

# 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](http://192.168.200.100)

Indirizzo IP Vittima (Destination): [192.168.200.150](http://192.168.200.150)

No.	Time	Source	Destination	Protocol	Length	Info
1	08:58:27.740	192.168.200.150	192.168.200.100	TCP	60	Initial Allocation Message (ACK=0, Sequence Number=1, Length=60) from Client to Server. ACK=0, Server, NT Workstation, NT Server, Potential Victim
2	23.765215995	192.168.200.100	192.168.200.150	TCP	74	53069 - 88 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810522427 Tsecr=810522427 MS=128
3	23.765207769	192.168.200.100	192.168.200.150	TCP	74	33876 - 443 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810522428 Tsecr=810522428 MS=128
4	23.764777323	192.168.200.150	192.168.200.150	TCP	74	80 + 53066 [SYN, ACK] Seq=1 Ack=1 Win=64260 MSS=1468 SACK PERM=1 Tsval=4294951185 Tsecr=810522427 MS=128
5	23.764777427	192.168.200.150	192.168.200.150	TCP	60	80 + 53067 [SYN, ACK] Seq=1 Ack=1 Win=64260 MSS=1468 SACK PERM=1 Tsval=4294951185 Tsecr=810522428 MS=128
6	23.764777428	192.168.200.150	192.168.200.150	TCP	60	80 + 53068 [SYN, ACK] Seq=1 Ack=1 Win=64260 MSS=1468 SACK PERM=1 Tsval=4294951185 Tsecr=810522428 MS=128
7	23.764800901	192.168.200.150	192.168.200.150	TCP	60	80 + 53069 [SYN, ACK] Seq=1 Ack=1 Win=64260 MSS=1468 SACK PERM=1 Tsval=4294951185 Tsecr=810522428 MS=128
8	28.765829461	PcsCompu_39:7d:fe	192.168.200.150	ARP	60	who has 192.168.200.150? Tell 192.168.200.158
9	28.765844819	PcsCompu_39:7d:fe	192.168.200.150	ARP	42	192.168.200.150 is at 08:08:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	192.168.200.150	ARP	42	192.168.200.150 is at 08:08:27:39:7d:fe
11	28.774852258	PcsCompu_39:7d:fe	192.168.200.150	ARP	40	192.168.200.150 is at 08:08:27:39:7d:fe
12	28.775433425	192.168.200.150	192.168.200.150	TCP	74	41384 - 32 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810525427 Tsecr=810525427 MS=128
13	38.774215115	192.168.200.150	192.168.200.150	TCP	74	56120 - 111 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810525437 Tsecr=810525437 MS=128
14	38.774257843	192.168.200.150	192.168.200.150	TCP	74	33878 - 443 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810525437 Tsecr=810525437 MS=128
15	38.774257844	192.168.200.150	192.168.200.150	TCP	74	33879 - 443 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810525437 Tsecr=810525437 MS=128
16	38.774406902	192.168.200.150	192.168.200.150	TCP	74	60356 - 195 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810535438 Tsecr=810535438 MS=128
17	38.774535934	192.168.200.150	192.168.200.150	TCP	74	60356 - 993 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810535438 Tsecr=810535438 MS=128
18	38.774851779	192.168.200.150	192.168.200.150	TCP	74	41182 - 21 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810535438 Tsecr=810535437 MS=128
19	38.774865969	192.168.200.150	192.168.200.150	TCP	74	41183 - 21 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810535438 Tsecr=810535437 MS=128
20	38.774865970	192.168.200.150	192.168.200.150	TCP	74	41184 - 21 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810535438 Tsecr=810535437 MS=128
21	36.774686569	192.168.200.150	192.168.200.150	TCP	60	443 - 33876 [EST, ACK] Seq=1 Ack=1 Win=8 Len=8
22	36.774689757	192.168.200.150	192.168.200.150	TCP	60	5954 - 58638 [EST, ACK] Seq=1 Ack=1 Win=8 Len=8
23	36.774689758	192.168.200.150	192.168.200.150	TCP	60	139 - 52358 [EST, ACK] Seq=1 Ack=1 Win=8 Len=8
24	36.774704464	192.168.200.150	192.168.200.150	TCP	60	41384 - 23 [SYN] Seq=0 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535438 Tsecr=8294952466 MS=64
25	36.774704465	192.168.200.150	192.168.200.150	TCP	74	60161 - 23 [SYN] Seq=0 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535438 Tsecr=8294952466 MS=64
26	36.775141194	192.168.200.150	192.168.200.150	TCP	60	993 - 46330 [EST, ACK] Seq=1 Ack=1 Win=8 Len=8
