

Threat Intelligence & IoC

Nel progetto odierno il compito era quello di effettuare l'analisi di un file **Wireshark**, nel quale vi è stato catturato un traffico di dati potenzialmente sospetto.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement WS/AS/POI/TABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation
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=1 TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	53076 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294951165 TSecr=810522427
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 53076 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PcsCompu_39:7d:fe	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_39:7d:fe	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_39:7d:fe	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775236999	PcsCompu_39:7d:fe	PcsCompu_39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:39:7d:fe
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=1 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=1 TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	53076 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
15	36.774366385	192.168.200.100	192.168.200.150	TCP	74	56636 → 555 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 134 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 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=1 TSval=810535438 TSecr=0 WS=128
19	36.774655595	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535437
20	36.774655652	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=1 TSval=4294952466 TSecr=810535437
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 53076 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 56636 [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	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711972	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	36.775141273	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=1 TSval=4294952466 TSecr=810535437
28	36.775174048	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	36.775337880	192.168.200.100	192.168.200.150	TCP	74	59174 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 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=1 TSval=810535439 TSecr=0 WS=128
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
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=1 TSval=4294952466 TSecr=810535437
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=1 TSval=4294952466 TSecr=810535437
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	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	36.775815984	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

Primo sguardo

A primo impatto, aperto il file mediante il tool **Wireshark**, la prima cosa che si può notare è la presenza di un notevole traffico di pacchetti **SYN** mediante il protocollo **TPC**. Inoltre, vi è anche la presenza di pacchetti **SYN, ACK ed ACK**, che indicano che il **Three Ways Handshake** è andato a buon fine tra le due macchine, ma partiamo ad analizzare il file dall'inizio.

Inizio Analisi

Dopo un primo sguardo l'approccio è stato quello di eseguire un'analisi ordinata in ordine crescente di **No.** e **Time** in modo da avere una visione corretta delle tempistiche con cui il traffico di dati si è sviluppato.

In cima si può notare un messaggio con destinazione **Broadcast (.255)** da parte dell'indirizzo IP **192.168.200.150**, con protocollo "**BROWSER**" nel quale viene riportato un annuncio. Questo è il primo dato che viene riportato il quale può rappresentare un messaggio di benvenuto o un annuncio di presenza proveniente da un server.

Questi pacchetti fanno parte del **protocollo Server Message Block (SMB)** e del relativo servizio **NetBIOS**, utilizzati per condividere informazioni tra dispositivi in una rete locale.

Si può quindi dedurre che l'indirizzo IP .150 possa essere un server.

Successivamente si nota che una seconda macchina, con indirizzo IP **192.168.200.100** effettua una connessione mediante protocollo **http** sulla porta **80**, inviando un pacchetto SYN, ricevendo in risposta un SYN, ACK, e rispondendo con un pacchetto ACK concludendo il **TWH**.

Mentre ciò avviene si nota che effettua anche una richiesta di connessione sulla porta **443** (https) alla quale però riceve una risposta **RST, ACK** che chiude la connessione.

*Il flag **RST, ACK** può indicare che il server (192.168.200.150) sta rigettando le connessioni o che c'è un sovraccarico causato da richieste simultanee.*

Infine subito dopo entra in gioco il protocollo **ARP** (livello 2 del modello ISO/OSI), mediante il quale vi è l'associazione tra gli indirizzi IP delle macchine e i rispettivi indirizzi MAC, in modo che possano quindi comunicare tra di loro all'interno della rete LAN.

Analisi del traffico

Fin qui non vi erano anomalie allarmanti, nessun **IoC**, per cui si prosegue con l'analisi dei dati riportati successivamente.

Qui iniziano le stranezze poiché si può notare la presenza di una grande mole di pacchetti **SYN** da parte dell'indirizzo IP **.100** verso l'indirizzo IP **.150**, tutti in un lasso di tempo veramente breve.

La prima ipotesi che si può fare è che si possa trattare di una **scansione** della nostra macchina, volta a scoprire quali porte sono attive su di essa. Ciò potrebbe avvenire mediante l'utilizzo di tool appositi come **Nmap**, il quale può effettuare scansioni con varie metodologie, omettendo il ping (**-PN**) inviando solo pacchetti SYN (**-sS**), modificato la velocità in modo da poter eludere eventuali difese come Firewall (**T0, T1...T5**) o anche mediante comandi specifici tentare alcuni script (**--script vuln**).

Un'altra ipotesi è che si possa essere trattato di un attacco **SYN flood**, quindi un possibile attacco DOS, ipotesi che però è stata scartata. Questo perché durante un attacco **SYN Flood**, un client invia un alto volume di pacchetti SYN per consumare le risorse del server, senza mai completare il processo di handshake, cosa che invece avviene e lo si può notare in modo particolare sulla porta **80** e su altre più in basso (**445, 139, 25, 53**).

