Aim of the Experiment:

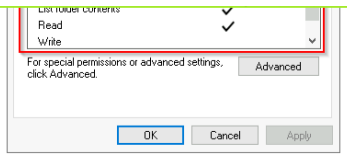
The **Windows Fundamentals 1** room on TryHackMe is designed to introduce users to the basics of the Windows operating system, focusing on system navigation, core components, and fundamental commands.

Algorithm for the Experiment:

A general step-by-step approach for solving the **Windows Fundamentals 1** challenge:

1. **Access the Virtual Machine** (if provided) or use your local Windows system.
2. **Explore Windows Versions:**
    - Identify different Windows editions (Home, Pro, Enterprise).
    - Check the Windows version using `winver` or `systeminfo`.
3. **Understand Windows File System:**
    - Navigate through `C:\Users`, `C:\Program Files`, `C:\Windows`, etc.
    - Learn about file extensions (`.exe`, `.dll`, `.bat`, `.ps1`).
4. **Use Basic Windows Commands:**
    - Open **Command Prompt** (`cmd.exe`) and run:

- **Explore Task Manager:**
    - Open Task Manager (`Ctrl + Shift + Esc`).
    - Identify running processes and their resource usage.
- **Answer TryHackMe Questions:**
    - Use the gathered information to answer the quiz or complete the challenge.



Refer to the Microsoft documentation to get a better understanding of the NTFS permissions for Special Permissions .

Another feature of NTFS is **Alternate Data Streams** (**ADS**).

Alternate Data Streams (ADS) is a file attribute specific to Windows **NTFS** (New Technology File System).

Every file has at least one data stream (`$DATA`), and ADS allows files to contain more than one stream of data. Natively Window Explorer doesn't display ADS to the user. There are 3rd party executables that can be used to view this data, but Powershell gives you the ability to view ADS for files.

From a security perspective, malware writers have used ADS to hide data.

Not all its uses are malicious. For example, when you download a file from the Internet, there are identifiers written to ADS to identify that the file was downloaded from the Internet.

To learn more about ADS, refer to the following link from MalwareBytes here .

Bonus : If you wish to interact hands-on with ADS, I suggest exploring Day 21 of Advent of Cyber 2 .

Answer the questions below

What is the meaning of NTFS?

New Technology File System ✓ Correct Answer

Note: The Run Dialog Box allows us to open items quickly.

Back to lusrmgr, you should see two folders: **Users** and **Groups**.

If you click on Groups, you see all the names of the local groups along with a brief description for each group.

Each group has permissions set to it, and users are assigned/added to groups by the Administrator. When a user is assigned to a group, the user inherits the permissions of that group. A user can be assigned to multiple groups.

Note: If you click on **Add someone else to this PC** from **Other users**, it will open **Local Users and Management**.

Answer the questions below

What is the name of the other user account?

tryhackmebilly ✓ Correct Answer

What groups is this user a member of?

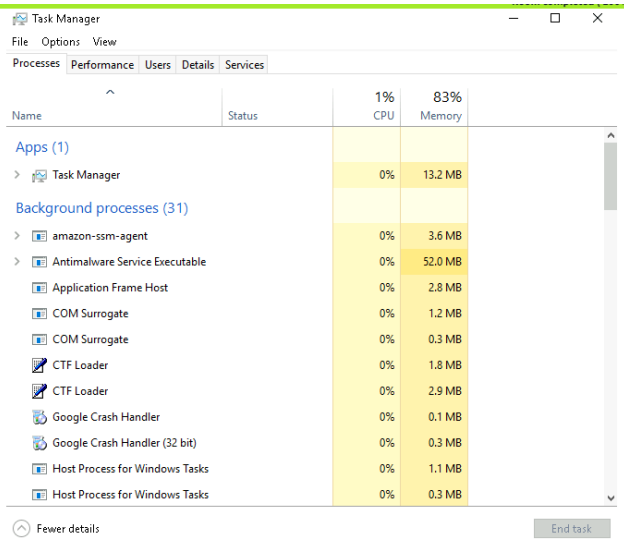
Remote Desktop Users,Users ✓ Correct Answer

What built-in account is for guest access to the computer?

Guest ✓ Correct Answer

What is the account description?

window$Fun1! ✓ Correct Answer



You can refer to this blog post for more detailed information about the Task Manager.

If you wish to learn more about the core Windows processes and what each process is responsible for, visit the Core Windows Processes room.

Answer the questions below

What is the keyboard shortcut to open Task Manager?

Ctrl+Shift+Esc ✓ Correct Answer