

Report Analisi Threat Intelligence: Incidente di Rete (PORT SCANNING)

Data: 06/02/2025

Analista: Nicola Cassandra

Oggetto: Analisi tecnica traffico di rete sospetto e identificazione IOC

1. Sintesi

Il presente rapporto analizza un evento di sicurezza rilevato tramite cattura di traffico di rete (PCAP). L'analisi evidenzia un'attività di **ricognizione attiva** condotta da un host interno alla rete verso un target specifico. L'attività è stata classificata come **TCP Port Scanning** massivo. Non sono state rilevate, in questa fase dell'analisi, evidenze di esfiltrazione dati, ma l'evento rappresenta un preludio a potenziali attacchi mirati.

2. Introduzione

Nell'ambito delle attività di monitoraggio e Threat Intelligence, è stato analizzato un file di log Wireshark ([Cattura_U3_W1_L3.pcapng](#)) contenente traffico di rete sospetto. L'obiettivo del documento è identificare gli attori coinvolti, isolare gli Indicatori di Compromissione (IOC) e proporre strategie di difesa basate sull'evidenza tecnica.

3. Analisi Tecnica dell'Incidente

3.1 Identificazione degli Attori

Dall'analisi dei pacchetti, sono stati identificati due attori principali:

- **Attaccante:** Indirizzo IP **192.168.200.100**. Questo host origina un alto volume di richieste di connessione.
- **Vittima:** Indirizzo IP **192.168.200.150**. L'host ricevente è identificato dal protocollo BROWSER come "METASPLOITABLE" (una macchina vulnerabile nota), workstation e server.

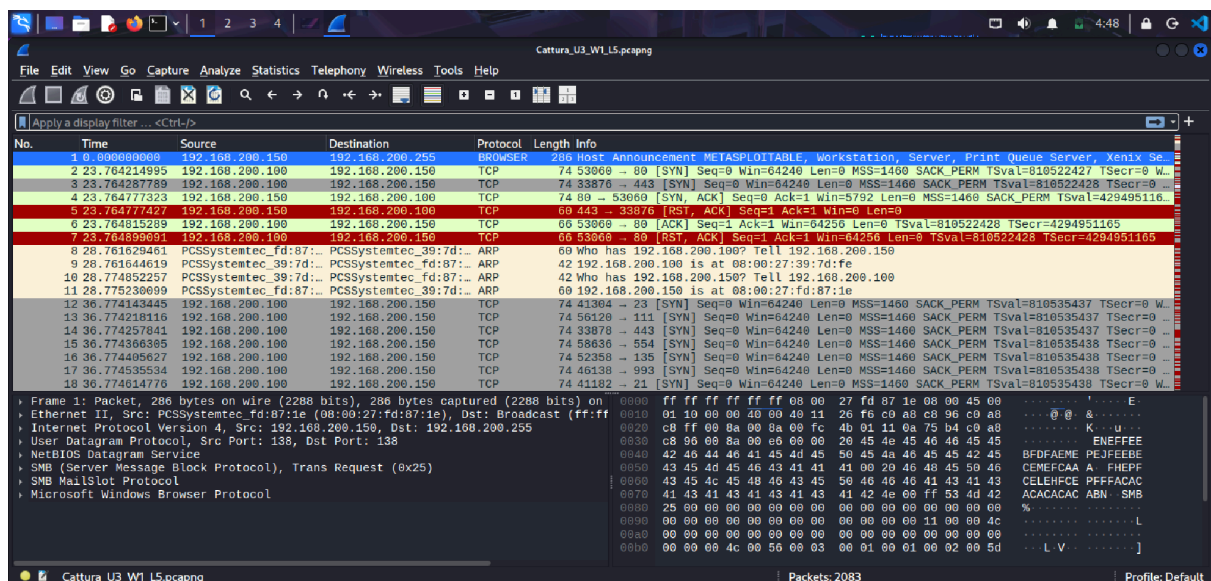


Figura 1: Evidenza iniziale. Al pacchetto n.1 si nota l'annuncio dell'host "Metasploitable" (vittima). Seguono immediatamente tentativi di connessione [SYN] multipli dall'IP .100 verso l'IP .150 su porte diverse.

3.2 Analisi del Traffico

L'attaccante utilizza una tecnica di scansione **TCP SYN Scan** (o "Stealth Scan"). Come visibile dalla cattura, l'IP sorgente **192.168.200.100** invia sequenze rapide di pacchetti con flag **[SYN]** attivato verso porte casuali o sequenziali della destinazione (es. porte 53060, 33076, 53068). L'obiettivo non è stabilire una connessione completa (Three-Way Handshake), ma analizzare la risposta per determinare lo stato della porta.

