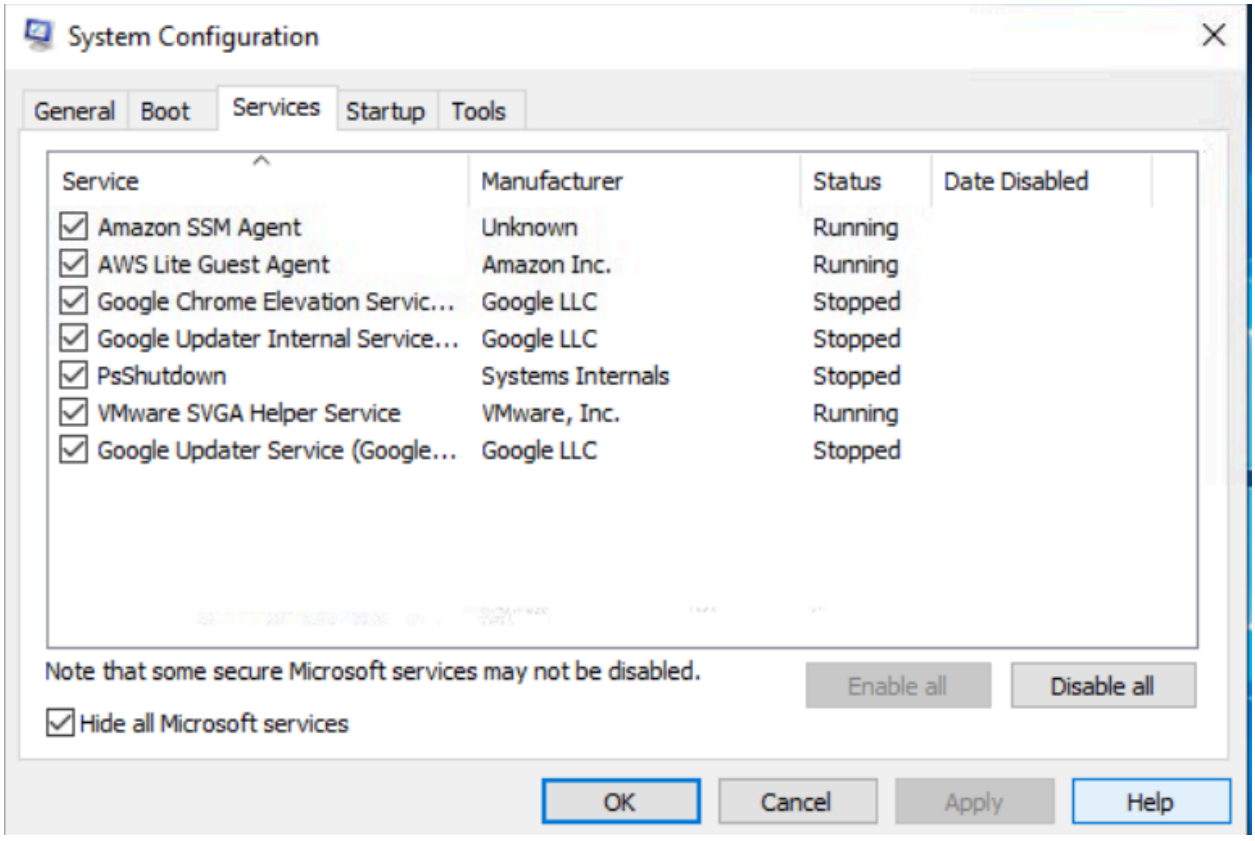
TryHackMe: Windows Fundamentals 2

Introduction

As a longtime Windows User, I realised that I did not know quite a lot about the inner workings of Windows. Hence, in part 2 of the Windows Fundamentals module in Try Hack Me, I aimed to discover more about the Windows Operating System, particularly System Configuration, UAC Settings, Resource Monitoring, the Windows Registry and more.

