Exp no 1 .B

Date:03-02-2025

INTRODUCTION TO WINDOWS 2

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:

- Computer Management
- System Information
- Resource Monitor
- Command Prompt
- Registry Editor
- Answers

Computer Management

The Computer Management (compmgmt) utility has three primary sections and we'll cover each one in detail.

System Tools

With Task Scheduler, we can create and manage common tasks that our computer will carry out automatically at the times we specify.

A task can run an application, a script, etc., and tasks can be configured to run at any point. A task can run at log in or at log off. Tasks can also be configured to run on a specific schedule, for example, every five minutes.

Event Viewer allows us to view events that have occurred on the computer. These records of events can be seen as an audit trail that can be used to understand the activity of the computer system. This information is often used to diagnose problems and investigate actions executed on the system.

I have details on events and logs which can be viewed on my Gitbook here.

Storage

Disk Management is a system utility in Windows that enables you to perform advanced storage tasks. Some tasks are:

- Set up a new drive
- Extend a partition
- Shrink a partition
- Assign or change a drive letter (ex. E:)

Services & Applications

WMI (Windows Management Instrumentation) allows scripting languages (such as VBScript or Windows PowerShell) to manage Microsoft Windows personal computers and servers, both locally and remotely. Microsoft also provides a command-line interface to WMI called Windows Management Instrumentation Command-line (WMIC).

System Information

The system information (msinfo32) tool gathers information about your computer and displays a comprehensive view of your hardware, system components, and software environment, which you can use to diagnose computer issues.

System Summary will display general technical specifications for the computer, such as processor brand and model.

Under Components, you can see specific information about the hardware devices installed on the computer. Some sections don't show any information, but some sections do, such as Display and Input.

In the Software Environment section, you can see information about software baked into the operating system and software you have installed. Other details are visible in this section as well, such as the Environment Variables and Network Connections.

Resource Monitor

Resource monitor (resmon) displays per-process and aggregate CPU, memory, disk, and network usage information, in addition to providing details about which processes are using individual file handles and modules. Advanced filtering allows users to isolate the data related to one or more processes (either applications or services), start, stop, pause, and resume services, and close unresponsive applications from the user interface.

Command Prompt

The command prompt (cmd) is not the only way to interact with the operating system on Windows, but on early systems, it was the sole way to interact with it.

When the GUI (Graphical User Interface) was introduced, it allowed users to perform complex tasks with a few clicks of a button instead of entering commands in the command prompt. Even though the GUI is the primary way to interact with the operating system, a computer user can still interact via the command prompt.

I have listed some commands and their uses in my Gitbook here.

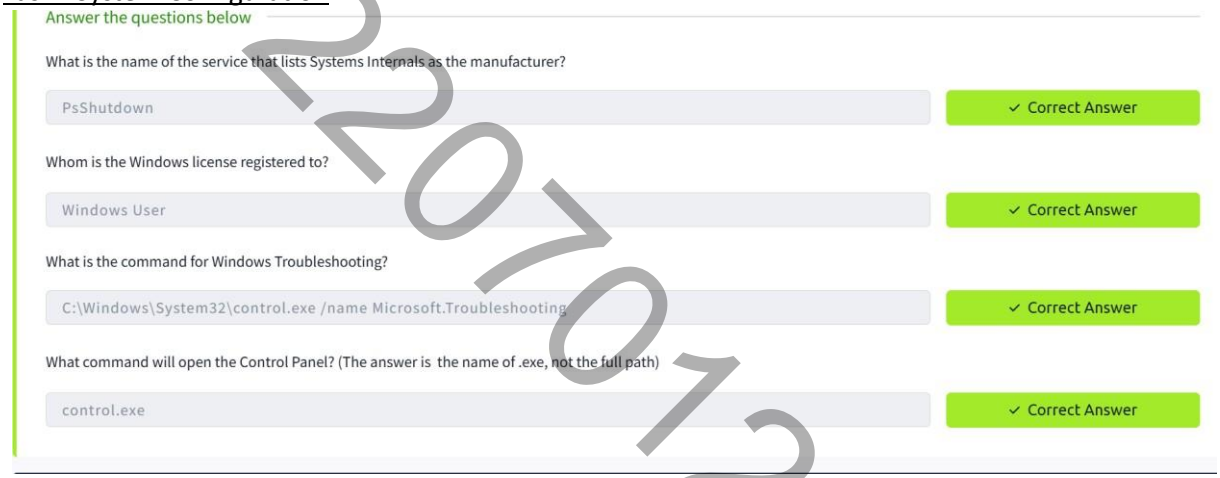
Registry Editor

The Windows Registry is a central hierarchical database used to store information necessary to configure the system for one or more users, applications, and hardware devices. The registry contains information that Windows continually references during operation.

There are various ways to view/edit the registry. One way is to use the Registry Editor (regedt32).

