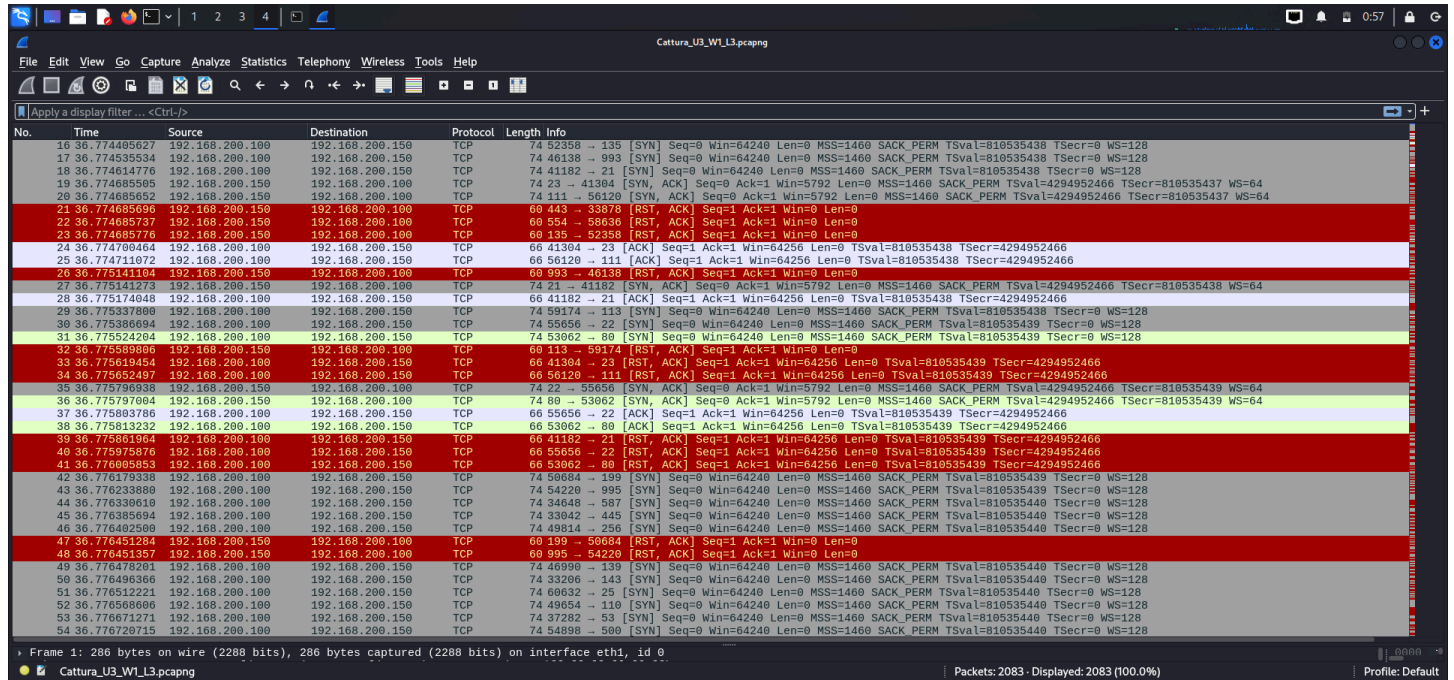


# Gestione degli IOC

Gli **IOC** (Indicators of Compromise) sono appunto degli indicatori di compromissione che evidenziano la presenza di un'attività malevola in un sistema o in una rete.

Possono contenere diversi tipi di dati, come **indirizzi IP** sospetti, **hash** di file malevoli, **URL** per phishing, **pattern** di traffico malevolo, firme di **malware**.

Nel nostro caso andremo ad analizzare i **pattern di traffico malevolo**, catturato da **Wireshark**.



No.	Time	Source	Destination	Protocol	Length	Info
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774503534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	36.774685595	192.168.200.150	192.168.200.100	TCP	74	23 → 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
21	36.774685690	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774709464	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141272	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174948	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775378808	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775539309	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775797084	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37	36.775803786	192.168.200.100	192.168.200.150	TCP	60	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36.776131333	192.168.200.100	192.168.200.150	TCP	74	50684 → 193 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44	36.776330619	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33842 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46	36.776402509	192.168.200.100	192.168.200.150	TCP	74	48914 → 250 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	193 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60	995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46998 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50	36.776496366	192.168.200.100	192.168.200.150	TCP	74	33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52	36.776586660	192.168.200.100	192.168.200.150	TCP	74	49654 → 119 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128

Abbiamo un file specifico (**.pcapng**) che contiene del traffico catturato, questo traffico contiene richieste e risposte tra **macchina vittima** (192.168.200.150) e **macchina attaccante** (192.168.200.100).

Possiamo notare che **Wireshark** ci semplifica la vita con i colori, ove ogni colore corrisponde a una data richiesta/risposta.

