Exp No: 1 INTRODUCTION TO WINDOWS 1

Date:

Aim:

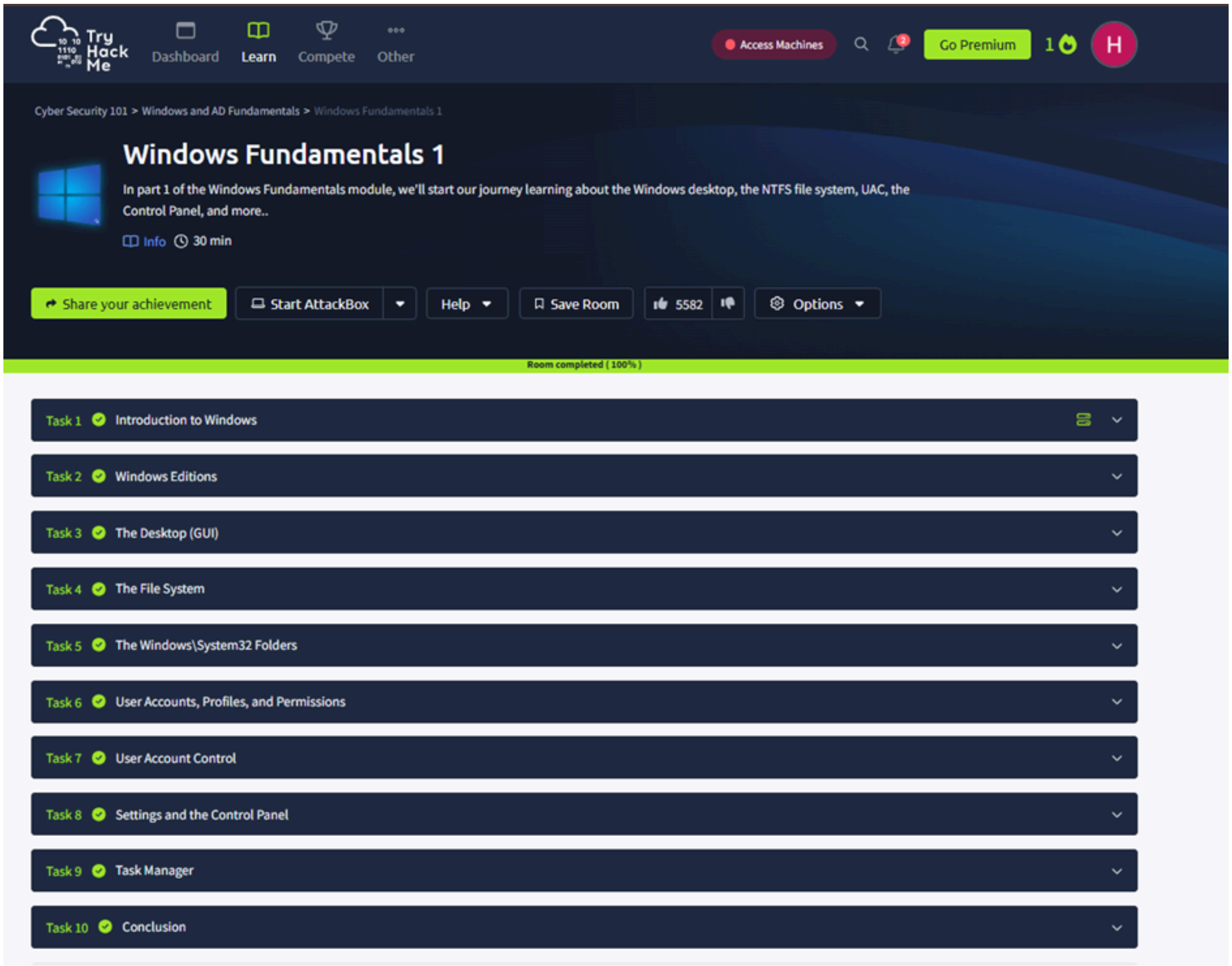
To understand and explore the fundamentals of the Windows operating system, including key components such as the file system, command prompt (CMD), task manager, and registry, to build a strong foundation for cybersecurity and system administration in the TryHackMe platform.

Algorithm:

1. Access the lab in TryHackMe platform using the link below-
2. https://tryhackme.com/r/room/windowsfundamentals1xbx
3. Click Start a Machine and AttackBox to run the instance of Kali Windows
4. distribution.
5. Solve the task questions starting with Windows OS edition and Desktop GUI.
6. Understand the importance of the NTFS file system and features.
7. Learn about the Windows folder and environmental variables for the Windows directory.
8. Learn Local User and Group Management.
9. Learn User Account Control and Practice in a Virtual Machine.
10. Do Control Panel setting - Network & Internet setting.

11. Learn Task Manager – applications and process running and performance of CPU & RAM.

Output:



Cyber Security 101 > Windows and AD Fundamentals > Windows Fundamentals 1

Windows Fundamentals 1

In part 1 of the Windows Fundamentals module, we'll start our journey learning about the Windows desktop, the NTFS file system, UAC, the Control Panel, and more..