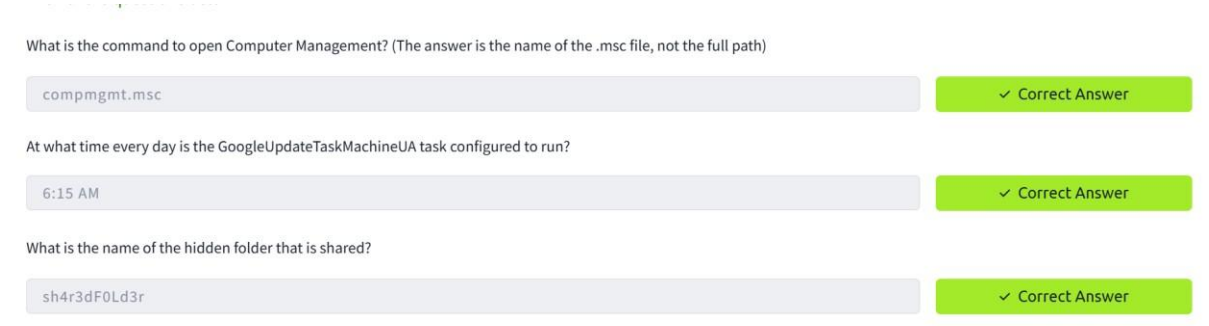
TASKS

Task 2System Configuration

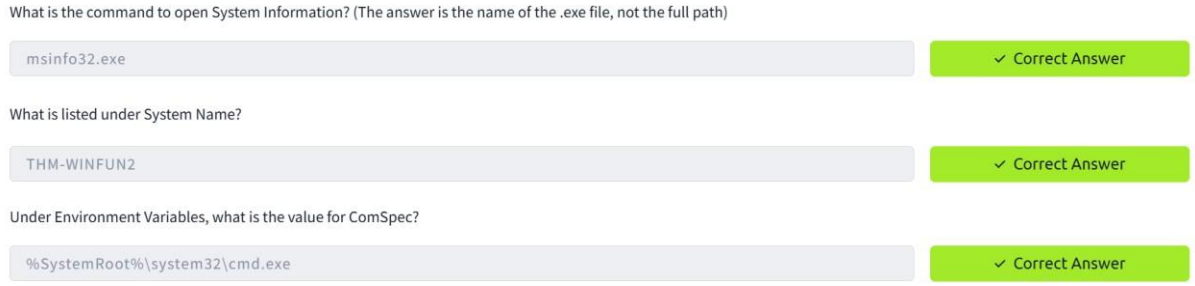


Task 3Change UAC Settings

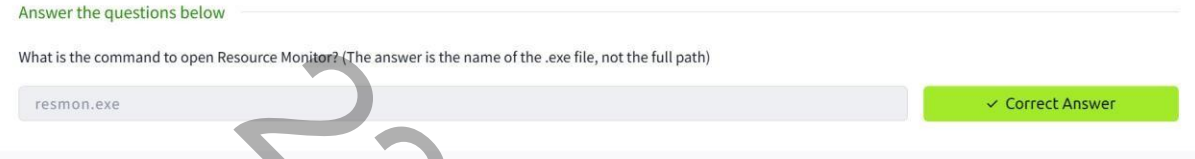
Task 4Computer Management



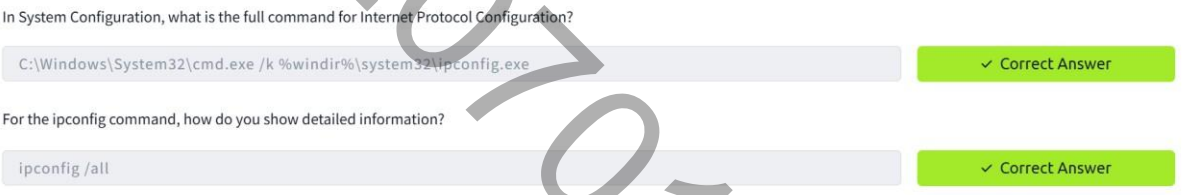
Task 5System Information



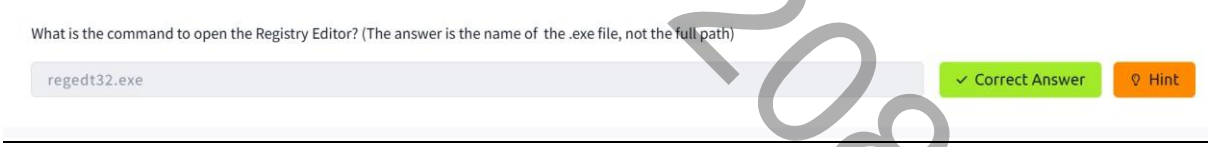
Task 6Resource Monitor



Task 7Command Prompt



Task 8Registry Editor



RESULT

Thus the introduction to windows part 2 has been sucessfully studied and implemented successfully