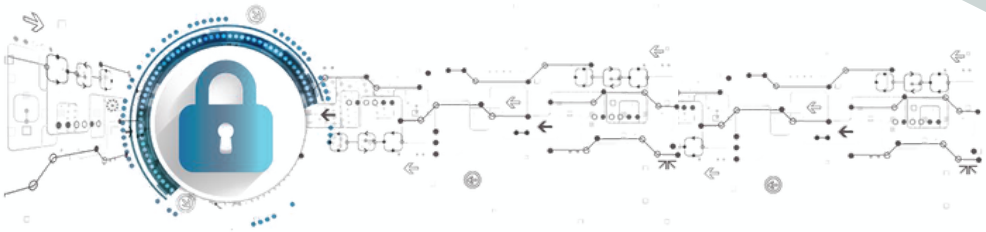


Esercizio per il progetto settimanale Unit 3 - S9 - L5

Data una cattura di rete effettuata con **Wireshark**. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare ed analizzare eventuali **IOC**, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali **vettori di attacco** utilizzati
- Consigliate un'azione per **ridurre** gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro

Threat Intelligence (TI)

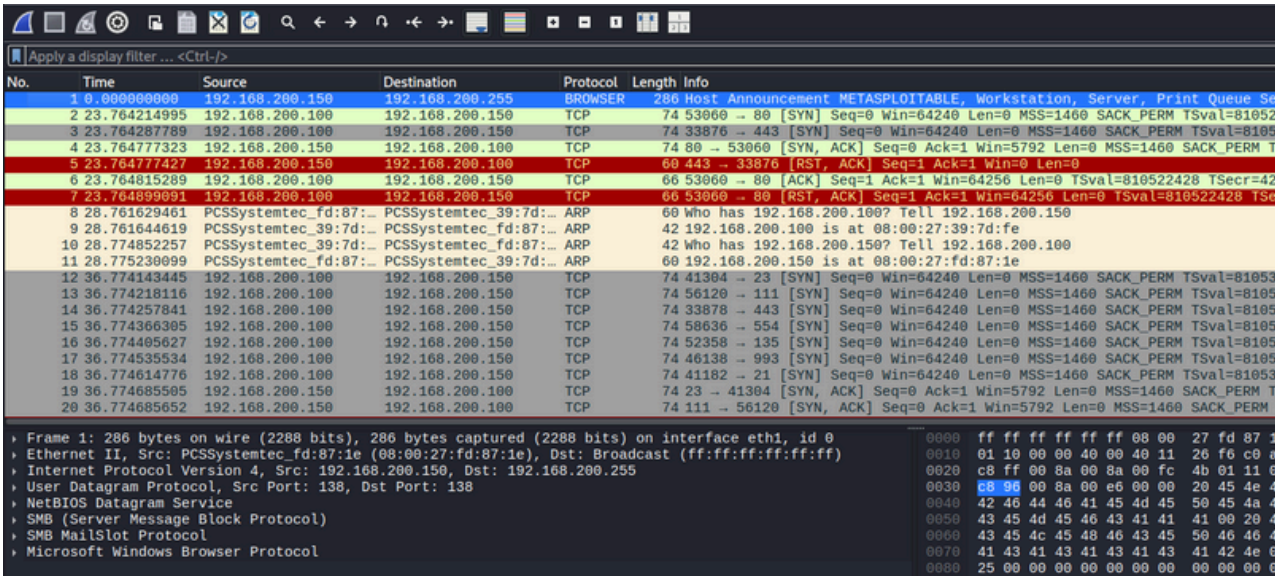
La Threat Intelligence (TI) è la **raccolta**, **l'analisi** e la condivisione di **informazioni** su minacce attuali e potenziali alla sicurezza informatica. Queste informazioni provengono da diverse fonti e includono **dettagli** sui cyber attacchi, sulle **vulnerabilità** dei sistemi, sulle tattiche degli attaccanti e sugli indicatori di compromissione (IoC).

Indicatori di Compromissione (IoC)

Gli Indicatori di Compromissione (IoC) sono **segnali** specifici che indicano che un sistema o una rete è stata **compromessa** da un attacco informatico. Tra i principali tipi di IoC si trovano indirizzi IP e **domini malevoli**, hash di file sospetti, **processi anomali** e modifiche non autorizzate ai file. Questi indicatori sono essenziali per la sicurezza informatica, poiché aiutano a **rilevare** le minacce, a guidare le azioni di **risposta** agli incidenti e a **prevenire** attacchi futuri attraverso l'uso di liste di controllo aggiornate.

La traccia di rete mostra un **attacco** in corso dove l'attaccante (192.168.200.100) sta eseguendo un attacco **brute-force** (data la ripetizione) contro un server (192.168.200.150), identificato come una macchina Metasploitable.

Oltre ad un attacco brute-force la traccia mostra la sequenza di pacchetti con flag **SYN, ACK e RST, ACK,** questo è il comportamento tipico di una **scansione di porte** automatizzata, in cui un attaccante cerca di identificare quali porte sono **aperte** su un host bersaglio.
I pacchetti inviati al server Metasploitable mirano a ottenere accesso **non autorizzato** al sistema.