Info 30 min

Task 1 Introduction to Windows

Task 2 Windows Editions

Task 3 The Desktop (GUI)

Task 4 The File System

Task 5 The Windows\System32 Folders

Task 6 User Accounts, Profiles, and Permissions

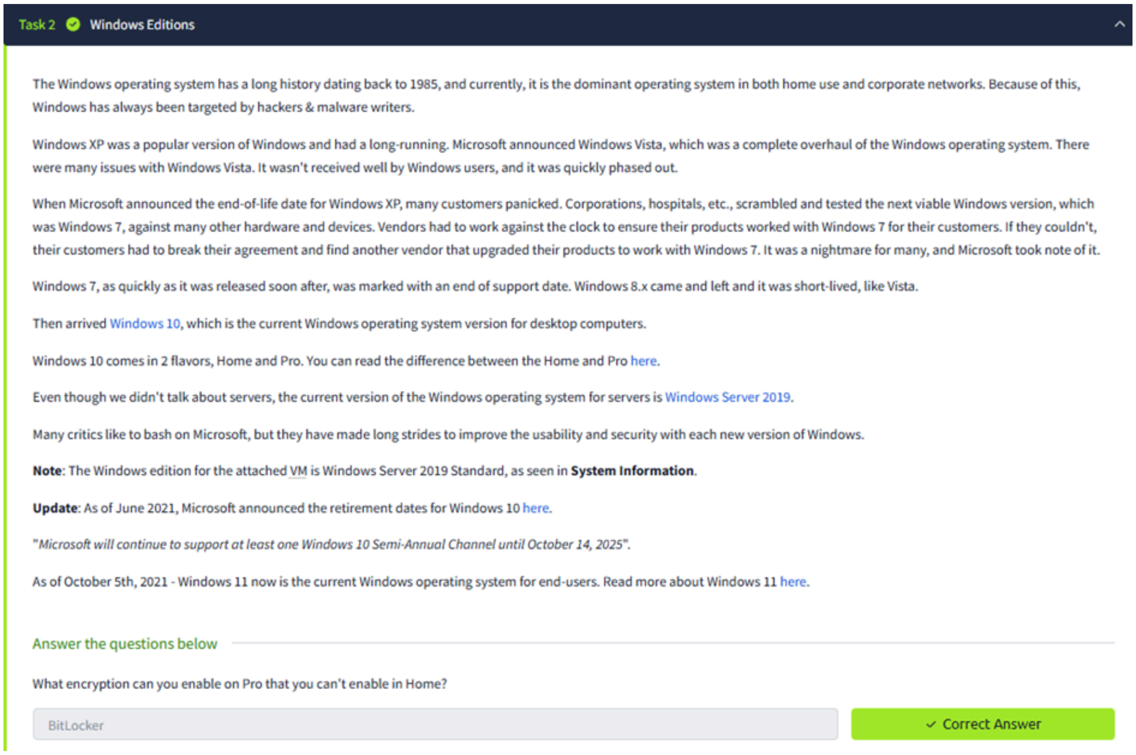
Task 7 User Account Control

Task 8 Settings and the Control Panel

Task 9 Task Manager

Task 10 Conclusion

Task 2:



Task 2 ✓ Windows Editions

The Windows operating system has a long history dating back to 1985, and currently, it is the dominant operating system in both home use and corporate networks. Because of this, Windows has always been targeted by hackers & malware writers.

Windows XP was a popular version of Windows and had a long-running. Microsoft announced Windows Vista, which was a complete overhaul of the Windows operating system. There were many issues with Windows Vista. It wasn't received well by Windows users, and it was quickly phased out.

When Microsoft announced the end-of-life date for Windows XP, many customers panicked. Corporations, hospitals, etc., scrambled and tested the next viable Windows version, which was Windows 7, against many other hardware and devices. Vendors had to work against the clock to ensure their products worked with Windows 7 for their customers. If they couldn't, their customers had to break their agreement and find another vendor that upgraded their products to work with Windows 7. It was a nightmare for many, and Microsoft took note of it.

Windows 7, as quickly as it was released soon after, was marked with an end of support date. Windows 8.x came and left and it was short-lived, like Vista.

Then arrived Windows 10, which is the current Windows operating system version for desktop computers.

Windows 10 comes in 2 flavors, Home and Pro. You can read the difference between the Home and Pro here.

Even though we didn't talk about servers, the current version of the Windows operating system for servers is Windows Server 2019.

Many critics like to bash on Microsoft, but they have made long strides to improve the usability and security with each new version of Windows.

Note: The Windows edition for the attached VM is Windows Server 2019 Standard, as seen in **System Information**.

Update: As of June 2021, Microsoft announced the retirement dates for Windows 10 here.

"*Microsoft will continue to support at least one Windows 10 Semi-Annual Channel until October 14, 2025*".

