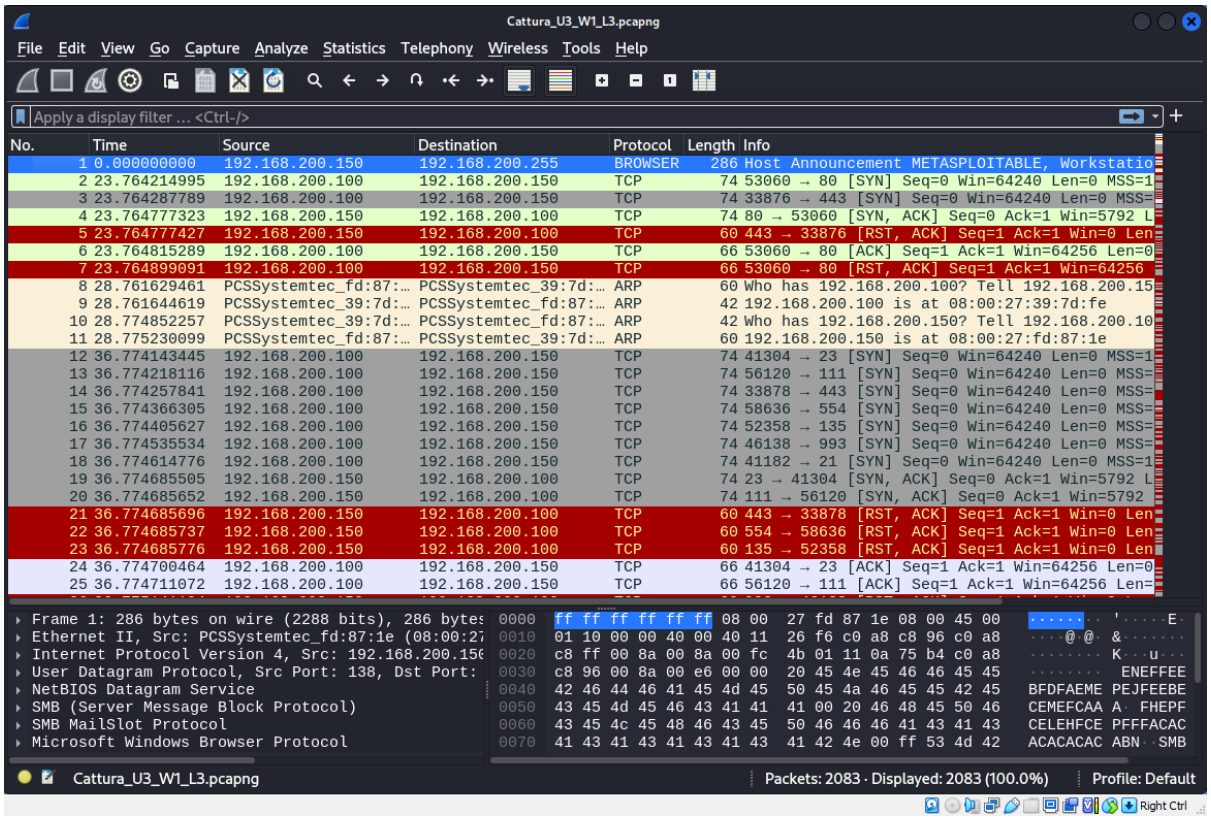
PROGETTO S9/L5

Wireshark:



Che attacco e':

Un attacco SYN scan è una tecnica comunemente usata per eseguire una scansione delle porte su un sistema di rete. Viene sfruttato durante la fase di ricognizione in un attacco informatico per identificare quali porte di un determinato host sono aperte e quindi potenzialmente vulnerabili a ulteriori exploit.

Come funziona:

Il SYN scan si basa sul protocollo TCP e sul suo processo di handshake a tre vie. Ecco come si svolge:

Inizio della scansione: L'attaccante invia un pacchetto TCP con il flag SYN attivo (che segnala l'inizio di una connessione) verso una porta specifica su un host di destinazione.

Risposta dell'host:

Se la porta è aperta, l'host risponde con un pacchetto SYN-ACK (che indica che accetta la richiesta di connessione).

Se la porta è chiusa, l'host risponde con un pacchetto RST (reset), che indica che la connessione non può essere stabilita.

Comportamento dell'attaccante:

Dopo aver ricevuto un SYN-ACK, l'attaccante invia un pacchetto RST per interrompere la connessione, senza completare l'handshake a tre vie (evitando di stabilire una connessione completa).

Se riceve un RST, l'attaccante sa che la porta è chiusa e non esegue alcuna azione successiva.

Vantaggi di un SYN Scan:

Rapido: Poiché non viene completata la connessione completa, la scansione è veloce e leggera in termini di traffico generato.

Discreto: Essendo che non viene stabilita una connessione completa, questo tipo di scansione può passare inosservato ai sistemi di rilevamento intrusione (IDS), che tendono a loggare connessioni complete.

Azioni consigliate per ridurre l'impatto o attacchi simili in futuro:

La mitigazione di un attacco SYN scan richiede l'implementazione di diverse misure di sicurezza per ridurre la possibilità che un attaccante riesca a eseguire con successo questo tipo di scansione delle porte. Ecco alcune tecniche comuni che possono essere adottate:

1. Utilizzo di un Firewall

Blocco del traffico non necessario: Configura il firewall per bloccare le richieste SYN provenienti da fonti sospette o non autorizzate. Puoi limitare il traffico TCP solo ai servizi effettivamente in uso e necessari per il corretto funzionamento della rete.
Filtraggio delle porte: Configura il firewall per ignorare i pacchetti SYN inviati verso porte che non dovrebbero essere pubbliche o esposte su Internet, nascondendo così le porte

non necessarie agli attaccanti. Stealth Mode: Alcuni firewall possono essere configurati per rispondere a qualsiasi pacchetto SYN con un RST, in modo che l'attaccante non sia in grado di distinguere tra porte aperte o chiuse.

2. Rate Limiting
   Limitazione della frequenza delle connessioni: Implementa meccanismi di rate limiting che limitano il numero di richieste SYN che un host può inviare in un dato intervallo di tempo. Ciò rende più difficile per un attaccante eseguire una scansione veloce su molte porte. SYN flood protection: Alcuni firewall o router possono applicare protezioni contro le inondazioni SYN (SYN flooding), bloccando o rallentando le richieste SYN che arrivano a una velocità anomala.

3. TCP SYN Cookies

   SYN cookies: Questa tecnica è una soluzione a livello di kernel che viene utilizzata per prevenire attacchi SYN flood. Funziona generando un cookie criptato nel campo sequenza TCP durante l'handshake SYN-ACK, che viene verificato quando la connessione viene confermata. Anche se non blocca le scansioni SYN, aiuta a mitigare gli effetti negativi di attacchi basati sull'inondazione di SYN.

4. Intrusion Detection Systems (IDS) e Intrusion Prevention Systems (IPS)
   Rilevamento delle scansioni: Gli IDS/IPS possono essere configurati per monitorare il traffico alla ricerca di segni di scansioni SYN sospette. Quando una scansione SYN viene rilevata, possono attivare allarmi o bloccare temporaneamente il traffico proveniente dall'indirizzo IP sospetto. Prevenzione delle minacce in tempo reale: Gli IPS possono bloccare automaticamente il traffico proveniente da IP che eseguono una scansione SYN, prevenendo eventuali futuri tentativi di attacco.