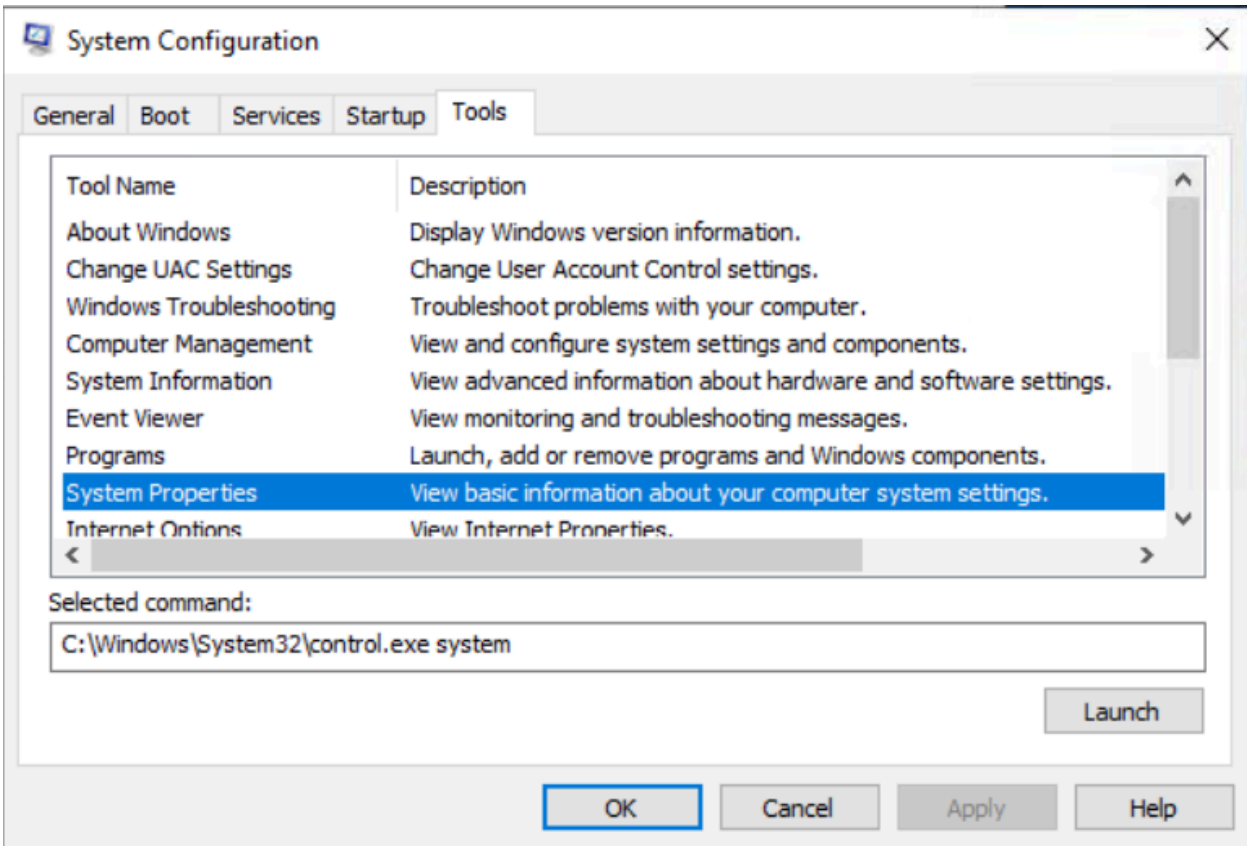
Task 1: System Configuration and Advanced System Settings

The System Configuration utility (MSConfig) is for advanced troubleshooting, and its main purpose is to help diagnose startup issues.



The utility has five tabs across the top. Below are the names for each tab.

