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:

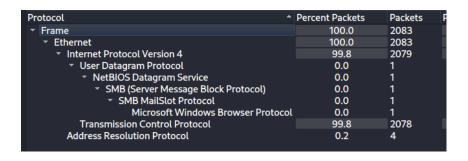
- Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso.
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco. utilizzati.
- Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro.

Svolgimento

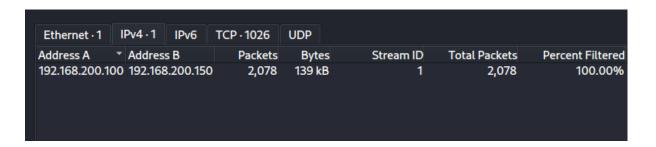
Per iniziare ho aperto il pcapng con wireshark.

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 quasi tutti i pacchetti avvengono su protocollo TCP.



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	Poi	rt A Add	ress B	Port B	Packets *	Bytes	Stream ID
192.168.200.10	00 41	182 192.	168.200.150	21	4	280 bytes	8
192.168.200.10	00 556	556 192.	168.200.150	22	4	280 bytes	10
192.168.200.10	00 413	04 192.	168.200.150	23	4	280 bytes	2
192.168.200.10	00 606	532 192.	168.200.150	25	4	280 bytes	19
192.168.200.10	00 372	282 192.	168.200.150	53	4	280 bytes	21
192.168.200.10	00 530	60 192.	168.200.150	80	4	280 bytes	0
192.168.200.10	00 530)62 192.	168.200.150	80	4	280 bytes	11
192.168.200.10	00 56	120 192.	168.200.150	111	4	280 bytes	3
192.168.200.10	00 469	90 192.	168.200.150	139	4	280 bytes	17
192.168.200.10	00 330	192.	168.200.150	445		280 bytes	15
192.168.200.10	00 456	48 192.	168.200.150	512	4	280 bytes	68
192.168.200.10	00 420	48 192.	168.200.150	513	4	280 bytes	480
192.168.200.10	00 513	396 192.	168.200.150	514		280 bytes	118
192.168.200.10	00 373	396 192.	168.200.150	1	2	134 bytes	874
192.168.200.10	00 347	48 192.	168.200.150	2	2	134 bytes	292
192.168.200.10	00 589	38 192.	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 N

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] Se
```

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 in UDP verso un indirizzo IP di broadcast 192.168.200.255 dove viene chiaramente enunciato che siamo dinanzi a una macchina METASPLOITABLE che presenta una versione 3.0.20 di Samba:

No. Time Source Destination Protocol Length Info 1 0.000000000 192.168.200.150 192.168.200.255 BROWSER 286 Host Announcement METASPLOITAL	smb							
1 0.000000000 192.168.200.150 192.168.200.255 BROWSER 286 Host Announcement METASPLOITA	No.	Time	Source	Destination	Protocol	Length Info		
		1 0.000000000	192.168.200.150	192.168.200.255	BROWSER	286 Host	Announcement	METASPLOITABLE

```
\MAILSL OT\BROWS
E METASPLO
ITABLE
U metasp loitable
server (Samba 3
.0.20-De bian)
```

Quando un host si collega a una rete, i servizi NetBIOS/SMB mandano un annuncio in broadcast (192.168.200.255) per "farsi conoscere".

L'host afferma di essere *METASPLOITABLE e che offre questi servizi:* workstation, server, print server ecc....

Lo scopo è permettere agli altri dispositivi della LAN di visualizzarlo, ad esempio nel vecchio "Risorse di rete" di Windows.

Implicazioni di sicurezza

In una rete reale, è un problema di information disclosure:

- o l'host espone il suo nome e i suoi ruoli.
- un attaccante che ascolta il traffico può subito capire che si tratta di una macchina vulnerabile.

Protocollo Arp

Controllando infine il protocollo arp, possiamo determinare ancora una volta che c'è stata comunicazione tra i due host analizzati in precedenza:

[II] arp					
No.	Time	Source	Destination	Protocol	Length Info
	8 28.761629461	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:fe	ARP	60 Who has 192.168.200.100? Tell 192.168.200.150
	9 28.761644619	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:1e	ARP	42 192.168.200.100 is at 08:00:27:39:7d:fe
	10 28.774852257	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:1e	ARP	42 Who has 192.168.200.150? Tell 192.168.200.100
	11 28.775230099	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:fe	ARP	60 192.168.200.150 is at 08:00:27:fd:87:1e

Nella cattura sono inoltre presenti pacchetti ARP tra i due host, con richieste "Who has ...?" e relative risposte. Questi pacchetti rappresentano la fase preliminare di risoluzione indirizzi che precede le connessioni TCP osservate. Dal punto di vista della threat intelligence, confermano che la macchina attaccante (192.168.200.100) ha rilevato e interagito con la macchina target (192.168.200.150), rafforzando l'ipotesi di attività di ricognizione e scanning in corso.

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) \rightarrow 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.