

S9 L5

Analisi Forense del Traffico di Rete: Rilevamento di Attività di Port Scanning

1. Introduzione

Il presente documento illustra l'analisi di una cattura di traffico di rete (file .pcapng) effettuata mediante lo strumento **Wireshark**. L'obiettivo dell'attività è esaminare i flussi di comunicazione registrati per identificare potenziali minacce alla sicurezza informatica e ricostruire la dinamica dell'incidente.

L'analisi si concentra sull'identificazione degli **Indicatori di Compromissione (IOC)**, sulla determinazione dei **vettori di attacco** esposti e sulla definizione delle **strategie di mitigazione** necessarie per mettere in sicurezza l'infrastruttura.

2. Identificazione e Analisi degli IOC (Indicatori di Compromissione)

Dall'analisi approfondita dei pacchetti, è stata rilevata un'attività ostile di **Ricognizione Attiva** (Active Reconnaissance). Di seguito sono dettagliati gli IOC identificati che confermano l'attacco in corso:

- **Attori Coinvolti:**
 - **Attaccante (Source):** IP 192.168.200.100.
Identificato come l'origine di un volume anomalo e massivo di richieste di connessione.

- **Vittima (Target):** IP 192.168.200.150. La macchina ha trasmesso un pacchetto di annuncio identificandosi con l'hostname METASPLOITABLE, indicando un sistema potenzialmente vulnerabile per natura.
- **Tipologia di Attacco: TCP SYN Scan (Port Scanning)**
 - **Evidenza:** È stata registrata una raffica di pacchetti TCP con flag **[SYN]** inviati dall'attaccante verso una moltitudine di porte diverse della vittima in un lasso di tempo inferiore al millisecondo.
 - **Analisi:** Questo comportamento indica l'utilizzo di uno scanner automatico (es. Nmap) che tenta di mappare le porte aperte senza completare il *Three-Way Handshake* per guadagnare velocità e tentare di eludere i log.
- **Pattern di Risposta Anomalo (Rifiuti Massivi)**
 - **Evidenza:** Il traffico evidenzia un elevato numero di pacchetti di risposta **[RST, ACK]** (Reset) provenienti dalla vittima.
 - **Analisi:** Questo "rumore di fondo" (visualizzato in rosso su Wireshark) conferma che l'attaccante sta scansionando indiscriminatamente un range di porte molto ampio (probabilmente tutte le 65.535 porte), la maggior parte delle quali risulta chiusa.
- **Fingerprinting dei Servizi (Apertura e Chiusura Immediata)**
 - **Evidenza:** Sulle porte che risultano aperte (dove la vittima risponde con SYN, ACK), l'attaccante invia immediatamente un pacchetto **[RST]** subito dopo aver ricevuto la conferma.
 - **Analisi:** Questo comportamento ("Bussare e scappare") è la firma digitale di uno scanner:

Il obiettivo non è utilizzare il servizio, ma solo annotarne l'esistenza nel database dell'attaccante.

