

Threat Intelligence & IOC

Introduzione

Il presente documento ha lo scopo di analizzare un file di cattura di rete (.pcapng) per identificare potenziali attività malevole intercorse tra due host. L'analisi è stata condotta in ambiente virtualizzato Kali Linux utilizzando il software Wireshark per l'ispezione profonda dei pacchetti.

Obiettivi dell'analisi

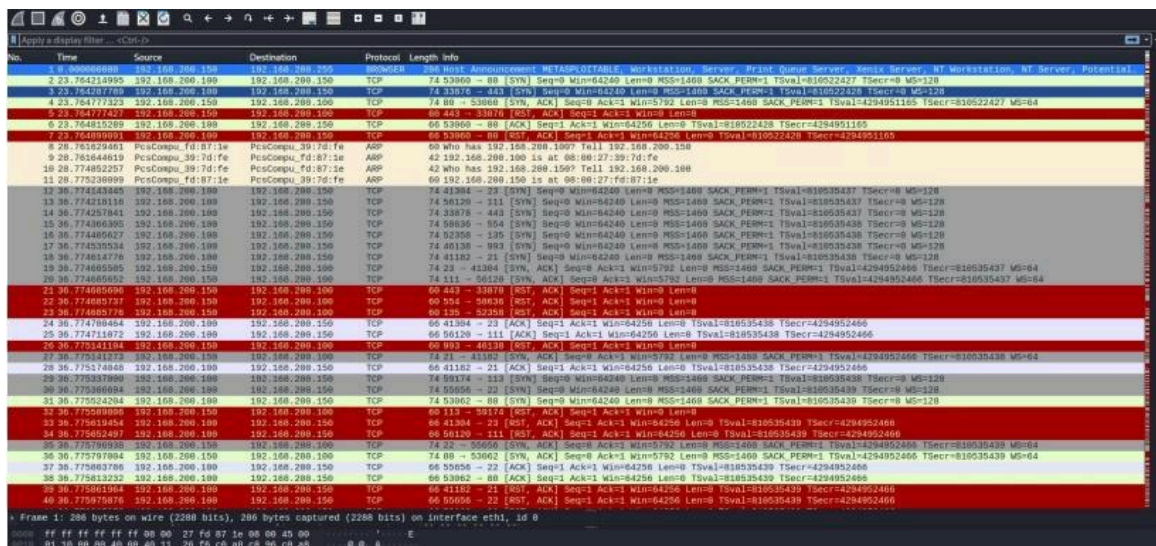
- Identificare gli host coinvolti (Attaccante e Vittima)
- Rilevare anomalie nel traffico di rete
- Isolare gli Indicatori di Compromissione (IOC)
- Mappare i servizi esposti e vulnerabili

Analisi dei Flussi e Identificazione Host

Dall'analisi preliminare dei log, è stato possibile distinguere i ruoli dei dispositivi nella rete:

Indirizzo IP Attaccante (Source): **192.168.200.100**

Indirizzo IP Vittima (Destination): **192.168.200.150**



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.200.150	192.168.200.150	ARP	60	Host 192.168.200.150 is at 08:00:27:1f:07:1e
2	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810522428 TSecr=0 MS=128
3	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810522428 TSecr=0 MS=128
4	0.000000	192.168.200.150	192.168.200.150	TCP	74	88 -> 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810522427 MS=64
5	0.000000	192.168.200.150	192.168.200.150	TCP	66	53060 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
6	0.000000	192.168.200.150	192.168.200.150	TCP	66	53060 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	0.000000	192.168.200.150	192.168.200.150	TCP	66	53060 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	0.000000	PcCompu.f0:07:1e	PcCompu.f0:07:1e	ARP	60	Who has 192.168.200.150? Tell 192.168.200.150
9	0.000000	PcCompu.f0:07:1e	PcCompu.f0:07:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.150
10	0.000000	PcCompu.f0:07:1e	PcCompu.f0:07:1e	ARP	60	Who has 192.168.200.150? Tell 192.168.200.150
11	0.000000	PcCompu.f0:07:1e	PcCompu.f0:07:1e	ARP	60	Who has 192.168.200.150? Tell 192.168.200.150
12	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
13	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
14	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
15	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
16	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
17	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
18	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
19	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
20	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
21	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
22	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
23	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
24	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
25	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
26	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
27	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
28	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
29	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
30	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
31	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
32	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
33	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
34	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
35	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
36	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
37	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
38	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
39	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128
40	0.000000	192.168.200.150	192.168.200.150	TCP	74	53060 -> 80 [ACK] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 MS=128

