REPORT TECNICO

Threat Intelligence & IOC

Redatto da: *Nicolò Calì Cybersecurity Student*

Data: 06/02/2026

Oggetto: Analisi tecnica file di cattura Wireshark e identificazione IOC

1. 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.

Dopo aver importato il file “Cattura_U3_W1_L5.pcapng” l’ho aperto con Wireshark.

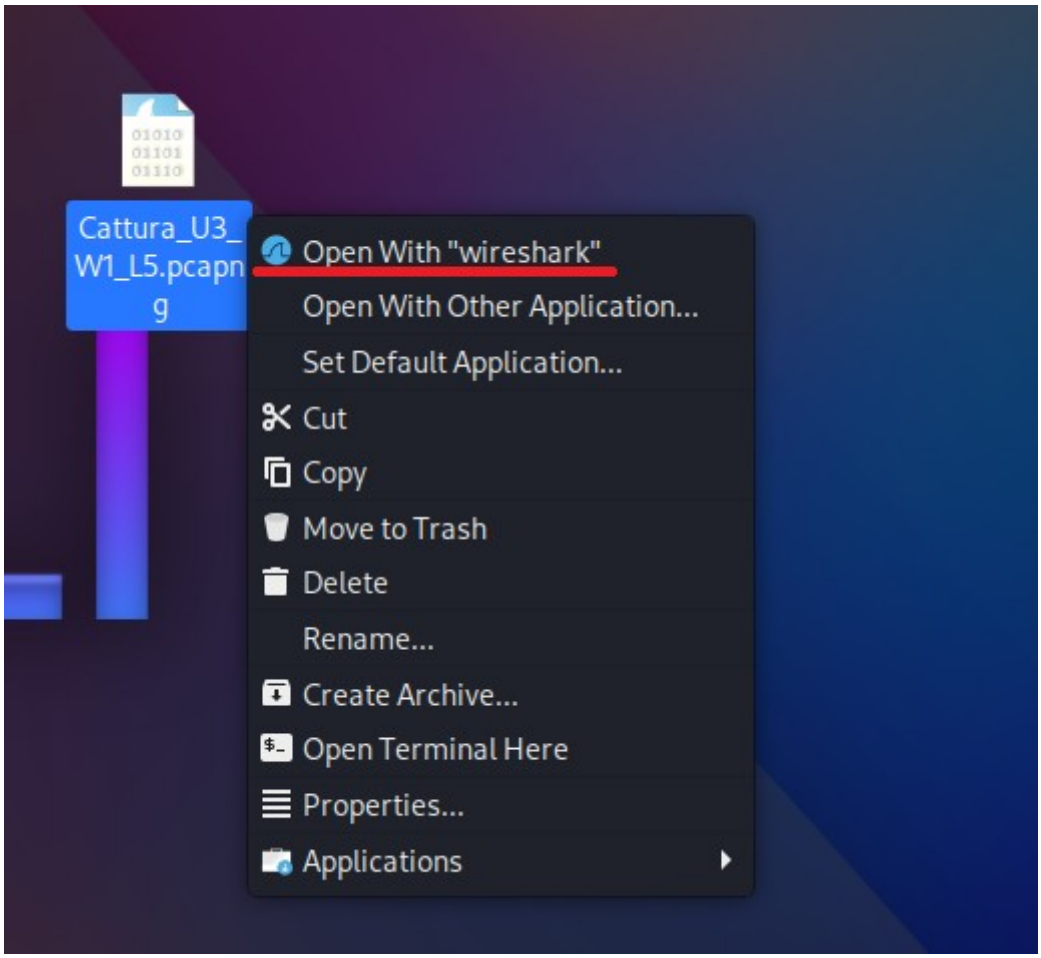


Fig 1. apertura del File da esaminare

Nell’immagine sottostante possiamo vedere la schermata di Wireshark.

