Report di Analisi del Traffico di Rete

1) Introduzione e obiettivo

L'attuale scenario della sicurezza informatica richiede un'analisi dettagliata del traffico di rete per identificare tempestivamente tentativi di intrusione e attività di ricognizione. Il presente report analizza una cattura di pacchetti (file ***Cattura_U3_W1_L5.pcapng***) effettuata tramite l'applicativo **Wireshark** all'interno di un ambiente di laboratorio controllato. La sessione di monitoraggio ha intercettato un flusso di dati tra un host attaccante (Kali Linux, IP ***192.168.200.100***) e un target vulnerabile (**Metasploitable**, IP ***192.168.200.150***). L'analisi si focalizza sulle prime fasi della **Cyber Kill Chain**, ovvero la ricognizione e l'identificazione degli asset, analizzando le anomalie nei protocolli TCP, ARP e NetBIOS.

L'attività di indagine si pone i seguenti obiettivi principali:

- **Identificazione della Metodologia di Scansione:** Determinare la tecnica utilizzata dall'attaccante per mappare la rete, analizzando la struttura dei flag TCP e la frequenza dei pacchetti.
- **Mappatura della Superficie di Attacco:** Individuare quali servizi e quali porte del target sono state sollecitate per determinare, in base alle risposte dell'host (***SYN/ACK vs RST/ACK***), quali risultino effettivamente esposte.
- **Rilevamento di Anomalie di Rete:** Documentare eventuali errori di protocollo, ritrasmissioni o tentativi di connessione falliti che possano indicare la presenza di sistemi di difesa o configurazioni di rete specifiche.

1) Riepilogo dell'Attività

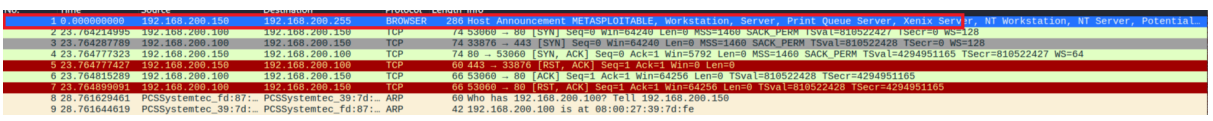
L'analisi del traffico evidenzia un interazione intensa tra due host principali sulla sottorete **`192.168.200.0/24`**. L'attività predominante è costituita da tentativi di connessione TCP rapidi verso diverse porte, molti dei quali terminano con un reset della connessione.

- **Sorgente (Attaccante/Scanner): `192.168.200.100`**
- **Destinazione (Target): `192.168.200.150`**

2) Analisi dei Protocolli e Flussi

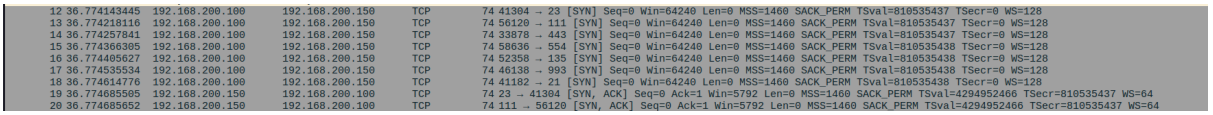
-Host Discovery (Pacchetto 1)

Il primo pacchetto mostra un annuncio browser (protocollo BROWSER) dove l'host ***.150*** si identifica esplicitamente come **METASPLOITABLE**. Questo indica che il target è una macchina vulnerabile intenzionale, spesso usata per laboratori di penetration testing.

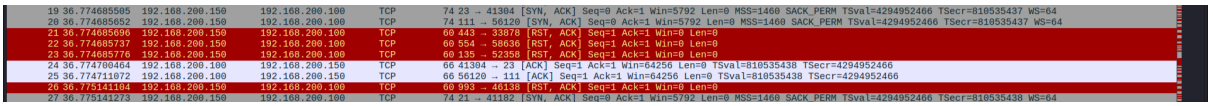


-Port Scanning (TCP SYN Scan)

A partire dal **pacchetto n. 12**, si osserva una sequenza di pacchetti **TCP SYN** provenienti dall'host ***.100*** verso l'host ***.150*** su diverse porte (es. 23, 111, 443, 554, 135, 993, 21, 110, ecc.).



