THREAT INTELLIGENCE & IOC

Traccia: 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:

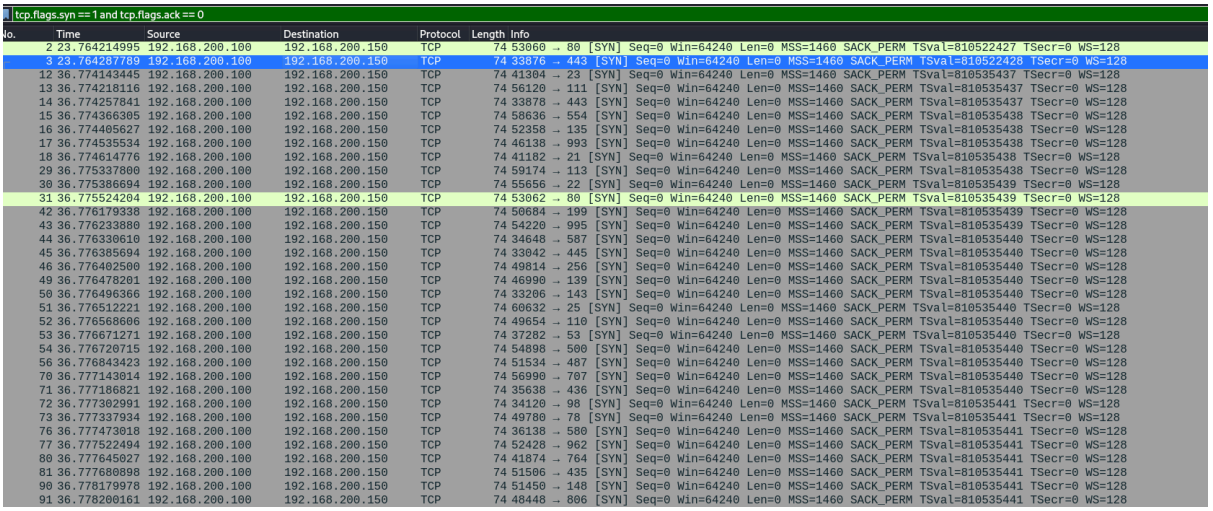
- Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro.

Svolgimento:
Il progetto odierno chiede un' analisi di Threat Intelligence basata su un file catturato da Wireshark che potenzialmente potrebbe illustrare un attacco in corso tramite diversi IOC (Indicatore of Compromise).
Per Threat Intelligence si intende la raccolta, analisi ed utilizzo di informazioni riguardanti minacce informatiche attuali o potenziali. Queste informazioni ottenute da fonti interne ed esterne, forniscono un quadro più chiaro su attacchi passati, presenti o futuri con lo scopo di migliorare la difesa e la resilienza delle infrastrutture IT di una organizzazione.
Un IOC invece è un segnale o traccia che indica la possibile compromissione di un sistema o di una rete da parte di un attacco informatico, utili ad identificare attività malevole o potenzialmente dannose.

IOC Identificati, possibili vettori di attacco e consigli per ridurre l'impatto o evitare l'attacco in futuro

Port Scanning
Utilizzando un particolare filtro, abbiamo potuto rilevare una quantità molto elevata di collegamenti TCP SYN senza una risposta ACK, si tratta di un comportamento adottato dagli attaccanti o dagli amministratori di rete per identificare i servizi in esecuzione su un server o dispositivo. Durante la scansione, l'host che la esegue, invia pacchetti SYN a diverse porte cercando di stabilire una connessione, se la porta è aperta il server risponde con un pacchetto SYN-ACK, altrimenti invia un pacchetto RST (reset) o non risponde affatto.
Ciò che rende sospetto questo traffico è l'elevato numero di richieste su diverse porte nell'arco di un tempo molto breve, potrebbe trattarsi di un utente malintenzionato che cerca di infiltrarsi nel sistema utilizzando le porte aperte o i servizi attivi sul dispositivo bersaglio, ma potenzialmente potrebbe trattarsi anche di un controllo di sicurezza interno o un vulnerability scanning.

Come possibili rimedi per mitigare questo tipo di attacco potremo eseguire una verifica interna per verificare se l'indirizzo IP 192.168.100 è un dispositivo autorizzato ad effettuare queste scansioni, un controllo del firewall per verificare che stia bloccando l'accesso non autorizzato su porte non necessarie, e tenere monitorati gli eventi di rete per la rilevazione di comportamenti simili in futuro e applicare regole di rilevamento delle minacce che possano allertare quando si verificano tentativi di scansione delle porte.