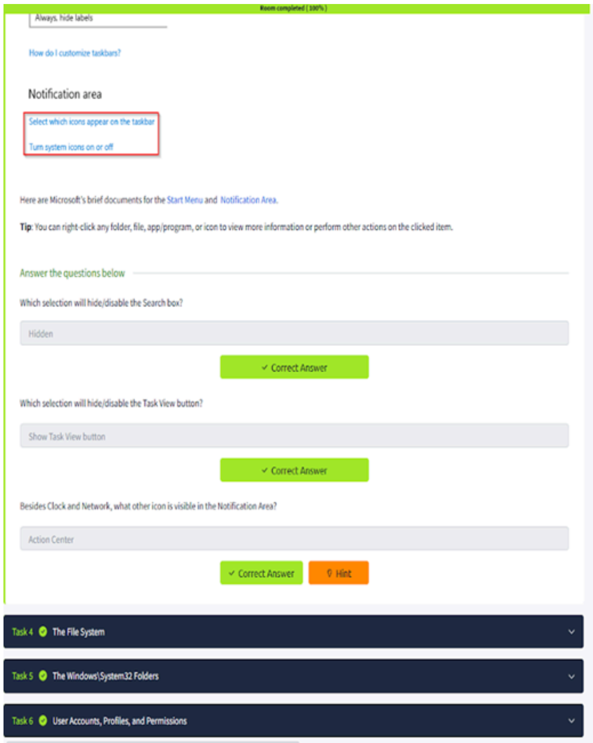
As of October 5th, 2021 - Windows 11 now is the current Windows operating system for end-users. Read more about Windows 11 here.

Answer the questions below

What encryption can you enable on Pro that you can't enable in Home?

BitLocker

Task 3:



Room completed (100%)

Always, hide labels

How do I customize taskbars?

Notification area

Select which icons appear on the taskbar

Turn system icons on or off

Here are Microsoft's brief documents for the Start Menu and Notification Area.

Tip: You can right-click any folder, file, app/program, or icon to view more information or perform other actions on the clicked item.

Answer the questions below

Which selection will hide/disable the Search box?

Hidden

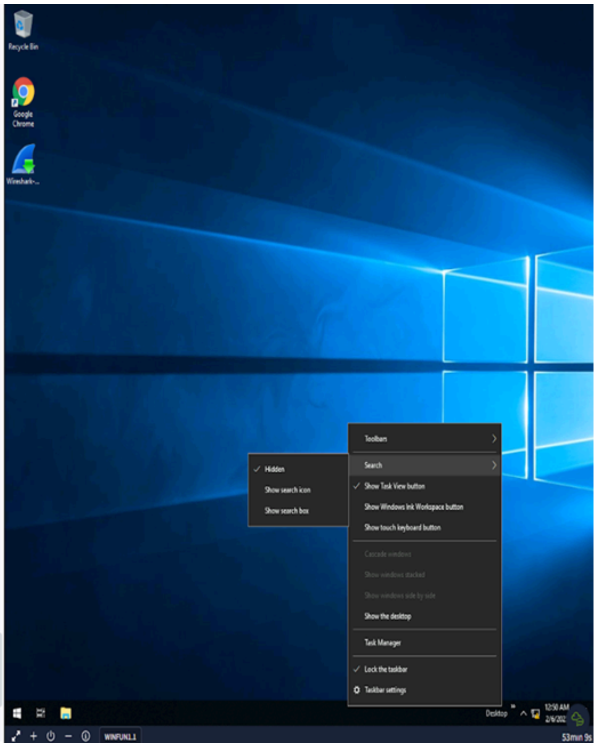
Which selection will hide/disable the Task View button?

Show Task View button

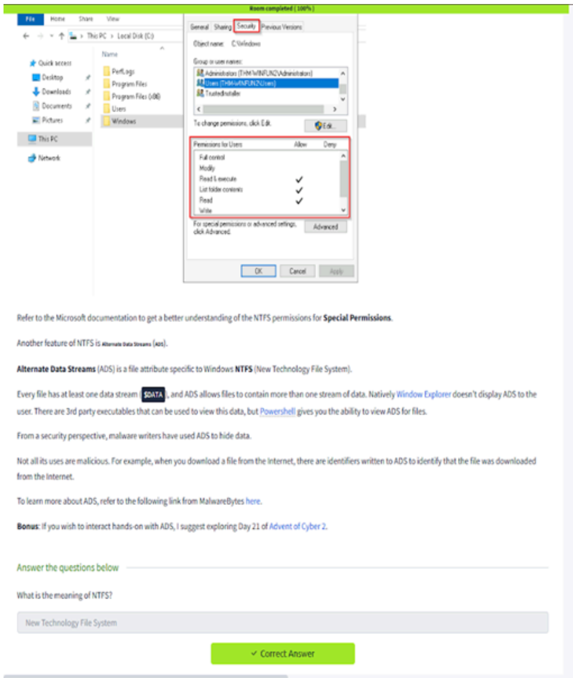
Besides Clock and Network, what other icon is visible in the Notification Area?

Action Center

✓ Correct Answer
✓ Correct Answer
✓ Correct Answer
Hint
Task 4 The File System
Task 5 The Windows\System32 Folders
Task 6 User Accounts, Profiles, and Permissions



Task 4:



Room completed (100%)

Object name: C:\Windows

Group or user names:
- Administrators (THM-WINFUN2\Administrators)
- Users (THM-WINFUN2\Users)
- TrustedInstaller

To change permissions, click Edit.

Permissions for Users	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		

For special permissions or advanced settings, click Advanced.

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.

