

ESERCIZIO S9 L5



Esercizio
Threat Intelligence & IOC

Traccia:

Durante la lezione teorica, abbiamo visto la **Threat Intelligence** e gli indicatori di compromissione.
Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark.
Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare ed analizzare eventuali IOC, ovvero evidenze di **attacchi in corso**
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro



Cattura_U3_W1_L3.pcapng

SVOLGIMENTO

Introduzione

Questo report analizza in dettaglio una cattura di rete, con l'obiettivo di identificare indicatori di compromissione (**IOC**), ipotizzare i **vettori di attacco** e suggerire azioni di **mitigazione**.

Si rileva facilmente il fatto che sono presenti solo **due dispositivi** coinvolti dove il dispositivo con **IP 192.168.200.100** invia pacchetti per lo più **SYN** ricevuti dalla macchina vittima con **IP 192.168.200.150**.

Scenario :

Indirizzo IP dell'attaccante: **192.168.200.100**

Indirizzo IP del bersaglio: **192.168.200.150** (con un sistema identificato come METASPLOITABLE).

Sezioni analizzate:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Worksta
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MS
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 M
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=579
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Le
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=642
8	28.761629461	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	Who has 192.168.200.100? Tell 192.168.200
9	28.761644619	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	Who has 192.168.200.150? Tell 192.168.200
11	28.775230099	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e

Analizzo l'apertura della cattura : L'attaccante avvia una scansione **TCP**. I pacchetti 23 inviano richieste **[SYN]** al bersaglio. I pacchetti da 4 a 7 mostrano le risposte di una scansione "half-open" con **[SYN, ACK]** del bersaglio e un **[RST, ACK]** dell'attaccante e del bersaglio.

La porta **80** risulta aperta in quanto il bersaglio risponde col SYN ACK (pacchetto 4) e l'attaccante conferma la comunicazione con l' ACK (pacchetto 6)

RST = è un segnale del protocollo TCP che chiude le comunicazioni quando qualcosa non va. *Per esempio: pacchetto arrivato su una porta dove non c'è nessun servizio.* Interrompe quindi le comunicazioni e può essere utilizzato per condurre un attacco RST Flood.

Un **RST flood** è un attacco in cui un aggressore invia **tantissimi** pacchetti TCP con il flag RST verso una vittima o verso endpoint di comunicazione. L'effetto può essere:

Interrompere connessioni legittime (client-server) facendo chiudere sessioni importanti.

Creare instabilità nelle applicazioni (drop di sessioni, riconessioni continue).

Sovraccaricare le risorse di rete o dei dispositivi che devono processare e registrare tutti quei pacchetti.

Spesso l'attaccante **spoofa** (falsifica) gli indirizzi sorgente, così è difficile risalire alla fonte e le risposte finiscono altrove.

Un'analisi più approfondita mostra anche **pacchetti ARP (Address Resolution Protocol)**. L'attaccante sta usando i pacchetti ARP per scoprire l'indirizzo MAC (livello 2) del bersaglio partendo dal suo indirizzo IP (livello 3).

Questo è un passo fondamentale prima di avviare la scansione TCP, in quanto l'attaccante ha bisogno dell'indirizzo MAC per inviare i pacchetti a livello fisico.

