# Esercizio\_S8\_L5\_Threat\_Intelligen ce\_&\_IOC

## Consegna

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 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.

# Svolgimento

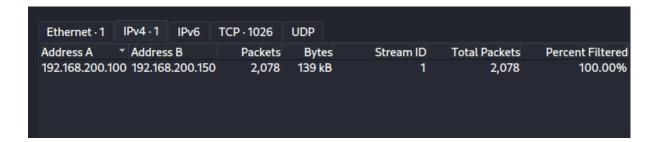
Per iniziare ho aperto il pcapng con wireshark.

Una volta aperto ci troviamo dinanzi a 2083 pacchetti.

Per avere una visuale quanto più chiara possibile mi sono subito spostato all'interno della sezione Statistics > Protocol Hierachy, per comprendere a che tipologia di connessioni fossero presenti ed in che quantità; qui ho potuto constatare che tutti i pacchetti avvengono su protocollo TCP.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
▼ Frame	100.0	2078	100.0	139382	85 k
▼ Ethernet	100.0	2078	25.2	35170	21 k
<ul> <li>Internet Protocol Version 4</li> </ul>	100.0	2078	29.8	41560	25 k
Transmission Control Protocol	100.0	2078	44.9	62652	38 k

A quel punto, ho deciso di visionare quali IP fossero coinvolti all'interno del pcapng e mi sono dunque diretto verso Statistics > Conversations; a questo punto notiamo chiaramente che tutte le comunicazioni avvengono tra un indirizzo A 192.168.200.100 ed un indirizzo B 192.168.200.150:



Spostandosi poi nella sezione TCP possiamo dare un'occhiata alle varie connessioni intraprese tra i due host. A questo punto si nota che esiste una comunicazione con **almeno due pacchetti** per tutte le prime 1024 porte.

Ordinando poi il tutto per le quantità di pacchetti trasmessi per ogni porta notiamo che le porte 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513 e 514 hanno tutte avute uno scambio di 4 pacchetti.

Ethernet · 1	IPv4·1	IPv6	TCP · 1026	UDP			
Address A	Port	A Add	ress B	Port B	Packets *	Bytes	Stream ID
192.168.200.10	0 4118	2 192.	168.200.150	21	4	280 bytes	8
192.168.200.10	0 5565	6 192.	168.200.150	22	4	280 bytes	10
192.168.200.10	0 4130	4 192.	168.200.150	23	4	280 bytes	2
192.168.200.10	0 6063	2 192.	168.200.150	25	4	280 bytes	19
192.168.200.10	0 3728	2 192.	168.200.150	53	4	280 bytes	21
192.168.200.10	0 5306	0 192.	168.200.150	80	4	280 bytes	0
192.168.200.10	0 5306	2 192.	168.200.150	80	4	280 bytes	11
192.168.200.10	0 5612	0 192.	168.200.150	111	4	280 bytes	3
192.168.200.10	0 4699	0 192.	168.200.150	139		280 bytes	17
192.168.200.10	0 3304	2 192.	168.200.150	445		280 bytes	15
192.168.200.10	0 4564	8 192.	168.200.150	512		280 bytes	68
192.168.200.10	0 4204	8 192.	168.200.150	513	4	280 bytes	480
192.168.200.10	5139	6 192.	168.200.150	514		280 bytes	118
192.168.200.10	0 3739	6 192.	168.200.150	1		134 bytes	874
192.168.200.10	3474	8 192.	168.200.150	2	2	134 bytes	292
192.168.200.10	0 5893	8 192.	168.200.150	3	2	134 bytes	966

Andando poi a filtrare le comunicazioni delle porte con 4 pacchetti, in questo caso la 21, tramite tcp.port==21 possiamo chiaramente notare che avviene una comunicazione three-way handshake che genera i seguenti pacchetti:

- L'IP 192.168.200.100 inizia una comunicazione SYN
- LIP 192.168.200.150 risponde con un SYN/ACK
- L'IP 192.168.200.100 accetta con un ACK
- Lo stesso IP 192.168.200.100 chiude la comunicazione con un pacchetto RST/ACK

```
Length Info

74 41182 → 21 [SYN] Seq=0 W

74 21 → 41182 [SYN, ACK] Se

66 41182 → 21 [ACK] Seq=1 A

66 41182 → 21 [RST, ACK] Se
```

Per le porte con 2 pacchetti notiamo invece semplicemente che L'IP 192.168.200.100 inizia una comunicazione SYN ma, non ricevendo risposta dall'ip 192.168.200.150, termina subito la comunicazione con un pacchetto RST/ACK.

