

Dhruv Aggarwal

227	30.723529	192.168.0.25	128.46.4.88	TCP	54	54747 → 80 [RST] Seq=1 Win=0 Len=0
228	30.723530	192.168.0.25	128.46.4.88	TCP	54	4799 → 80 [RST] Seq=1 Win=0 Len=0
229	30.723530	192.168.0.25	128.46.4.88	TCP	54	53900 → 80 [RST] Seq=1 Win=0 Len=0
230	30.723530	192.168.0.25	128.46.4.88	TCP	54	31050 → 80 [RST] Seq=1 Win=0 Len=0
231	30.723531	192.168.0.25	128.46.4.88	TCP	54	17127 → 80 [RST] Seq=1 Win=0 Len=0
232	30.723531	192.168.0.25	128.46.4.88	TCP	54	45195 → 80 [RST] Seq=1 Win=0 Len=0
233	30.843428	128.46.4.88	192.168.0.25	TCP	60	[TCP Retransmission] 80 → 59972 [SYN, ACK] Seq=
234	30.843507	192.168.0.25	128.46.4.88	TCP	54	59972 → 80 [RST] Seq=1 Win=0 Len=0
235	30.847795	128.46.4.88	192.168.0.25	TCP	60	[TCP Retransmission] 80 → 25374 [SYN, ACK] Seq=
236	30.847877	192.168.0.25	128.46.4.88	TCP	54	25374 → 80 [RST] Seq=1 Win=0 Len=0
237	30.923292	SamsungE_cc:0b:56	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.23
238	31.042143	128.46.4.88	192.168.0.25	TCP	60	[TCP Retransmission] 80 → 3440 [SYN, ACK] Seq=0
239	31.042215	192.168.0.25	128.46.4.88	TCP	54	3440 → 80 [RST] Seq=1 Win=0 Len=0
240	31.044929	128.46.4.88	192.168.0.25	TCP	60	[TCP Retransmission] 80 → 4125 [SYN, ACK] Seq=

The above shows my attack from my IP to my ECN IP. It shows the spike and shows the syn attack via the TCP. The dark red ones highlighted are the ones that attacked my ECN.

```
→ HW8 git:(master) cat openports.txt
```

This shows my openports.txt after running the command and the open port that I got is 22.

[illegible]

The above picture shows the way I ran the code and the print statement “port was open to be attacked”