No.	Time	Source	Destination	Protocol	Length	Info
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	36.776179338	192.168.200.100	192.168.200.150	TCP	74	50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
43	36.776233000	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 TSval=810535440 TSecr=0 WS=128
45	36.776385094	192.168.200.100	192.168.200.150	TCP	74	33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
46	36.776402508	192.168.200.100	192.168.200.150	TCP	74	48014 → 250 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
47	36.776451024	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	36.776478281	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 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=1 TSval=810535440 TSecr=0 WS=128
52	36.776568896	192.168.200.100	192.168.200.150	TCP	74	49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 TSval=810535440 TSecr=0 WS=128
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	34898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 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=1 TSval=4294952466 TSecr=810535440 WS=64
58	36.776934022	192.168.200.150	192.168.200.100	TCP	60	250 → 48014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36.776949061	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=1 TSval=4294952466 TSecr=810535440 WS=64
60	36.776959004	192.168.200.150	192.168.200.100	TCP	60	143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776959043	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=1 TSval=4294952466 TSecr=810535440 WS=64
62	36.776959082	192.168.200.150	192.168.200.100	TCP	60	110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776959123	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=1 TSval=4294952466 TSecr=810535440 WS=64
64	36.776959162	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	36.777143014	192.168.200.100	192.168.200.150	TCP	74	50990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
71	36.777186821	192.168.200.100	192.168.200.150	TCP	74	35638 → 430 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 TSval=810535441 TSecr=0 WS=128
73	36.777379334	192.168.200.100	192.168.200.150	TCP	74	49780 → 71 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
74	36.777430032	192.168.200.150	192.168.200.100	TCP	60	707 → 50990 [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	36.777473010	192.168.200.100	192.168.200.150	TCP	74	36138 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
77	36.777522484	192.168.200.100	192.168.200.150	TCP	74	52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
78	36.777623032	192.168.200.150	192.168.200.100	TCP	60	962 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	76 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

La scansione continua con lo stesso metodo. L'attaccante continua a testare un'ampia gamma di porte, confermato dal susseguirsi di richieste **[SYN]** e risposte **[RST]** per le porte chiuse.

Le righe **65-68** mostrano un **ACK Scan**, dove l'attaccante sta testando i filtri del firewall inviando pacchetti **[ACK]** a porte comuni come **445(SMB)** e **139 (NetBios)**.

No.	Time	Source	Destination	Protocol	Length	Info
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	36.777645927	192.168.200.100	192.168.200.150	TCP	74	41874 - 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535441 TSecr=0 WS=128
81	36.777690309	192.168.200.100	192.168.200.150	TCP	74	51569 - 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535441 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	36.777817245	192.168.200.150	192.168.200.100	TCP	60	764 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777817293	192.168.200.150	192.168.200.100	TCP	60	435 - 51569 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66	33842 - 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=818535441 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 Tsva=818535441 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 Tsva=818535441 TSecr=4294952466
89	36.778031505	192.168.200.100	192.168.200.150	TCP	66	37282 - 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=818535441 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=1 Tsva=818535441 TSecr=0 WS=128
91	36.778209161	192.168.200.100	192.168.200.150	TCP	74	48448 - 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535441 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=1 Tsva=818535441 TSecr=0 WS=128
93	36.778385946	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	886 - 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.778449484	192.168.200.150	192.168.200.100	TCP	60	221 - 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96	36.778452791	192.168.200.100	192.168.200.150	TCP	74	42420 - 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535442 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=1 Tsva=818535442 TSecr=0 WS=128
98	36.778614995	192.168.200.100	192.168.200.150	TCP	74	54282 - 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535442 TSecr=0 WS=128
99	36.778635364	192.168.200.150	192.168.200.100	TCP	60	1007 - 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100	36.778721888	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	48318 - 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535442 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=1 Tsva=818535442 TSecr=0 WS=128
103	36.778823234	192.168.200.150	192.168.200.100	TCP	60	311 - 51276 [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 Tsva=818535442 TSecr=0 WS=128
105	36.778939327	192.168.200.150	192.168.200.100	TCP	60	392 - 48318 [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	36.779035153	192.168.200.100	192.168.200.150	TCP	74	41231 - 44 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535442 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=1 Tsva=818535442 TSecr=0 WS=128
110	36.779122220	192.168.200.150	192.168.200.100	TCP	60	807 - 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	36.779145084	192.168.200.100	192.168.200.150	TCP	74	49138 - 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535442 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	43148 - 234 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535443 TSecr=0 WS=128
114	36.779309462	192.168.200.150	192.168.200.100	TCP	74	46886 - 166 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535443 TSecr=0 WS=128
115	36.779345464	192.168.200.100	192.168.200.150	TCP	60	948 - 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116	36.779378638	192.168.200.100	192.168.200.150	TCP	74	50284 - 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535443 TSecr=0 WS=128
117	36.779397023	192.168.200.100	192.168.200.150	TCP	74	51262 - 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535443 TSecr=0 WS=128
118	36.779505548	192.168.200.150	192.168.200.100	TCP	60	214 - 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

La scansione prosegue con un ritmo elevato. L'attaccante sta eseguendo una scansione estesa e automatizzata su un ampio range di porte.