3. Analisi Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	00:00:00.000000	192.168.200.158	192.168.200.158	HTTP/1.1	256	Host: Announcement.METASPLITABLE
2	23.764214995	192.168.200.100	192.168.200.158	TCP	74 530660 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810522427 Tscr=0 WS=128	
3	23.764267789	192.168.200.100	192.168.200.158	TCP	74 33576 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810522428 Tscr=0 WS=128	
4	23.764777323	192.168.200.100	192.168.200.158	TCP	74 88 - 530660 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810522428 Tscr=0 WS=64	
5	23.764815289	192.168.200.158	192.168.200.100	TCP	66 530660 - 80 [ACK] Seq=1 Win=64256 Len=0 Tsvl=810522428 Tscr=4294951165	
6	23.764815289	192.168.200.158	192.168.200.100	TCP	66 530660 - 80 [ACK] Seq=1 Win=64256 Len=0 Tsvl=810522428 Tscr=4294951165	
7	23.764899901	192.168.200.100	192.168.200.158	TCP	66 530660 - 80 [RST, ACK] Seq=1 Win=64256 Len=0 Tsvl=810522428 Tscr=4294951165	
8	28.761629461	PcsComp.fdu:87:1fe	PcsComp.fdu:87:1fe	ARP	66 who has 192.168.200.100? Tell 192.168.200.158	
9	28.761640919	PcsComp.fdu:87:1fe	PcsComp.fdu:87:1fe	ARP	66 192.168.200.100 has 192.168.200.100? Tell 192.168.200.158	
10	28.761640919	PcsComp.fdu:87:1fe	PcsComp.fdu:87:1fe	ARP	66 192.168.200.100 has 192.168.200.100? Tell 192.168.200.158	
11	23.775280899	PcsComp.fdu:87:1fe	PcsComp.fdu:87:1fe	ARP	66 192.168.200.158 has 192.168.200.100? Tell 192.168.200.158	
12	36.774145394	192.168.200.100	192.168.200.158	TCP	74 41384 - 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535437 Tscr=0 WS=128	
13	36.774218116	192.168.200.100	192.168.200.158	TCP	74 56120 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535437 Tscr=0 WS=128	
14	36.774275826	192.168.200.100	192.168.200.158	TCP	74 33878 - 44 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535437 Tscr=0 WS=128	
15	36.774335520	192.168.200.100	192.168.200.158	TCP	74 41182 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=0 WS=128	
16	36.774465637	192.168.200.100	192.168.200.158	TCP	74 52358 - 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=0 WS=128	
17	36.774553324	192.168.200.100	192.168.200.158	TCP	74 46138 - 99 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=0 WS=128	
18	36.774614776	192.168.200.100	192.168.200.158	TCP	74 41182 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=0 WS=128	
19	36.774686596	192.168.200.100	192.168.200.158	TCP	74 23 - 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=4294952466 WS=64	
20	36.774686596	192.168.200.100	192.168.200.158	TCP	74 23 - 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=4294952466 WS=64	
21	36.774686596	192.168.200.100	192.168.200.158	TCP	66 443 - 33878 [RST, ACK] Seq=1 Win=1 Len=0	
22	36.774686597	192.168.200.100	192.168.200.158	TCP	66 554 - 50863 [RST, ACK] Seq=1 Win=1 Len=0	
23	36.774665776	192.168.200.100	192.168.200.158	TCP	66 135 - 52358 [RST, ACK] Seq=1 Win=1 Len=0	
24	36.774706044	192.168.200.100	192.168.200.158	TCP	66 41384 - 23 [ACK] Seq=1 Win=64256 Len=0 Tsvl=810535438 Tscr=4294952466	
25	36.774706044	192.168.200.100	192.168.200.158	TCP	66 41384 - 23 [ACK] Seq=1 Win=64256 Len=0 Tsvl=810535438 Tscr=4294952466	
26	36.775111104	192.168.200.158	192.168.200.100	TCP	66 997 - 40138 [RST, ACK] Seq=1 Win=1 Len=0	
27	36.775145273	192.168.200.158	192.168.200.100	TCP	74 21 - 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=4294952466	
28	36.775174048	192.168.200.100	192.168.200.158	TCP	66 41182 - 21 [ACK] Seq=1 Win=84240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=4294952466	
29	36.775337899	192.168.200.100	192.168.200.158	TCP	74 59374 - 99 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=0 WS=128	
30	36.775337899	192.168.200.100	192.168.200.158	TCP	74 59374 - 99 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=0 WS=128	
31	36.775524204	192.168.200.100	192.168.200.158	TCP	74 53062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=0 WS=128	
32	36.775589006	192.168.200.158	192.168.200.100	TCP	66 113 - 50174 [RST, ACK] Seq=1 Win=1 Len=0	
33	36.775616454	192.168.200.100	192.168.200.158	TCP	66 41304 - 23 [RST, ACK] Seq=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	
34	36.775652497	192.168.200.100	192.168.200.158	TCP	66 56120 - 111 [RST, ACK] Seq=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	
35	36.7757797004	192.168.200.100	192.168.200.158	TCP	66 41304 - 23 [RST, ACK] Seq=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	
36	36.7757797004	192.168.200.100	192.168.200.158	TCP	74 88 - 53063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535436 Tscr=4294952466	
37	36.775897376	192.168.200.100	192.168.200.158	TCP	66 55565 - 22 [ACK] Seq=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	
38	36.775813232	192.168.200.100	192.168.200.158	TCP	66 53062 - 80 [ACK] Seq=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	
39	36.775986194	192.168.200.100	192.168.200.158	TCP	66 41182 - 21 [RST, ACK] Seq=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	
40	36.7759975876	192.168.200.100	192.168.200.158	TCP	66 55565 - 22 [RST, ACK] Seq=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	

Dalla prima immagine abbiamo stabilito:

- 1. Chi è la vittima:** IP 192.168.200.150 (Hostname: METASPLOITABLE).
 - 2. Chi è l'attaccante:** IP 192.168.200.100.
 - 3. Cosa sta succedendo:** Un **Port Scan TCP SYN**.
L'attaccante invia pacchetti SYN rapidi; la vittima risponde con RST se la porta è chiusa.

