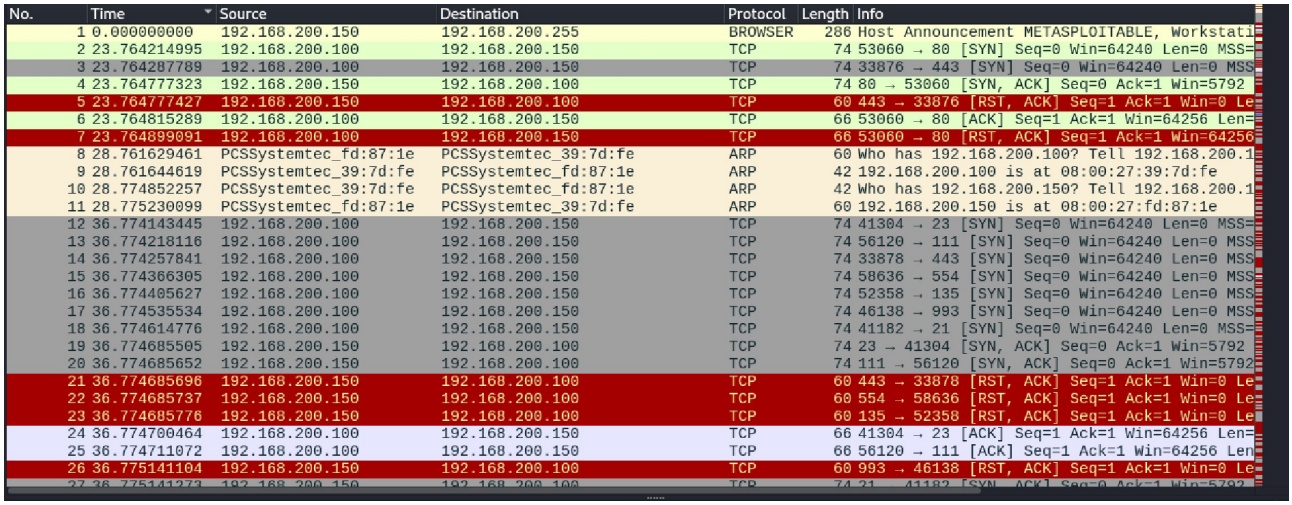
Relazione sull'Analisi di Rete



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstati
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Le
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256
8	28.761629461	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.1
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 192.168.200.1
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
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Le
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Le
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Le
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Le
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792

Durante l'analisi di una cattura di pacchetti tramite Wireshark, è stato osservato un traffico anomalo tra un indirizzo IP sorgente e l' IP di destinazione. Il traffico è caratterizzato da numerosi pacchetti SYN senza la conclusione dell' handshake TCP (assenza di pacchetti ACK) e una presenza significativa di pacchetti RST (Reset). Questo comportamento suggerisce la presenza di attacchi SYN flood e scansioni di porte in corso, che rappresentano fasi comuni di attacco per raccogliere informazioni e compromettere i sistemi.

Tipi di attacco rilevati:

1. SYN Flood (Denial-of-Service):
    - L'attaccante inonda il server con pacchetti SYN, che avviano una connessione TCP senza mai completarla. Questo consuma le risorse del server, esaurendo la sua capacità di gestire nuove connessioni legittime. Il SYN flood mira a rendere il servizio non disponibile (Denial-of-Service).
    - La presenza di un elevato numero di pacchetti SYN senza le risposte ACK corrispondenti suggerisce che l'attaccante sta tentando di saturare le risorse del server attraverso un attacco SYN flood.
2. Scansione di Porte :
    - La scansione delle porte è una tecnica utilizzata per identificare quali porte su un sistema sono aperte e quali servizi sono attivi. Gli attaccanti cercano porte esposte che possono offrire un punto di ingresso per sfruttare vulnerabilità o eseguire attacchi mirati.
    - Numerosi pacchetti SYN inviati a diverse porte, seguiti da pacchetti RST, indicano una scansione in corso. L'attaccante tenta di stabilire connessioni con più servizi per identificare quali sono attivi.
3. Diversificazione dell'attacco:
    - L'attacco coinvolge un tentativo su porte multiple, diversificando il target e cercando di evitare che i meccanismi di difesa (come firewall e IDS) riescano a bloccare tutte le attività sospette. In questo modo, l'attaccante massimizza le probabilità di trovare una vulnerabilità su una porta aperta e meno protetta.
    - Gli attacchi sono distribuiti su diverse porte e servizi, probabilmente per sondare ogni possibile punto di accesso. La diversificazione dell'attacco permette di eludere le misure di sicurezza focalizzate solo su porte o servizi specifici, cercando vulnerabilità meno conosciute o configurazioni deboli.

Obiettivo dell’attacco:

L'obiettivo principale è raccogliere informazioni su quali servizi sono attivi e vulnerabili, identificando potenziali punti di ingresso per attacchi futuri, oppure causare un'interruzione del servizio tramite un Denial-of-Service (DoS).

1. Saturare il sistema (nel caso del SYN flood), impedendo al sistema di gestire nuove richieste legittime.
2. Mappare la rete (con la scansione di porte), scoprendo quali servizi sono attivi e potenzialmente vulnerabili per attacchi successivi.

Possibili soluzioni:

1. **Protezione contro SYN flood**:
    - Implementare SYN cookies per evitare che il server allochi risorse fino al completamento del handshake TCP.
    - Limitare il numero di richieste SYN per IP nell'unità di tempo, per impedire attacchi volumetrici e garantire che solo un numero ragionevole di connessioni venga stabilito.
2. **Prevenzione della scansione di porte**:
    - Utilizzare il port knocking per nascondere porte critiche, aprendo le porte solo dopo una sequenza di tentativi di connessione specifica.
    - **IDS/IPS**: Utilizzare sistemi di rilevamento/prevenzione delle intrusioni (IDS/IPS) per monitorare e bloccare attività sospette di scansione di porte.
3. **Diversificazione della protezione**:
    - **Firewall avanzati**: Configurare un firewall che non solo chiuda le porte non necessarie, ma che sia anche in grado di identificare comportamenti anomali come attacchi distribuiti su più porte.
    - **Monitoraggio continuo**: Implementare un monitoraggio continuo della rete per rilevare attività di scansione o SYN flood in corso, e agire proattivamente per bloccare gli attaccanti.
4. **Rafforzamento delle policy di accesso**:
    - **Limitare gli IP autorizzati**: Impostare regole che permettano l'accesso ai servizi critici solo da IP di fiducia.
    - **Chiusura delle porte non necessarie**: Ridurre la superficie d'attacco chiudendo tutte le porte non utilizzate e limitando l'esposizione dei servizi solo a quelli essenziali.

Conclusione:

L'attività osservata rappresenta un potenziale **attacco SYN flood** combinato con una **scansione delle porte**. L'attaccante sta sondando la rete e cercando di identificare quali porte e servizi sono esposti, sfruttando una diversificazione dell’attacco su più porte per evitare i meccanismi di sicurezza.