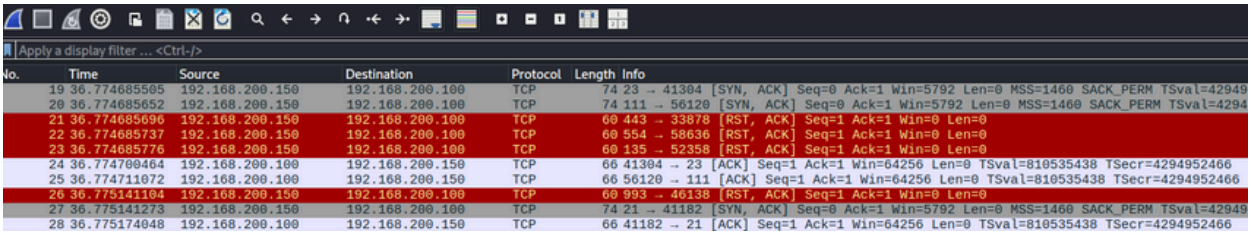


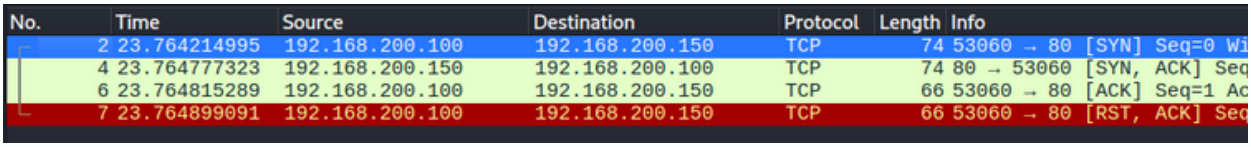
La stringa TCP 66 53908 -> 80 mostra che l'attaccante sta tentando di **scansionare** le porte aperte sul server Metasploitable per trovare una vulnerabilità.
Il traffico mostra numerosi tentativi di connessione, in particolare verso la **porta 445**, che è la porta standard del protocollo Server Message Block (**SMB**). Ciò indica che l'attaccante ha identificato il servizio SMB come un potenziale punto debole mirando l'attacco brute-force nel sfruttare una potenziale **vulnerabilità** in questo servizio.

Il protocollo **SMB** (Server Message Block) usato per la condivisione di file è spesso preso di mira negli attacchi brute-force per tentare di accedere a cartelle condivise o altri servizi. Molti attacchi di malware e **ransomware** (come WannaCry) hanno sfruttato in passato vulnerabilità in SMB.

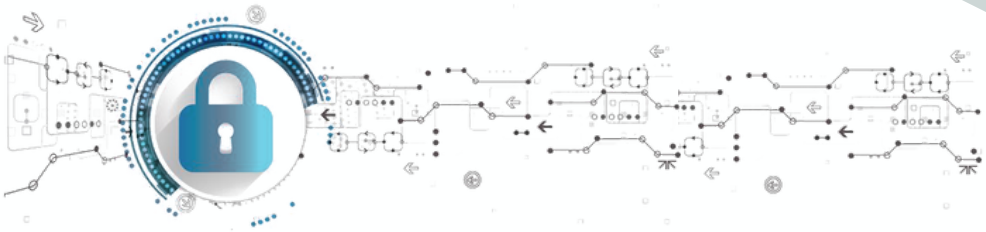
Dettagli sull'attacco:
L'attaccante ha iniziato una scansione di porte per capire quali servizi sono attivi sul server 192.168.200.255. Troviamo pacchetti con i flag SYN inviati a diverse porte, come la porta 80 (HTTP) e la porta 445 (SMB). La scansione della porta 80, è un tentativo per capire se c'è un server web in esecuzione.
La scansione della porta 445 e il traffico SMB che abbiamo visto successivamente indicano che l'attaccante ha identificato il servizio SMB come un potenziale **punto debole**.

Il pacchetto **RST** viene usato per interrompere una connessione in modo anomalo. Se l'attaccante sta eseguendo una scansione stealth (-sS), dopo aver ricevuto un SYN, ACK dal server, invia un RST per chiudere la connessione prima che sia completamente stabilita. L'obiettivo è sondare una porta aperta senza lasciare tracce nei log del server. In questo caso, l'attaccante ha ottenuto le informazioni che cercava e non ha bisogno di continuare la connessione.
Per esempio nella port 80 dopo la scansione full connect (-sT) usa RST per chiudere immediatamente la connessione che ha appena stabilito. Questo è un modo per minimizzare il tempo di connessione e nascondere la sua attività.





Per un attacco di successo era necessaria la mancanza di RST cosi che dopo la risposta con un pacchetto ACK per completare l'handshake a tre vie (three-way handshake) si sarebbe stabilita la connessione e l'attaccante avrebbe iniziato a scambiare dati con il server. Questo poteva includere l'invio di comandi, il download di dati sensibili o l'upload di **malware**.



Vettori di attacco

- **Attacco di forza bruta (brute-force)**: La serie di tentativi di connessione falliti indica un attacco di forza bruta.
- **Sfruttamento di vulnerabilità**: L'attaccante sta tentando di sfruttare una vulnerabilità nel protocollo SMB per ottenere l'accesso non autorizzato al server**.**
- **Scansione di porta**: L'attaccante sta cercando una porta aperta per penetrare nel sistema.

Azioni di prevenzione

- **Bloccare** l'indirizzo IP dell'attaccante sul firewall per interrompere immediatamente la scansione e l'attacco.
- **Isolare** il server compromesso dalla rete per evitare che possa essere usato come punto di partenza per ulteriori attacchi.
- **Applicare patch di sicurezza**: Verificare che il sistema operativo e i servizi esposti (in questo caso, SMB) siano completamente aggiornati con le ultime patch di sicurezza per correggere eventuali vulnerabilità note.
- **Configurare un firewall**: Impostare regole sul firewall per limitare il traffico in entrata solo alle porte e agli indirizzi IP necessari, bloccando tutto il resto.
- **Implementare un IPS**: Utilizzare un Intrusion Prevention System (IPS) per rilevare e bloccare automaticamente comportamenti sospetti come le scansioni di porte. In aggiunta implementare un **EDR o XDR** per rilevare e rispondere a minacce che bypassano l'IPS.