REPORT 21/12/2022

FACCILONGO DOMENICO

THREAT INTELLIGENCE & IOC

TASK

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare 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

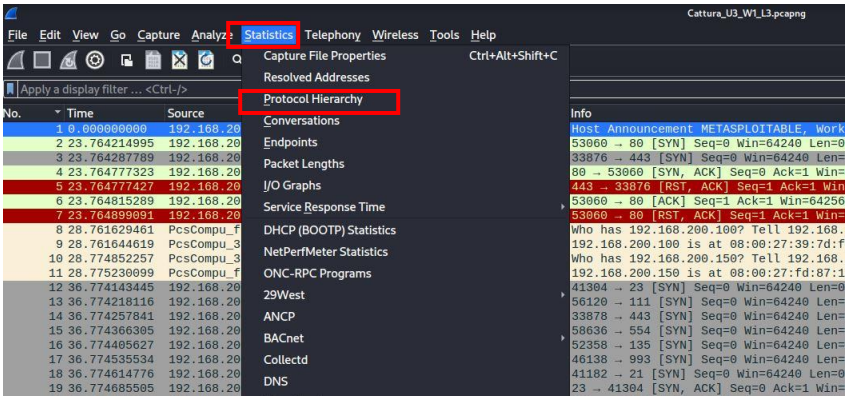
Cattura_U3_W1_L3.pcapng

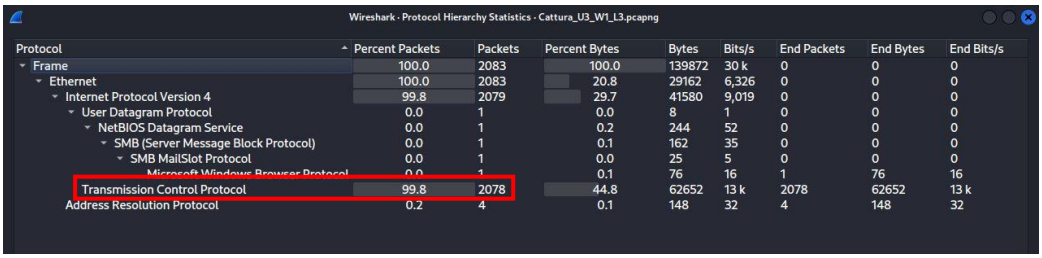
ANALISI E VALUTAZIONE DEL FILE

Come prima cosa andiamo ad analizzare i file di Wireshark per andare a identificare eventuali IOC. Quest'ultimi "**indicatori di compromissione"** non sono altro che delle prove/indizi di una violazione dei dati. Questi indicatori infatti possono rilevare che si è verificato un attacco, quali strumenti sono stati utilizzati nell'attacco e chi c'è dietro.

Andando ad analizzare il file di wireshark come da esercizio ritroviamo che i pacchetti inviati sono tutti del tipo TCP, e lo si può notare andando nella sezione di wireshark che segue:

statistics → Protocol Hierarchy

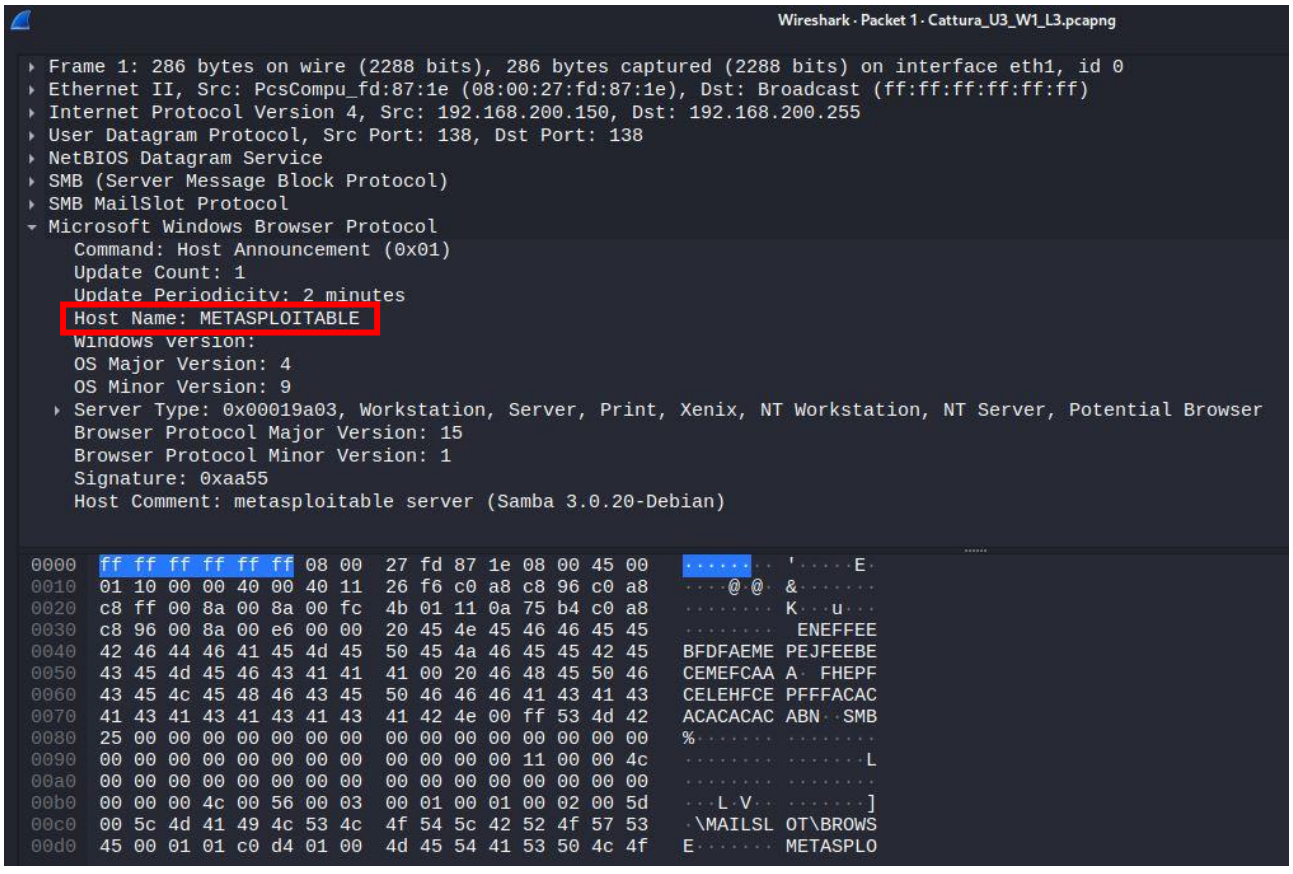




Questo ci permette di intuire che tutti i pacchetti trasmessi sono del tipo TCP, i rimanenti invece sono:

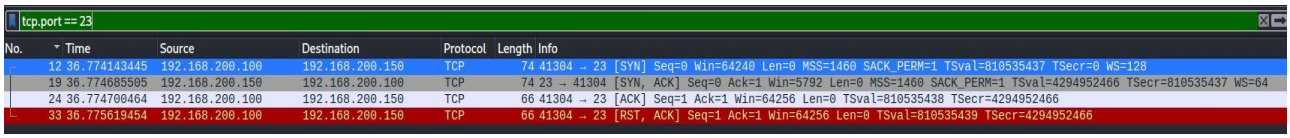
- 1 BROWSER: Che instaura la connessione tra Source e Host server.
- 4 ARP: Che serve per conoscere l'indirizzo MAC una volta noto l'indirizzo IP di destinazione.

