Report di Analisi Threat Intelligence

Target: `192.168.200.150` (Metasploitable)

Analista: Victor Rosati

Data: 06/02/2026

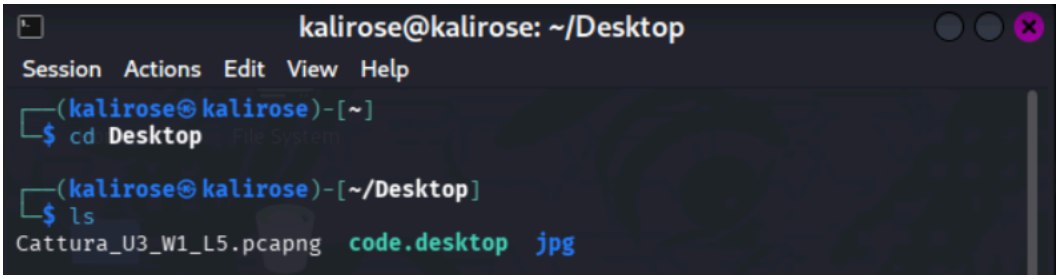
Obiettivo: Identificare evidenze di compromissione (IOC) e potenziali vettori di attacco tramite l'analisi del traffico di rete.

Cos'è Wireshark?

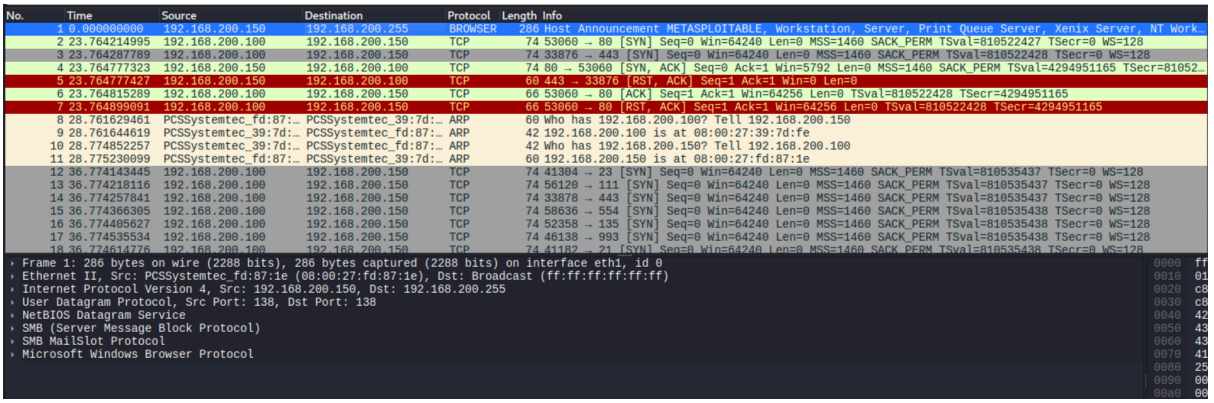
Wireshark è un software di "network sniffing" che permette di catturare e analizzare in tempo reale o tramite file (come il `.pcapng`) tutto il traffico che viaggia su una rete.

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

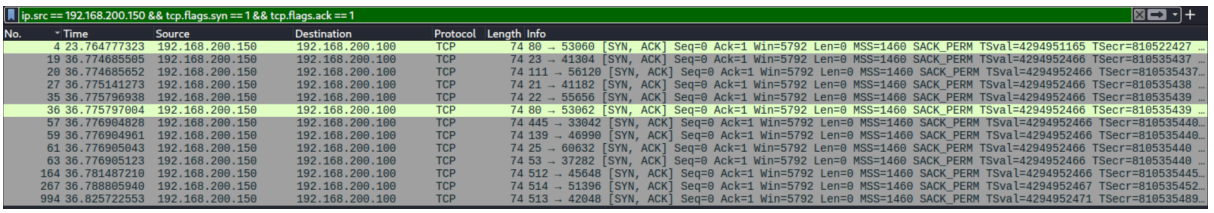
Step dell'Analisi:



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.



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.



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.