3.3 Risposta del Target

Nella maggior parte dei casi analizzati nella cattura fornita, il target **192.168.200.150** risponde con pacchetti aventi flag **[RST, ACK]** (Reset, Acknowledge). Tecnicamente, questo indica che **la porta scansionata è chiusa** e il sistema operativo rifiuta attivamente la connessione. L'elevata frequenza di righe rosse (RST) è sintomatica di una scansione "rumorosa" e non mirata.

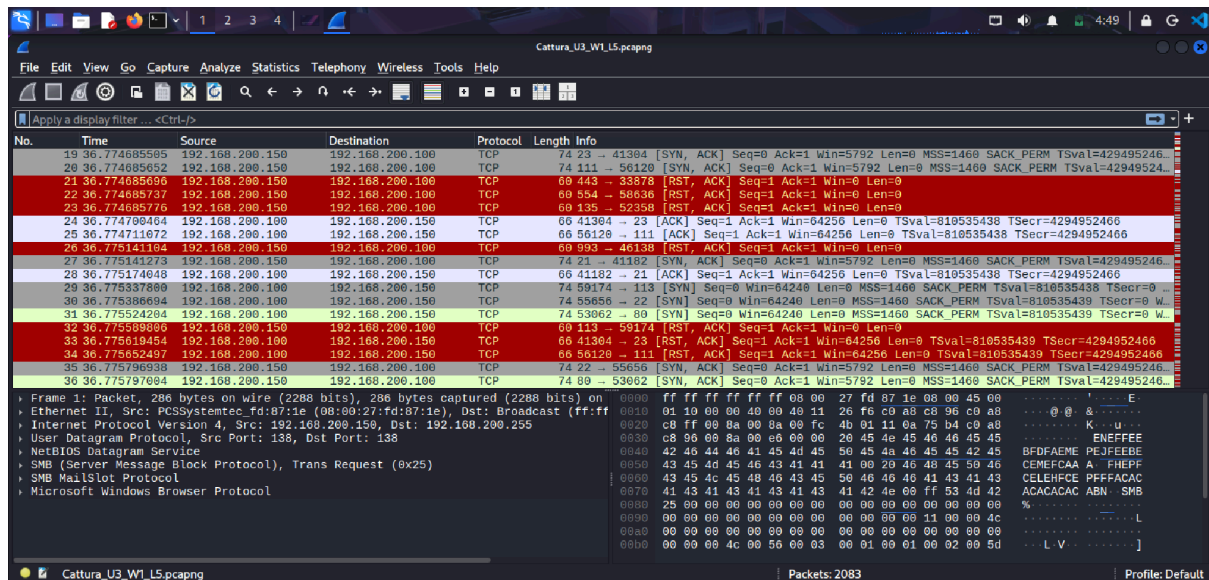


Figura 2: Flusso della scansione. Si evidenzia la massiccia quantità di risposte [RST, ACK] (in rosso) da parte della vittima, indicando che le porte sondate dall'attaccante sono chiuse.

4. Indicatori di Compromissione (IOC)

In base all'analisi effettuata, sono stati isolati i seguenti IOC di tipo "Network":

Tipo	Valore	Descrizione
IP Sorgente	192.168.200.100	Host che origina la scansione (potenziale macchina Kali Linux o attaccante interno).
Pattern	TCP SYN Flood	Alto volume di pacchetti SYN senza completamento handshake in breve lasso di tempo.
IP Destinazione	192.168.200.150	Macchina Target (Metasploitable).

5. Ipotesi sui Vettori di Attacco

L'attività osservata corrisponde alla fase di **Information Gathering** (Raccolta Informazioni) della Cyber Kill Chain.

- **Vettore Ipotezzato:** Utilizzo di tool automatizzati di Network Scanning come **Nmap** o scanner di vulnerabilità.
- **Scopo:** Mappatura della superficie di attacco (Attack Surface Mapping) per individuare servizi attivi vulnerabili da sfruttare in una fase successiva.

6. Strategie di Difesa e Raccomandazioni

Per mitigare l'attacco attuale e prevenire occorrenze future, si consiglia:

1. **Blocco Immediato:** Implementare una regola di blocco (Drop) sul firewall perimetrale o sulle ACL dello switch per il traffico proveniente dall'IP **192.168.200.100**.
2. **Configurazione Firewall (Best Practice):** Modificare la policy di risposta del firewall da **REJECT** (che invia RST e rivela la presenza dell'host) a **DROP** (che scarta il pacchetto silenziosamente), rallentando drasticamente la scansione dell'attaccante.
3. **Intrusion Detection System (IDS):** Configurare regole su IDS (es. Snort/Suricata) per rilevare pattern di "Port Scanning" e attivare un blocco automatico dell'IP sorgente se supera una soglia di richieste al secondo.

7. Conclusioni

L'incidente rappresenta una minaccia di livello medio-alto in quanto preliminare a un attacco mirato. Sebbene la maggior parte delle porte risulti chiusa (come evidenziato dai pacchetti RST), è fondamentale isolare l'host attaccante **192.168.200.100** prima che possa individuare un servizio aperto e vulnerabile.