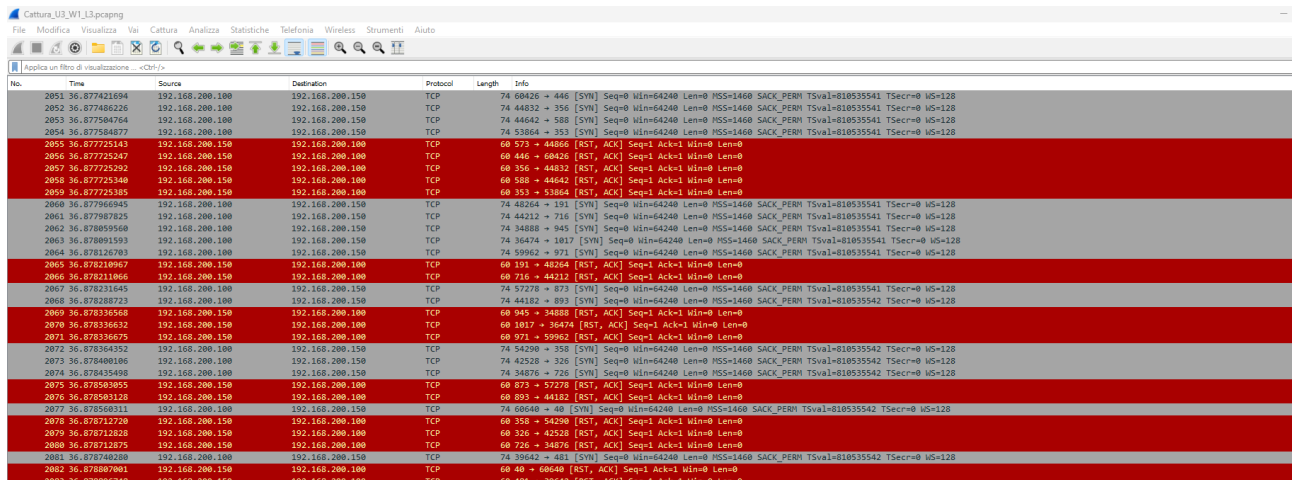


PRATICA S9L3

Consideriamo la cattura effettuata con wireshark relativa all'esercizio di oggi, in basso in figura vediamo parte di essa:



No.	Time	Source	Destination	Protocol	Length	Info
2051	36.877421694	192.168.200.100	192.168.200.150	TCP	74	60426 → 446 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2052	36.877480226	192.168.200.100	192.168.200.150	TCP	74	44832 → 358 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2053	36.877590764	192.168.200.100	192.168.200.150	TCP	74	44642 → 588 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2054	36.877594877	192.168.200.100	192.168.200.150	TCP	74	53864 → 353 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2055	36.877725143	192.168.200.150	192.168.200.100	TCP	60	573 → 44866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2056	36.877725247	192.168.200.150	192.168.200.100	TCP	60	446 → 60426 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2057	36.877725292	192.168.200.150	192.168.200.100	TCP	60	358 → 44832 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2058	36.877725340	192.168.200.150	192.168.200.100	TCP	60	588 → 44642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2059	36.877725385	192.168.200.150	192.168.200.100	TCP	60	353 → 53864 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2060	36.877960945	192.168.200.150	192.168.200.100	TCP	74	48264 → 191 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2061	36.877987825	192.168.200.100	192.168.200.150	TCP	74	44212 → 716 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2062	36.878059560	192.168.200.100	192.168.200.150	TCP	74	34888 → 945 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2063	36.878091593	192.168.200.100	192.168.200.150	TCP	74	36474 → 1017 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2064	36.878126781	192.168.200.100	192.168.200.150	TCP	74	59962 → 971 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2065	36.878221092	192.168.200.150	192.168.200.100	TCP	60	812 → 40264 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2066	36.878211866	192.168.200.150	192.168.200.100	TCP	60	716 → 44212 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2067	36.878231645	192.168.200.100	192.168.200.150	TCP	74	57278 → 873 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2068	36.878280723	192.168.200.150	192.168.200.100	TCP	74	44182 → 893 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535542 TSecr=0 WS=128
2069	36.878335542	192.168.200.150	192.168.200.100	TCP	60	945 → 34888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2070	36.878356632	192.168.200.150	192.168.200.100	TCP	60	1017 → 36474 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2071	36.878366675	192.168.200.150	192.168.200.100	TCP	60	971 → 59962 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2072	36.878364352	192.168.200.100	192.168.200.150	TCP	74	54290 → 358 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535542 TSecr=0 WS=128
2073	36.878400106	192.168.200.100	192.168.200.150	TCP	74	42528 → 326 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535542 TSecr=0 WS=128
2074	36.878435498	192.168.200.100	192.168.200.150	TCP	74	34876 → 726 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535542 TSecr=0 WS=128
2075	36.878503055	192.168.200.150	192.168.200.100	TCP	60	873 → 57278 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2076	36.878581128	192.168.200.150	192.168.200.100	TCP	60	893 → 44182 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2077	36.878595311	192.168.200.150	192.168.200.100	TCP	74	60440 → 40 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535542 TSecr=0 WS=128
2078	36.878712720	192.168.200.150	192.168.200.100	TCP	60	358 → 54290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2079	36.878712828	192.168.200.150	192.168.200.100	TCP	60	326 → 42528 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2080	36.878712875	192.168.200.150	192.168.200.100	TCP	60	726 → 34876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2081	36.878740200	192.168.200.100	192.168.200.150	TCP	74	39542 → 421 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535542 TSecr=0 WS=128
2082	36.878887081	192.168.200.150	192.168.200.100	TCP	60	40 → 60640 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2083	36.878887248	192.168.200.150	192.168.200.100	TCP	60	401 → 39542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

La comunicazione è fra due host con ip 192.168.200.100 e 192.168.200.150

In base ai dati raccolti dalla cattura si può concludere che l'host .100 stia effettuando una scansione (ad esempio con nmap) per enumerare i servizi attivi sull'host .150

Possiamo arrivare a questa conclusione vedendo come il primo host invii tante richieste SYN su porte sempre diverse (in rosso vediamo invece le risposte del secondo host)

Oltre a recuperare informazioni che potrebbero essere utili al primo host per lanciare un attacco sul secondo, questo tipo di traffico potrebbe anche impedire il corretto funzionamento dell'host 2 in quanto potrebbe congestionare il traffico verso tale macchina da parte di altri utenti legittimi.

Un buon modo per reagire in questo caso sarebbe bloccare l'ip 192.168.200.100 sull'IPS o sul Firewall (in una situazione aziendale) una volta rilevato il comportamento anomalo. Per evitare casi simili in futuro sarebbe una buona idea permettere le richieste sulle porte in ascolto della macchina .150 solo da utenti o ip autorizzati, e negare eventuali altre richieste su altre porte, configurando il firewall o l'ips di conseguenza.