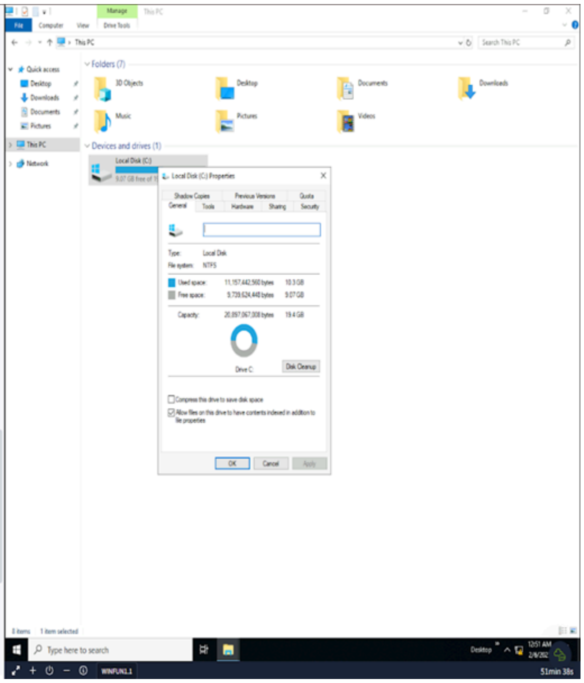
Bonus: If you wish to interact hands-on with ADS, I suggest exploring Day 21 of Advent of Cyber 2.

Answer the questions below

What is the meaning of NTFS?

New Technology File System

✓ Correct Answer



Local Disk (C:) Properties

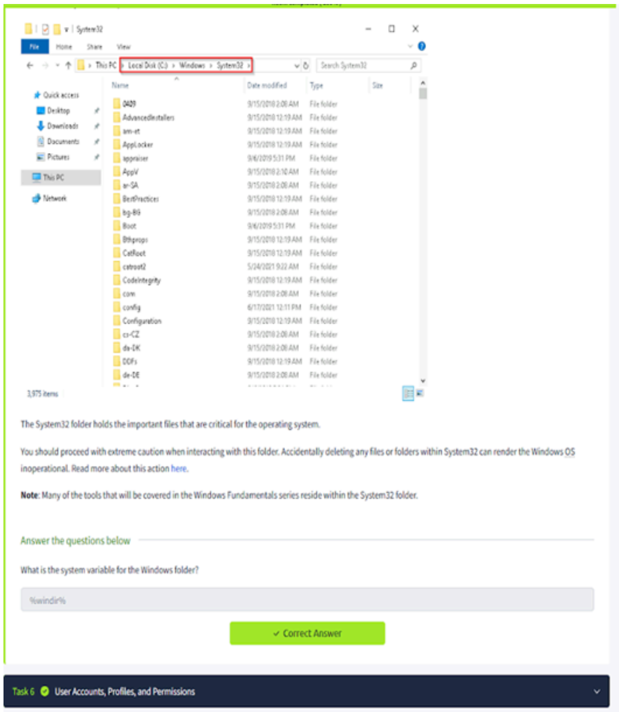
Type:	Local Disk	
File system:	NTFS	
Used space:	11,157,442,560 bytes	10.3 GB
Free space:	9,739,624,448 bytes	9.07 GB
Capacity:	20,897,067,008 bytes	19.4 GB

Drive C:

☐ Compress this drive to save disk space

☑ Allow files on this drive to have contents indexed in addition to file properties

Task 5:



This PC > Local Disk (C:) > Windows > System32

3,975 items

The System32 folder holds the important files that are critical for the operating system.

You should proceed with extreme caution when interacting with this folder. Accidentally deleting any files or folders within System32 can render the Windows OS inoperational. Read more about this action here.

Note: Many of the tools that will be covered in the Windows Fundamentals series reside within the System32 folder.

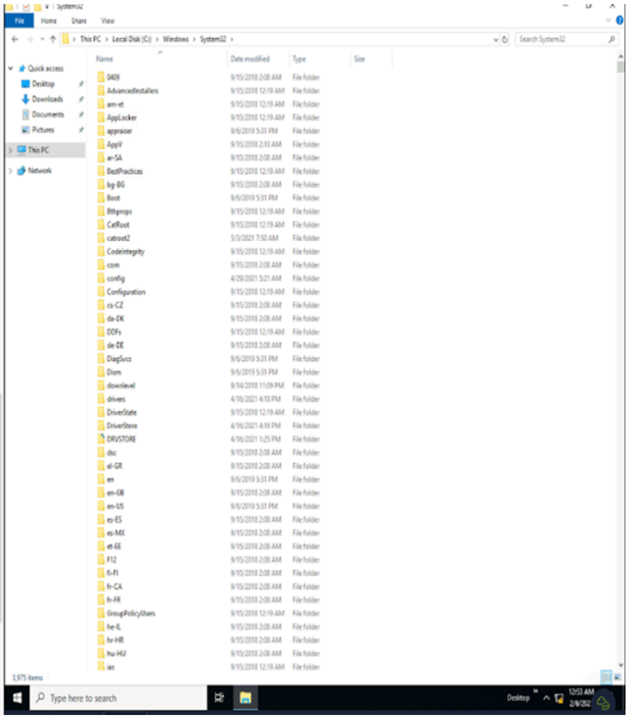
Answer the questions below

What is the system variable for the Windows folder?