Analizzando il singolo pacchetto **Browser** si possono ottenere informazioni riguardante l'Host, andando nella sezione che segue come da immagine:

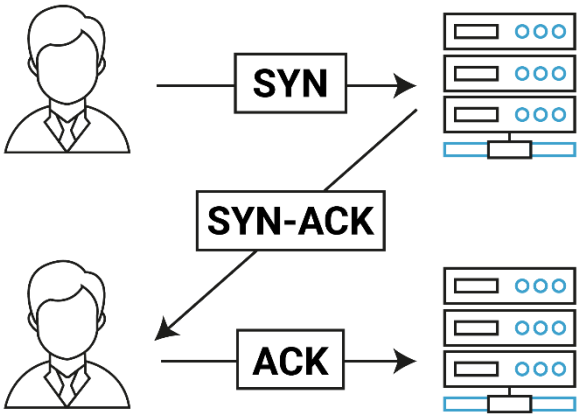


Quindi abbiamo scoperto in questo caso che la macchina vittima è METASPLOITABLE.

Analizzando i pacchetti TCP filtrando ad una porta (es. 23), con il comando ***<<tcp.port == 23>>*** i risultati ottenuti sono:



Questo ci permette di intuire che è stata avviata una connessione tra le due macchine, con indirizzo IP dell'attaccante del tipo 192.168.200.100 e quello della vittima 192.168.200.150, il tutto dovuto al **Three-Way Handshake** il quale permette di instaurare la connessione inviando i pacchetti:



1. SYN
2. SYN + ACK
3. ACK

Nell'analisi dei pacchetti inviati ad una singola porta notiamo che la connessione è stata instaurata e dopo conclusa come si evince dall'ultimo pacchetto (RST, ACK). Il sospetto principale è che l'attaccante abbia voluto scansionare la nostra macchina vittima, attraverso esempio con il tool **nmap** dovuto a delle multiple richieste TCP su ampi intervalli di porte.

Possiamo ora ipotizzare che tipo di scansione abbia potuto sfruttare l'attaccante. Tra quelle conosciute, sappiamo che:

- **sS**: è una scansione che non instaura la connessione è che quindi dopo il primo SYN + ACK la connessione si conclude
- **sT**: è una scansione che instaura la connessione e che quindi conclude il Three-way Handshake
- **sV**: è una scansione molto più invasiva delle ultime due con risultato finale simile ad esse con aggiunta delle versioni dei servizi.
- **A**: anch'essa scansione invasiva simile alla precedente fornendo anche informazioni del dispositivo vittima.

Andando per esclusione: -sS nell'analisi con Wireshark non avrebbe dovuto fornire l'ACK finale di avvenuta connessione e quindi scartata. Pertanto le uniche opzioni sarebbero potuto essere -sT, -sV e -A.

Quindi possiamo supporre che il nostro attaccante avrebbe voluto avere informazioni sulla nostra macchina per andare a sfruttare, tra i risultati della scansione, le porte aperte. Ad esempio potrebbe sfruttare il tool Nessus per andare ad analizzare le vulnerabilità più critiche tra le porte aperte e utilizza Metasploit per entrarci.

RISOLUZIONE DEL PROBLEMA:

Supponiamo in questo esempio di essere noi la vittima, come avremmo potuto evitare che un utente esterno possa scansionare il nostro dispositivo?

1. Tra le soluzioni la prima mi sembrerebbe la più ovvia, ovvero inserimento di un firewall che permetta di evitare questa scansione. Essendo Host Metasploitable la soluzione sarebbe quella di sfruttare **iptables** e creare di conseguenza una regola che non permetta la comunicazione con altre macchine.
2. Un'altra soluzione è quella di inserire l'IP sorgente dell'attaccante all'interno di una **blacklist** e di conseguenza non permettere a quest'ultimo di avere alcuna comunicazione con la nostra macchina. Di seguito una guida per come bloccare un indirizzo IP: https://verytech.smartworld.it/come-bloccare-un-indirizzo-ip-274978.html#steps_3