Le righe dominanti, colorate di rosso, indicano che la maggior parte delle porte testate sono chiuse (**RST,ACK** e nessuna risposta al SYN che segnala la presenza di un blocco o filtro). Questo permette all'attaccante di **delimitare** rapidamente i potenziali obiettivi, **escludendo le porte non attive**.

No.	Time	Source	Destination	Protocol	Length	Info
118	36.779695648	192.168.200.150	192.168.200.100	TCP	60	214 - 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	36.779695759	192.168.200.150	192.168.200.100	TCP	60	186 - 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120	36.779695798	192.168.200.150	192.168.200.100	TCP	60	186 - 50204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	36.779695843	192.168.200.150	192.168.200.100	TCP	60	884 - 51262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122	36.779637573	192.168.200.100	192.168.200.150	TCP	74	44244 - 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535443 TSecr=0 WS=128
123	36.779762088	192.168.200.100	192.168.200.150	TCP	74	43630 - 703 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535443 TSecr=0 WS=128
124	36.779855044	192.168.200.150	192.168.200.100	TCP	60	659 - 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	36.779911109	192.168.200.100	192.168.200.150	TCP	74	55138 - 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535443 TSecr=0 WS=128
126	36.779946174	192.168.200.100	192.168.200.150	TCP	74	48522 - 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535443 TSecr=0 WS=128
127	36.780035851	192.168.200.150	192.168.200.100	TCP	60	703 - 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128	36.780121127	192.168.200.150	192.168.200.100	TCP	60	274 - 55138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129	36.780143472	192.168.200.100	192.168.200.150	TCP	74	57552 - 518 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535443 TSecr=0 WS=128
130	36.780170333	192.168.200.100	192.168.200.150	TCP	74	48822 - 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535443 TSecr=0 WS=128
131	36.780215176	192.168.200.150	192.168.200.100	TCP	60	42 - 48522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132	36.780301760	192.168.200.150	192.168.200.100	TCP	60	58 - 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133	36.780325337	192.168.200.100	192.168.200.150	TCP	74	3752 - 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535444 TSecr=0 WS=128
134	36.780346429	192.168.200.100	192.168.200.150	TCP	74	46648 - 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535444 TSecr=0 WS=128
135	36.780409918	192.168.200.100	192.168.200.150	TCP	74	36548 - 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535444 TSecr=0 WS=128
136	36.780427899	192.168.200.100	192.168.200.150	TCP	74	38866 - 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535444 TSecr=0 WS=128
137	36.780472838	192.168.200.100	192.168.200.150	TCP	74	52136 - 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535444 TSecr=0 WS=128
138	36.780490897	192.168.200.100	192.168.200.150	TCP	74	38822 - 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535444 TSecr=0 WS=128
139	36.780577888	192.168.200.150	192.168.200.100	TCP	60	266 - 48822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	36.780577891	192.168.200.150	192.168.200.100	TCP	60	11 - 3752 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	36.780578026	192.168.200.150	192.168.200.100	TCP	60	235 - 46648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142	36.780578074	192.168.200.150	192.168.200.100	TCP	60	739 - 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143	36.780578119	192.168.200.150	192.168.200.100	TCP	60	55 - 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144	36.780578158	192.168.200.150	192.168.200.100	TCP	60	999 - 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145	36.780578198	192.168.200.150	192.168.200.100	TCP	60	317 - 38822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146	36.780617071	192.168.200.100	192.168.200.150	TCP	74	49446 - 961 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535444 TSecr=0 WS=128
147	36.780761025	192.168.200.100	192.168.200.150	TCP	74	51192 - 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535444 TSecr=0 WS=128
148	36.780805109	192.168.200.150	192.168.200.100	TCP	60	961 - 49446 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149	36.780824710	192.168.200.100	192.168.200.150	TCP	74	42642 - 593 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535444 TSecr=0 WS=128
150	36.780889399	192.168.200.150	192.168.200.100	TCP	60	241 - 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151	36.780906549	192.168.200.100	192.168.200.150	TCP	74	41828 - 974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535444 TSecr=0 WS=128
152	36.780950307	192.168.200.100	192.168.200.150	TCP	74	49014 - 137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535444 TSecr=0 WS=128
153	36.781007559	192.168.200.150	192.168.200.100	TCP	60	293 - 42642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
154	36.781116869	192.168.200.150	192.168.200.100	TCP	60	974 - 41828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155	36.781116971	192.168.200.150	192.168.200.100	TCP	60	137 - 49014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
156	36.781158109	192.168.200.100	192.168.200.150	TCP	74	45544 - 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535444 TSecr=0 WS=128
157	36.781159927	192.168.200.100	192.168.200.150	TCP	74	42700 - 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsva=818535444 TSecr=0 WS=128