Apply a display filter ... <Ctrl>/								
No.	Time	Source	Destination	Protocol	Length	Info		
49	36.7795786	192.168.200.100	192.168.200.150	TCP	66 55056 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466			
41	36.776065853	192.168.200.100	192.168.200.150	TCP	66 53062 - 80 [SYN, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466			
42	36.776065853	192.168.200.100	192.168.200.150	TCP	74 50896 - 139 [SYN, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466 WS=128			
43	36.776233889	192.168.200.100	192.168.200.150	TCP	74 44229 - 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535439 Tscr=0 WS=128			
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74 34640 - 507 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128			
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74 33942 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128			
46	36.776402590	192.168.200.100	192.168.200.150	TCP	74 49834 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128			
47	36.776402590	192.168.200.100	192.168.200.150	TCP	68 189 - 50884 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
48	36.776402590	192.168.200.100	192.168.200.150	TCP	68 200 - 42426 [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=1 Tsvl=810535440 Tscr=0 WS=128			
50	36.776496336	192.168.200.100	192.168.200.150	TCP	74 33260 - 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128			
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74 66932 - 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128			
52	36.776512221	192.168.200.100	192.168.200.150	TCP	74 45942 - 37 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128			
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74 31792 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128			
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74 54898 - 509 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128			
55	36.776813123	192.168.200.100	192.168.200.150	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 - 20 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128			
57	36.776904828	192.168.200.100	192.168.200.150	TCP	74 445 - 33842 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=64			
58	36.776904828	192.168.200.100	192.168.200.150	TCP	74 445 - 33842 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=64			
59	36.776954951	192.168.200.100	192.168.200.150	TCP	74 135 - 46998 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=64			
60	36.776959094	192.168.200.100	192.168.200.150	TCP	68 143 - 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
61	36.776965984	192.168.200.100	192.168.200.150	TCP	74 25 - 66932 [RST, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=64			
62	36.776965982	192.168.200.100	192.168.200.150	TCP	68 110 - 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
63	36.776983701	192.168.200.100	192.168.200.150	TCP	74 51534 - 51541 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
64	36.776983702	192.168.200.100	192.168.200.150	TCP	68 598 - 54998 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
65	36.776914772	192.168.200.100	192.168.200.150	TCP	66 33842 - 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535440 Tscr=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 Tsvl=810535440 Tscr=4294952466			
67	36.776962323	192.168.200.100	192.168.200.150	TCP	66 66932 - 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535440 Tscr=4294952466			
68	36.776983702	192.168.200.100	192.168.200.150	TCP	66 37282 - 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535440 Tscr=4294952466			
69	36.777143934	192.168.200.100	192.168.200.150	TCP	74 56996 - 137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128			
70	36.777143934	192.168.200.100	192.168.200.150	TCP	74 56996 - 137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128			
71	36.777186821	192.168.200.100	192.168.200.150	TCP	74 35630 - 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128			
72	36.777362993	192.168.200.100	192.168.200.150	TCP	74 34120 - 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tscr=0 WS=128			
73	36.777373793	192.168.200.100	192.168.200.150	TCP	74 45942 - 37 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tscr=0 WS=128			
74	36.777373794	192.168.200.100	192.168.200.150	TCP	60 574 - 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
75	36.7774393741	192.168.200.100	192.168.200.150	TCP	68 456 - 35636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
76	36.777473018	192.168.200.100	192.168.200.150	TCP	74 36138 - 598 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tscr=0 WS=128			
77	36.777522493	192.168.200.100	192.168.200.150	TCP	74 52428 - 902 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tscr=0 WS=128			
78	36.777623082	192.168.200.100	192.168.200.150	TCP	68 98 - 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
79	36.777623149	192.168.200.100	192.168.200.150	TCP	60 78 - 49789 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			

Dalla seconda immagine deduciamo:

