Exp no 1 .A

Date:03-02-2025

INTRODUCTION TO WINDOWS 1

PROCEDURE

 Log in to TryHackMe: Go to tryhackme.com, log in or sign up if you don't have an account.

 Search and Join the Room: Use the search bar to find **"Intro to Windows"** and click **"Join Room"**.

 Start the Machine: Click **"Start Machine"** to get the target Windows system's IP address.

 Connect to THM Network: Use the **AttackBox** (web terminal) or your own VM with **OpenVPN** to connect to TryHackMe's network.

 Go Through Each Task: Read the explanations and follow the steps in tasks covering Windows basics like files, users, services, and registry.

 Use Windows Commands: Use commands like whoami, tasklist, netstat, and reg query to find answers for the questions in the tasks.

 Submit Answers and Complete: Type in the correct answers to each question. After finishing all tasks, the room will be marked as **"Completed"**.

Topics:

- Windows Editions
- The File System
- Windows / System 32 Folders
- Users
- UAC
- Control Panel
- Task Manager
- Answers

Windows Editions

- Windows XP
- Windows Vista
- Windows 7
- Windows 10
- Windows 11

Note: In Windows 11 Pro, you can enable BitLocker encryption which you cannot do in Windows 11 Home.

The File System

In modern versions of Windows, the file system used is NTFS. Before NTFS (New Technology File System), there was FAT16/FAT32 (File Allocation Table) and HPFS (High-Performance File System). You still see FAT partitions in use today. For example, you typically see FAT partitions in USB devices, MicroSD cards, etc. but traditionally not on personal Windows computers/laptops or Windows servers.

NTFS addresses many of the limitations of the previous file systems; such as:

- Supports files larger than 4GB
- Set specific permissions on folders and files
- Folder and file compression
- Encryption (Encryption File System) or EFS

Another feature of NTFS is ADS (Alternate Data Stream) which allows files to contain more than one stream of data.

Windows / System 32 Folders

The Windows folder (C:\Windows) is traditionally known as the folder which contains the Windows operating system. The folder doesn't have to reside in the C drive necessarily. It can reside in any other drive and technically can reside in a different folder.

This is where environment variables, more specifically system environment variables, come into play. Even though not discussed yet, the system environment variable for the Windows directory is %windir%.

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

Users

User accounts can be one of two types on a typical local Windows system: Administrator & Standard User. The user account type will determine what actions the user can perform on that specific Windows system.

- An Administrator can make changes to the system: add users, delete users, modify groups, modify settings on the system, etc.
- A Standard User can only make changes to folders/files attributed to the user & can’t perform system-level changes, such as install programs.

Run the command lusrmgr.msc to view the Local User & Group Management tab.

UAC

A user doesn’t need to run with high (elevated) privileges on the system to run tasks that don’t require such privileges, such as surfing the Internet, working on a Word document, etc. This elevated privilege increases the risk of system compromise because it makes it easier for malware to infect the system. Consequently, since the user account can make changes to the system, the malware would run in the context of the logged-in user.

UAC (User Account Control) was introduced to protect the local user with such privileges but doesn't apply to the local administrator account by default.

How does UAC work? When a user with an account type of administrator logs into a system, the current session doesn't run with elevated permissions. When an operation requiring higher-level privileges needs to execute, the user will be prompted to confirm if they permit the operation to run.

Control Panel

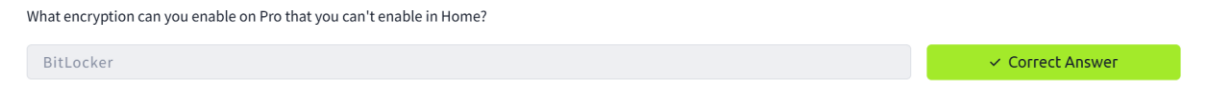
The Settings menu was introduced in Windows 8, the first Windows operating system catered to touchscreen tablets. The Control Panel is the menu where you will access more complex settings and perform more complex actions. In some cases, you can start in Settings and end up in the Control Panel.

Task Manager

The Task Manager provides information about the applications and processes currently running on the system. Other information is also available, such as how much CPU and RAM are being utilized, which falls under Performance.