%windir%

✓ Correct Answer

Task 6 User Accounts, Profiles, and Permissions

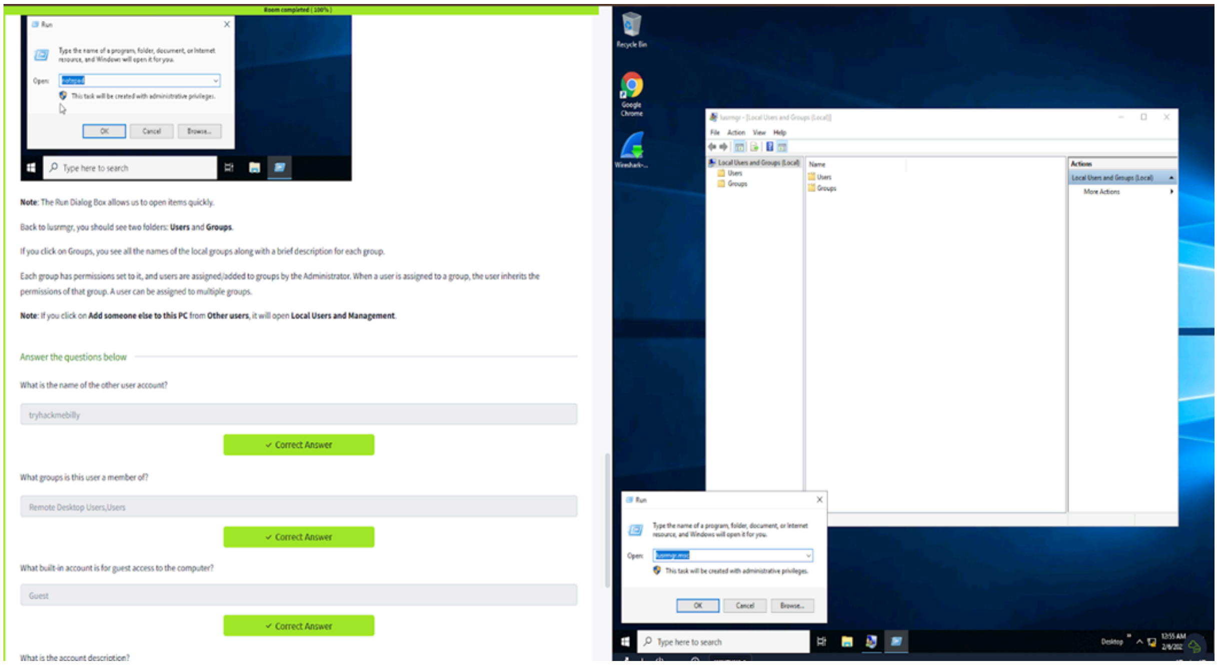


This PC > Local Disk (C:) > Windows > System32

Name	Date modified	Type	Size
0409	9/15/2018 2:08 AM	File folder	
AdvancedInstallers	9/15/2018 12:19 AM	File folder	
am-et	9/15/2018 12:19 AM	File folder	
AppLocker	9/15/2018 12:19 AM	File folder	
appraiser	9/6/2019 5:31 PM	File folder	
AppV	9/15/2018 2:10 AM	File folder	
ar-SA	9/15/2018 2:08 AM	File folder	
BestPractices	9/15/2018 12:19 AM	File folder	
bg-BG	9/15/2018 2:08 AM	File folder	
Boot	9/6/2019 5:31 PM	File folder	
Bthprops	9/15/2018 12:19 AM	File folder	
CatRoot	9/15/2018 12:19 AM	File folder	
catroot2	5/3/2021 7:50 AM	File folder	
CodeIntegrity	9/15/2018 12:19 AM	File folder	
com	9/15/2018 2:08 AM	File folder	
config	4/29/2021 5:21 AM	File folder	
Configuration	9/15/2018 12:19 AM	File folder	
cs-CZ	9/15/2018 2:08 AM	File folder	
da-DK	9/15/2018 2:08 AM	File folder	
DDFs	9/15/2018 12:19 AM	File folder	
de-DE	9/15/2018 2:08 AM	File folder	
DiagSvcs	9/6/2019 5:31 PM	File folder	
Dism	9/6/2019 5:31 PM	File folder	
downlevel	9/14/2018 11:09 PM	File folder	
drivers	4/16/2021 4:10 PM	File folder	
DriverState	9/15/2018 12:19 AM	File folder	
DriverStore	4/16/2021 4:16 PM	File folder	
DRVSTORE	4/16/2021 1:25 PM	File folder	
dsc	9/15/2018 2:08 AM	File folder	
el-GR	9/15/2018 2:08 AM	File folder	
en	9/6/2019 5:31 PM	File folder	
en-GB	9/15/2018 2:08 AM	File folder	
en-US	9/6/2019 5:31 PM	File folder	
es-ES	9/15/2018 2:08 AM	File folder	
es-MX	9/15/2018 2:08 AM	File folder	
et-EE	9/15/2018 2:08 AM	File folder	
F12	9/15/2018 2:08 AM	File folder	
fi-FI	9/15/2018 2:08 AM	File folder	
fr-CA	9/15/2018 2:08 AM	File folder	
fr-FR	9/15/2018 2:08 AM	File folder	
GroupPolicyUsers	9/15/2018 12:19 AM	File folder	
he-IL	9/15/2018 2:08 AM	File folder	
hr-HR	9/15/2018 2:08 AM	File folder	
hu-HU	9/15/2018 2:08 AM	File folder	
ias	9/15/2018 12:19 AM	File folder	