tcp.flags.syn == 1 and tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46	36.776402500	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50	36.776496366	192.168.200.100	192.168.200.150	TCP	74	33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52	36.776568606	192.168.200.100	192.168.200.150	TCP	74	49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
70	36.777143014	192.168.200.100	192.168.200.150	TCP	74	56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
71	36.777186821	192.168.200.100	192.168.200.150	TCP	74	35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
72	36.777302991	192.168.200.100	192.168.200.150	TCP	74	34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
73	36.777337934	192.168.200.100	192.168.200.150	TCP	74	49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
76	36.777473018	192.168.200.100	192.168.200.150	TCP	74	36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
77	36.777522494	192.168.200.100	192.168.200.150	TCP	74	52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
80	36.777645027	192.168.200.100	192.168.200.150	TCP	74	41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
81	36.777680898	192.168.200.100	192.168.200.150	TCP	74	51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
90	36.778179978	192.168.200.100	192.168.200.150	TCP	74	51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
91	36.778200161	192.168.200.100	192.168.200.150	TCP	74	48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128

Attacco DoS

Insieme alla scansione delle porte, sarà possibile notare un possibile attacco DoS (Denial of Service) tramite SYN Flooding, si tratta di una tecnica che sfrutta il processo della stretta di mano a tre vie del protocollo TCP.

L'obiettivo dell'attacco sarà quello di inondare un server di richieste di connessione TCP senza completare il processo di handshake per esaurire le risorse del server e renderlo incapace di rispondere a connessioni legittime.

Le fasi di un attacco SYN Flood sono le seguenti:

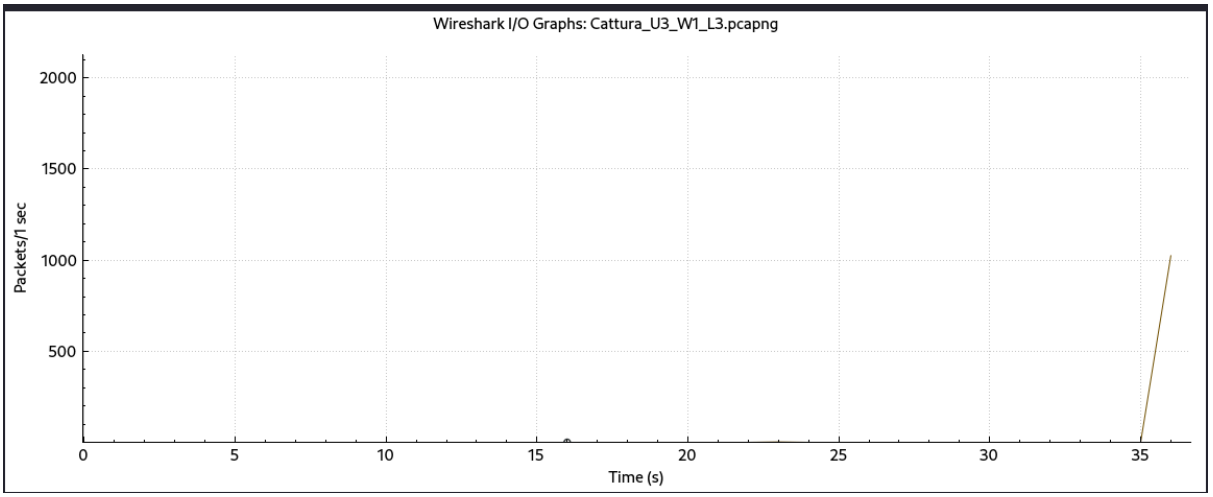
- Inizio dell'handshake tramite invio ripetuto di pacchetti TCP in SYN, per stabilire la connessione;
- Risposta del Server con un pacchetto SYN-ACK, attendendo il completamento della connessione;
- Assenza di risposta, in quanto l'attaccante non risponde con un pacchetto ACK, lasciando il server in attesa con la connessione aperta, occupando risorse per un certo periodo di tempo fino alla scadenza del tentativo.

Lo scopo dell'attacco è quello di creare una coda delle connessioni pendenti del server, impedendo connessioni legittime.

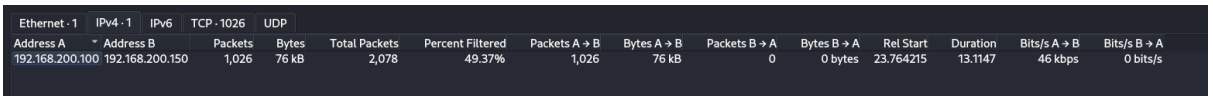
Se vi è l'utilizzo di IP falsificati (spoofing), l'attacco è più difficile da rilevare e mitigare.

Dagli stessi dati del port scanning, possiamo dedurre la presenza di un' alta quantità di pacchetti SYN inviati in un tempo molto breve e le porte di destinazione variano continuamente, questi sono fattori che potrebbero far pensare ad un SYN Flood.