In particolare abbiamo le richieste TCP [**SYN**]:

No.	Time	Source	Destination	Protocol	Length	Info
1284	36.835104563	192.168.200.100	192.168.200.150	TCP	74	47804 → 815 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535498 TSecr=0 WS=128
1285	36.835168257	192.168.200.100	192.168.200.150	TCP	74	36960 → 48 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535498 TSecr=0 WS=128
1286	36.835212147	192.168.200.100	192.168.200.150	TCP	74	42224 → 162 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535498 TSecr=0 WS=128
1287	36.835296061	192.168.200.100	192.168.200.150	TCP	74	50746 → 875 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1288	36.835362548	192.168.200.100	192.168.200.150	TCP	74	38352 → 222 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1289	36.835426559	192.168.200.100	192.168.200.150	TCP	74	45820 → 122 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1290	36.835490897	192.168.200.100	192.168.200.150	TCP	74	56484 → 454 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1291	36.835560415	192.168.200.100	192.168.200.150	TCP	74	42742 → 37 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1292	36.835624620	192.168.200.100	192.168.200.150	TCP	74	44816 → 118 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1293	36.835689161	192.168.200.100	192.168.200.150	TCP	74	41010 → 136 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1294	36.835753319	192.168.200.100	192.168.200.150	TCP	74	59510 → 134 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1295	36.835816973	192.168.200.100	192.168.200.150	TCP	74	56112 → 441 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1296	36.835890815	192.168.200.100	192.168.200.150	TCP	74	44332 → 910 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1297	36.835945031	192.168.200.100	192.168.200.150	TCP	74	55668 → 480 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1298	36.836008884	192.168.200.100	192.168.200.150	TCP	74	57498 → 744 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1299	36.836072760	192.168.200.100	192.168.200.150	TCP	74	58808 → 161 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1299	36.836136952	192.168.200.100	192.168.200.150	TCP	74	47654 → 774 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1299	36.836200972	192.168.200.100	192.168.200.150	TCP	74	37098 → 608 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
1299	36.836265031	192.168.200.100	192.168.200.150	TCP	74	48190 → 658 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.836338288	192.168.200.100	192.168.200.150	TCP	74	48366 → 614 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.836402293	192.168.200.100	192.168.200.150	TCP	74	47864 → 140 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.836466649	192.168.200.100	192.168.200.150	TCP	74	42052 → 246 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.836531670	192.168.200.100	192.168.200.150	TCP	74	45940 → 952 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.836598519	192.168.200.100	192.168.200.150	TCP	74	41254 → 760 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.836661285	192.168.200.100	192.168.200.150	TCP	74	44012 → 940 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.836724991	192.168.200.100	192.168.200.150	TCP	74	43698 → 1013 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.836793803	192.168.200.100	192.168.200.150	TCP	74	49964 → 694 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.836854051	192.168.200.100	192.168.200.150	TCP	74	41092 → 577 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.836917770	192.168.200.100	192.168.200.150	TCP	74	44094 → 410 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.836981177	192.168.200.100	192.168.200.150	TCP	74	46540 → 216 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.837044822	192.168.200.100	192.168.200.150	TCP	74	33884 → 408 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.837108120	192.168.200.100	192.168.200.150	TCP	74	51052 → 325 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.837162100	192.168.200.100	192.168.200.150	TCP	74	38224 → 531 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535500 TSecr=0 WS=128
1299	36.837395062	192.168.200.100	192.168.200.150	TCP	74	42462 → 31 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535501 TSecr=0 WS=128
1299	36.837460008	192.168.200.100	192.168.200.150	TCP	74	40290 → 792 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535501 TSecr=0 WS=128
1299	36.837523814	192.168.200.100	192.168.200.150	TCP	74	37756 → 263 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535501 TSecr=0 WS=128
1299	36.837582778	192.168.200.100	192.168.200.150	TCP	74	33902 → 715 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535501 TSecr=0 WS=128
1299	36.837652783	192.168.200.100	192.168.200.150	TCP	74	52524 → 734 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535501 TSecr=0 WS=128
1299	36.837733206	192.168.200.100	192.168.200.150	TCP	74	59998 → 100 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535501 TSecr=0 WS=128

Queste richieste di accesso sulle porte, puo' portare ad un'idea di attacco con un tool di scansione come nmap, in base alla risposta della macchina vittima avremo piu' informazioni.