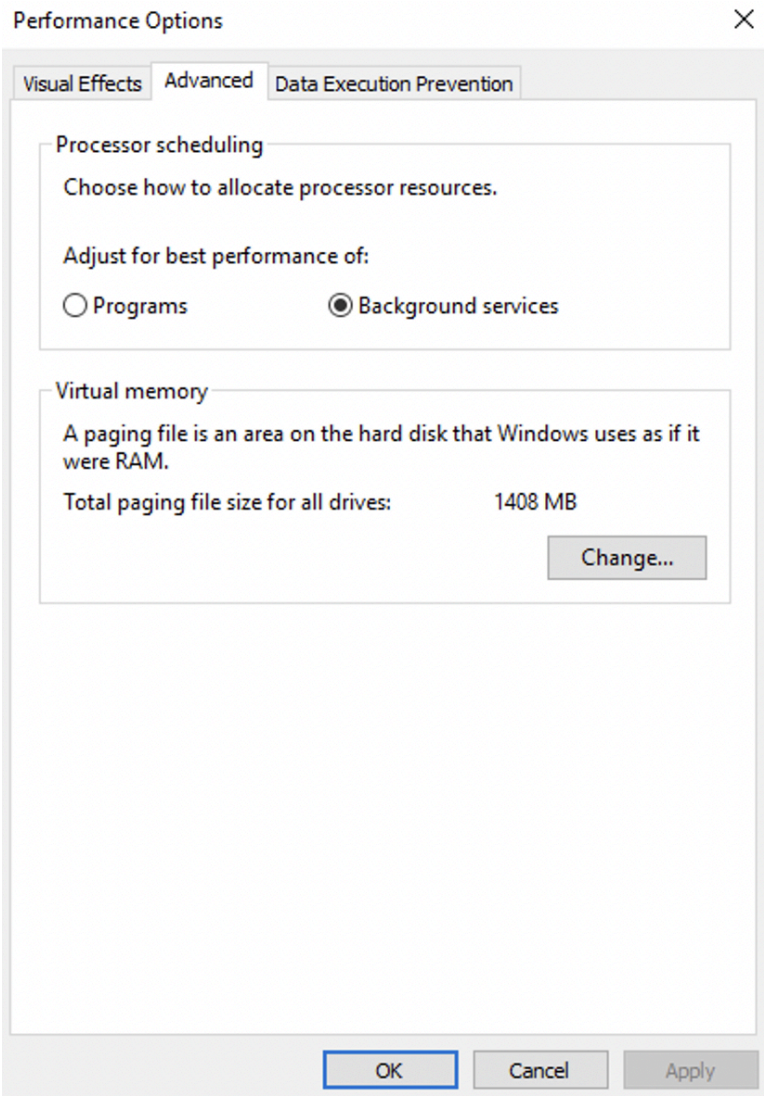
1. **General** - select what devices and services for Windows to load upon boot. The options are: Normal, Diagnostic, or Selective.
2. **Boot -** define various boot options for the Operating System.
3. **Services -** lists all services configured for the system regardless of their state (running or stopped).
    - A service is a special type of application that runs in the background.
4. **Startup -** Microsoft advises using Task Manager (taskmgr) to manage (enable/disable) startup items. The System Configuration utility is NOT a startup management program.
    - On Windows server machines, the only reliable way to view user-level startup items is through the Startup folder itself. I accessed it by pressing Win + R, which opens the Run Dialog, typing ***shell:startup***, and then pressing Enter. This will display all startup programs as shortcuts or executables that are configured to run automatically the next time a user logs in.
5. **Tools -** Contains a list of various utilities (tools) that one can run to configure the operating system further. There is a brief description of each tool to provide some insight into what the tool is for.
    - Notice the Selected command section. The information in this textbox will change per tool.
    - To run a tool, we can use the command to launch the tool via the run prompt, command prompt, or by clicking the Launch button.