- Scansione Attiva:** Continua il bombardamento di pacchetti SYN.
- Porte Chiuse (Rifiutate):** La vittima risponde con RST su porte come 995 o 587 (Righe Rosse).
- Porte Aperte (Vulnerabili):** Il traffico cambia pattern (Righe 65-68) per le porte **TCP 139, 445, 25 e 53**. Questo conferma che i servizi SMB, SMTP e DNS sono attivi e raggiungibili dall'attaccante. Questa informazione permetterà all'hacker di passare alla fase successiva

Apply a display filter ... <Ctrl>/								
No.	Time	Source	Destination	Protocol	Length	Info		
79	36.777623149	192.168.200.100	192.168.200.150	TCP	60 78 - 49789 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
80	36.777680998	192.168.200.100	192.168.200.150	TCP	74 51596 - 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tscr=0 WS=128			
81	36.777680997	192.168.200.100	192.168.200.150	TCP	74 51596 - 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tscr=0 WS=128			
82	36.777586936	192.168.200.100	192.168.200.150	TCP	60 589 - 36139 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
83	36.777586936	192.168.200.100	192.168.200.150	TCP	60 764 - 41374 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
84	36.777586936	192.168.200.100	192.168.200.150	TCP	60 764 - 41374 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
85	36.77787245	192.168.200.100	192.168.200.150	TCP	68 438 - 51500 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
86	36.777879328	192.168.200.100	192.168.200.150	TCP	66 33642 - 445 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 Tsvl=810535441 Tscr=4294952466			
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66 46990 - 133 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 Tsvl=810535441 Tscr=4294952466			
88	36.777912717	192.168.200.100	192.168.200.150	TCP	66 66932 - 25 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 Tsvl=810535441 Tscr=4294952466			
89	36.777912717	192.168.200.100	192.168.200.150	TCP	66 66932 - 25 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 Tsvl=810535441 Tscr=4294952466			
90	36.778179576	192.168.200.100	192.168.200.150	TCP	74 51536 - 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tscr=0 WS=128			
91	36.778209161	192.168.200.100	192.168.200.150	TCP	74 48448 - 804 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tscr=0 WS=128			
92	36.778307838	192.168.200.100	192.168.200.150	TCP	74 54566 - 224 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=0 WS=128			
93	36.778385946	192.168.200.100	192.168.200.150	TCP	60 148 - 51540 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
94	36.778385946	192.168.200.100	192.168.200.150	TCP	60 598 - 45606 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
95	36.778385946	192.168.200.100	192.168.200.150	TCP	60 598 - 45606 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
96	36.778428273	192.168.200.100	192.168.200.150	TCP	74 42428 - 198 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=0 WS=128			
97	36.778511226	192.168.200.100	192.168.200.150	TCP	74 34466 - 208 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=0 WS=128			
98	36.778614995	192.168.200.100	192.168.200.150	TCP	74 54202 - 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=0 WS=128			
99	36.778630664	192.168.200.100	192.168.200.150	TCP	60 189 - 42428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
100	36.778630664	192.168.200.100	192.168.200.150	TCP	60 48248 - 34364 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
101	36.778755397	192.168.200.100	192.168.200.150	TCP	74 48218 - 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=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=1 Tsvl=810535442 Tscr=0 WS=128			
103	36.778826294	192.168.200.100	192.168.200.150	TCP	60 131 - 54282 [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=1 Tsvl=810535442 Tscr=0 WS=128			
105	36.778935247	192.168.200.100	192.168.200.150	TCP	60 409 - 40948 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
106	36.778935247	192.168.200.100	192.168.200.150	TCP	60 877 - 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
107	36.778931533	192.168.200.100	192.168.200.150	TCP	74 47238 - 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=0 WS=128			
108	36.779029210	192.168.200.100	192.168.200.150	TCP	60 856 - 39560 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
109	36.779052423	192.168.200.100	192.168.200.150	TCP	74 56542 - 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=0 WS=128			
110	36.779122299	192.168.200.100	192.168.200.150	TCP	60 854 - 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
111	36.779122299	192.168.200.100	192.168.200.150	TCP	74 47238 - 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=0 WS=128			
112	36.779252084	192.168.200.100	192.168.200.150	TCP	60 887 - 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=1 Tsvl=810535443 Tscr=0 WS=128			
114	36.779309462	192.168.200.100	192.168.200.150	TCP	74 46886 - 104 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535443 Tscr=0 WS=128			
115	36.779354564	192.168.200.100	192.168.200.150	TCP	60 948 - 40130 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
116	36.779354564	192.168.200.100	192.168.200.150					

Dalla terza immagine deduciamo:

- Questo conferma che si tratta di un **Full Port Scan** (probabilmente una scansione di tutte le 65.535 porte o delle "Top 1000"). L'attaccante non sta cercando solo i servizi famosi, sta cercando *qualsiasi* porta aperta. La sequenzialità e la velocità confermano l'uso di un tool automatico (bot/scanner).