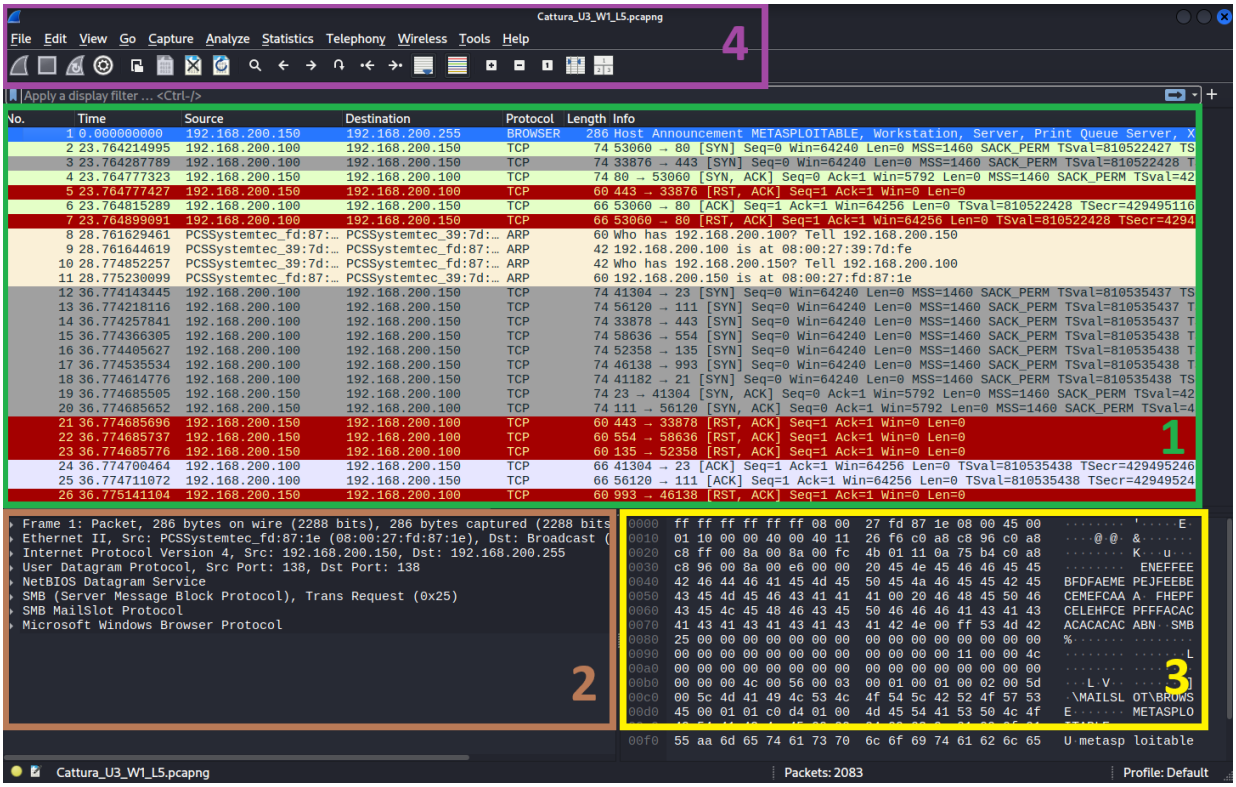


Fig 2. Schermata Wireshark

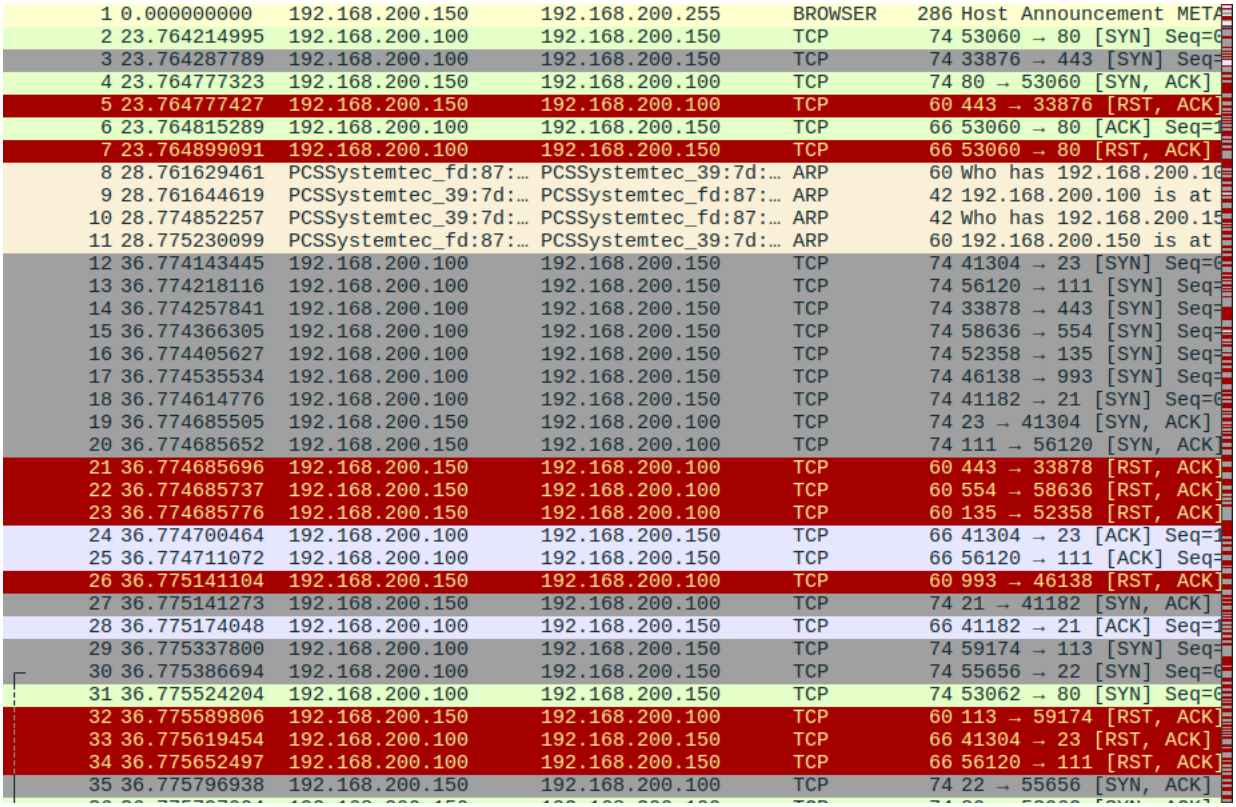
Osserviamo le sue funzioni principali:

- **1** → Elenco dei Log
- **2** → Pacchetto di dati
- **3** → Pacchetto di dati in esadecimale
- **4** → Menu di gestione di Wireshark

2. Analisi dei Flussi e Identificazione Host

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

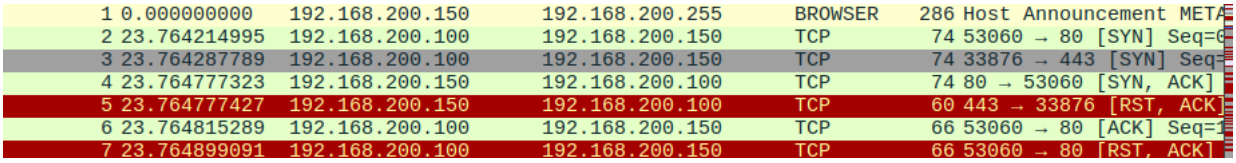
- **192.168.200.100 (Attaccante):** Genera un alto volume di richieste sequenziali.
- **192.168.200.150 (Vittima):** Riceve le richieste.



1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286 Host Announcement META
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74 53060 → 80 [SYN] Seq=0
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74 33876 → 443 [SYN] Seq=
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74 80 → 53060 [SYN, ACK]
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60 443 → 33876 [RST, ACK]
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [ACK] Seq=1
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [RST, ACK]
8	28.761629461	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60 Who has 192.168.200.10
9	28.761644619	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42 192.168.200.100 is at
10	28.774852257	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42 Who has 192.168.200.15
11	28.775230099	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60 192.168.200.150 is at
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74 41304 → 23 [SYN] Seq=0
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74 56120 → 111 [SYN] Seq=
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74 33878 → 443 [SYN] Seq=
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74 58636 → 554 [SYN] Seq=
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74 52358 → 135 [SYN] Seq=
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74 46138 → 993 [SYN] Seq=
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74 41182 → 21 [SYN] Seq=0
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74 23 → 41304 [SYN, ACK]
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74 111 → 56120 [SYN, ACK]
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60 443 → 33878 [RST, ACK]
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60 554 → 58636 [RST, ACK]
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60 135 → 52358 [RST, ACK]
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [ACK] Seq=1
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [ACK] Seq=
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60 993 → 46138 [RST, ACK]
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74 21 → 41182 [SYN, ACK]
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66 41182 → 21 [ACK] Seq=1
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74 59174 → 113 [SYN] Seq=
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74 55656 → 22 [SYN] Seq=0
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74 53062 → 80 [SYN] Seq=0
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60 113 → 59174 [RST, ACK]
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [RST, ACK]
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [RST, ACK]
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74 22 → 55656 [SYN, ACK]

Fig 3. panoramica della schermata dei Log

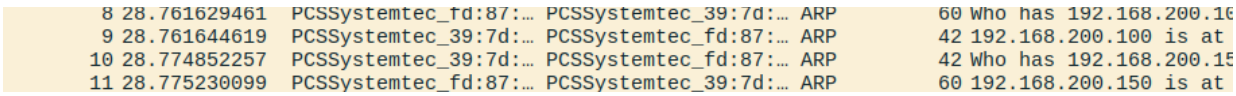
Il log iniziale (Riga 0) mostra un messaggio **broadcast** che identifica la macchina come "**Metasploitable**", un sistema volutamente vulnerabile utilizzato per test di sicurezza.