Broadcast iniziale e identificazione sistema

Il log iniziale (Riga 0) mostra un messaggio **broadcast** che identifica la macchina come "**Metasploitable**", un sistema volutamente vulnerabile utilizzato per test di sicurezza. *Traffico iniziale e scambi ARP tra attaccante e vittima*

Risoluzione indirizzi (ARP)

Nelle righe da 8 a 11, si osserva traffico **ARP (Address Resolution Protocol)**, necessario alle macchine per identificare i rispettivi indirizzi MAC e iniziare la comunicazione a livello 2 del modello OSI.

Analisi dell'Attacco: Scansione Porte

L'anomalia principale è rappresentata da una raffica di pacchetti TCP con flag **[SYN]** inviati dall'attaccante verso la vittima in un brevissimo lasso di tempo (pochi millisecondi).

No.	Time	Source	Destination	Protocol	Length	Info
118	36.779605648	192.168.200.150	192.168.200.100	TCP	60	214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	36.779605750	192.168.200.150	192.168.200.100	TCP	60	186 → 40880 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120	36.779605790	192.168.200.150	192.168.200.100	TCP	60	138 → 50284 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	36.779605843	192.168.200.150	192.168.200.100	TCP	60	984 → 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 TSval=810535443 TSecr=0 WS=128
123	36.779776208	192.168.200.100	192.168.200.150	TCP	74	43638 → 703 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
124	36.779805041	192.168.200.150	192.168.200.100	TCP	60	852 → 42244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	36.779911109	192.168.200.100	192.168.200.150	TCP	74	55136 → 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
126	36.779946174	192.168.200.100	192.168.200.150	TCP	74	40522 → 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
127	36.780035051	192.168.200.150	192.168.200.100	TCP	60	703 → 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128	36.780221121	192.168.200.150	192.168.200.100	TCP	60	274 → 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129	36.780448475	192.168.200.150	192.168.200.100	TCP	74	51552 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
130	36.780170333	192.168.200.100	192.168.200.150	TCP	74	40822 → 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
131	36.780215176	192.168.200.150	192.168.200.100	TCP	60	42 → 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132	36.780301750	192.168.200.100	192.168.200.150	TCP	60	58 → 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133	36.780325231	192.168.200.150	192.168.200.100	TCP	74	37252 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
134	36.780346429	192.168.200.100	192.168.200.150	TCP	74	40648 → 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
135	36.780409018	192.168.200.100	192.168.200.150	TCP	74	36548 → 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
136	36.780427899	192.168.200.100	192.168.200.150	TCP	74	38868 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
137	36.780472836	192.168.200.100	192.168.200.150	TCP	74	52136 → 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
138	36.780490897	192.168.200.100	192.168.200.150	TCP	74	30822 → 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
139	36.780577080	192.168.200.150	192.168.200.100	TCP	60	206 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	36.780577985	192.168.200.150	192.168.200.100	TCP	60	11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	36.780578026	192.168.200.150	192.168.200.100	TCP	60	235 → 40648 [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 → 38868 [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	36.780578190	192.168.200.150	192.168.200.100	TCP	60	317 → 30822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146	36.780621774	192.168.200.100	192.168.200.150	TCP	74	43440 → 951 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
147	36.780701625	192.168.200.100	192.168.200.150	TCP	74	51192 → 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
148	36.780805705	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 → 293 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
150	36.780830192	192.168.200.150	192.168.200.100	TCP	60	241 → 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151	36.780900540	192.168.200.100	192.168.200.150	TCP	74	41928 → 974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 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 TSval=810535444 TSecr=0 WS=128
153	36.781070559	192.168.200.150	192.168.200.100	TCP	60	293 → 42642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
154	36.781118860	192.168.200.150	192.168.200.100	TCP	60	974 → 41928 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155	36.781118971	192.168.200.150	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	192.168.200.150	TCP	74	45464 → 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 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 TSval=810535444 TSecr=0 WS=128