3,975 items

Task 6:



Room completed (100%)
Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open: notepad
This task will be created with administrative privileges.
OK
Cancel
Browse...
Type here to search
Recycle Bin
Google Chrome
Wireshark-...
lusrmgr - [Local Users and Groups (Local)]
File Action View Help
Local Users and Groups (Local)
Users
Groups
Name
Actions
More Actions
Open: lusrmgr.msc
Desktop

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

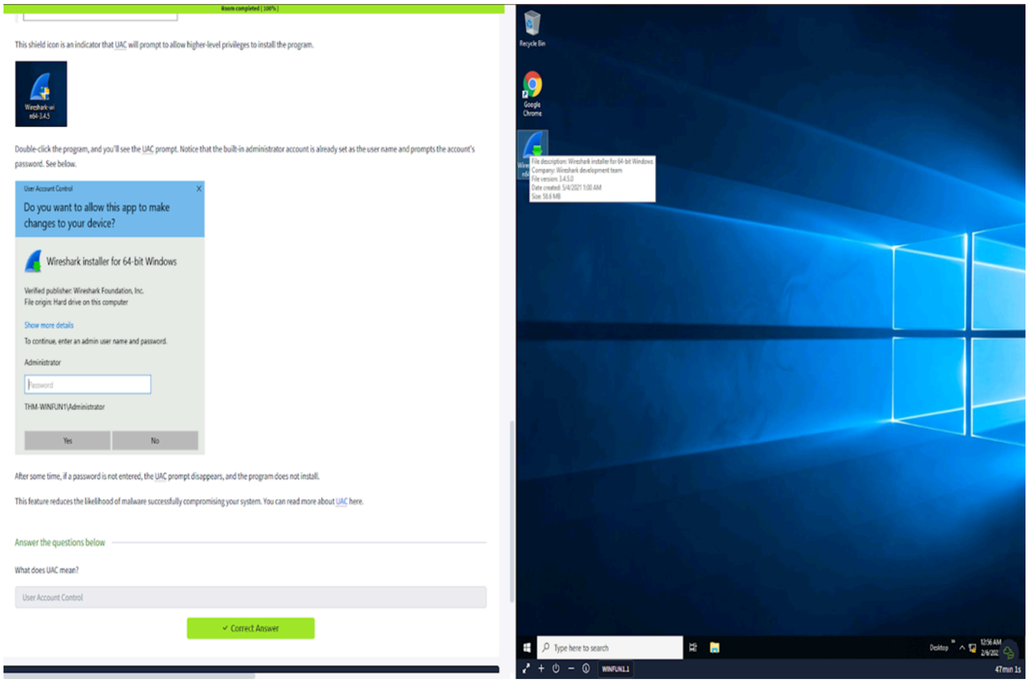
What built-in account is for guest access to the computer?

Guest

✓ Correct Answer

What is the account description?

Task 7:



This shield icon is an indicator that UAC will prompt to allow higher-level privileges to install the program.

Double-click the program, and you'll see the UAC prompt. Notice that the built-in administrator account is already set as the user name and prompts the account's password. See below.

User Account Control

Do you want to allow this app to make changes to your device?

Wireshark installer for 64-bit Windows

Verified publisher: Wireshark Foundation, Inc.
File origin: Hard drive on this computer

Show more details

To continue, enter an admin user name and password.

Administrator

Password

THM-WINFUN1\Administrator

Yes No

After some time, if a password is not entered, the UAC prompt disappears, and the program does not install.

This feature reduces the likelihood of malware successfully compromising your system. You can read more about UAC here.

