

# 1 - Take Away, Tools, and Commands:

---

"#sudo xfreerdp /v:IP\_TO\_CONNECT /u:administrator /p:letmein123!" -This is a free RDP tool. It comes by default in kali.

"#net user tryhackmebilly" or any other user in the local computer. This is to check user privs, groups, and other profile info in Windows OS.

The name of the program to be run to see the Local Users and Groups is (Windows OS) :

#lusrmgr.msc

We can run using the "Run" program by right clicking the Windows logo, and selecting "Run". Or, we can also type the full name of the file in the search bar. It looks like the full name of the program is "Microsoft Common Console Document". If we search by the name, we can also open the program. Here it shows a lot more info than when we "#net user" an account, I wonder if there is a way to find all this information through cmd.

To see what groups a user account belongs to using the Command Prompt, you can use the following command:

```
cmd Copy code  
  
whoami /groups
```

This will display the list of groups that the current user is a member of. If you want to check the groups for a different user, you can use:

```
cmd Copy code  
  
net user [username]
```

Replace [username] with the specific account name you want to check. This will provide details about the user, including the groups they belong to.

🔊 📄 👍 🗨️ ↻

To check the privilege requirements of a program in the Command Prompt, you can use the `icacls` or `accesschk` commands:

1. Using `icacls`: This command shows the permissions on a file, which can help determine if administrative privileges are required.

cmd

Copy code

```
icacls "C:\Path\To\Program.exe"
```

This will display the permissions set on the program file, indicating which users or groups have read, write, or execute access. If it shows "Administrators" with full control, it often means administrative privileges are required.

2. Using `accesschk`: `accesschk` is part of the Sysinternals Suite, which can be downloaded separately. It provides more detailed information.

cmd

Copy code

```
accesschk.exe -d "C:\Path\To\Program.exe"
```

This command will display the access permissions for the specified program. If `accesschk` shows only administrators having permissions, it indicates that elevated privileges may be required.

*Note:* You may need to download and install Sysinternals Suite from Microsoft's website to use `accesschk`.

```
C:\Users\Administrator\Desktop>icacls Wireshark-win64-3.4.5.exe
Wireshark-win64-3.4.5.exe NT AUTHORITY\SYSTEM:(I)(F)
                        BUILTIN\Administrators:(I)(F)
                        THM-WINFUN1\Administrator:(I)(F)

Successfully processed 1 files; Failed processing 0 files
```

The next command did not work in the machine we are testing (machine booted in the room/lesson):

```
C:\Users\Administrator\Desktop>accesschk.exe -d Wireshark-win64-3.4.5.exe
'accesschk.exe' is not recognized as an internal or external command,
operable program or batch file.
```

To check the privileges of the current user in the Command Prompt, you can use:

1. `whoami /priv`:

```
cmd Copy code  
  
whoami /priv
```

This command will display a list of privileges assigned to the current user, including information on whether those privileges are enabled or disabled.

To run a program that requires administrator privileges from a regular user account, you can use the `runas` command. This command allows you to execute a program as a different user, including an administrator account.

Here's how you can do it:

### Using `runas` Command

```
cmd Copy code  
  
runas /user:Administrator "C:\Path\To\Program.exe"
```

1. Replace `Administrator` with the username of an account that has administrative privileges.
2. Replace `"C:\Path\To\Program.exe"` with the actual path to the program you want to run.

When you execute this command, you will be prompted to enter the password for the specified administrator account.

### Example:

```
cmd Copy code  
  
runas /user:Administrator "C:\Users\YourUsername\Desktop\Program.exe"
```

### Note:

- You need to know the password for the administrator account you're using.
- If you're not on a domain, you might need to specify `.\Administrator` to refer to the local administrator account.
- If UAC (User Account Control) is enabled, you will still see a prompt to allow the program to run with elevated permissions.



```
C:\Users\Administrator\Desktop>runas /user:administrator Wireshark-win64-3.4.5.exe
Enter the password for administrator:
Attempting to start Wireshark-win64-3.4.5.exe as user "THM-WINFUN1\administrator" ...
```

we can also use any other user in the local machine.

The keyboard shortcut to open Task Manager in Windows is:

`Ctrl + Shift + Esc`

This will immediately bring up the Task Manager window. Alternatively, you can also use:

`Ctrl + Alt + Delete`

and then select Task Manager from the menu that appears.

To learn more about Task Manager:

<https://www.howtogeek.com/405806/windows-task-manager-the-complete-guide/>