Cyber Security Report

W19D4

19/11/2025

Autore :
Pace Massimiliano

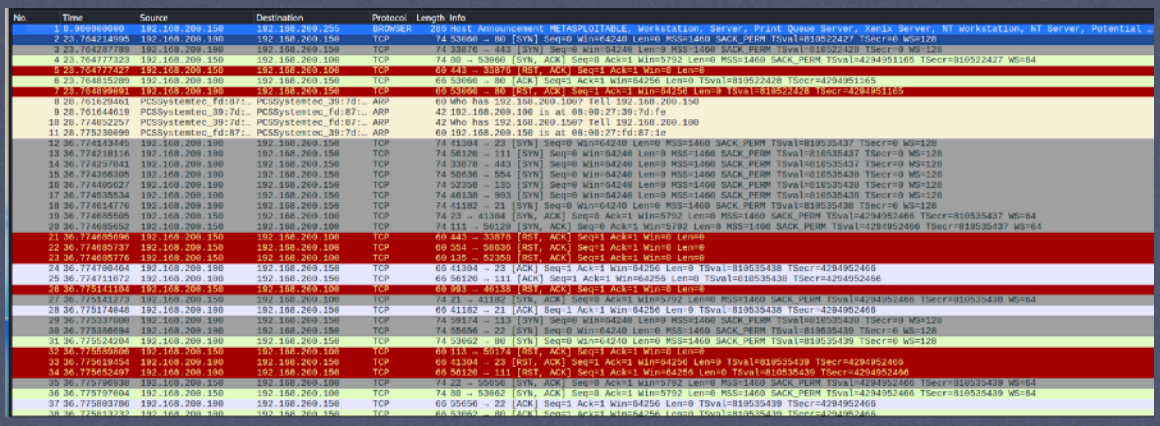
email : *efmpas@gmail.com*

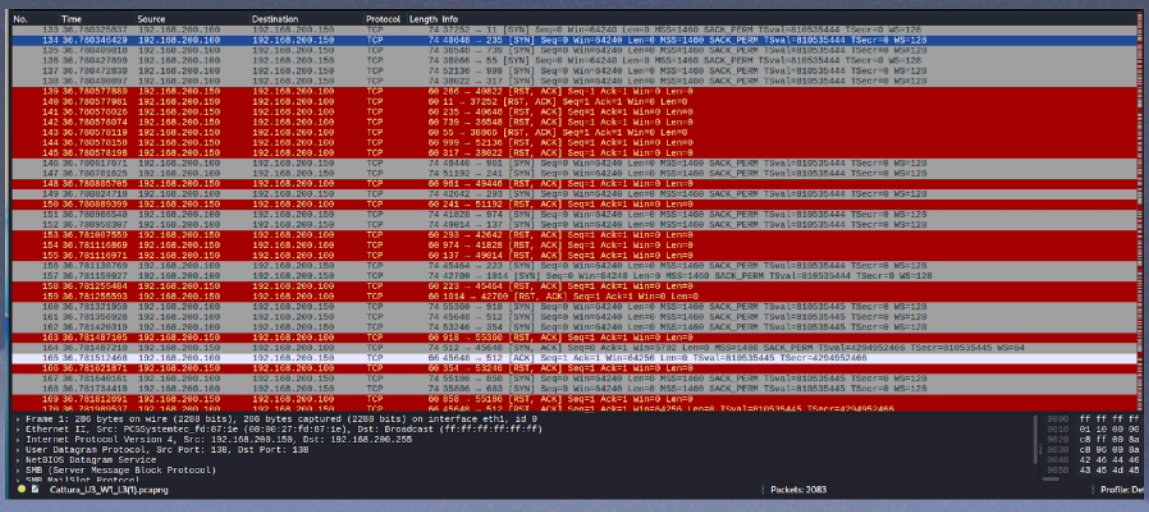
Indice :