27	36.775341273	192.168.200.150	192.168.200.150	TCP	74	21 - 41382 [SYN, ACK] Seq=0 Ack=1 Win=3792 Len=0 MSS=1468 SACK PERM=1 Tsval=4294952466 Tsecr=810535437 MS=64
28	36.775174843	192.168.200.150	192.168.200.150	TCP	66	41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535437 Tsecr=8294952466
29	36.775340594	192.168.200.150	192.168.200.150	TCP	74	56120 - 111 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810535437 Tsecr=810535437 MS=128
30	36.775340595	192.168.200.150	192.168.200.150	TCP	74	56056 - 23 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810535437 Tsecr=810535437 MS=128
31	36.775524269	192.168.200.150	192.168.200.150	TCP	74	53067 - 88 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810535437 Tsecr=810535437 MS=128
32	36.775818008	192.168.200.150	192.168.200.150	TCP	60	113 - 58174 [EST, ACK] Seq=1 Ack=1 Win=8 Len=8
33	36.775818154	192.168.200.150	192.168.200.150	TCP	66	41384 - 23 [EST, ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
34	36.775818155	192.168.200.150	192.168.200.150	TCP	66	56120 - 111 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=810535439 MS=128
35	36.775702655	192.168.200.150	192.168.200.150	TCP	74	56056 - 23 [SYN] Seq=0 Win=64260 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=810535439 MS=128
36	36.775797869	192.168.200.150	192.168.200.150	TCP	74	88 - 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1468 SACK PERM=1 Tsval=4294952466 Tsecr=810535439 MS=64
37	36.775800786	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
38	36.775800787	192.168.200.150	192.168.200.150	TCP	66	41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
39	36.775800788	192.168.200.150	192.168.200.150	TCP	66	41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
40	36.775807654	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
41	36.775807655	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
42	36.775807656	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
43	36.775807657	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
44	36.775807658	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
45	36.775807659	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
46	36.775807660	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
47	36.775807661	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
48	36.775807662	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
49	36.775807663	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
50	36.775807664	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
51	36.775807665	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
52	36.775807666	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
53	36.775807667	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
54	36.775807668	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
55	36.775807669	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
56	36.775807670	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
57	36.775807671	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
58	36.775807672	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
59	36.775807673	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
60	36.775807674	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
61	36.775807675	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
62	36.775807676	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
63	36.775807677	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
64	36.775807678	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
65	36.775807679	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
66	36.775807680	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
67	36.775807681	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
68	36.775807682	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
69	36.775807683	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
70	36.775807684	192.168.200.150	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK PERM=1 Tsval=810535439 Tsecr=8294952466
71	36.775807685	192.168.200.150	192.168.200.			