Sequenza di pacchetti SYN durante la fase di port scanning

Caratteristiche dell'attacco

Questa attività è classificabile come **Port Scan**, presumibilmente eseguito tramite il tool **Nmap**. L'attaccante non sta scansionando tutte le porte sequenzialmente, ma mira alle porte "Well-Known" (es. 21, 22, 23, 25, 53, 80, 111, 139, 445), suggerendo l'uso di un comando di scansione veloce.

Risposta del sistema target

Analizzando le risposte della vittima, possiamo distinguere i servizi attivi da quelli inattivi:

- **Porte Chiuse (Closed):** La vittima risponde con un pacchetto **[RST, ACK]** (Reset). Questo indica che nessun servizio è in ascolto su quella porta.

- **Porte Aperte (Open):** La vittima risponde con **[SYN, ACK]**, accettando la connessione e completando il three-way handshake TCP.

No.	Time	Source	Destination	Protocol	Length	Info
78	0.777623149	192.168.200.150	192.168.200.100	TCP	60	78 → 49786 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
79	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	49786 → 784 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
80	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	51506 → 435 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
81	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	580 → 38138 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
82	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	982 → 52420 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
83	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	764 → 41874 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
84	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	435 → 51506 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
85	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	38042 → 440 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
86	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	46999 → 139 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
87	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	68632 → 25 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
88	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	27292 → 53 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
89	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	51458 → 148 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
90	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	48448 → 886 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
91	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	51506 → 221 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
92	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	8148 → 51458 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
93	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	886 → 48448 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
94	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	221 → 54560 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
95	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	42422 → 1107 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
96	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	34648 → 206 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
97	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	42422 → 1107 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
98	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	286 → 34648 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
99	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	48318 → 392 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
100	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	51278 → 827 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
101	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	131 → 54262 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
102	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	39560 → 858 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
103	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	392 → 49338 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
104	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	477 → 51256 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
105	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	47238 → 84 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
106	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	858 → 39560 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
107	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	51278 → 827 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
108	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	84 → 47238 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
109	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	48318 → 848 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
110	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	827 → 51256 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
111	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	43148 → 214 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
112	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	40886 → 106 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
113	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	948 → 49338 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
114	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	51278 → 135 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
115	0.85717645957	192.168.200.100	192.168.200.150	TCP	74	51262 → 864 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
116	0.85717645957	192.168.200.100	192.168.200.150	TCP	60	214 → 43148 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0