La scansione continua. L'attaccante sta procedendo in modo sistematico, testando un vasto intervallo di porte. Le risposte **[RST,ACK]** come nella riga 119 indicano che le porte sono chiuse. L'attaccante sta metodicamente mappando la rete del bersaglio per completare la sua fase di ricognizione.

No.	Time	Source	Destination	Protocol	Length	Info
157	36.781159927	192.168.200.100	192.168.200.150	TCP	74	42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
158	36.781255484	192.168.200.150	192.168.200.100	TCP	60	223 → 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
159	36.781259593	192.168.200.150	192.168.200.100	TCP	60	1914 → 42700 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
160	36.781321950	192.168.200.100	192.168.200.150	TCP	74	55360 → 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=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 TSval=810535445 TSecr=0 WS=128
162	36.781420319	192.168.200.100	192.168.200.150	TCP	74	53240 → 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
163	36.781497105	192.168.200.150	192.168.200.100	TCP	60	918 → 55360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535445 WS=64
165	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
166	36.781613154	192.168.200.150	192.168.200.100	TCP	60	55360 → 53240 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
167	36.781648101	192.168.200.100	192.168.200.150	TCP	74	55180 → 858 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
168	36.781734418	192.168.200.100	192.168.200.150	TCP	74	35800 → 663 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
169	36.781844001	192.168.200.150	192.168.200.100	TCP	60	663 → 55180 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170	36.781898937	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
171	36.782069902	192.168.200.150	192.168.200.100	TCP	60	663 → 35800 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172	36.782120740	192.168.200.100	192.168.200.150	TCP	74	35210 → 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
173	36.782140866	192.168.200.100	192.168.200.150	TCP	74	47090 → 501 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
174	36.782215091	192.168.200.100	192.168.200.150	TCP	74	32950 → 570 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
175	36.782248180	192.168.200.100	192.168.200.150	TCP	74	38390 → 371 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
176	36.782390780	192.168.200.150	192.168.200.100	TCP	60	681 → 35210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177	36.782398084	192.168.200.150	192.168.200.100	TCP	60	501 → 47090 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
178	36.782398930	192.168.200.150	192.168.200.100	TCP	60	570 → 32950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
179	36.782399978	192.168.200.150	192.168.200.100	TCP	60	371 → 38390 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
180	36.782422713	192.168.200.100	192.168.200.150	TCP	74	43002 → 906 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
181	36.782459487	192.168.200.100	192.168.200.150	TCP	74	42102 → 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=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 TSval=810535446 TSecr=0 WS=128
183	36.782552077	192.168.200.100	192.168.200.150	TCP	74	33102 → 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
184	36.782600930	192.168.200.150	192.168.200.100	TCP	60	595 → 43002 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
185	36.782606055	192.168.200.150	192.168.200.100	TCP	60	595 → 42102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186	36.782606713	192.168.200.150	192.168.200.100	TCP	60	838 → 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
187	36.782618058	192.168.200.100	192.168.200.150	TCP	74	53004 → 501 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
188	36.782854473	192.168.200.150	192.168.200.100	TCP	60	51 → 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
189	36.782887993	192.168.200.100	192.168.200.150	TCP	74	41104 → 144 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
190	36.783020102	192.168.200.150	192.168.200.100	TCP	60	50 → 59484 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
191	36.783042408	192.168.200.100	192.168.200.150	TCP	74	42020 → 874 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
192	36.783084243	192.168.200.100	192.168.200.150	TCP	74	58110 → 920 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
193	36.783329650	192.168.200.150	192.168.200.100	TCP	60	144 → 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
194	36.783329705	192.168.200.150	192.168.200.100	TCP	60	874 → 42020 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
195	36.783372830	192.168.200.150	192.168.200.100	TCP	60	920 → 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
196	36.783391839	192.168.200.100	192.168.200.150	TCP	74	42090 → 964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535447 TSecr=0 WS=128

