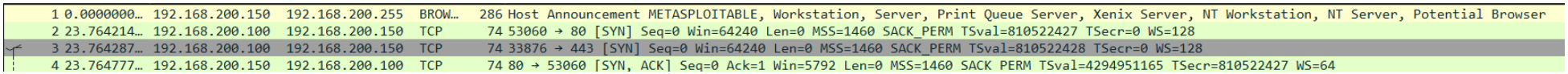
RELAZIONE CATTURA

SCENARIO:



1	0.0000000…	192.168.200.150	192.168.200.255	BROW…	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser
2	23.764214…	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	23.764287…	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
4	23.764777…	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

Dall'analisi della cattura e considerando gli indirizzi Ip sorgente e destinazione, posso affermare che la comunicazione avvenga all'interno di una rete locale e che l'indirizzo ip 192.168.200.150 sia l'indirizzo ip di una Metasploitable, macchina vulnerabile.

70	36.777143…	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	36.777186…	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	36.777302…	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	36.777337…	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
74	36.777430…	192.168.200.150	192.168.200.100	TCP	60	707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777430…	192.168.200.150	192.168.200.100	TCP	60	436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	36.777473…	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	36.777522…	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
78	36.777623…	192.168.200.150	192.168.200.100	TCP	60	98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623…	192.168.200.150	192.168.200.100	TCP	60	78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	36.777645…	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	36.777680…	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
82	36.777758…	192.168.200.150	192.168.200.100	TCP	60	580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758…	192.168.200.150	192.168.200.100	TCP	60	962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871…	192.168.200.150	192.168.200.100	TCP	60	764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777871…	192.168.200.150	192.168.200.100	TCP	60	435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893…	192.168.200.100	192.168.200.150	TCP	66	33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
87	36.777912…	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36.777986…	192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
89	36.778031…	192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
90	36.778179…	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	36.778200…	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
92	36.778307…	192.168.200.100	192.168.200.150	TCP	74	54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
93	36.778385…	192.168.200.150	192.168.200.100	TCP	60	148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	36.778385…	192.168.200.150	192.168.200.100	TCP	60	806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.778449…	192.168.200.150	192.168.200.100	TCP	60	221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96	36.778482…	192.168.200.100	192.168.200.150	TCP	74	42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
97	36.778591…	192.168.200.100	192.168.200.150	TCP	74	34646 → 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
98	36.778614…	192.168.200.100	192.168.200.150	TCP	74	54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
99	36.778663…	192.168.200.150	192.168.200.100	TCP	60	1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100	36.778721…	192.168.200.150	192.168.200.100	TCP	60	206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	36.778759…	192.168.200.100	192.168.200.150	TCP	74	40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
102	36.778781…	192.168.200.100	192.168.200.150	TCP	74	51276 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
103	36.778826…	192.168.200.150	192.168.200.100	TCP	60	131 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	36.778864…	192.168.200.100	192.168.200.150	TCP	74	39566 → 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128

ANALISI E IDENTIFICAZIONE IOC

1)Alto volume di pacchetti SYN:

Si osserva un numero elevato di pacchetti TCP con flag SYN da 192.168.200.100 a 192.168.200.150. Questi pacchetti SYN vengono inviati in rapida successione, come indicato dai timestamp ravvicinati.

2)Connessioni incomplete:

Molti pacchetti SYN non sono seguiti da una sequenza completa di handshake TCP. Ciò suggerisce tentativi di connessione non completati.

3)Dimensioni dei pacchetti:

La maggior parte dei pacchetti SYN ha dimensioni simili (74 byte), indicando una possibile generazione automatizzata.

4)Risposte anomale:

Il sistema target (192.168.200.150) invia molte risposte RST, ACK. Queste risposte indicano che il sistema sta cercando di gestire un numero eccessivo di connessioni.

5)Sequenze e finestre anomale:

I pacchetti SYN hanno sempre Seq=0 e una finestra consistente (Win=64240).
Le risposte RST, ACK mostrano Win=0, indicando che il sistema target sta cercando di chiudere le connessioni poiché non è in grado di accettare uteriori dati.