- **Comportamento:** La sorgente invia **SYN**; se la porta è chiusa, la destinazione risponde con **RST, ACK** (le righe rosse, es. pacchetti 21, 26, 32).



- **Tecnica:** Questo pattern è probabilmente un ***nmap -st*** che chiede al sistema operativo di completare l'intera procedura di connessione standard con ogni porta che sta scansionando.

  -SYN: Nmap invia un pacchetto di richiesta connessione.

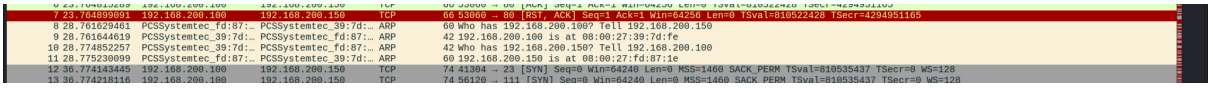
  -SYN/ACK: Se la porta è **aperta**, il bersaglio risponde accettando.

  -ACK: Nmap risponde a sua volta, **completando la connessione** (handshake).

  -RST: Subito dopo, Nmap chiude la connessione per passare così alla porta successiva.

-Analisi ARP (Pacchetti 8-11)

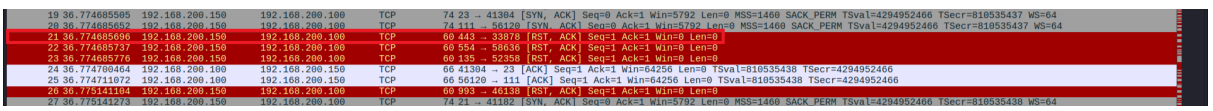
Si notano diverse richieste **ARP** ("**Who has**..."). Questo indica che gli host stanno risolvendo gli indirizzi MAC per comunicare nel segmento di rete locale.



3) Analisi degli Alert (Righe Rosse)

Le righe evidenziate in **rosso** in Wireshark indicano pacchetti con flag **RST (Reset)** o problemi di ritrasmissione.

- **Significato:** L'host ***.150*** sta attivamente rifiutando le connessioni sulle porte che non ha attive. Ad esempio, nel pacchetto 21, la porta 443 (HTTPS) risponde con un RST, indicando che il servizio non è disponibile o è filtrato.



4) Conclusioni Tecniche

In conclusione, l'analisi del traffico catturato nel file ***Cattura_U3_W1_L5.pcapng*** evidenzia un'attività sistematica di **network scanning** e tentativi di connessione tra gli host della sottorete ***192.168.200.0/24.***

I punti chiave emersi sono:

- **Scansione delle Porte:** Si osserva un elevato numero di pacchetti TCP con flag [**SYN**] diretti verso varie porte (come la 21, 22, 23, 80, 111, 135, 139, 443, 445 e altre) dell'host ***192.168.200.150***. Questo comportamento è tipico di una fase di **Enumerazione** o **Port Scanning**.
- **Risposte del Target:** Molte di queste richieste ricevono un pacchetto [***RST, ACK***] (evidenziato in rosso), il che indica che le porte corrispondenti sul target sono chiuse o che un firewall sta attivamente rifiutando la connessione.
- **Protocolli Identificati:** Oltre al traffico TCP, la presenza di pacchetti **ARP** per la risoluzione degli indirizzi MAC e di annunci **BROWSER/NetBIOS** suggerisce una fase di scoperta dei servizi Windows/Samba all'interno della rete locale.
- **Configurazione dell'Ambiente:** L'annuncio iniziale ("METASPLOITABLE, Workstation, Server...") conferma che l'analisi si sta svolgendo in un ambiente di test controllato, mirato all'identificazione di vulnerabilità su macchine bersaglio specifiche.