1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286 Host Announcement META
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74 53060 → 80 [SYN] Seq=0
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74 33876 → 443 [SYN] Seq=
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74 80 → 53060 [SYN, ACK]
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60 443 → 33876 [RST, ACK]
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [ACK] Seq=1
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [RST, ACK]

Fig 4. Log iniziali

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



8	28.761629461	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60 Who has 192.168.200.10
9	28.761644619	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42 192.168.200.100 is at
10	28.774852257	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42 Who has 192.168.200.15
11	28.775230099	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60 192.168.200.150 is at

Fig 5. ARP Request

3. 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**).

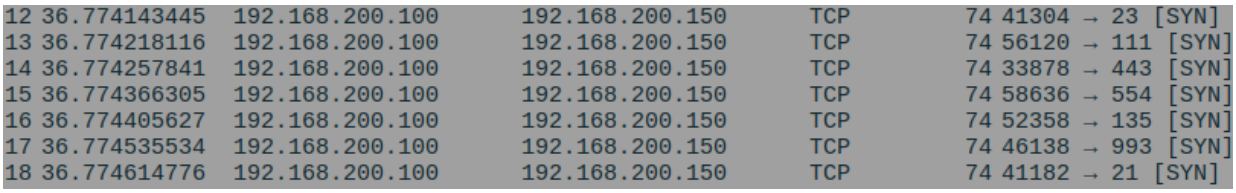


Fig 6. Pacchetti TCP

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.

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.

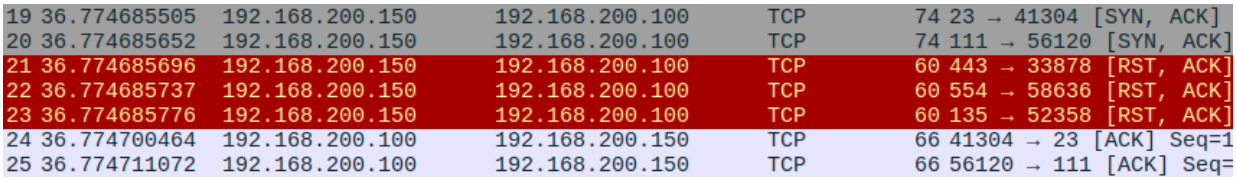


Fig 7. porte 23 e 111 aperte

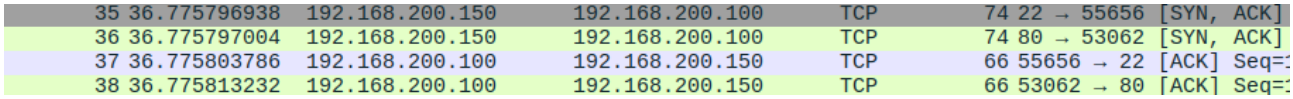


Fig 8. Porta 22 (SSH)

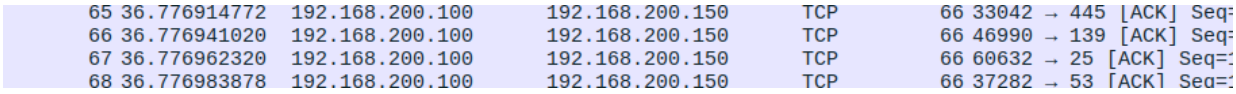


Fig 9. Porte 445, 139, 25, 53

4. 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:

1. **Porta 23 - Telnet:** è un protocollo obsoleto che trasmette tutti i dati, incluse username e password, in chiaro.
    - **Criticità**: Alta.
    - **Rischio**: Un attaccante sulla stessa rete può intercettare le credenziali tramite sniffing (Man-in-the-Middle) e ottenere accesso root alla macchina.

2. **Porte 139 e 445 – Samba/SMB:** Questi servizi gestiscono la condivisione di file e stampanti in rete.
    - **Criticità**: Critica.
    - **Rischio**: SMB è vulnerabile a exploit noti che permettono l'esecuzione di codice remoto (**RCE**). È spesso il punto di ingresso principale per **ransomware** e **worm**.

3. **Porta 21 – FTP:** Come Telnet, FTP trasmette spesso le credenziali in chiaro.
    - **Criticità**: Media/Alta.
    - **Rischio**: Oltre allo sniffing, versioni vecchie di server FTP possono contenere **backdoor** o permettere l'accesso anonimo ai file di sistema.

4. **Porta 111 – RPCbind:** Mappa i numeri dei programmi RPC alle porte di rete.
    - **Criticità**: Media.
    - **Rischio**: Può essere utilizzata per enumerare i servizi RPC attivi sulla macchina, fornendo all'attaccante ulteriori informazioni per mirare l'attacco.

5. Conclusione e Considerazioni

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:

1. **Dismissione Servizi Insicuri:** Disattivare immediatamente **Telnet (23)** e sostituirlo con **SSH (22)**, che garantisce la cifratura del traffico.
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.