No.	Time	Source	Destination	Protocol	Length	Info
118	36.77969548	192.168.200.159	192.168.200.100	TCP	60	214 - 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	36.77969576	192.168.200.159	192.168.200.100	TCP	60	106 - 46880 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120	36.779695798	192.168.200.159	192.168.200.100	TCP	60	138 - 50204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	36.779695843	192.168.200.159	192.168.200.100	TCP	60	99 - 51200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122	36.779695848	192.168.200.159	192.168.200.100	TCP	74	44744 - 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535443 TSectr=0 WS=128
123	36.779776288	192.168.200.159	192.168.200.100	TCP	74	43636 - 763 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535443 TSectr=0 WS=128
124	36.779856041	192.168.200.159	192.168.200.100	TCP	60	699 - 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	36.779911169	192.168.200.100	192.168.200.159	TCP	74	55131 - 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535443 TSectr=0 WS=128
126	36.779946174	192.168.200.100	192.168.200.159	TCP	60	11 - 43636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
127	36.779946201	192.168.200.159	192.168.200.100	TCP	60	274 - 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128	36.779812127	192.168.200.159	192.168.200.100	TCP	74	55136 - 55136 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535443 TSectr=0 WS=128
129	36.779814973	192.168.200.159	192.168.200.100	TCP	74	57552 - 58 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535443 TSectr=0 WS=128
130	36.779817933	192.168.200.159	192.168.200.100	TCP	74	40822 - 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535443 TSectr=0 WS=128
131	36.780215176	192.168.200.159	192.168.200.100	TCP	60	42 - 49522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132	36.780303098	192.168.200.159	192.168.200.100	TCP	60	99 - 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133	36.780325337	192.168.200.159	192.168.200.100	TCP	74	3752 - 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128
134	36.780344298	192.168.200.159	192.168.200.100	TCP	74	40648 - 238 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128
135	36.780409918	192.168.200.159	192.168.200.100	TCP	74	36548 - 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128
136	36.780427599	192.168.200.159	192.168.200.100	TCP	74	38866 - 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128
137	36.780439303	192.168.200.159	192.168.200.100	TCP	74	32122 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128
138	36.780499997	192.168.200.159	192.168.200.100	TCP	74	32122 - 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128
139	36.780577880	192.168.200.159	192.168.200.100	TCP	60	266 - 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	36.780577981	192.168.200.159	192.168.200.100	TCP	60	11 - 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	36.780578026	192.168.200.159	192.168.200.100	TCP	60	235 - 40848 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142	36.780578074	192.168.200.159	192.168.200.100	TCP	60	739 - 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143	36.780578100	192.168.200.159	192.168.200.100	TCP	60	99 - 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144	36.780578156	192.168.200.159	192.168.200.100	TCP	60	999 - 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145	36.780578198	192.168.200.159	192.168.200.100	TCP	60	317 - 39022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146	36.780617671	192.168.200.159	192.168.200.100	TCP	74	49446 - 961 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128
147	36.780781025	192.168.200.159	192.168.200.100	TCP	74	51192 - 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128
148	36.780808231	192.168.200.159	192.168.200.100	TCP	60	42642 - 238 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128
149	36.780812411	192.168.200.159	192.168.200.100	TCP	74	41828 - 972 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128
150	36.780889399	192.168.200.159	192.168.200.100	TCP	60	241 - 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151	36.780906540	192.168.200.159	192.168.200.100	TCP	74	41828 - 972 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128
152	36.780955307	192.168.200.159	192.168.200.100	TCP	74	49014 - 137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128
153	36.781116971	192.168.200.159	192.168.200.100	TCP	60	99 - 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
154	36.781116985	192.168.200.159	192.168.200.100	TCP	60	974 - 41828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155	36.781116971	192.168.200.159	192.168.200.100	TCP	60	137 - 49014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
156	36.781138769	192.168.200.100	192.168.200.159	TCP	74	4564 - 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128
157	36.781159927	192.168.200.100	192.168.200.159	TCP	74	42700 - 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=810535444 TSectr=0 WS=128

Dalla quarta immagine deduciamo:

- Qui non succede nulla di "nuovo", ma è fondamentale per il contesto. Conferma che l'attaccante sta eseguendo un **Full Port Scan** (scansione completa). Non si sta limitando alle porte standard; sta cercando *qualsiasi* porta aperta.