Questa cattura rivela che l'attaccante ha identificato un obiettivo specifico e sta testando una porta non comune.

Il punto chiave è il **pacchetto 165**. L'attaccante ha inviato un pacchetto **[SYN]** alla porta di destinazione **512**. La risposta del bersaglio, un pacchetto **[SYN, ACK]**, conferma che la porta **512 è aperta e in ascolto**.

La porta **TCP 512** è assegnata al servizio chiamato **exec** (noto anche come **rexec**, Remote Execution). È un vecchio servizio Unix che permetteva a un utente di far eseguire comandi su una macchina remota: il client si connette e invia credenziali + comando, il server (**rexecd**) esegue il comando e rimanda indietro l'output.

Come funziona

Il client apre una connessione TCP verso la porta 512 del server.

Invia al server nome utente e password (testo in chiaro) e il comando da eseguire.

Se l'autenticazione va a buon fine, il server avvia il comando e inoltra standard input/output/error sulla connessione.

Il fatto che venga scansionata una porta così specifica e obsoleta suggerisce che l'attaccante stia cercando **vulnerabilità** in sistemi **non aggiornati** o configurati in modo non sicuro.

Indicando che la porta è aperta, viene offerto un potenziale punto di ingresso per l'esecuzione di comandi da remoto che probabilmente l'attaccante potrà sfruttare.

