



## Introduzione

### Analizzazione cattura di movimenti sospetti con Wireshark



- 1° Identificheremo ed analizzeremo eventuali IOC, ovvero evidenze di attacchi in corso
- 2° In base agli IOC trovati, faremo delle ipotesi sui potenziali vettori di attacco utilizzati
- 3° Consigliero un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro

No.	Time	Source	Destination	Protocol	Length	Info
1	00:00:00:00:00:00	192.168.200.150	192.168.200.155	BROWSER	286	Host Announcement METASPLITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522427 TSecr=0 WS=128
3	23.764267789	192.168.200.100	192.168.200.150	TCP	74	33876 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 - 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=810522427 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	66	443 - 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PcsCompu_fd:87:1e	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150	
9	28.761644619	PcsCompu_39:7d:fe	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe	
10	28.774852597	PcsCompu_39:7d:fe	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100	
11	28.775230099	PcsCompu_fd:87:1e	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e	
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 - 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 - 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 - 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 - 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
19	36.774685508	192.168.200.100	192.168.200.150	TCP	74	23 - 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	192.168.200.100	192.168.200.150	TCP	74	111 - 56120 [SYN, ACK] Seq=0 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535437 WS=64
21	36.774685696	192.168.200.150	192.168.200.100	TCP	66	443 - 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.100	192.168.200.150	TCP	66	554 - 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	66	135 - 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774709464	192.168.200.100	192.168.200.150	TCP	66	41304 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711972	192.168.200.100	192.168.200.150	TCP	66	56120 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	66	993 - 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 - 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535438 WS=64
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337899	192.168.200.100	192.168.200.150	TCP	74	59174 - 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
30	36.775386699	192.168.200.100	192.168.200.150	TCP	74	585656 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
31	36.775524269	192.168.200.100	192.168.200.150	TCP	74	53062 - 8 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
32	36.775589808	192.168.200.150	192.168.200.100	TCP	66	113 - 50174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 - 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=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=1 TSval=4294952466 TSecr=810535439 WS=64
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 - 8 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.77681964	192.168.200.100	192.168.200.150	TCP	66	41182 - 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.776975876	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

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0

# Relazione sull'Analisi del Traffico di Rete

Dall'analisi della cattura, è stato osservato un traffico TCP significativo tra gli host delle seguenti reti:

- 192.168.200.100 (probabilmente una macchina Metasploitable).
- 192.168.200.150 (potrebbe essere un client che sta interagendo con la macchina Metasploitable).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPOITABLE, Workstation, Server, Print Queue Serv
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=81052
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=8105
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 T
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr
8	28.761629461	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e

La cattura mostra flussi di pacchetti, evidenziando molteplici eventi relativi al protocollo TCP.

No.	Time	Source	Destination	Protocol	Length	Info
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 →
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060

## Dettagli Osservati

### 1. Handshake TCP e Pacchetti SYN/ACK

- Righe TCP con stato SYN: La comunicazione mostra molteplici richieste TCP (flag SYN) inviate dall'host 192.168.200.150 verso 192.168.200.100, suggerendo un tentativo di instaurare una connessione.
- Risposte RST/ACK: In quasi tutti i casi, il server Metasploitable risponde con pacchetti RST (Reset), chiudendo immediatamente le connessioni tentate.

192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=
192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=
192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=
192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- Ciò indica che il server rifiuta attivamente le connessioni, potenzialmente perché
  - 1°I servizi targetati non sono attivi.
  - 2°I tentativi provengono da un host non autorizzato.
  - 3°Il server potrebbe essere sotto attacco.

## 2. Flusso di pacchetti (RST/ACK in evidenza)

La maggioranza dei pacchetti è contrassegnata con flag RST (Reset), il che rappresenta un'interruzione immediata delle connessioni. Questo comportamento è coerente con:

0.100	TCP	60 764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
0.100	TCP	60 435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- Un'attività di scansione o enumerazione da parte dell'host 192.168.200.150
- Misure di autodifesa del server Metasploitable, che nega connessioni a porte non attive o accessi sospetti.

## 3. Tempistica

Il traffico catturato avviene in un periodo molto ristretto (millisecondi), suggerendo un'attività automatizzata, come uno scanner di rete o vulnerability scanner (es. Nmap, Nessus o script personalizzati).