No.	Time	Source	Destination	Protocol	Length	Info
157	36.781150972	192.168.200.100	192.168.200.150	TCP	60 423 - 1014 [SYN] Seq=0 Win=61240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535444 TSeqc=0 WS=128	
158	36.781258484	192.168.200.150	192.168.200.100	TCP	60 423 - 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
159	36.781255933	192.168.200.150	192.168.200.100	TCP	60 1814 - 42799 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
160	36.781321958	192.168.200.100	192.168.200.150	TCP	74 55360 - 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535445 TSeqc=0 WS=128	
161	36.781356928	192.168.200.100	192.168.200.150	TCP	74 45648 - 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535445 TSeqc=0 WS=128	
162	36.781378019	192.168.200.100	192.168.200.150	TCP	74 53246 - 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535445 TSeqc=0 WS=128	
163	36.781414036	192.168.200.100	192.168.200.150	TCP	60 423 - 550 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
164	36.781437219	192.168.200.150	192.168.200.100	TCP	74 45424 - 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
165	36.781512468	192.168.200.100	192.168.200.150	TCP	60 45648 - 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSeqval=810535445 TSeqc=4294952466	
166	36.781621871	192.168.200.150	192.168.200.100	TCP	60 354 - 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
167	36.781734510	192.168.200.100	192.168.200.150	TCP	74 55360 - 588 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535445 TSeqc=0 WS=128	
168	36.781734510	192.168.200.150	192.168.200.100	TCP	74 45648 - 512 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
169	36.781812691	192.168.200.150	192.168.200.100	TCP	60 658 - 55186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
170	36.781989537	192.168.200.100	192.168.200.150	TCP	60 45648 - 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSeqval=810535445 TSeqc=4294952466	
171	36.782099082	192.168.200.150	192.168.200.100	TCP	60 663 - 35806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
172	36.782126749	192.168.200.100	192.168.200.150	TCP	74 48212 - 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535445 TSeqc=0 WS=128	
173	36.782140665	192.168.200.100	192.168.200.150	TCP	74 47896 - 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535445 TSeqc=0 WS=128	
174	36.782150050	192.168.200.100	192.168.200.150	TCP	74 48212 - 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535445 TSeqc=0 WS=128	
175	36.782248189	192.168.200.100	192.168.200.150	TCP	74 58396 - 371 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535445 TSeqc=0 WS=128	
176	36.782390780	192.168.200.150	192.168.200.100	TCP	60 681 - 38210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
177	36.782390884	192.168.200.150	192.168.200.100	TCP	60 561 - 47998 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
178	36.782390930	192.168.200.150	192.168.200.100	TCP	60 576 - 32595 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
179	36.782390930	192.168.200.150	192.168.200.100	TCP	60 576 - 38396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
180	36.782422713	192.168.200.150	192.168.200.100	TCP	74 48212 - 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
181	36.782459497	192.168.200.100	192.168.200.150	TCP	74 42102 - 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
182	36.782534412	192.168.200.100	192.168.200.150	TCP	74 55234 - 838 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
183	36.782528077	192.168.200.100	192.168.200.150	TCP	74 33102 - 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
184	36.782600055	192.168.200.150	192.168.200.100	TCP	60 595 - 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
185	36.782600055	192.168.200.100	192.168.200.150	TCP	60 838 - 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
186	36.782690713	192.168.200.150	192.168.200.100	TCP	60 51 - 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
187	36.782690738	192.168.200.150	192.168.200.100	TCP	74 59404 - 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
188	36.782694743	192.168.200.150	192.168.200.100	TCP	60 51 - 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
189	36.782694743	192.168.200.100	192.168.200.150	TCP	74 42102 - 144 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
190	36.782694743	192.168.200.150	192.168.200.100	TCP	74 55234 - 284 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
191	36.783329559	192.168.200.150	192.168.200.100	TCP	60 144 - 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
192	36.783329795	192.168.200.150	192.168.200.100	TCP	60 874 - 42626 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
193	36.783329836	192.168.200.150	192.168.200.100	TCP	60 926 - 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
194	36.783351039	192.168.200.100	192.168.200.150	TCP	74 42626 - 874 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