No.	Time	Source	Destination	Protocol	Length	Info
193	36.783329650	192.168.200.150	192.168.200.100	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 → 42620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
195	36.783329830	192.168.200.150	192.168.200.100	TCP	60	920 → 50110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
196	36.783330330	192.168.200.100	192.168.200.150	TCP	74	42650 → 904 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535447 TSecr=0 WS=128
197	36.783426736	192.168.200.100	192.168.200.150	TCP	74	57372 → 333 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535447 TSecr=0 WS=128
198	36.783557923	192.168.200.150	192.168.200.100	TCP	60	964 → 42690 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
199	36.783557992	192.168.200.150	192.168.200.100	TCP	60	353 → 57372 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
200	36.783557956	192.168.200.100	192.168.200.150	TCP	74	57372 → 253 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535449 TSecr=0 WS=128
201	36.785443154	192.168.200.100	192.168.200.150	TCP	74	37880 → 880 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535449 TSecr=0 WS=128
202	36.785551331	192.168.200.100	192.168.200.150	TCP	74	59932 → 939 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535449 TSecr=0 WS=128
203	36.785624018	192.168.200.100	192.168.200.150	TCP	74	47472 → 743 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535449 TSecr=0 WS=128
204	36.785675017	192.168.200.150	192.168.200.100	TCP	60	203 → 52872 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
205	36.785675093	192.168.200.150	192.168.200.100	TCP	60	880 → 37880 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
206	36.785721042	192.168.200.100	192.168.200.150	TCP	74	41984 → 831 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535449 TSecr=0 WS=128
207	36.785723953	192.168.200.100	192.168.200.150	TCP	74	57054 → 122 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535449 TSecr=0 WS=128
208	36.785824050	192.168.200.150	192.168.200.100	TCP	60	939 → 59932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
209	36.785824723	192.168.200.150	192.168.200.100	TCP	60	743 → 47472 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
210	36.785880908	192.168.200.100	192.168.200.150	TCP	74	57402 → 237 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535449 TSecr=0 WS=128
211	36.785943368	192.168.200.100	192.168.200.150	TCP	74	33710 → 359 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535449 TSecr=0 WS=128
212	36.786299855	192.168.200.150	192.168.200.100	TCP	60	831 → 41984 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
213	36.786299878	192.168.200.150	192.168.200.100	TCP	60	122 → 57054 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
214	36.786210619	192.168.200.150	192.168.200.100	TCP	60	237 → 57402 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
215	36.786210609	192.168.200.150	192.168.200.100	TCP	60	359 → 33710 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
216	36.786254145	192.168.200.100	192.168.200.150	TCP	74	35164 → 580 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535449 TSecr=0 WS=128
217	36.786292420	192.168.200.100	192.168.200.150	TCP	74	59734 → 129 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535450 TSecr=0 WS=128
218	36.786455822	192.168.200.150	192.168.200.100	TCP	60	580 → 35164 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
219	36.786455938	192.168.200.150	192.168.200.100	TCP	60	129 → 59734 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
220	36.786768894	192.168.200.100	192.168.200.150	TCP	74	45416 → 545 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535450 TSecr=0 WS=128
221	36.786815129	192.168.200.100	192.168.200.150	TCP	74	45154 → 400 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535450 TSecr=0 WS=128
222	36.786864504	192.168.200.100	192.168.200.150	TCP	74	38100 → 239 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535450 TSecr=0 WS=128
223	36.786899954	192.168.200.100	192.168.200.150	TCP	74	37952 → 520 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535450 TSecr=0 WS=128
224	36.787023089	192.168.200.150	192.168.200.100	TCP	60	545 → 45416 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
225	36.787023195	192.168.200.150	192.168.200.100	TCP	60	400 → 45154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
226	36.787060911	192.168.200.100	192.168.200.150	TCP	74	43106 → 769 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535450 TSecr=0 WS=128
227	36.787191086	192.168.200.150	192.168.200.100	TCP	60	239 → 38100 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
228	36.787191781	192.168.200.150	192.168.200.100	TCP	60	520 → 37952 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
229	36.787229017	192.168.200.100	192.168.200.150	TCP	74	42468 → 489 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535450 TSecr=0 WS=128
230	36.787229091	192.168.200.150	192.168.200.100	TCP	60	489 → 42468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
231	36.787346317	192.168.200.100	192.168.200.150	TCP	74	43988 → 19 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535451 TSecr=0 WS=128
232	36.787470054	192.168.200.100	192.168.200.150	TCP	74	44644 → 846 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tval=810535451 TSecr=0 WS=128

L'attaccante sta completando la sua scansione. La grande quantità di pacchetti e la ripetizione del comportamento dimostrano che si tratta di un'azione sistematica e automatizzata. La scansione ha fornito all'attaccante una mappa completa delle porte aperte e chiuse del bersaglio, che ora userà per pianificare il suo prossimo passo, che sarà probabilmente l'attacco effettivo.

