

THREAT INTELLIGENCE & IOC

Nella simulazione andremo ad analizzare una cattura di rete effettuata da Wireshark con il fine di individuare eventuali IOC, vettori di attacco utilizzati ed infine proporre delle soluzioni per ridurre l'impatto in futuro.

Da un primo sguardo possiamo notare del traffico "anomalo" dall'indirizzo IP 192.168.200.100 all'indirizzo IP di destinazione 192.168.200.150.

73	36.777337934	192.168.200.100	192.168.200.150	TCP	74	49780 + 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
74	36.777430632	192.168.200.150	192.168.200.100	TCP	60	707 + 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777430741	192.168.200.150	192.168.200.100	TCP	60	436 + 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	36.777473018	192.168.200.100	192.168.200.150	TCP	74	36138 + 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
77	36.777522494	192.168.200.100	192.168.200.150	TCP	74	52428 + 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
78	36.777623082	192.168.200.150	192.168.200.100	TCP	60	98 + 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 + 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	36.777645027	192.168.200.100	192.168.200.150	TCP	74	41874 + 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
81	36.777680898	192.168.200.100	192.168.200.150	TCP	74	51506 + 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60	580 + 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60	962 + 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60	764 + 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777871293	192.168.200.150	192.168.200.100	TCP	60	435 + 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66	33042 + 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66	46990 + 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66	60632 + 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
89	36.778031265	192.168.200.100	192.168.200.150	TCP	66	37282 + 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
90	36.778179978	192.168.200.100	192.168.200.150	TCP	74	51450 + 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
91	36.778200161	192.168.200.100	192.168.200.150	TCP	74	48448 + 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
92	36.778307830	192.168.200.100	192.168.200.150	TCP	74	54566 + 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
93	36.778385846	192.168.200.150	192.168.200.100	TCP	60	148 + 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	36.778385948	192.168.200.150	192.168.200.100	TCP	60	806 + 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.778449494	192.168.200.150	192.168.200.100	TCP	60	221 + 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96	36.778482791	192.168.200.100	192.168.200.150	TCP	74	42420 + 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
97	36.778591226	192.168.200.100	192.168.200.150	TCP	74	34646 + 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
98	36.778614095	192.168.200.100	192.168.200.150	TCP	74	54202 + 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
99	36.778663064	192.168.200.150	192.168.200.100	TCP	60	1007 + 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100	36.778721080	192.168.200.150	192.168.200.100	TCP	60	286 + 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	36.778759636	192.168.200.100	192.168.200.150	TCP	74	40318 + 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
102	36.778781327	192.168.200.100	192.168.200.150	TCP	74	51276 + 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
103	36.778826294	192.168.200.150	192.168.200.100	TCP	60	131 + 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	36.778864493	192.168.200.100	192.168.200.150	TCP	74	39566 + 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
105	36.778939327	192.168.200.150	192.168.200.100	TCP	60	392 + 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106	36.778939427	192.168.200.150	192.168.200.100	TCP	60	677 + 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	36.778983153	192.168.200.100	192.168.200.150	TCP	74	47238 + 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
108	36.779029210	192.168.200.150	192.168.200.100	TCP	60	856 + 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	36.779055243	192.168.200.100	192.168.200.150	TCP	74	56542 + 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
110	36.779122299	192.168.200.150	192.168.200.100	TCP	60	84 + 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	36.779145004	192.168.200.100	192.168.200.150	TCP	74	40138 + 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
112	36.779252884	192.168.200.150	192.168.200.100	TCP	60	807 + 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	36.779273781	192.168.200.100	192.168.200.150	TCP	74	43140 + 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
114	36.779309462	192.168.200.100	192.168.200.150	TCP	74	46886 + 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
115	36.779354564	192.168.200.150	192.168.200.100	TCP	60	948 + 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Per traffico anomalo intendiamo una grande quantità di pacchetti **SYN senza ACK** e una mole importante di pacchetti con risposta **RST, ACK** tipico quando una porta risulta chiusa, un altro **IOC** che salta all'occhio è relativo al fatto che le richieste SYN dei pacchetti hanno una dimensione di **74 byte** e che vengono inviati alle porte note, la loro dimensione ci fa ipotizzare che i pacchetti inviati, presentano delle **opzioni TCP aggiuntive** che ne aumentano la dimensione, tipico di attacchi di **Port Scan** effettuate con tool come *nmap* dove si tenta di rilevare la versione del servizio presente sulle porte. Ultimo ma non per importanza è il tempo di esecuzione, nella colonna del TIME possiamo notare che tutto il traffico catturato pochissimo questo potrebbe dipendere sempre da una scansione aggressiva di nmap con **-T4** o **-T5**. Un altro dettaglio importante è quello

Per un'analisi approfondita utilizziamo i filtri di Wireshark per andare ad analizzare meglio il traffico.

In primis utilizziamo questo filtro per visualizzare solo il traffico di pacchetti con richieste di SYN senza ACK: **tcp.flags.syn == 1 && tcp.flags.ack == 0**

tcp.flags.syn == 1 && tcp.flags.ack == 0							
No.	Time	Source	Destination	Protocol	Length	Info	
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
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	36.774535534	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
29	36.775337800	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
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	50684 → 199	[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	36.776330610	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	33042 → 445	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46	36.776402500	192.168.200.100	192.168.200.150	TCP	74	49814 → 256	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46990 → 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	36.776568606	192.168.200.100	192.168.200.150	TCP	74	49654 → 110	[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

Come detto prima possiamo notare molti pacchetti di richieste TCP SYN senza l'ACK sulle porte note, tutte con una lunghezza di 74 byte.