No.	Time	Source	Destination	Protocol	Length	Info
1249	36.837937099	192.168.200.150	192.168.200.100	TCP	60	200 → 49132 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1250	36.837937138	192.168.200.150	192.168.200.100	TCP	60	88 → 47594 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1251	36.837937179	192.168.200.150	192.168.200.100	TCP	60	451 → 44292 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1252	36.837991413	192.168.200.150	192.168.200.100	TCP	60	815 → 47004 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1253	36.837991463	192.168.200.150	192.168.200.100	TCP	60	48 → 36660 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1254	36.837991502	192.168.200.150	192.168.200.100	TCP	60	162 → 42224 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1255	36.837991541	192.168.200.150	192.168.200.100	TCP	60	875 → 50746 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1256	36.837991587	192.168.200.150	192.168.200.100	TCP	60	1022 → 38352 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1257	36.837991626	192.168.200.150	192.168.200.100	TCP	60	225 → 45820 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1258	36.837991672	192.168.200.150	192.168.200.100	TCP	60	454 → 56484 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1259	36.838002881	192.168.200.150	192.168.200.100	TCP	60	37 → 42742 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1260	36.838002962	192.168.200.150	192.168.200.100	TCP	60	118 → 44816 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1261	36.838003000	192.168.200.150	192.168.200.100	TCP	60	136 → 41010 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1262	36.838003041	192.168.200.150	192.168.200.100	TCP	60	124 → 59510 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1263	36.838003080	192.168.200.150	192.168.200.100	TCP	60	441 → 56112 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1264	36.838003120	192.168.200.150	192.168.200.100	TCP	60	910 → 44332 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1265	36.838003160	192.168.200.150	192.168.200.100	TCP	60	480 → 55668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1266	36.838003200	192.168.200.150	192.168.200.100	TCP	60	744 → 57498 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1267	36.838003238	192.168.200.150	192.168.200.100	TCP	60	161 → 58808 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1268	36.838003276	192.168.200.150	192.168.200.100	TCP	60	774 → 47654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1269	36.838003312	192.168.200.150	192.168.200.100	TCP	60	608 → 37098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1269	36.838003351	192.168.200.150	192.168.200.100	TCP	60	774 → 37098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1270	36.838003385	192.168.200.150	192.168.200.100	TCP	60	658 → 48190 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1271	36.838003420	192.168.200.150	192.168.200.100	TCP	60	614 → 48366 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1272	36.838003455	192.168.200.150	192.168.200.100	TCP	60	124 → 47864 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1273	36.838003489	192.168.200.150	192.168.200.100	TCP	60	246 → 42052 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1274	36.838147340	192.168.200.150	192.168.200.100	TCP	60	952 → 45940 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1275	36.838147408	192.168.200.150	192.168.200.100	TCP	60	766 → 41254 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1276	36.838147451	192.168.200.150	192.168.200.100	TCP	60	940 → 44012 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1277	36.838147490	192.168.200.150	192.168.200.100	TCP	60	1013 → 43698 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1278	36.838147529	192.168.200.150	192.168.200.100	TCP	60	694 → 49964 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1279	36.838147570	192.168.200.150	192.168.200.100	TCP	60	577 → 41092 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1280	36.838147615	192.168.200.150	192.168.200.100	TCP	60	410 → 44094 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1281	36.838147662	192.168.200.150	192.168.200.100	TCP	60	216 → 46540 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1282	36.838169832	192.168.200.150	192.168.200.100	TCP	60	408 → 33884 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1283	36.838169892	192.168.200.150	192.168.200.100	TCP	60	325 → 51052 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1284	36.838169932	192.168.200.150	192.168.200.100	TCP	60	531 → 38224 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1285	36.838169971	192.168.200.150	192.168.200.100	TCP	60	31 → 42462 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1286	36.838170011	192.168.200.150	192.168.200.100	TCP	60	792 → 40290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1287	36.838170051	192.168.200.150	192.168.200.100	TCP	60	263 → 37756 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Le risposte **[RST-ACK]** dimostrano che la macchina vittima respinge le richieste o semplicemente non ci sono servizi attivi su quelle date porte.

Di solito se la macchina vittima e' sotto firewall e trovi risposte **[RST-ACK]** e' perche' lo stesso firewall impedisce la tentata connessione a quella data porta, mentre se la vittima non e' in presenza di firewall, quel tipo di risposta potrebbe significare che non ci sono servizi attivi sulla data porta.

Se invece riceviamo una risposta **[ACK]**, significa che il servizio e' attivo e possiamo connetterci al esso:

65	36.776914772	192.168.200.100	192.168.200.150	TCP	66	33042 → 445	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
66	36.776941020	192.168.200.100	192.168.200.150	TCP	66	46990 → 139	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
67	36.776962320	192.168.200.100	192.168.200.150	TCP	66	60632 → 25	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68	36.776983878	192.168.200.100	192.168.200.150	TCP	66	37282 → 53	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466

Quindi basandosi sui tipi di richiesta, i tipi di risposte, possiamo arrivare ad una conclusione:

Questo tipo di attacco e' un **port scanning** mandato da tools specifici.

Infatti possiamo notare la richiesta ad ogni porta specifica e la possibile risposta 'buona' o 'cattiva' o 'non risposta' (ignorandola richiesta) .

Per migliorare la sicurezza, consiglieri di ampliare le regole dei firewall, **impementare nuove regole** per limitare i tentativi di connessione da un singolo IP, oppure utilizzare tecniche di **port Knoking** per nascondere porte sensibili.