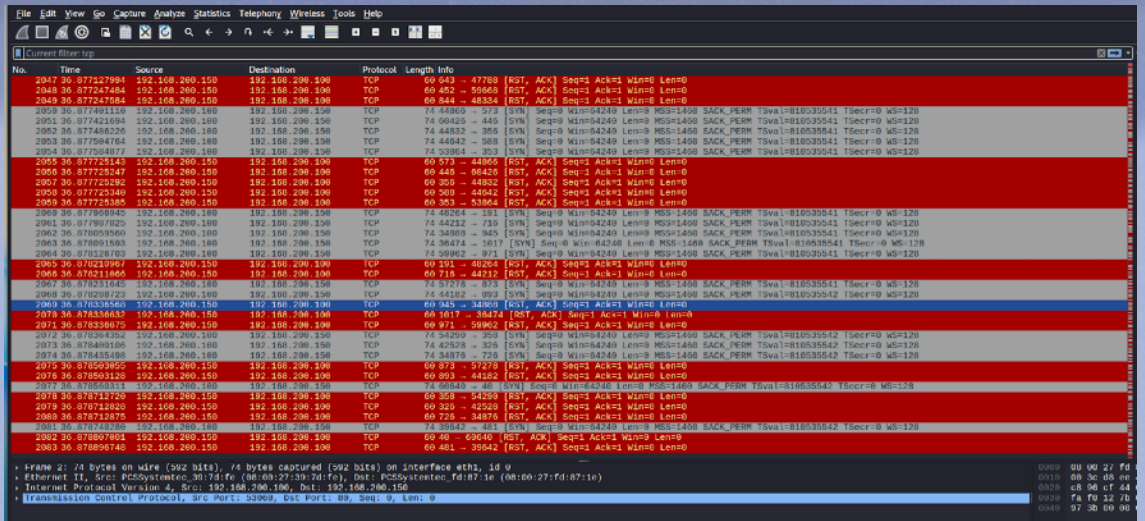
INTRODUZIONE ANALISI FILE PCAPNG CON WIRESHARK

° L'ESERCIZIO W19D4 CONSISTE NELL'ANALISI DI UN FILE DI CATTURA DEL TRAFFICO DI RETE VISUALIZZABILE TRAMITE WIRESHARK

FOTO ALLEGATE :







DESCRIZIONE ATTACCO

Questi screenshot mostrano il traffico di rete catturato ed analizzato tramite Wireshark, concentrandosi soprattutto sui pacchetti TCP tra gli host della rete locale nelle IP 192.168.200.150/100/109/159. Si osservano diversi pattern che permettono di dedurre la natura dell'attacco.

Osservazioni principali

•La maggior parte del traffico consiste in pacchetti TCP con flag SYN, ACK, RST, ACK, spesso alternati e generati in successione molto rapida, come visibile nei numerosi pacchetti evidenziati in rosso (RST).
•La costante presenza di pacchetti SYN seguiti da RST, ACK suggerisce un tentativo di connessione TCP che viene sistematicamente rifiutata o resettata dal server di destinazione.
•Spuntano anche pacchetti ARP e qualche annuncio NetBIOS, ma il volume maggiore riguarda sempre il TCP a livello di handshake.
•Nei flag SYN visualizzati, i numeri di porta di destinazione cambiano spesso, mentre la porta sorgente rimane stabile. Questo pattern è tipico di uno scan.

Analisi del pattern di traffico

•Il traffico mostrato negli screenshot è compatibile con un TCP SYN scan (detto anche "half-open scan"), spesso utilizzato dagli strumenti di scanning come Nmap per mappare le porte aperte senza stabilire una connessione completa (Three-way handshake).
•L'altro pattern, ovvero la presenza massiccia di pacchetti RST, ACK, può puntare anche ad un Denial of Service (DoS) oppure, tenendo conto della sistematicità e dei diversi IP coinvolti, ad un Distributed Denial of Service (DDoS). Tuttavia, qui pare che il traffico sia generato da pochi host interni, quindi la natura più probabile è quella di uno scan e non di un DDoS di ampia scala.

Dettaglio sulle specifiche degli screenshot

•Gli screenshot mostrano l'utilizzo di un filtro TCP su Wireshark, riportando solo pacchetti TCP, riducendo il rumore dei protocolli diversi e facendo emergere l'anomalia nel flusso handshake/reset.
•Il flusso di pacchetti SYN, seguito immediatamente o dopo breve tempo da RST, è fortemente indicativo di un ambiente in cui si sta cercando attivamente di rilevare le porte aperte su un server/host, molto probabilmente tramite uno strumento automatizzato.

Conclusione

Il tipo di attacco che risulta più evidente dagli screenshot è un TCP SYN Scan, tipicamente usato per mappare porte e servizi attivi su uno o più host della LAN. Questo comportamento è compatibile con una fase di reconnaissance precedente ad un exploitation.

Se il traffico fosse ancora più massiccio e da molteplici sorgenti, potrebbe leggersi come tentativo di DoS/DDoS, ma da questi screenshots il pattern è quello del port scanning.

Se hai usato tool come Nmap, Masscan o simili su questa rete, questo tipo di cattura è il risultato normale del loro utilizzo. Se invece non hai avviato alcun tool di scanning, potresti essere di fronte a una ricognizione non autorizzata sulla tua LAN.