For the advanced systems(search for View advanced system settings):

In this Performance tab, the Advanced option can also tell you about the page file size configured for the drives. In this case, it's 1048 MB. The other settings here can give you the following information:

- The drive where the page file is stored
- The initial size (MB)
- The maximum size
- Whether Windows manages the size automatically

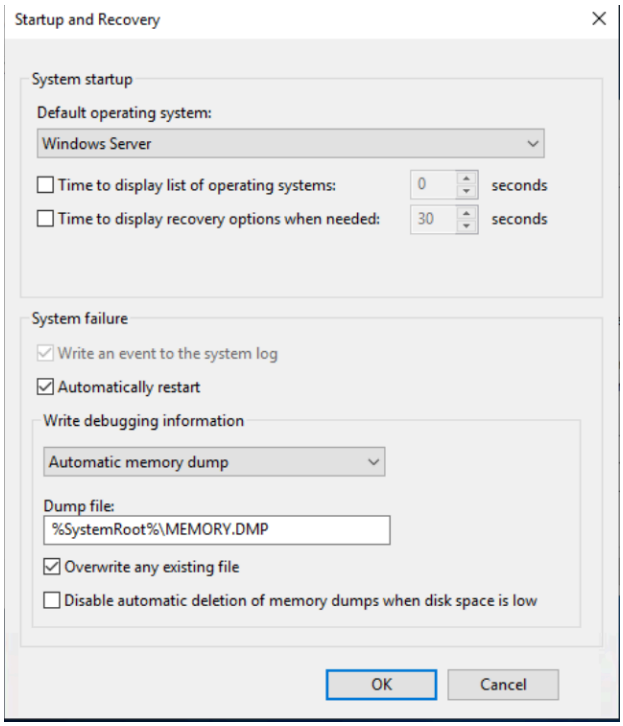


There is another cool configuration that you can find in the Advanced System Settings. It is known as Startup and Recovery. Windows can create a crash dump file whenever it encounters a critical error, such as a Blue Screen of Death. This crash dump helps the administrators or analysts understand what went wrong during the crash. You can view or modify the crash dump settings by navigating to the Advanced option at the top and then clicking Settings under the Startup and Recovery section.

Here, you will find different settings for the startup and recovery. The Write debugging information dropdown tells you the type of crash dump configured for the system. Windows supports different dump types, such as:

- Automatic memory dump
- Kernel memory dump
- Small memory dump (256 KB)
- Complete memory dump
- None