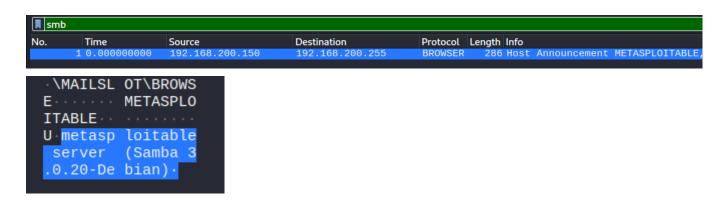
```
ol Length Info
74 37396 → 1 [SYN] Seq=0
60 1 → 37396 [RST, ACK] S
```

Qualora non fosse ancora chiaro, è evidente che siamo dinanzi ad una scansione di porte da parte di una macchina **attaccante** con IP 192.168.200.100 verso una macchina **target** con IP 192.168.200.150; le aventi i servizi operativi sono quelle che hanno risposto al SYN packet con un SYN/ACK, le altre risultano invece chiuse.

# Identificazione macchina Target

Spulciando tra i servizi su cui è stata effettuata la scansione è stato altresì possibile comprendere che la macchina target è una Metasploitable.

Filtrando infatti verso il traffico SMB, troviamo un pacchetto trasmesso dalla macchina target verso l'attaccante dove viene chiaramente enunciato che siamo dinanzi a una macchina METASPLOITABLE che presenta una versione 3.0.20 di Samba:



### IOC

- Host sospetto: 192.168.200.100 (attaccante).
- Host target: 192.168.200.150 (Metasploitable).
- Pattern di connessioni SYN/SYN-ACK/RST su porte multiple (indicatore di scanning).
- Servizi attivi individuati: FTP (21), SSH (22), Telnet (23), SMTP (25), DNS (53), HTTP (80), RPC (111), NetBIOS (139), SMB (445), r-services (512–514).

#### Potenziali Vettori

FTP (porta 21) → rischio di credenziali debali o trasferimento file malevali.

SSH (porta 22) → brute force o exploit di versioni vulnerabili.

**Telnet (porta 23)** → protocollo in chiaro, spesso con password banali → accesso remoto non sicuro.

SMTP (porta 25) → relay abusivo o exploit di server di posta obsoleti.

**DNS (porta 53)** → potenziale uso per esfiltrazione o tunneling (anche se non osservato qui).

HTTP (porta 80) → exploit di web server vulnerabili o applicazioni non patchate.

RPC (porta 111) → vettore tipico per exploit remoti su Unix/Linux.

**NetBIOS/SMB** (porte 139, 445) → attacchi come EternalBlue, esfiltrazione file, movimento laterale.

**r-services (porte 512–514)** → protocolli legacy usati per esecuzione remota, facilmente sfruttabili.

#### Conclusioni

Dall'analisi del file di cattura emerge chiaramente un'attività di **port scanning sistematico** da parte dell'host 192.168.200.100 nei confronti della macchina 192.168.200.150, identificata come **Metasploitable**.

Il comportamento osservato, pacchetti SYN inviati in sequenza alle prime 1024 porte, handshake completati e chiusura immediata con RST per le porte aperte, corrisponde a una TCP connect scan (-sT) tipica di strumenti come Nmap o Metasploit.

Gli IOC raccolti indicano che diversi servizi risultano esposti ed attivi sulla macchina target (FTP, SSH, Telnet, HTTP, SMB, ecc.), molti dei quali sono notoriamente vulnerabili. Questo fa ipotizzare che, dopo la fase di ricognizione, l'attaccante avrebbe potuto lanciare exploit mirati (ad esempio sfruttando debolezze note in SMB o credenziali deboli su Telnet/FTP).

Dal punto di vista difensivo, le **azioni raccomandate** includono:

- **contenimento immediato**, isolando l'host attaccante e segmentando la macchina vulnerabile;
- prevenzione futura, riducendo la superficie d'attacco (chiudendo i servizi non necessari, applicando patch ai software esposti) e attivando sistemi di rilevamento intrusioni (IDS/IPS) per intercettare precocemente attività di scanning.

In sintesi, la cattura evidenzia un classico scenario di fase di **ricognizione** all'interno del ciclo di un attacco, che se non mitigata porterebbe facilmente a compromissioni più gravi della macchina target e potenzialmente all'intera rete.