195	36.783351039	192.168.200.150	192.168.200.100	TCP	74 58110 - 920 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
196	36.783351039	192.168.200.100	192.168.200.150	TCP	74 42626 - 874 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
197	36.783351039	192.168.200.150	192.168.200.100	TCP	74 58110 - 920 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
198	36.783357923	192.168.200.150	192.168.200.100	TCP	60 364 - 42696 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
199	36.783357992	192.168.200.150	192.168.200.100	TCP	60 333 - 57327 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
200	36.783357992	192.168.200.100	192.168.200.150	TCP	74 59404 - 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
201	36.783357992	192.168.200.150	192.168.200.100	TCP	74 59404 - 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
202	36.783357992	192.168.200.100	192.168.200.150	TCP	74 59404 - 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
203	36.783357992	192.168.200.150	192.168.200.100	TCP	74 59404 - 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535446 TSeqc=0 WS=128	
204	36.783575017	192.168.200.150	192.168.200.100	TCP	60 203 - 52872 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
205	36.783575017	192.168.200.100	192.168.200.150	TCP	60 889 - 37888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
206	36.783575017	192.168.200.150	192.168.200.100	TCP	74 57854 - 122 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535447 TSeqc=0 WS=128	
207	36.783575017	192.168.200.100	192.168.200.150	TCP	74 57854 - 122 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535447 TSeqc=0 WS=128	
208	36.783582456	192.168.200.150	192.168.200.100	TCP	60 939 - 56932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
209	36.783582473	192.168.200.150	192.168.200.100	TCP	60 743 - 47472 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
210	36.783588968	192.168.200.100	192.168.200.150	TCP	74 57464 - 237 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535449 TSeqc=0 WS=128	
211	36.783629555	192.168.200.150	192.168.200.100	TCP	74 57464 - 237 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535449 TSeqc=0 WS=128	
212	36.786289955	192.168.200.150	192.168.200.100	TCP	60 821 - 41984 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
213	36.786289978	192.168.200.150	192.168.200.100	TCP	60 122 - 57854 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
214	36.786210019	192.168.200.150	192.168.200.100	TCP	60 237 - 57402 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
215	36.786210059	192.168.200.150	192.168.200.100	TCP	60 33173 - 33178 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
216	36.786455822	192.168.200.150	192.168.200.100	TCP	60 886 - 35164 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
217	36.786455822	192.168.200.100	192.168.200.150	TCP	60 129 - 59734 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
218	36.786455822	192.168.200.150	192.168.200.100	TCP	74 45454 - 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535450 TSeqc=0 WS=128	
219	36.786455822	192.168.200.100	192.168.200.150	TCP	74 45454 - 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535450 TSeqc=0 WS=128	
220	36.786455822	192.168.200.150	192.168.200.100	TCP	74 45454 - 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535450 TSeqc=0 WS=128	
221	36.786455822	192.168.200.100	192.168.200.150	TCP	74 45454 - 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535450 TSeqc=0 WS=128	
222	36.786455822	192.168.200.150	192.168.200.100	TCP	74 45454 - 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535450 TSeqc=0 WS=128	
223	36.786455822	192.168.200.100	192.168.200.150	TCP	74 45454 - 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535450 TSeqc=0 WS=128	
224	36.787023889	192.168.200.150	192.168.200.100	TCP	60 545 - 45416 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
225	36.787023895	192.168.200.150	192.168.200.100	TCP	60 409 - 45414 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
226	36.787069399	192.168.200.150	192.168.200.100	TCP	74 43106 - 769 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535456 TSeqc=0 WS=128	
227	36.787191866	192.168.200.150	192.168.200.100	TCP	60 439 - 38188 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
228	36.787191866	192.168.200.100	192.168.200.150	TCP	60 886 - 37285 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
229	36.787228917	192.168.200.150	192.168.200.100	TCP	74 42406 - 486 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535456 TSeqc=0 WS=128	
230	36.787306501	192.168.200.150	192.168.200.100	TCP	60 769 - 43106 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
231	36.787346317	192.168.200.100	192.168.200.150	TCP	74 49898 - 19 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535451 TSeqc=0 WS=128	
232	36.787476054	192.168.200.100	192.168.200.150	TCP	74 44644 - 848 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535451 TSeqc=0 WS=128	

