Analysis of the Attack

Analysis of the Attack

- Analysis of the DoS attack
- Wireshark helps identify
  - Rapid SYNs originating from one location (source)
  - TCP issues (retransmissions, RSTs)
  - Flooding from one or multiple sources
- Wireshark capture
  - Review the capture to identify these issues

Analysis of the Attack

172.23.125.110	10.140.170.7	TCP	49162→135 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.23.125.110	10.140.170.7	TCP	49163→3048 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.23.125.110	64.12.109.91	TCP	[TCP Retransmission] 53956→443 [FIN, ACK] Seq=235 Ack=2 Win=65330 Len=
172.23.125.110	64.12.109.91	TCP	[TCP Retransmission] 53957→443 [FIN, ACK] Seq=203 Ack=2 Win=65330 Len=
172.23.125.110	64.12.109.91	TCP	[TCP Retransmission] 53958→443 [FIN, ACK] Seq=91 Ack=2 Win=65330 Len=0
172.23.125.110	209.244.0.4	ICMP	Destination unreachable (Port unreachable)

Questions?