## 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	36.779405845	192.168.200.150	192.168.200.100	TCP	60	3.24 - 4340 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	36.779405750	192.168.200.150	192.168.200.100	TCP	60	106 - 46800 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120	36.779405790	192.168.200.150	192.168.200.100	TCP	60	138 - 50240 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	36.779405843	192.168.200.150	192.168.200.100	TCP	60	884 - 51200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122	36.779437285	192.168.200.100	192.168.200.150	TCP	74	44244 - 699 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535443 Tsecr=0 WS=128
123	36.779437288	192.168.200.100	192.168.200.150	TCP	74	43638 - 703 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535443 Tsecr=0 WS=128
124	36.779456943	192.168.200.150	192.168.200.100	TCP	60	699 - 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	36.779456946	192.168.200.150	192.168.200.100	TCP	74	5033 - 47 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535443 Tsecr=0 WS=128
126	36.779456947	192.168.200.150	192.168.200.100	TCP	74	49822 - 264 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535443 Tsecr=0 WS=128
127	36.780035451	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 - 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129	36.780148473	192.168.200.100	192.168.200.150	TCP	74	57552 - 58 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535443 Tsecr=0 WS=128
130	36.780170333	192.168.200.100	192.168.200.150	TCP	74	49822 - 264 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535443 Tsecr=0 WS=128
131	36.780215170	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	192.168.200.150	192.168.200.100	TCP	60	58 - 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133	36.780301753	192.168.200.100	192.168.200.150	TCP	74	317 - 47 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535444 Tsecr=0 WS=128
134	36.780346420	192.168.200.100	192.168.200.150	TCP	74	5048 - 23 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535444 Tsecr=0 WS=128
135	36.780409818	192.168.200.100	192.168.200.150	TCP	74	36548 - 739 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535444 Tsecr=0 WS=128
136	36.780427899	192.168.200.100	192.168.200.150	TCP	74	38866 - 55 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535444 Tsecr=0 WS=128
137	36.780472838	192.168.200.100	192.168.200.150	TCP	74	52136 - 994 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535444 Tsecr=0 WS=128
138	36.780499897	192.168.200.100	192.168.200.150	TCP	74	36022 - 317 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535444 Tsecr=0 WS=128
139	36.780577788	192.168.200.150	192.168.200.100	TCP	60	266 - 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	36.780577791	192.168.200.150	192.168.200.100	TCP	60	11 - 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	36.780577794	192.168.200.150	192.168.200.100	TCP	60	295 - 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142	36.780578571	192.168.200.150	192.168.200.100	TCP	60	739 - 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143	36.780578519	192.168.200.150	192.168.200.100	TCP	60	55 - 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144	36.780578159	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 - 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146	36.780577167	192.168.200.100	192.168.200.150	TCP	74	49446 - 501 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535444 Tsecr=0 WS=128
147	36.780701626	192.168.200.100	192.168.200.150	TCP	74	51192 - 241 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535444 Tsecr=0 WS=128
148	36.780701629	192.168.200.100	192.168.200.150	TCP	60	961 - 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149	36.780885399	192.168.200.150	192.168.200.100	TCP	60	241 - 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
150	36.780885399	192.168.200.150	192.168.200.100	TCP	74	41268 - 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151	36.780905540	192.168.200.100	192.168.200.150	TCP	74	41268 - 974 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535444 Tsecr=0 WS=128
152	36.780905307	192.168.200.100	192.168.200.150	TCP	74	49914 - 137 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535444 Tsecr=0 WS=128
153	36.781005759	192.168.200.150	192.168.200.100	TCP	60	293 - 42642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
154	36.781110800	192.168.200.150	192.168.200.100	TCP	60	974 - 41820 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155	36.781110971	192.168.200.150	192.168.200.100	TCP	60	137 - 40914 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
156	36.781138769	192.168.200.100	192.168.200.150	TCP	74	42464 - 223 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=810535444 Tsecr=0 WS=128
157	36.781138927	192.168.200.100	192.168.200.150	TCP	74	42780 - 1014 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM=1 Tsvai=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
99	30. 777623149	192.168.200.190	192.168.200.190	TCP	69 70 - 49780	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	36. 777645627	192.168.200.190	192.168.200.190	TCP	74 41874 - 764	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535441 TSec=r 9 WS=128
