source	Destination	Protocol	Length	Info
2600	147.324406	128.46.144.123	10.186.97.170	TCP	54	1709 → 62821 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2601	147.428942	10.186.97.170	128.46.144.123	TCP	66	62822 → 1710 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2602	147.441865	128.46.144.123	10.186.97.170	TCP	54	1710 → 62822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2603	147.538214	10.186.97.170	128.46.144.123	TCP	66	62823 → 1711 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2604	147.549662	128.46.144.123	10.186.97.170	TCP	54	1711 → 62823 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2605	147.649399	10.186.97.170	128.46.144.123	TCP	66	62824 → 1712 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2606	147.698252	128.46.144.123	10.186.97.170	TCP	54	1712 → 62824 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2607	147.759691	10.186.97.170	128.46.144.123	TCP	66	62825 → 1713 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2608	147.767735	128.46.144.123	10.186.97.170	TCP	54	1713 → 62825 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2613	147.869525	10.186.97.170	128.46.144.123	TCP	66	62826 → 1714 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2614	147.873535	128.46.144.123	10.186.97.170	TCP	54	1714 → 62826 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2616	147.981028	10.186.97.170	128.46.144.123	TCP	66	62827 → 1715 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2617	147.985992	128.46.144.123	10.186.97.170	TCP	54	1715 → 62827 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2619	148.093370	10.186.97.170	128.46.144.123	TCP	66	62828 → 1716 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2620	148.098146	128.46.144.123	10.186.97.170	TCP	66	1716 → 62828 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1250 SACK_PERM WS=128
2621	148.098397	10.186.97.170	128.46.144.123	TCP	54	62828 → 1716 [ACK] Seq=1 Ack=1 Win=131072 Len=0
2622	148.099122	10.186.97.170	128.46.144.123	TCP	54	62828 → 1716 [FIN, ACK] Seq=1 Ack=1 Win=131072 Len=0
2623	148.100302	10.186.97.170	128.46.144.123	TCP	66	62829 → 1717 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2624	148.104599	128.46.144.123	10.186.97.170	TCP	54	1716 → 62828 [FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0
2625	148.104599	128.46.144.123	10.186.97.170	TCP	54	1717 → 62829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2626	148.104721	10.186.97.170	128.46.144.123	TCP	54	62828 → 1716 [ACK] Seq=2 Ack=2 Win=131072 Len=0
2627	148.203250	10.186.97.170	128.46.144.123	TCP	66	62830 → 1718 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2628	148.217170	128.46.144.123	10.186.97.170	TCP	54	1718 → 62830 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2629	148.314253	10.186.97.170	128.46.144.123	TCP	66	62831 → 1719 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2630	148.322116	128.46.144.123	10.186.97.170	TCP	54	1719 → 62831 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Figure 1: Snapshot of port 1716 and the 100 syn packets flooding part
The block of gray is the open port with the attacks.

The image shows a Wireshark packet capture of a SYN flood attack. The filter is 'ip.addr==128.46.144.123'. The packet list shows a continuous stream of SYN packets from various source IP addresses to the destination IP 128.46.144.123 on port 3128. The packet details pane shows the TCP header with the SYN flag set. The packet bytes pane shows the raw data of the SYN packet.

No.	Time	Source	Destination	Protocol	Length	Info
7067	304.199086	128.46.144.123	10.186.97.170	TCP	54	3124 → 64273 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7068	304.276285	10.186.97.170	128.46.144.123	TCP	66	64274 → 3125 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7069	304.386397	10.186.97.170	128.46.144.123	TCP	66	64275 → 3126 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7070	304.401572	128.46.144.123	10.186.97.170	TCP	54	3125 → 64274 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7071	304.401572	128.46.144.123	10.186.97.170	TCP	54	3126 → 64275 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7072	304.496360	10.186.97.170	128.46.144.123	TCP	66	64276 → 3127 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7073	304.513212	128.46.144.123	10.186.97.170	TCP	54	3127 → 64276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7074	304.606467	10.186.97.170	128.46.144.123	TCP	66	64277 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7075	304.649380	128.46.144.123	10.186.97.170	TCP	66	3128 → 64277 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1250 SACK_PERM WS=128
7076	304.649590	10.186.97.170	128.46.144.123	TCP	54	64277 → 3128 [ACK] Seq=1 Ack=1 Win=131072 Len=0
7077	304.650154	10.186.97.170	128.46.144.123	TCP	54	64277 → 3128 [FIN, ACK] Seq=1 Ack=1 Win=131072 Len=0
7078	304.651174	10.186.97.170	128.46.144.123	TCP	66	64278 → 3129 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7079	304.730820	128.46.144.123	10.186.97.170	TCP	54	3129 → 64278 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7080	304.730820	128.46.144.123	10.186.97.170	TCP	54	3128 → 64277 [FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0
7081	304.730941	10.186.97.170	128.46.144.123	TCP	54	64277 → 3128 [ACK] Seq=2 Ack=2 Win=131072 Len=0
7082	304.764401	10.186.97.170	128.46.144.123	TCP	66	64279 → 3130 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7083	304.805403	128.46.144.123	10.186.97.170	TCP	54	3130 → 64279 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7084	304.874974	10.186.97.170	128.46.144.123	TCP	66	64280 → 3131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7085	304.940600	128.46.144.123	10.186.97.170	TCP	54	3131 → 64280 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7086	304.983896	10.186.97.170	128.46.144.123	TCP	66	64281 → 3132 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7087	305.000349	128.46.144.123	10.186.97.170	TCP	54	3132 → 64281 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7088	305.093538	10.186.97.170	128.46.144.123	TCP	66	64282 → 3133 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7089	305.138143	128.46.144.123	10.186.97.170	TCP	54	3133 → 64282 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7090	305.203642	10.186.97.170	128.46.144.123	TCP	66	64283 → 3134 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7091	305.266427	128.46.144.123	10.186.97.170	TCP	54	3134 → 64283 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Figure 2: Snapshot of port 3128 and the 100 syn packets flooding part
The block of gray is the open ports with the syn packets

In my code I first begin with scanning ports. This identifies the open ports which are 1716 and 3128 and outputs it to an output file. Basically I run through a range of ports and identify which ports are open and then I convert those values into a string and output to an output file

Then I go through the attack function. We first set the source and destination of the IP address. Then we create the TCP header and a random source port and we set the destination port. Then we send the packets and any possible exceptions are printed.