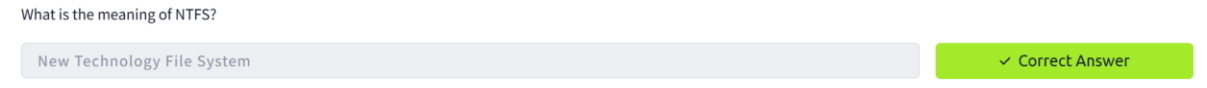
TASKS

Task 2:Windows Editions

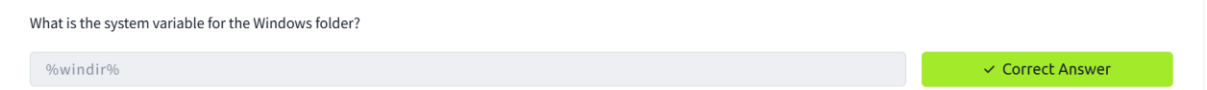


Task 3The Desktop (GUI)

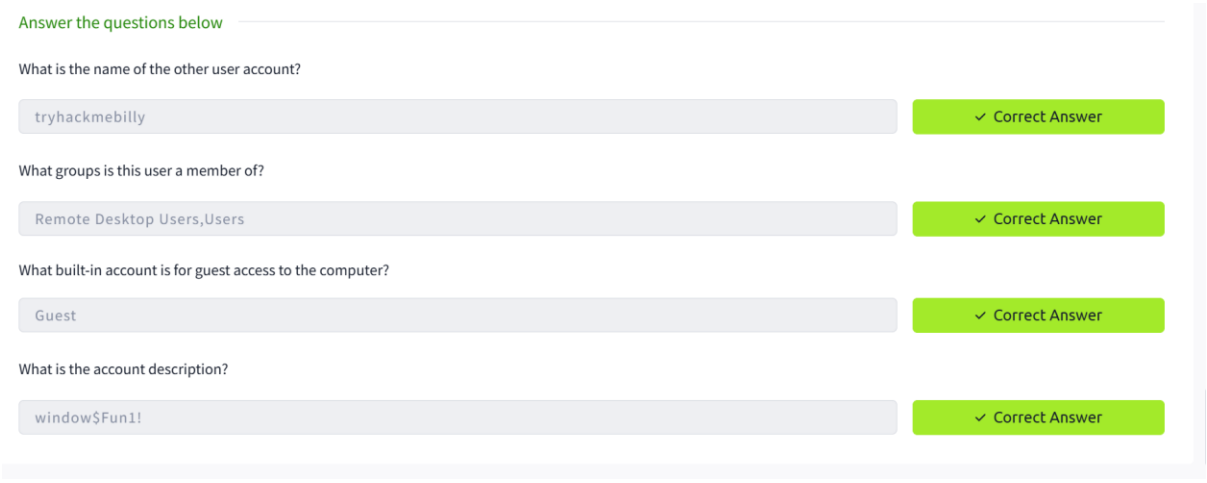
Task 4The File System



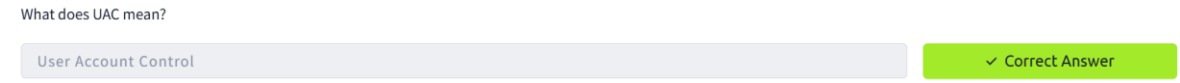
Task 5The Windows\System32 Folders



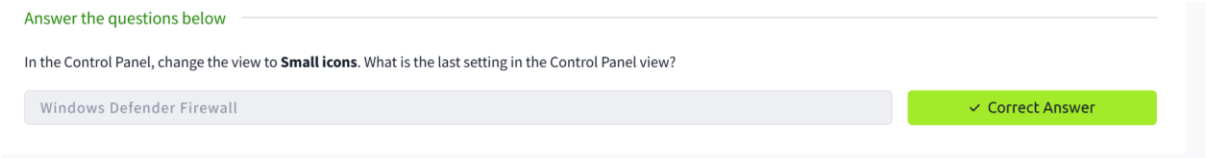
Task 6User Accounts, Profiles, and Permissions



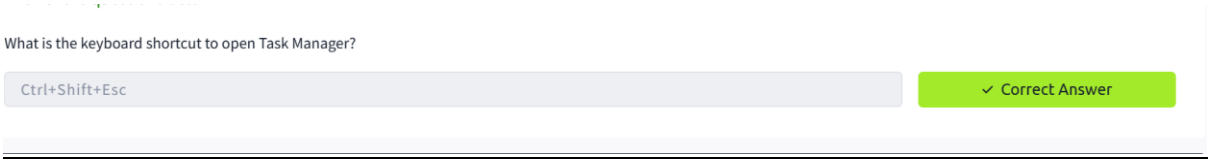
Task 7User Account Control



Task 8Settings and the Control Panel



Task 9Task Manager



RESULT

Thus the introduction to windows part 1 has been sucessfully studied and implemented successfully