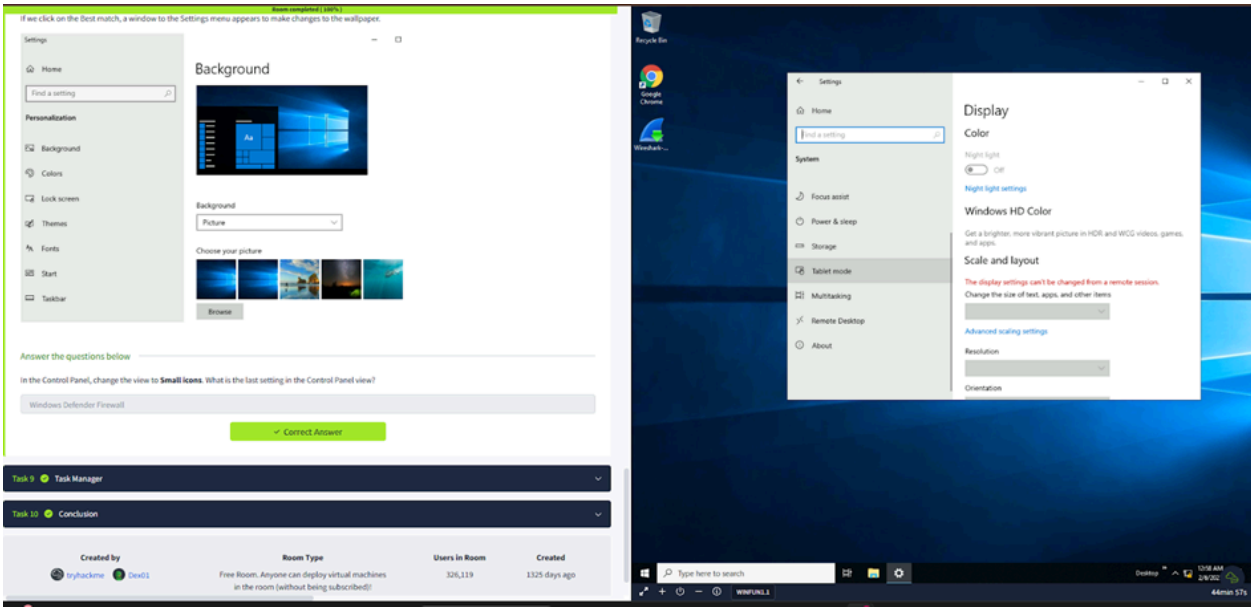
Answer the questions below

What does UAC mean?

User Account Control

✓ Correct Answer

Task 8:



Room completed (100%)

If we click on the Best match, a window to the Settings menu appears to make changes to the wallpaper.

Answer the questions below

In the Control Panel, change the view to **Small icons**. What is the last setting in the Control Panel view?

Windows Defender Firewall

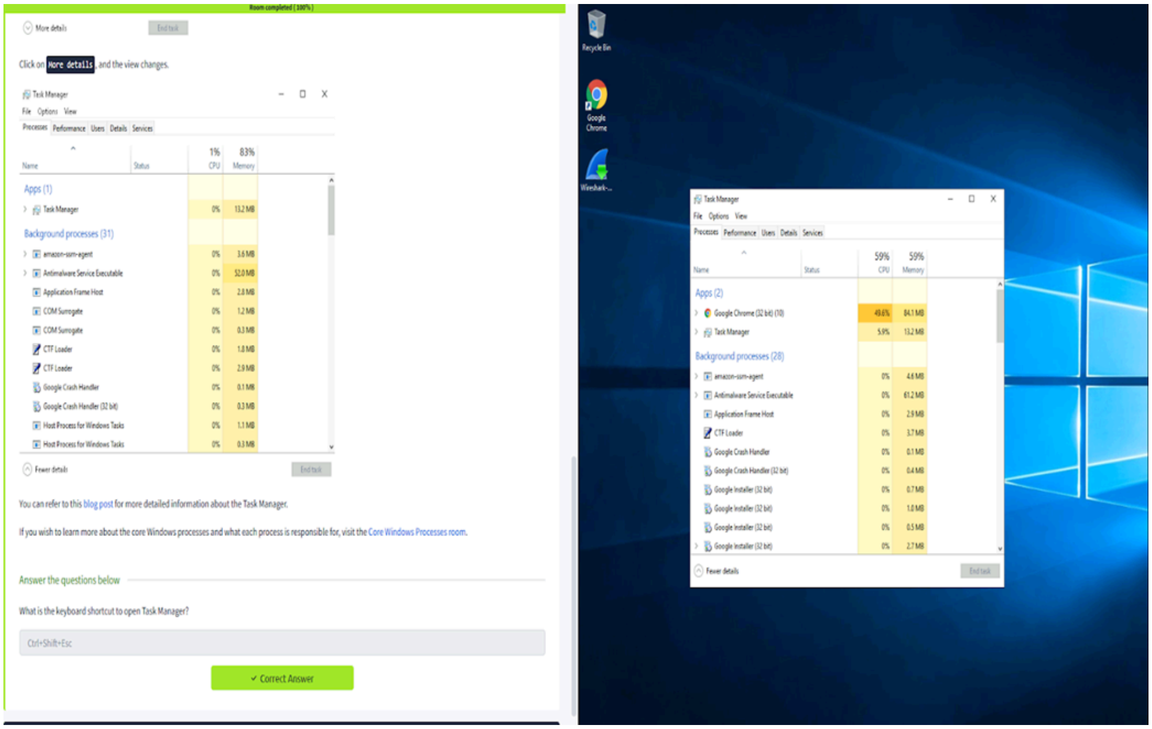
✓ Correct Answer

Task 9 Task Manager

Task 10 Conclusion

Created by	Room Type	Users in Room	Created
tryhackme Dex01	Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	326,119	1325 days ago

Task 9:



Room completed (100%)

Click on `More details`, and the view changes.

Name	Status	1% CPU	83% Memory
Apps (1)			
Task Manager		0%	13.2 MB
Background processes (31)			
amazon-ssm-agent		0%	3.6 MB
Antimalware Service Executable		0%	52.0 MB
Application Frame Host		0%	2.8 MB
COM Surrogate		0%	1.2 MB
COM Surrogate		0%	0.3 MB
CTF Loader		0%	1.8 MB
CTF Loader		0%	2.9 MB
Google Crash Handler		0%	0.1 MB
Google Crash Handler (32 bit)		0%	0.3 MB
Host Process for Windows Tasks		0%	1.1 MB
Host Process for Windows Tasks		0%	0.3 MB

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.