Andiamo ora ad analizzare solo le risposte RST, ACK utilizzando questo filtro **tcp.flags.reset == 1 && tcp.flags.ack == 1**

tcp.flags.reset == 1 && tcp.flags.ack == 1							
No.	Time	Source	Destination	Protocol	Length	Info	
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	23.764899091	192.168.200.150	192.168.200.100	TCP	66	53060 → 80	[RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
21	36.774685696	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
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
32	36.775589806	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	41304 → 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
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
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	199 → 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
55	36.776813123	192.168.200.150	192.168.200.100	TCP	60	587 → 34648	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60	256 → 49814	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60	36.776905004	192.168.200.150	192.168.200.100	TCP	60	143 → 33206	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62	36.776905082	192.168.200.150	192.168.200.100	TCP	60	110 → 49654	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
64	36.776905162	192.168.200.150	192.168.200.100	TCP	60	500 → 54898	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
69	36.777118481	192.168.200.150	192.168.200.100	TCP	60	487 → 51534	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
74	36.777430632	192.168.200.150	192.168.200.100	TCP	60	707 → 56990	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777430741	192.168.200.150	192.168.200.100	TCP	60	436 → 35638	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78	36.777623082	192.168.200.150	192.168.200.100	TCP	60	98 → 34120	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 → 49780	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60	580 → 36138	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60	962 → 52428	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60	764 → 41874	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777871293	192.168.200.150	192.168.200.100	TCP	60	435 → 51506	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66	33042 → 445	[RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66	46990 → 139	[RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66	60632 → 25	[RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
89	36.778031265	192.168.200.100	192.168.200.150	TCP	66	37282 → 53	[RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466

Se facciamo attenzione anche alle opzioni come MSS, Windows Scaling e Timestamp possiamo notare che sono presenti sia nei pacchetti RST,ACK e nei pacchetti SYN analizzati precedentemente. Queste opzioni sono tipiche di scansioni di porte con NMAP quando utilizza funzioni di rilevamento del servizio (-sV) oppure con scansioni SYN (-sS).

Dall'analisi degli IOC individuati possiamo ipotizzare che Wireshark ha catturato traffico di rete derivante da una scansione di porte con NMAP, vedendo nel dettaglio possiamo dire che il comando di scansione usato potrebbe essere il seguente: **nmap -sS -sV -Pn 192.168.200.150**

Un'altra importante considerazione va fatta sugli indirizzi IP che risultano essere appunto sulla stessa **ip network 192.168.200.0**, questo ci fa determinare che la scansione di porte non autorizzata sia partita da un dispositivo interno all'azienda, il che ci fa presupporre che può essere un dipendente o un attaccante che si è impossessato della macchina.

Azioni per poter ridurre l'impatto di questo attacco

Per poterci difendere da attacchi come questo possiamo adottare diverse soluzioni:

Configurare il Firewall per filtrare le porte ovvero bloccando i pacchetti SYN che non hanno la risposta ACK e bloccare l'accesso a client non autorizzati.

Configurare IDS/IPS per monitorare il traffico e rilevare pacchetti con opzioni TCP non comuni come ad esempio Suricata e Snort

Implementazione di honeypots

Impostare un Rate Limiting per poter limitare la velocità delle connessioni rallentando di conseguenza un attacco di port scan aggressivo

Hardening del sistema mantenendo aggiornati i servizi e disabilitando quelli non necessari ci permetterà di poterci proteggere da un eventuale attacco successivo alla scansione delle porte.

Per concludere il monitoraggio di pacchetti TCP con opzioni aggiuntive come MSS, Window Scaling e Timestamp ci è di vitale importanza per poter identificare subito traffico anomalo o sospetto. La combinazione di tecnologie come IDS/IPS, configurazioni Firewall, Wireshark etc ci permette di poter rilevare attacchi di questo tipo o manipolazioni delle connessioni consentendoci di conseguenza di poter impostare filtri e regole adatte a migliorare la nostra sicurezza.

CONCLUSIONI

Per arrivare a queste conclusioni abbiamo prima ipotizzato scenari peggiori come un attacco DoS e SYN Flood.

Facendo un passo indietro l'attacco DoS comune mira a saturare la rete sovraccaricando le risorse mentre l'attacco DoS di tipo SYN Flood sfrutta pacchetti SYN per esaurire la capacità di un server di avere altre connessioni inviando molti pacchetti SYN senza completare il 3 way handshake.

Detto questo possiamo vedere che analizzando nel dettaglio il traffico catturato vediamo pacchetti SYN con opzioni TCP aggiuntive e risposte RST,ACK il che ci ha fatto escludere appunto altri attacchi come DoS e SYN Flood perchè la scansione di porte va a determinare lo stato di quest'ultime. Per distinguerli meglio abbiamo osservato il traffico la quantità e soprattutto la frequenza d'invio dei pacchetti e la loro dimensione.