43	36.77623880	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	
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					
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	36.776568066	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	
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					
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534	+ 487	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535440	TSecr=0	WS=128	
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445	+ 33042	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	TSval=810535440	TSecr=810535440	WS=64
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					
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139	+ 46990	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	TSval=810535440	TSecr=810535440	WS=64
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					
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25	+ 60632	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	TSval=810535440	TSecr=810535440	WS=64
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					
63	36.776905123	192.168.200.150	192.168.200.100	TCP	74	53	+ 37282	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	TSval=810535440	TSecr=810535440	WS=64
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					
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			
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					
70	36.7771143014	192.168.200.100	192.168.200.150	TCP	74	56990	+ 707	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535440	TSecr=0	WS=128	
71	36.777186821	192.168.200.100	192.168.200.150	TCP	74	35638	+ 436	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535440	TSecr=0	WS=128	
72	36.777302991	192.168.200.100	192.168.200.150	TCP	74	34120	+ 98	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535441	TSecr=0	WS=128	
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	36.777680098	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	36.777967559	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			

Con lo scopo di approfondire ulteriormente l'analisi sono stati utilizzati alcuni filtri sul tool Wireshark. Uno di questi è `tcp.flags.syn == 1 && tcp.flags.ack == 0` il quale ha fornito soltanto le connessioni SYN in modo da poterle analizzare accuratamente.

Esse si presentano tutte al medesimo modo, con la stessa lunghezza, e valori non allarmanti, ma che possano però suggerire una scansione.

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	36.776568066	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	+ 580	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535440	TSecr=0	WS=128
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534	+ 487	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535440	TSecr=0	WS=128
60	36.777134301	192.168.200.100	192.168.200.150	TCP	74	56990	+ 707	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535440	TSecr=0	WS=128
71	36.777186812	192.168.200.100	192.168.200.150	TCP	74	35638	+ 436	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535440	TSecr=0	WS=128
72	36.777302991	192.168.200.100	192.168.200.150	TCP	74	34120	+ 78	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535441	TSecr=0	WS=128
73	36.777337934	192.168.200.100	192.168.200.150	TCP	74	49780	+ 98	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535441	TSecr=0	WS=128
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	36.777524204	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
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
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	36.778208611	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
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	36.778591126	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
01	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
02	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
04	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
07	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
09	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
11	36.779145804	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
13	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
16	36.779309642	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
19	36.779373956	192.168.200.100	192.168.200.150	TCP	74	40904	+ 138	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535443	TSecr=0	WS=128

Considerazioni Analisi

Ci troviamo all'interno della medesima rete, per cui si deduce che l'attaccante (IP 192.168.200.100) è già all'interno della nostra LAN, poiché si parla di due indirizzi IP privati di classe C.

Si evince dal traffico di dati esaminato che si tratti di una scansione **Nmap**, probabilmente mediante l'ausilio di un comando:

Nmap -Pn -sT 192.168.200.150 -T4 (T5)

Posso dedurre ciò perché non vi è alcuna traccia del protocollo **ICMP**, cosa che ci fa intuire l'uso del comando **-Pn**; inoltre l'attaccante conclude alcuni TWH cosa che invece mi fa dedurre che non si possa trattare di un comando **-sS**, bensì di un comando come **-sT**, il quale invece effettua una scansione tentando di concludere la TWH.

Altro parametro non meno importante, è la **velocità**. La scansione che si è estesa soltanto sulle porte note, quindi le prime **1024**, è avvenuta in un lasso di tempo veramente breve. Tutto si svolge al **36esimo secondo**, il che fa intuire in maniera lampante che non si tratta di una scansione lenta, ma bensì veloce, con lo scopo di raccogliere informazioni nel minor tempo possibile.

Conclusione

*Avendo appurato che si tratti di una scansione, si possono intraprendere alcune azioni volte a **limitare** il traffico di dati ricevuto da quel preciso indirizzo IP.*

***Questo perché azioni drastiche come bloccarlo potrebbero rivelarsi problematiche** visto che non si hanno maggiori informazioni sull'accaduto. Non si sa se sia un dipendente curioso o se sia in corso un pentesting di cui non siamo stati avvisati ad esempio, ragion per cui se bloccassimo l'IP otremmo bloccare o limitare il lavoro del dipendente causando problemi per l'azienda.*

*Utilizzando delle limitazioni invece, possiamo limitare i danni e tenere sotto controllo ol'indirizzo IP in questione. Ciò può essere preso in considerazione, in questa specifica situazione **in base ai dati che sono stati forniti**.*

Allo scopo di intercettare traffici malevoli, si possono inoltre installare IDS/IPS, dispositivi volti a reagire mediante allarmi (IDS) o bloccando il traffico sospetto in automatico (IPS). Si possono inoltre implementare regole specifiche, particolari all'interno del Firewall, o anche impostare regole specifiche per il Rate Limit.

Ovviamente, molto importante, mantenere sempre un costante monitoraggio della rete mediante appositi Tool, eseguendo le relative analisi.