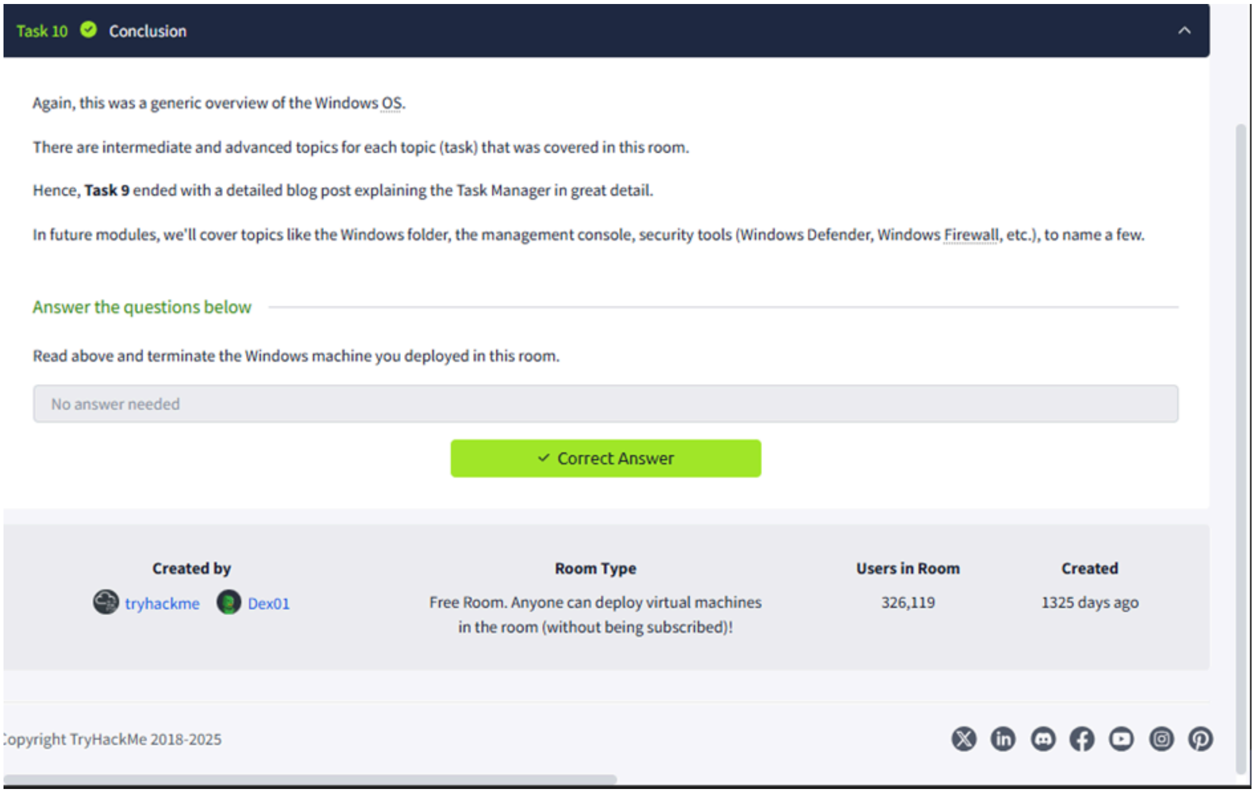
Answer the questions below

What is the keyboard shortcut to open Task Manager?

Ctrl+Shift+Esc

✓ Correct Answer

Task 10:



Task 10 Conclusion

Again, this was a generic overview of the Windows OS.

There are intermediate and advanced topics for each topic (task) that was covered in this room.

Hence, **Task 9** ended with a detailed blog post explaining the Task Manager in great detail.

In future modules, we'll cover topics like the Windows folder, the management console, security tools (Windows Defender, Windows Firewall, etc.), to name a few.

Answer the questions below

Read above and terminate the Windows machine you deployed in this room.

No answer needed

Created by	Room Type	Users in Room	Created
tryhackme Dex01	Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	326,119	1325 days ago

:opyright TryHackMe 2018-2025

Observation:

1. **Remote Desktop/Virtual Machine:**
    - Accessing Windows through an Instance of Virtual Machine.
    - Using Remote Desktop
2. **Windows Edition:**
    - Various Windows edition and their unique features compared to the before one
    - Popular versions of Windows
3. **Graphical User Interface of Windows:**
    - The Desktop GUI
    - Unique Features of Each Windows
4. **The File System:**
    - New Technology File System
    - Partition in the file system (FAT16/FAT32)
    - Encryption File System
5. **Windows Config files, User Accounts, Profiles:**
    - Having multiple profiles for the same user.
    - Storing the configuration files in the System32 folder of Windows
6. **User Access Control, Settings, Task Manager:**
    - Using the control panel to easily access the files and folders.
    - Using the run command to access the applications directly
    - Using the settings to manipulate the desktop

Result:

This experiment provides a practical introduction to Windows system fundamentals, enabling us to navigate, manage, and analyze system components efficiently.