81	36. 777608098	192.168.200.190	192.168.200.190	TCP	74 51506 - 135	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535441 TSec=r 9 WS=128
82	36. 777645627	192.168.200.190	192.168.200.190	TCP	69 992 - 52428	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36. 777586966	192.168.200.190	192.168.200.190	TCP	69 992 - 52428	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36. 777671245	192.168.200.190	192.168.200.190	TCP	69 764 - 41874	[ACK, Seq=1 Ack=1 Win=0 Len=0]
85	36. 777671239	192.168.200.190	192.168.200.190	TCP	69 435 - 51506	[ACK, Seq=1 Ack=1 Win=0 Len=0]
86	36. 777832929	192.168.200.190	192.168.200.190	TCP	69 33842 - 445	[ACK, Seq=1 Ack=1 Win=0 Len=0]
87	36. 777832929	192.168.200.190	192.168.200.190	TCP	69 33842 - 445	[ACK, Seq=1 Ack=1 Win=0 Len=0]
88	36. 777895739	192.168.200.190	192.168.200.190	TCP	69 66632 - 25	[ACK, Seq=1 Ack=1 Win=64256 Len=8 TStamp=810535441 TSec=r 2494952466
89	36. 777895739	192.168.200.190	192.168.200.190	TCP	69 66632 - 25	[ACK, Seq=1 Ack=1 Win=64256 Len=8 TStamp=810535441 TSec=r 2494952466]
90	36. 777895739	192.168.200.190	192.168.200.190	TCP	69 37282 - 53	[RST, ACK] Seq=1 Ack=1 Win=64256 Len=8 TStamp=810535441 TSec=r 2494952466
91	36. 778179798	192.168.200.190	192.168.200.190	TCP	74 51459 - 148	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535441 TSec=r 9 WS=128
92	36. 778179798	192.168.200.190	192.168.200.190	TCP	74 51459 - 148	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535441 TSec=r 9 WS=128
93	36. 778365646	192.168.200.190	192.168.200.190	TCP	69 148 - 51549	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	36. 778365648	192.168.200.190	192.168.200.190	TCP	69 806 - 48448	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36. 778449494	192.168.200.190	192.168.200.190	TCP	69 273 - 54566	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96	36. 778522126	192.168.200.190	192.168.200.190	TCP	74 34648 - 206	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535442 TSec=r 9 WS=128
97	36. 778522126	192.168.200.190	192.168.200.190	TCP	74 34648 - 206	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535442 TSec=r 9 WS=128
98	36. 778614895	192.168.200.190	192.168.200.190	TCP	74 54296 - 131	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535442 TSec=r 9 WS=128
99	36. 778663664	192.168.200.190	192.168.200.190	TCP	69 1897 - 42420	[RST, ACK] Seq=1 Ack=1 Win=8 Len=0
100	36. 778721806	192.168.200.190	192.168.200.190	TCP	69 295 - 34648	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	36. 778781327	192.168.200.190	192.168.200.190	TCP	74 51279 - 077	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535442 TSec=r 9 WS=128
102	36. 778781327	192.168.200.190	192.168.200.190	TCP	74 51279 - 077	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535442 TSec=r 9 WS=128
103	36. 778862024	192.168.200.190	192.168.200.190	TCP	69 103 - 54202	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	36. 778862024	192.168.200.190	192.168.200.190	TCP	74 39594 - 506	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535442 TSec=r 9 WS=128
105	36. 778862024	192.168.200.190	192.168.200.190	TCP	69 477 - 49370	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535442 TSec=r 9 WS=128
106	36. 778862024	192.168.200.190	192.168.200.190	TCP	69 477 - 49370	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535442 TSec=r 9 WS=128
107	36. 778933513	192.168.200.190	192.168.200.190	TCP	74 4732 - 34	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535442 TSec=r 9 WS=128
108	36. 778969210	192.168.200.190	192.168.200.190	TCP	69 856 - 39566	[ACK, Seq=1 Ack=1 Win=0 Len=0]
109	36. 778955243	192.168.200.190	192.168.200.190	TCP	74 5054 - 197	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535442 TSec=r 9 WS=128
110	36. 778955243	192.168.200.190	192.168.200.190	TCP	74 5054 - 197	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535442 TSec=r 9 WS=128
111	36. 779145604	192.168.200.190	192.168.200.190	TCP	74 4337 - 248	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535442 TSec=r 9 WS=128
112	36. 779252064	192.168.200.190	192.168.200.190	TCP	69 887 - 55642	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	36. 779273781	192.168.200.190	192.168.200.190	TCP	74 43138 - 214	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535443 TSec=r 9 WS=128
114	36. 779345664	192.168.200.190	192.168.200.190	TCP	69 948 - 40738	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
115	36. 779354664	192.168.200.190	192.168.200.190	TCP	74 59250 - 135	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535443 TSec=r 9 WS=128
116	36. 779378086	192.168.200.190	192.168.200.190	TCP	74 51268 - 864	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535443 TSec=r 9 WS=128
117	36. 779397823	192.168.200.190	192.168.200.190	TCP	74 51268 - 864	[SYN] Seq=0 Win=64240 Len=8 MSS=1469 SACK_PERM=1 TStamp=810535443 TSec=r 9 WS=128
118	36. 779695648	192.168.200.190	192.168.200.190	TCP	69 214 - 43148	[ACK, Seq=1 Ack=1 Win=0 Len=0]

*Risposte RST e ACK alle scansioni su porte chiuse*

*Risposte SYN-ACK indicanti porte aperte con servizi attivi*

### **Porte identificate come aperte**

<b>Porta</b>	<b>Servizio</b>	<b>Risposta</b>
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)
-