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth0, id 0

In questa fase della cattura abbiamo identificato un nuovo vettore di attacco specifico:

1. **Servizio Rilevato:** exec (Porta TCP 512).
2. **Stato:** Aperto e raggiungibile.
3. **Implicazione:** Oltre alla vulnerabilità Samba (porte 139/445 trovate prima), l'attaccante ha ora un secondo potenziale punto di ingresso per eseguire comandi arbitrari sul server vittima.

No.	Time	Source	Destination	Protocol	Length	Info
193	36.783329659	192.168.200.100	192.168.200.150	TCP	60 144 - 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
194	36.783329795	192.168.200.150	192.168.200.100	TCP	60 874 - 42269 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
195	36.783329795	192.168.200.150	192.168.200.100	TCP	60 237 - 42269 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
196	36.783329795	192.168.200.100	192.168.200.150	TCP	74 42626 - 874 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535447 TSeqc=0 WS=128	
197	36.7					

2. Serve a confermare che l'attaccante non sta cercando solo servizi specifici, ma sta eseguendo una scansione **volumetrica** (probabilmente un range di 1000 porte o tutte le 65535).
 3. Il volume di traffico "Rifiutato" (Rosso) è un IOC molto forte per i sistemi di rilevamento intrusione (IDS).
-

4. Ipotesi sui Potenziali Vettori di Attacco

Basandosi sulle porte che hanno risposto positivamente alla scansione (status **APERTO**), sono stati individuati i seguenti vettori di attacco che l'attore malevolo potrebbe sfruttare nella fase successiva (Exploitation):

- **Vettore Primario: Vulnerabilità SMB/Samba (Porte 139 e 445)**
 - L'analisi ha confermato che le porte **NetBIOS-SSN (139)** e **Microsoft-DS (445)** sono aperte e raggiungibili.
 - **Ipotesi di Attacco:** Dato che il target è una macchina "Metasploitable", è altamente probabile che esegua una versione obsoleta di Samba. L'attaccante tenterà quasi certamente un exploit RCE (Remote Code Execution), come il noto *Samba "Username Map Script"* (CVE-2007-2447), per ottenere accesso root.
- **Vettore Critico Secondario: Remote Execution (Porta 512)**
 - La scansione ha rilevato la porta **TCP 512** aperta, corrispondente al servizio **exec**.
 - **Ipotesi di Attacco:** Il protocollo rexec è obsoleto, trasmette dati in chiaro e spesso si basa su relazioni di fiducia deboli. La sua presenza offre all'attaccante

una via semplice per l'esecuzione di comandi arbitrari o per attacchi di Brute Force sulle credenziali.

- **Vettori di Enumerazione (Porte 25 e 53)**

- Sono state rilevate aperte le porte **SMTP (25)** e **DNS (53)**. Sebbene meno critiche per una shell immediata, possono essere sfruttate per enumerare gli utenti del sistema (tramite comandi VRFY su SMTP) o mappare la rete interna (tramite Zone Transfer su DNS).
-

5. Azioni Consigliate di Mitigazione e Rimedio

Per ridurre gli impatti dell'attacco attuale e prevenire compromissioni future, si raccomandano le seguenti azioni:

Azioni Immediate (Contenimento)

1. **Blocco IP Attaccante:** Implementare una regola di blocco sul firewall perimetrale per scartare (DROP) tutto il traffico proveniente dall'IP 192.168.200.100.
2. **Isolamento dell'Host:** Disconnettere la macchina 192.168.200.150 dalla rete di produzione per impedire movimenti laterali dell'attaccante verso altri server.

Azioni a Lungo Termine (Prevenzione e Hardening)

1. **Disabilitazione Servizi Obsoleti:** Arrestare e disabilitare immediatamente il servizio exec (porta 512), sostituendolo interamente con SSH configurato in modo sicuro.
2. **Patch Management:** Aggiornare il servizio Samba all'ultima versione stabile supportata. La versione presente su Metasploitable è nota per essere gravemente vulnerabile.

3. **Segmentazione di Rete:** Configurare il firewall per limitare l'accesso alle porte sensibili (139, 445) solo agli IP strettamente necessari e fidati, bloccando l'accesso generico dalla LAN.
4. **Monitoraggio IDS/IPS:** Implementare un sistema di rilevamento intrusioni (es. Snort) configurato per generare alert in caso di pattern di scansione volumetrica (es. soglia di pacchetti SYN/RST superata in un intervallo di tempo ristretto).