Utilizzo filtri Wireshark:

Scelgo di utilizzare il filtro di Wireshark per visualizzare i SYN/ACK quindi le risposte che indicano che la porta interessata è aperta:

tcp.flags.syn == 1 && tcp.flags.ack == 1

No.	Time	Source	Destination	Protocol	Length	Info
4	23.674777393	192.168.200.150	192.168.200.100	TCP	74	80 → 53069 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tval=4294951165 TSecr=810522427 WS=64
19	36.774685505	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 Tval=4294952466 TSecr=810535437 WS=64
20	36.774685052	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 Tval=4294952466 TSecr=810535437 WS=64
27	36.778141273	192.168.200.150	192.168.200.100	TCP	74	22 → 55556 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tval=4294952466 TSecr=810535438 WS=64
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55556 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tval=4294952466 TSecr=810535439 WS=64
36	36.775797004	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 Tval=4294952466 TSecr=810535439 WS=64
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445 → 33642 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tval=4294952466 TSecr=810535440 WS=64
59	36.776904981	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 Tval=4294952466 TSecr=810535440 WS=64
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 Tval=4294952466 TSecr=810535440 WS=64
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 Tval=4294952466 TSecr=810535440 WS=64
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tval=4294952466 TSecr=810535445 WS=64
267	36.788059449	192.168.200.150	192.168.200.100	TCP	74	514 → 51396 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tval=4294952467 TSecr=810535452 WS=64
994	36.825722553	192.168.200.150	192.168.200.100	TCP	74	513 → 42048 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tval=4294952471 TSecr=810535489 WS=64

Porte aperte : 20, 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514.

Servizi e Valutazione del Rischio

- **Porta 20/21 - FTP (File Transfer Protocol)**

Descrizione: Utilizzato per il trasferimento di file. Spesso configurato in modo insicuro.

Rischio: Se l'autenticazione è debole (ad esempio, l'uso di credenziali predefinite o anonime), un attaccante potrebbe caricare o scaricare file, inclusi potenziali **malware** o **backdoor**. Le versioni obsolete del server FTP possono avere vulnerabilità note.

- **Porta 22 - SSH (Secure Shell)**

Descrizione: Un protocollo crittografato per l'accesso remoto. È considerato sicuro.

Rischio: Nonostante sia sicuro, un attaccante può tentare un attacco brute-force se la password è debole o se l'autenticazione basata su chiavi non è implementata correttamente.

- **Porta 23 - Telnet**

Descrizione: Un protocollo obsoleto per l'accesso remoto.

Rischio: Estremamente alto. Telnet trasmette tutte le informazioni, inclusi nome utente e password, in chiaro. Un attaccante che intercetta il traffico può rubare le credenziali.

- **Porta 25 - SMTP (Simple Mail Transfer Protocol)**

Descrizione: Utilizzato per l'invio di email.

Rischio: Se non è configurato correttamente, può essere sfruttato per inviare email di spam o phishing.

- **Porta 53 - DNS (Domain Name System)**

Descrizione: Traduce nomi di dominio in indirizzi IP.

Rischio: Se il server DNS è mal configurato, può essere vulnerabile a attacchi di cache poisoning, che reindirizzano gli utenti a siti malevoli, o può essere utilizzato per attacchi DDoS.

- **Porta 80 - HTTP (Hypertext Transfer Protocol)**

Descrizione: Il protocollo base per la navigazione web.

Rischio: Le vulnerabilità qui dipendono dal server web (es. Apache) e dalle applicazioni (es. CMS come WordPress). Un attaccante può cercare vulnerabilità note (come **SQL injection** o **Cross-Site Scripting**) o tentare di sfruttare versioni obsolete del software.

- **Porta 111 - RPC (Remote Procedure Call)**

Descrizione: Permette a un programma di eseguire codice su un sistema remoto.

Rischio: Un servizio che necessita di una stretta gestione della sicurezza. Se mal configurato, può essere sfruttato ottenere il controllo del sistema.

- **Porte 139 (NetBIOS) e 445 (SMB/CIFS)**

Descrizione: Protocolli per la condivisione di file e stampanti in ambienti Windows.

Rischio: Elevato. Queste porte sono state storicamente l'obiettivo di attacchi critici come quello del worm **WannaCry**. Se il sistema non è patchato, un attaccante può facilmente ottenere il controllo.