Risposte RST e ACK alle scansioni su porte chiuse

No.	Time	Source	Destination	Protocol	Length	Info
183	0.783329050	192.168.200.150	192.168.200.100	TCP	60	144 → 41184 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
184	0.783327995	192.168.200.150	192.168.200.100	TCP	60	874 → 42620 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
185	0.783329050	192.168.200.150	192.168.200.100	TCP	60	92 → 36110 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
186	0.783329050	192.168.200.150	192.168.200.100	TCP	74	42596 → 904 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535447 TSecr=0 WS=128
187	0.783426730	192.168.200.100	192.168.200.150	TCP	74	57372 → 333 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535447 TSecr=0 WS=128
188	0.783557923	192.168.200.100	192.168.200.150	TCP	60	84 → 47372 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
189	0.783557923	192.168.200.100	192.168.200.150	TCP	60	333 → 57372 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
190	0.783557923	192.168.200.100	192.168.200.150	TCP	74	52872 → 263 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
191	0.785443154	192.168.200.100	192.168.200.150	TCP	74	37888 → 886 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
192	0.785531331	192.168.200.100	192.168.200.150	TCP	74	58932 → 309 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
193	0.785624918	192.168.200.100	192.168.200.150	TCP	74	47472 → 743 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
194	0.785675017	192.168.200.100	192.168.200.150	TCP	60	203 → 52872 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
195	0.785675017	192.168.200.100	192.168.200.150	TCP	60	886 → 37888 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
196	0.785725841	192.168.200.100	192.168.200.150	TCP	74	41884 → 931 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
197	0.785738953	192.168.200.100	192.168.200.150	TCP	74	57854 → 122 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
198	0.785823154	192.168.200.100	192.168.200.150	TCP	60	5002 → 57372 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
199	0.785823154	192.168.200.100	192.168.200.150	TCP	60	743 → 47472 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
200	0.785899808	192.168.200.100	192.168.200.150	TCP	74	57402 → 237 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
201	0.785943368	192.168.200.100	192.168.200.150	TCP	74	33718 → 358 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
202	0.786200050	192.168.200.100	192.168.200.150	TCP	60	812 → 41884 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
203	0.786200050	192.168.200.100	192.168.200.150	TCP	60	122 → 57854 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
204	0.786210019	192.168.200.100	192.168.200.150	TCP	60	237 → 57402 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
205	0.786210019	192.168.200.100	192.168.200.150	TCP	60	358 → 33718 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
206	0.786241416	192.168.200.100	192.168.200.150	TCP	74	35164 → 546 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
207	0.786292426	192.168.200.100	192.168.200.150	TCP	74	58734 → 129 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
208	0.786455822	192.168.200.100	192.168.200.150	TCP	60	129 → 58734 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
209	0.786455822	192.168.200.100	192.168.200.150	TCP	74	45418 → 545 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128
210	0.786455822	192.168.200.100	192.168.200.150	TCP	74	45154 → 486 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128
211	0.786455822	192.168.200.100	192.168.200.150	TCP	74	38186 → 238 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128
212	0.78689954	192.168.200.100	192.168.200.150	TCP	74	37952 → 526 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128
213	0.787923089	192.168.200.100	192.168.200.150	TCP	60	545 → 45418 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
214	0.787923089	192.168.200.100	192.168.200.150	TCP	60	486 → 45154 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
215	0.787923089	192.168.200.100	192.168.200.150	TCP	74	43196 → 709 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128
216	0.787923089	192.168.200.100	192.168.200.150	TCP	60	238 → 38186 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
217	0.787923089	192.168.200.100	192.168.200.150	TCP	60	526 → 37952 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
218	0.787923089	192.168.200.100	192.168.200.150	TCP	74	45456 → 409 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128
219	0.787923089	192.168.200.100	192.168.200.150	TCP	60	709 → 43196 [RST, ACK] Seq=1, Ack=1, Win=0, Len=0
220	0.787923089	192.168.200.100	192.168.200.150	TCP	74	49888 → 19 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535451 TSecr=0 WS=128
221	0.787923089	192.168.200.100	192.168.200.150	TCP	74	44444 → 846 [SYN] Seq=9, Min=64240, Len=0 MSS=1460 SACK_PERM=1 TSval=810535451 TSecr=0 WS=128

Risposte SYN-ACK indicanti porte aperte con servizi attivi

Porte identificate come aperte

Porta	Servizio	Risposta
21	FTP	[SYN, ACK]
22	SSH	[SYN, ACK]
23	Telnet	[SYN, ACK]
25	SMTP	[RST, ACK]
53	DNS	[RST, ACK]
80	HTTP	[SYN, ACK]

111	RPCbind	[SYN, ACK]
139	NetBIOS-SSN	[RST, ACK]
445	SMB	[RST, ACK]

Risultati della scansione porte

Analisi dei Servizi Vulnerabili: Threat Intelligence

Dall'analisi delle risposte positive (**[SYN, ACK]**), sono stati identificati i seguenti servizi attivi, che rappresentano vettori di attacco critici per la macchina Metasploitable:

Porta 23 – Telnet

Telnet è un protocollo datato che invia tutto il traffico, comprese le credenziali di accesso, in formato non cifrato.