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 36.777645627	192.168.200.100	192.168.200.150	TCP	74 41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535441 TSecr=0 WS=128		
81 36.777680898	192.168.200.100	192.168.200.150	TCP	74 51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535441 TSecr=0 WS=128		
82 36.777758636	192.168.200.150	192.168.200.100	TCP	60 588 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
83 36.777758696	192.168.200.150	192.168.200.100	TCP	60 962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
84 36.777871245	192.168.200.150	192.168.200.100	TCP	60 764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
85 36.777891293	192.168.200.150	192.168.200.100	TCP	60 435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
86 36.777893298	192.168.200.100	192.168.200.150	TCP	66 33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSeqval=810535441 TSecr=4294952466		
87 36.777912717	192.168.200.100	192.168.200.150	TCP	66 46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSeqval=810535441 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 TSeqval=810535441 TSecr=4294952466		
89 36.778031265	192.168.200.100	192.168.200.150	TCP	66 37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSeqval=810535441 TSecr=4294952466		
90 36.778179978	192.168.200.100	192.168.200.150	TCP	74 51458 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535441 TSecr=0 WS=128		
91 36.778200161	192.168.200.100	192.168.200.150	TCP	74 48448 → 886 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535441 TSecr=0 WS=128		
92 36.778397830	192.168.200.100	192.168.200.150	TCP	74 54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535442 TSecr=0 WS=128		
93 36.778385846	192.168.200.150	192.168.200.100	TCP	66 148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
94 36.778385948	192.168.200.150	192.168.200.100	TCP	66 896 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
95 36.778449494	192.168.200.150	192.168.200.100	TCP	66 221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
96 36.778482791	192.168.200.100	192.168.200.150	TCP	74 42428 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535442 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 TSeqval=810535442 TSecr=0 WS=128		
98 36.778614095	192.168.200.100	192.168.200.150	TCP	74 54262 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535442 TSecr=0 WS=128		
99 36.778663064	192.168.200.150	192.168.200.100	TCP	66 1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
100 36.778721089	192.168.200.150	192.168.200.100	TCP	66 206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
101 36.778759636	192.168.200.100	192.168.200.150	TCP	74 49318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535442 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 TSeqval=810535442 TSecr=0 WS=128		
103 36.778826294	192.168.200.150	192.168.200.100	TCP	60 131 → 54282 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
104 36.778864493	192.168.200.100	192.168.200.150	TCP	74 39566 → 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535442 TSecr=0 WS=128		
105 36.778939327	192.168.200.150	192.168.200.100	TCP	60 392 → 40318 [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 36.778983153	192.168.200.100	192.168.200.150	TCP	74 47238 → 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535442 TSecr=0 WS=128		
108 36.779092910	192.168.200.150	192.168.200.100	TCP	66 856 → 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 → 897 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535442 TSecr=0 WS=128		
110 36.779122299	192.168.200.150	192.168.200.100	TCP	66 84 → 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
111 36.779145004	192.168.200.100	192.168.200.150	TCP	74 40138 → 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535442 TSecr=0 WS=128		
112 36.779252884	192.168.200.150	192.168.200.100	TCP	66 807 → 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
113 36.779273781	192.168.200.100	192.168.200.150	TCP	74 43140 → 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535443 TSecr=0 WS=128		
114 36.779309462	192.168.200.100	192.168.200.150	TCP	74 46886 → 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535443 TSecr=0 WS=128		
115 36.779354564	192.168.200.150	192.168.200.100	TCP	66 948 → 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
116 36.779378630	192.168.200.100	192.168.200.150	TCP	74 50284 → 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535443 TSecr=0 WS=128		
117 36.779397923	192.168.200.100	192.168.200.150	TCP	74 51262 → 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=810535443 TSecr=0 WS=128		
118 36.779665648	192.168.200.150	192.168.200.100	TCP	66 214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		

## Possibili Cause del Traffico

### 1° Scansione delle Porte (Port Scanning)

Gli eventi osservati sono coerenti con una scansione delle porte TCP, in cui un client invia pacchetti SYN per rilevare servizi attivi. Il server risponde con:

- RST (Reset): La porta non è aperta.
- SYN/ACK: La porta è aperta (in questo caso, non visibile nei dati analizzati).

### 2° Tentativi di Enumerazione di Servizi:

I pacchetti potrebbero essere parte di un tentativo di identificare servizi attivi su Metasploitable, come SSH, FTP, HTTP o altri.

### 3° Potenziale Attacco DoS (Denial of Service)

L'elevato numero di pacchetti RST/ACK in un breve intervallo di tempo potrebbe indicare:

- Un tentativo di saturazione del server tramite richieste non valide.
- Una configurazione deliberata di autodifesa per bloccare scansioni o traffico anomalo.

## Analisi delle Minacce

### Minacce Osservate:

L'host 192.168.200.150 sta tentando di interagire con Metasploitable (192.168.200.100) in modo ripetitivo e automatizzato. Questo può essere:

- Un'attività di scansione non autorizzata.
- Un possibile exploit in corso.
- Se il server Metasploitable ospita vulnerabilità note, potrebbe essere esposto a un potenziale attacco.

### Risposta del Server

Il server risponde con RST/ACK, il che impedisce connessioni dannose. Tuttavia, non è chiaro se ciò sia una difesa configurata o un comportamento standard per porte non aperte.

## Azioni Raccomandate

### 1° Analisi del Traffico con Wireshark:

- Seguire i flussi TCP per ottenere una visione più chiara della comunicazione.
- Filtrare pacchetti con **ip.src == 192.168.200.150 && ip.dst == 192.168.200.100** per concentrarsi sul client sospetto.

### 2° Verifica dei Servizi su Metasploitable:

- Utilizzare un comando come **netstat -tuln** su Metasploitable per identificare le porte aperte e i servizi in ascolto.
- Disabilitare eventuali servizi non necessari o pericolosi.

### 3° Esaminare l'Host Sorgente:

Verificare i processi e gli strumenti attivi sull'host 192.168.200.150 per identificare:

- Scanner di rete in esecuzione (es. Nmap).
- Script o attività malevole.

### 4° Applicare Contromisure:

- Configurare un firewall (ad esempio con pfSense) per bloccare traffico sospetto da 192.168.200.150.
- Monitorare il traffico in tempo reale per rilevare ulteriori anomalie

## Conclusioni

L'analisi del traffico di rete catturato evidenzia un'attività sospetta tra due host nella rete locale, 192.168.200.100 (probabilmente una macchina vulnerabile Metasploitable) e 192.168.200.150 (il client che invia richieste). I dati suggeriscono diversi scenari possibili che meritano approfondimento e misure preventive.