

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
File System
(kalirose@kalirose)-[~/Desktop]
$ ls
Cattura_U3_W1_L5.pcapng code.desktop jpg
```

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

No.	Time	Source	Destination	Protocol	Length	Info
1	23.7645214995	192.168.200.150	192.168.200.150	TCP	266	HOST Announcement METASPLITABLE, Workstation Server, Print Queue Server, Xenix Server, NT Work...
2	23.7645214995	192.168.200.150	192.168.200.150	TCP	74	53066 - 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.7645214995	192.168.200.150	192.168.200.150	TCP	74	53067 - 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.7645214995	192.168.200.150	192.168.200.150	TCP	74	53069 - [SYN, ACK] Seq=0 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
5	23.7645214995	192.168.200.150	192.168.200.150	TCP	69	443 - 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.150	192.168.200.150	TCP	66	53066 - 88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764815289	192.168.200.150	192.168.200.150	TCP	66	53068 - 88 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PCSSystemtec_fd:87...	PCSSystemtec_39:7d:...	ARP	69	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_fd:87...	PCSSystemtec_39:7d:...	ARP	42	192.168.200.100 is at 00:00:27:39:7d:fe
10	28.77485257	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230699	PCSSystemtec_fd:87...	PCSSystemtec_39:7d:...	ARP	60	192.168.200.150 is at 00:00:27:fd:87:1e
12	36.774143444	192.168.200.150	192.168.200.150	TCP	74	41384 - 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218119	192.168.200.150	192.168.200.150	TCP	74	56126 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774220843	192.168.200.150	192.168.200.150	TCP	74	33878 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774266055	192.168.200.150	192.168.200.150	TCP	74	56116 - 56126 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437
16	36.7744058627	192.168.200.150	192.168.200.150	TCP	74	52280 - 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535532	192.168.200.150	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	36.774614776	192.168.200.150	192.168.200.150	TCP	74	41182 - 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 (00:00:27:39:7d:fe), 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

- 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.

No.	Time	Source	Destination	Protocol	Length	Info
4	23.764777323	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 TSval=810522427 TSecr=0 WS=128
19	23.764777323	192.168.200.150	192.168.200.100	TCP	74	22 - 53089 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
27	36.775141273	192.168.200.150	192.168.200.150	TCP	74	21 - 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438
35	36.775396338	192.168.200.150	192.168.200.150	TCP	74	22 - 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438
36	36.775397894	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 TSval=4294952466 TSecr=810535438
57	36.776994845	192.168.200.150	192.168.200.150	TCP	74	445 - 33842 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535448
59	36.776994961	192.168.200.150	192.168.200.150	TCP	74	139 - 46996 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535448
61	36.776995043	192.168.200.150	192.168.200.150	TCP	74	25 - 66632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535448
63	36.776995123	192.168.200.150	192.168.200.150	TCP	74	53 - 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535448
104	36.781487219	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=810535448
267	36.788869546	192.168.200.150	192.168.200.100	TCP	74	514 - 51398 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535448
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=810535448

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.