Threat Intelligence & IOC

Nell'esercitazione di oggi andremo ad analizzare una cattura di rete effettuata con Wireshark e faremo attenzione a:

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

Identificazione e analisi degli IOC

Gli IOC sono evidenze che suggeriscono un'attività malevola. Dalla cattura di rete, emergono diversi pattern che indicano un possibile attacco in corso:

1. Scansione delle porte

La maggior parte del traffico consiste in pacchetti TCP con flag [SYN] inviati da 192.168.200.100 verso 192.168.200.150 su varie porte (es. 80, 443, 23, 21, ecc.), seguiti da risposte [SYN, ACK] o [RST, ACK] da 192.168.200.150.

Questo comportamento è tipico di una scansione delle porte, in cui un attaccante tenta di identificare servizi attivi su un sistema bersaglio. La varietà di porte (da quelle comuni come 80 e 443 a quelle meno usuali come 199, 487, 707) suggerisce un tentativo di mappatura della rete.

IOC: Elevato numero di tentativi [SYN] su porte diverse in un breve intervallo di tempo.

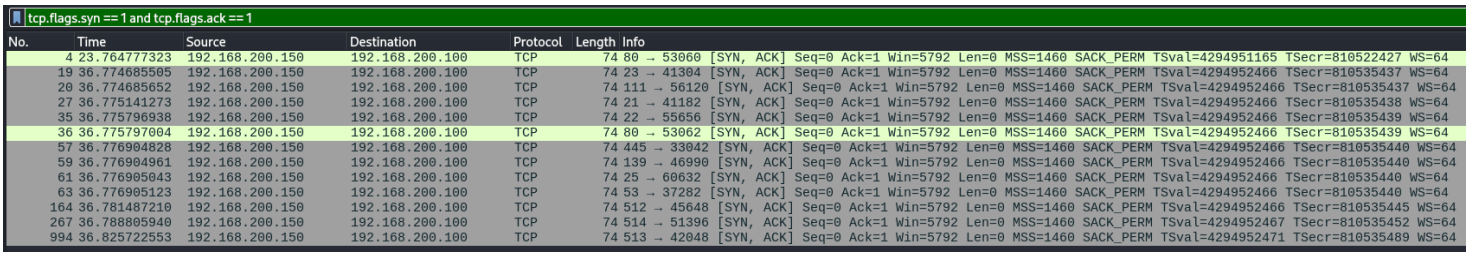
2. Risposte [RST, ACK] su molte porte

Molte porte rispondono con [RST, ACK], indicando che il servizio non è attivo o che la macchina target rifiuta la connessione.

Le risposte [RST, ACK] indicano che il sistema bersaglio (192.168.200.150) non ha servizi in ascolto su quelle porte o che un firewall sta bloccando i tentativi. Tuttavia, l'alto volume di tali risposte in risposta ai [SYN] conferma che il sistema è sotto scansione attiva.

3. Connessioni riuscite su porte specifiche

Alcune porte rispondono con [SYN, ACK] seguite da [ACK], le connessioni riuscite (es. porta 80, 23, 22) indicano che alcuni servizi sono attivi. Il programma che esegue la scansione completa il Three-Way Handshake, per poi chiudere la connessione al servizio.


tcp.flags.syn == 1 and tcp.flags.ack == 1

No.	Time	Source	Destination	Protocol	Length	Info
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
63	36.776905123	192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535445 WS=64
267	36.788805940	192.168.200.150	192.168.200.100	TCP	74	514 → 51396 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535452 WS=64
994	36.825722553	192.168.200.150	192.168.200.100	TCP	74	513 → 42048 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952471 TSecr=810535489 WS=64

Questo è un IOC significativo, poiché l'attaccante potrebbe sfruttare questi servizi aperti.

4. Traffico ARP

I pacchetti ARP (8-11) mostrano una risoluzione degli indirizzi IP 192.168.200.100 e 192.168.200.150 con i rispettivi MAC address (08:00:27:39:7d:fe e 08:00:27:fd:87:1e).

```
 8 28.761629461  PCSSystemtec_fd:87:… PCSSystemtec_39:7d:… ARP         60 Who has 192.168.200.100? Tell 192.168.200.150
 9 28.761644619  PCSSystemtec_39:7d:… PCSSystemtec_fd:87:… ARP         42 192.168.200.100 is at 08:00:27:39:7d:fe
10 28.774852257  PCSSystemtec_39:7d:… PCSSystemtec_fd:87:… ARP         42 Who has 192.168.200.150? Tell 192.168.200.100
11 28.775230099  PCSSystemtec_fd:87:… PCSSystemtec_39:7d:… ARP         60 192.168.200.150 is at 08:00:27:fd:87:1e
```

Questo è un comportamento normale in una rete locale, ma in combinazione con la scansione delle porte, potrebbe indicare che l'attaccante sta mappando la rete per identificare dispositivi attivi.

Ipotesi sui potenziali vettori di attacco

In base agli IOC identificati, e dopo un'analisi approfondita condotta su Wireshark, possiamo dedurre che è in corso una scansione delle porte. Nel caso specifico, 192.168.200.100 sta inviando un elevato numero di pacchetti TCP con flag [SYN] verso 192.168.200.150, su un elevato numero di porte in poco tempo.

L'obiettivo di questa attività è chiaro: identificare quali porte sono aperte e ospitano servizi in ascolto, come confermato dalle risposte [SYN, ACK] ricevute su porte comuni (es. 80 per HTTP, 22 per SSH, 23 per Telnet, 445 e 139 per SMB).

Azioni per Ridurre gli Impatti e Prevenire Attacchi Futuri

Per mitigare gli impatti dell'attività osservata e prevenire attacchi futuri, ecco alcune azioni consigliate:

1. **Isolamento del dispositivo sospetto:**
   Scollegare 192.168.200.100 dalla rete, l'isolamento consente di contenere l'attività malevola, permettendo un'indagine approfondita sul dispositivo per determinare se è stato compromesso (es. da malware) o se è sotto il controllo diretto di un attaccante.
2. **Verifica dei log di sistema:**
   Analizzare i log di 192.168.200.150 (es. file di log di SSH, HTTP o SMB) per identificare eventuali tentativi di accesso o anomalie correlate alla scansione.
3. **Modifica delle regole del firewall:**
   Configurare il firewall per rilevare e bloccare tentativi di scansione delle porte provenienti da qualsiasi dispositivo della rete, ad esempio implementando una regola basata su rate-limiting, per consentire solo un numero limitato di richieste SYN al secondo, respingendo il resto.
4. **Implementazione di un sistema di rilevamento delle intrusioni (IDS):**
   Installare e configurare un IDS per monitorare il traffico di rete e generare avvisi in caso di scansioni delle porte o attività anomale.
5. **Applicare patch di sicurezza e mantenere i dispositivi aggiornati.**

Conclusioni

La cattura di rete evidenzia un sistema (192.168.200.150, "METASPLOITABLE") reso visibile da un annuncio BROWSER e sottoposto a una scansione delle porte da 192.168.200.100, un’attività di reconnaissance volta a mappare i servizi attivi. Le azioni immediate, come la modifica delle regole firewall per bloccare scansioni su tutti i dispositivi e l’isolamento del sospetto, unite a misure preventive come la restrizione delle porte e il monitoraggio, sono fondamentali per mitigare l’attuale scansione e proteggere la rete da future attività simili.