- **Porte 512 (Exec), 513 (Rlogin), 514 (Rshell)**

Descrizione: Servizi obsoleti per l'esecuzione di comandi remoti.

Rischio: Estremamente alto. Simili a Telnet, questi servizi trasmettono **dati in chiaro** e non prevedono **meccanismi di autenticazione robusti**. L'attaccante può tentare l'esecuzione di comandi da remoto, ottenendo il controllo totale del sistema. La presenza di questi servizi su un sistema esposto indica una grave lacuna di sicurezza.

Ipotesi sui Potenziali Vettori di Attacco Utilizzati

L'attaccante sta eseguendo un'attività di ricognizione per aggirare le difese e preparare la fase di exploitation.

Vettore di Attacco 1: Nmap -sT >>> esegue una scansione TCP connect.

L'attaccante invia pacchetti **[SYN]** al bersaglio. Quando una porta è aperta, il bersaglio risponde con un **[SYN, ACK]**, e l'attaccante risponde subito con un **[RST]**. Questo comportamento gli permette di identificare le porte aperte senza apparire nei log di connessione del bersaglio, rendendo la scansione difficile da rilevare. L'attaccante sta cercando servizi specifici, per trovare potenziali punti di ingresso.

Vettore di Attacco 2: Nmap -sA >>> ACK Scan L'attaccante invia pacchetti con il solo flag **[ACK]** a porte note (come la **445** per **SMB** e la **139** per **NetBIOS**). Questo non ha lo scopo di scoprire se le porte sono aperte, ma di capire se sono filtrate da un firewall.

Se riceve un [RST], la porta è considerata **"non filtrata"** (il firewall non la blocca, anche se il servizio è inattivo).

Se non riceve alcuna risposta, la porta è **"filtrata"** (il firewall la sta bloccando attivamente).

Attacco DoS - RST Flood : La presenza di 47 richieste SYN dalla riga 1196 a 1243 mi ha fatto pensare ad un piccolo test di DoS, quasi come per verificare la reazione e capire se quel tipo di attacco possa funzionare in futuro. Rimane comunque veramente poco probabile non essendo presente lo spoofing dell'IP e date le poche richieste inviate.

Indicatori di compromissione (IOC)

IP Malevolo: **192.168.200.100**

IP Vittima: **192.168.200.150**

Tecnica Usata: **Invio pacchetti TCP**

L'attaccante ha tentato di sfruttare il three way handshake TCP + invio di pacchetti RST di chiusura immediata + ACK

Azioni Consigliate per la Mitigazione

Azione Immediata: Bloccare l'indirizzo IP dell'attaccante (**192.168.200.100**) a livello del firewall.

Mitigazione a Lungo Termine:

Implementare un IDS/IPS: Un sistema di rilevamento e prevenzione delle intrusioni (IDS/IPS)

Disabilitare tutti i servizi non necessari, specialmente quelli obsoleti e insicuri come **exec** (porta 512). Questo riduce drasticamente la superficie di attacco.

Mantenere tutti i sistemi e le applicazioni aggiornati per correggere le vulnerabilità note.

Rivedere e rafforzare le regole del firewall, in particolare per le porte esposte verso l'esterno, assicurandosi che il traffico non necessario sia filtrato.

CONCLUSIONE

Per concludere, l'analisi del traffico di rete ha rivelato un'attività di ricognizione da parte dell'attaccante.

L'attaccante ha utilizzato una combinazione di due diverse tecniche di scansione utilizzando **nmap**.

L'attaccante sta cercando attivamente di aggirare le difese del bersaglio. La scoperta di servizi obsoleti e insicuri come **exec** (**porta 512**) indica l'obiettivo di sfruttare vulnerabilità note per ottenere l'accesso remoto al sistema.

Le azioni di mitigazione, come il blocco immediato dell'IP dell'attaccante, l'installazione di un IDS/IPS e l'**hardening del sistema**, sono fondamentali per prevenire che questa fase di ricognizione si trasformi in un attacco riuscito.