

# Report di Analisi Threat Intelligence

**Target:** 192.168.200.150 ( Metasploitable)

**Analista:**Victor Rosati **Data:** 06/02/2026

**Obiettivo:** Identificare evidenze di compromissione (IOC) e potenziali vettori di attacco tramite l'analisi del traffico di rete.

## Cos'è Wireshark?

Wireshark è un software di "network sniffing" che permette di catturare e analizzare in tempo reale o tramite file (come il .pcapng) tutto il traffico che viaggia su una rete.

È come un microscopio per i dati: permette di vedere chi parla con chi e cosa si dicono.

## Step dell'Analisi

Hai fatto bene a dirmelo! Il "drag and drop" (trascinamento) è molto più immediato e pratico. Ho aggiornato il report riflettendo esattamente quello che hai fatto tu, mantenendo però la spiegazione tecnica richiesta dall'esercizio.

---



# Report di Analisi Threat Intelligence

**Target:** 192.168.200.150 (Macchina Metasploitable) **Analista:** [Il Tuo Nome] **Data:** 06/02/2026

**Obiettivo:** Analizzare la cattura di rete per identificare evidenze di attacchi (IOC) e vulnerabilità.

---



## Cos'è Wireshark?

È un software che "fotografa" il traffico di rete. Permette di vedere ogni singolo messaggio inviato tra i computer, aiutando a capire se qualcuno sta cercando di forzare una porta o rubare dati.

---

## Step dell'Analisi (Semplificati)

```
kalirose@kalirose: ~/Desktop
Session Actions Edit View Help
(kalirose@kalirose)-[~]
$ cd Desktop
(kalirose@kalirose)-[~/Desktop]
$ ls
Cattura_U3_W1_L5.pcapng  code.desktop  jpg
```

1. **Importazione:** Il file di cattura **.pcapng** è stato trascinato direttamente all'interno della macchina **Kali Linux**.
2. **Accesso:** Il file è stato aperto con Wireshark per visualizzare l'elenco dei pacchetti catturati.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Work...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53600 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
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 TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 -> 53600 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427
5	23.764777427	192.168.200.150	192.168.200.100	TCP	68	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	53600 -> 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	53600 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PCSSystemtec fd:87:...	PCSSystemtec 39:7d:...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
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 192.168.200.100
11	28.775230999	PCSSystemtec fd:87:...	PCSSystemtec 39:7d:...	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 TSval=810535437 TSecr=0 WS=128
13	36.774210116	192.168.200.100	192.168.200.150	TCP	74	56120 -> 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM 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 TSval=810535438 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 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 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 TSval=810535438 TSecr=0 WS=128
18	36.774614726	192.168.200.100	192.168.200.150	TCP	74	41102 -> 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
* Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0						
* Ethernet II, Src: PCSSystemtec fd:87:1e (08:00:27:fd:87:1e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
* Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.255						
* User Datagram Protocol, Src Port: 138, Dst Port: 138						
* NetBIOS Datagram Service						
* SMB (Server Message Block Protocol)						
* SMB Mailslot Protocol						
* Microsoft Windows Browser Protocol						

3. **Filtraggio:** È stato applicato un filtro (**tcp.flags.syn == 1 && tcp.flags.ack == 1**) per vedere solo le porte che hanno risposto positivamente all'attaccante.

ip.src==192.168.200.150 && tcp.flags.syn==1 && tcp.flags.ack==1						
No.	Time	Source	Destination	Protocol	Length	Info
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 -> 53600 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810522427
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 TSval=4294952466 TSecr=810535437
20	36.774685652	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 TSval=4294952466 TSecr=810535437
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 -> 41102 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438
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 TSval=4294952466 TSecr=810535439
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 -> 53600 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445 -> 33842 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139 -> 40990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 -> 09632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440
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 TSval=4294952466 TSecr=810535440
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 TSval=4294952466 TSecr=810535445
267	36.788095940	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 TSval=4294952471 TSecr=810535452
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 TSval=4294952471 TSecr=810535489

## Risultati (IOC e Vettori)

L'analisi ha rivelato una **scansione delle porte** (Port Scanning) massiva da parte dell'IP **192.168.200.100**.

- **IOC Trovati:** Elevato numero di pacchetti TCP SYN in breve tempo e risposte SYN/ACK da porte critiche.
- **Servizi Esposti (Vettori):** Le porte **21 (FTP)**, **22 (SSH)**, **23 (Telnet)** e **80 (HTTP)** sono risultate aperte e vulnerabili a tentativi di accesso o exploit.

## Conclusioni e Consigli

Il sistema target è in una fase avanzata di ricognizione da parte di un utente malintenzionato.

1. **Azione Immediata:** Isolare la macchina 192.168.200.150 dalla rete.
2. **Rimedio:** Disabilitare i protocolli non sicuri (Telnet e FTP) e configurare un firewall per bloccare le scansioni dall'IP dell'attaccante.