Livello di criticità: **Alto**

Impatto: Un aggressore presente sulla stessa rete può catturare il traffico, ricostruire username e password tramite attività di sniffing e arrivare fino ai privilegi di root sulla macchina bersaglio (attacco Man-in-the-Middle).

Esempi di vulnerabilità note: CVE-2011-4862, CVE-2020-10188

Mitigazione consigliata: Disabilitare il servizio Telnet e utilizzare esclusivamente SSH per l'accesso remoto sicuro.

Porte 139 e 445 – Samba/SMB

Le porte 139 e 445 sono usate dai servizi Samba/SMB per la condivisione di cartelle e stampanti in ambito di rete locale.

Livello di criticità: **Critico**

Impatto: Lo stack SMB è stato spesso al centro di exploit che consentono esecuzione di codice da remoto, rappresentando un vettore privilegiato per campagne ransomware e worm, come dimostrato dagli attacchi WannaCry ed EternalBlue.

Esempi di vulnerabilità note: CVE-2017-0144 (EternalBlue), CVE-2017-7494 (SambaCry)

Mitigazione consigliata: Aggiornare immediatamente a versioni non vulnerabili o chiudere completamente le porte se il servizio non è strettamente necessario.

Porta 21 – FTP

FTP, analogamente a Telnet, trasferisce spesso le credenziali di autenticazione e i dati applicativi in chiaro.

Livello di criticità: **Medio/Alto**

Impatto: Oltre alla possibilità di intercettare username e password, implementazioni obsolete di server FTP possono includere backdoor (ad esempio vsftpd 2.3.4) o permettere accessi anonimi a directory sensibili del sistema.

Esempi di vulnerabilità note: CVE-2011-2523 (backdoor in vsftpd)

Mitigazione consigliata: Migrare a protocolli sicuri come SFTP o FTPS e disabilitare ogni forma di accesso anonimo.

Porta 111 – RPCbind

Il servizio RPCbind associa i numeri di programma RPC alle porte utilizzate sulla rete, fungendo da "registro" per i servizi RPC.

Livello di criticità: Medio

Impatto: Un uso improprio di RPCbind permette a un attaccante di enumerare i servizi RPC disponibili, ottenendo informazioni utili per preparare un attacco mirato e aumentando la superficie di esposizione (information disclosure).

Esempi di vulnerabilità note: CVE-2017-8779 (vulnerabilità rpcbind)

Mitigazione consigliata: Limitare l'accesso al servizio tramite regole di firewall, consentendo le richieste solo da host fidati, e, ove possibile, vincolare l'ascolto all'interfaccia di loopback.

Conclusioni e Raccomandazioni

L'analisi forense ha confermato che l'host **192.168.200.150** è stato oggetto di una ricognizione attiva (**Port Scanning**) da parte dell'host **192.168.200.100**, la quale ha esposto numerosi servizi obsoleti e non sicuri.

Azioni raccomandate per la messa in sicurezza

Priorità **Critica** (Immediate)

1. **Dismissione Servizi Insicuri:** Disattivare immediatamente Telnet (23) e sostituirlo con SSH (22), che garantisce la cifratura del traffico end-to-end
2. **Hardening SMB:** Se la condivisione file non è strettamente necessaria, chiudere le porte 139/445. Se necessaria, aggiornare il servizio all'ultima versione e disabilitare l'accesso anonimo
3. **Configurazione Firewall:** Implementare regole di firewall per bloccare il traffico in ingresso su porte non essenziali e limitare l'accesso alle sole sottoreti di gestione autorizzate

Priorità **Alta** (Breve termine)

1. Implementazione sistema IDS/IPS per rilevamento port scanning
2. Segmentazione della rete per isolare sistemi critici
3. Implementazione logging centralizzato e SIEM
4. Configurazione rate limiting su servizi esposti

Priorità **Media (Medio termine)**

1. Vulnerability assessment periodici con scanner automatizzati
 2. Implementazione di policy di patch management
 3. Security awareness training per il personale
 4. Implementazione di network access control (NAC)
-