Chiedendo a Wireshark di effettuare una rappresentazione grafica del trasporto dei pacchetti TCP sarà evidente un picco di pacchetti intorno ai 35 secondi dall'inizio del monitoraggio:



Un secondo tipo di controllo che sarà possibile eseguire è un controllo che riguarda gli indirizzi IP che inviano i vari pacchetti SYN. Generando una semplice tabella, sempre grazie alle funzionalità di Wireshark, potremo constatare che c'è un unico IP che invia i pacchetti, ed è quello che potrebbe essere l'origine dell'attacco.



Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 1026 | UDP

Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.200.100	192.168.200.150	1,026	76 kB	2,078	49.37%	1,026	76 kB	0	0 bytes	23.764215	13.1147	46 kbps	0 bits/s

Dai dati raccolti possiamo ipotizzare lo scenario in cui è avvenuto l'attacco, ovvero in un ambiente legittimo avremmo dovuto notare che i pacchetti SYN avrebbero dovuto avere le risposte SYN-ACK e ACK, completando, come già detto, la 3 way handshake, cosa che in questa situazione non accade.
Si tratta, probabilmente, di un attacco interno alla rete in quanto gli indirizzi IP coinvolti fanno parte dello stesso Gateway, a meno che non si tratti di un episodio di spoofing, ovvero falsificazione degli indirizzi IP.
Nel caso in cui si fosse sotto attacco SYN Flood con spoofing, sarebbe molto più complesso riuscire ad individuarli e mitigarli, in quanto il server risponde ad indirizzi IP non appartenenti all'attaccante, il quale resta ugualmente in ascolto. I server legittimi rispondono con pacchetti SYN-ACK agli indirizzi falsificati, ma gli host reali non sono a conoscenza di aver inviato una richiesta SYN, quindi non invieranno mai una risposta ACK, in questa maniera le connessioni TCP rimarranno pendenti, intasando il traffico e consumando risorse, causando così il down del servizio. Come detto precedentemente, le caratteristiche di un SYN Flood con spoofing e SYN Flood tradizionale sono praticamente le stesse, quindi difficili da distinguere, tuttavia, se si trattasse di spoofing, noteremmo un numero maggiore di indirizzi IP potenzialmente esterni alla rete o provenienti da fonti geografiche improbabili, inoltre sarà possibile

notare una grande quantità di risposte SYN-ACK, ma assenza di risposte ACK, caratteristica che, nel caso preso in esame, sembra essere assente.
Per la mitigazione di questo attacco e, di conseguenza, ridurre l'impatto, può essere utile abilitare il SYN Cookies, il quale aumenta la capacità del server di gestire grandi volumi di richieste SYN, senza esaurire le risorse e riducendo il rischio di mandare in down in sistema, oppure limitare il rate delle richieste SYN, ma anche un miglioramento della configurazione del firewall che agisca sempre sulle richieste SYN o sugli IP sospetti, filtrandoli.

Conclusioni
Dall'analisi della cattura di rete effettuata con Wireshark, sono emersi due IOC rilevanti che suggeriscono la presenza di attività malevola sul dispositivo bersaglio.
La prima a saltare all'occhio è il Port Scanning per via dei numerosi pacchetti SYN inviati senza completamento dell'3 way handshake, si tratta di un pattern spesso facente parte di un attacco in quanto ha la funzione di verificare quali sono le porte ed i servizi vulnerabili attivi o non aggiornati, per poter eseguire exploit specifici per ottenere permessi di root o compromettere il sistema.
Il secondo tipo di attacco individuato è stato un attacco DoS, dagli stessi dati del port scanning possiamo dedurre un possibile attacco DoS, probabilmente un DoS SYN Flood, attacco che mira a sovraccaricare le risorse del server target, che diventa incapace di rispondere a richieste legittime, andando in disservizio.
Le azioni suggerite per ridurre l'impatto, e abbassare il rischio di attacchi futuri saranno le seguenti:

- Implementare SYN Cookies per la gestione delle connessioni parziali, fino a quando il 3 way handshake non venga completato;
- Configurare un limite di rate delle richieste SYN che un singolo IP può inviare in un breve periodo di tempo;
- Configurare un Firewall o sistemi IDS/IPS per la rilevazione del traffico sospetto e ripetitivo, soprattutto nei confronti dei dispositivi che non rispondono ai pacchetti SYN-ACK;
- Configurare un Firewall con politiche più restrittive riguardo all'accesso delle porte non necessarie, bloccandole o limitandone l'accesso;
- Effettuare un monitoraggio continuo e costante del traffico, dei log di rete ed altri elementi a rischio, generando alert in caso di movimenti sospetti;
- Effettuare dei regolari pen testing per individuare e correggere eventuali vulnerabilità.

Con queste azioni sarà possibile contenere il danno subìto, e migliorare la risposta ad attacchi futuri.

Progetto a cura di
Sonia Laterza