Questi IOC forniscono forti evidenze di un attacco SYN flood in corso.

Un attacco SYN flood è un tipo di attacco Denial of Service (DoS) che sfrutta il processo di handshake a tre vie del protocollo TCP. La macchina attaccante(192.168.200.100) sta inondando la macchina target(192.168.200.150) con richieste di connessione SYN, nel tentativo di esaurire le sue risorse di rete.

La macchina target sta rispondendo con RST, ACK tentando di gestire l'eccesso di connessioni, ma questo pattern continua, indicando che l'attacco è persistente e potenzialmente efficace nel sovraccaricare il sistema.

Basandoci sugli IOC identificati, possiamo formulare alcune ipotesi sui potenziali vettori di attacco utilizzati per questo SYN flood:

Attacco interno alla rete:

Gli indirizzi IP coinvolti (192.168.200.x) suggeriscono che l'attacco proviene dalla stessa rete locale del target.
Ipotesi: Un dispositivo compromesso all'interno della rete sta conducendo l'attacco.

Utilizzo di tool automatizzati:

La consistenza nei numeri di sequenza (Seq=0) e nelle dimensioni della finestra indica l'uso di strumenti automatizzati.
Ipotesi: L'attaccante sta utilizzando software specializzato per SYN flood, come hping3 o LOIC.

Singola fonte di attacco:

Il traffico proviene da un singolo IP (192.168.200.100).
Ipotesi: Un singolo dispositivo compromesso o un insider malevolo sta conducendo l'attacco.

Sfruttamento di dispositivi IoT:

Data la natura interna dell'attacco, dispositivi IoT mal configurati potrebbero essere stati compromessi.
Ipotesi: Un attaccante potrebbe aver preso il controllo di dispositivi IoT sulla rete per lanciare l'attacco.

Per mitigare l'attacco SYN flood in corso e prevenire attacchi simili in futuro, consiglio le seguenti azioni:

1. Mitigazione immediata:
   a) Filtraggio del traffico:
      - Configurare il firewall per limitare il numero di connessioni SYN da un singolo IP.
      - Implementare regole per bloccare il traffico dall'IP sorgente dell'attacco (192.168.200.100).
   b) Attivare SYN cookies:
      - Abilitare i SYN cookies sul sistema target per gestire meglio le connessioni incomplete.
   c) Aumentare la coda delle connessioni in sospeso:
      - Incrementare temporaneamente la dimensione della coda SYN backlog sul sistema target.
   d) Isolare il sistema attaccante:
      - Scollegare o isolare temporaneamente l'IP 192.168.200.100 dalla rete.

2. Prevenzione futura:
   a) Segmentazione della rete:
      - Implementare VLAN e microsegmentazione per limitare la propagazione di attacchi interni.
   b) Implementare IPS/IDS:
      - Installare e configurare sistemi di rilevamento e prevenzione delle intrusioni per identificare rapidamente comportamenti anomali.
   c) Consolidamento della sicurezza dei sistemi:
      - Rafforzare la sicurezza di tutti i dispositivi nella rete, inclusi quelli IoT.
      - Applicare regolarmente patch e aggiornamenti di sicurezza.
   d) Monitoraggio del traffico:
      - Implementare soluzioni di monitoraggio del traffico di rete in tempo reale per rilevare anomalie.
   e) Implementare autenticazione a più fattori:
      - Rafforzare l'accesso alla rete e ai sistemi critici con autenticazione multi-fattore.
   f) Formazione sulla sicurezza:

- Educare il personale sui rischi di sicurezza e sulle best practices.

g) Politiche di accesso:

- Implementare il principio del minimo privilegio per tutti gli account di rete.

h) Backup e piani di continuità:

- Assicurarsi che siano in atto backup regolari e piani di disaster recovery.

i) Test di penetrazione:

- Condurre regolarmente test di penetrazione autorizzati per identificare vulnerabilità.

j) Implementare soluzioni anti-DoS:

- Considerare l'implementazione di soluzioni hardware o software specifiche anti-DoS.

k) Logging e analisi:

- Migliorare le capacità di logging e analisi per una rapida identificazione e risposta agli incidenti.