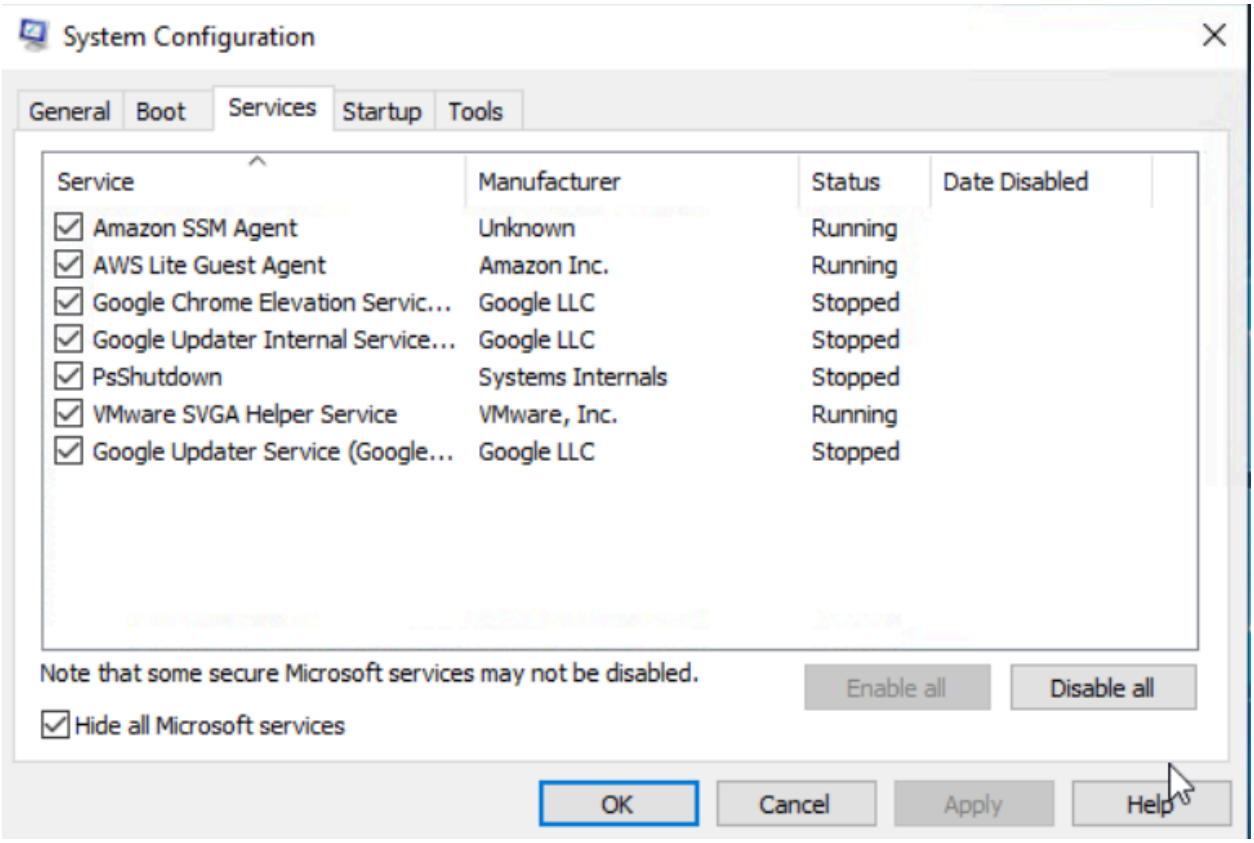
This setting shows how much information Windows will save in the crash dump when a system crash occurs.



Questions

1. **What is the name of the service that lists Systems Internals as the manufacturer?**

   I proceeded to the services tab and hid all Microsoft services(those manufactured by Microsoft to check the service)



The answer is **PsShutdown**

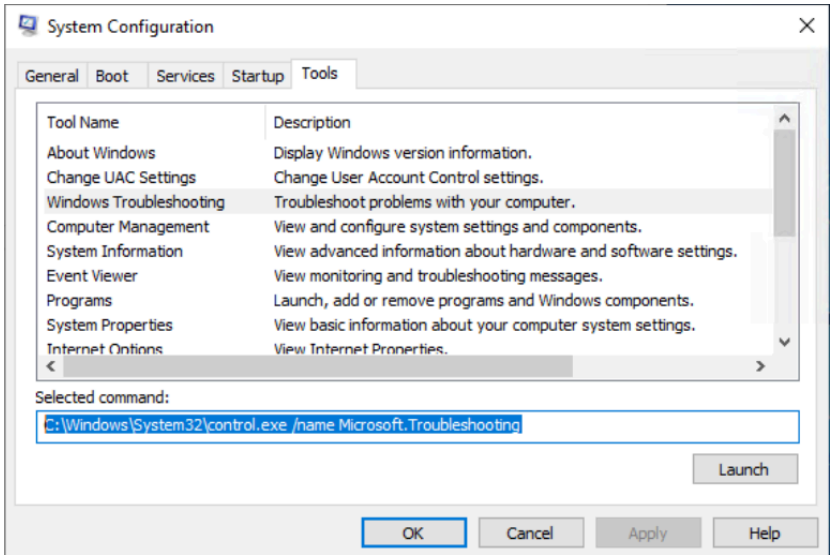
2. Whom is the Windows license registered to?

   Using *winver(*winver is a built-in Windows command that opens the "About Windows" dialog, showing your operating system's edition (like Windows 11 Pro), version (e.g., 24H2), the license registration owner and OS build number*)*

Answer: **Windows User**

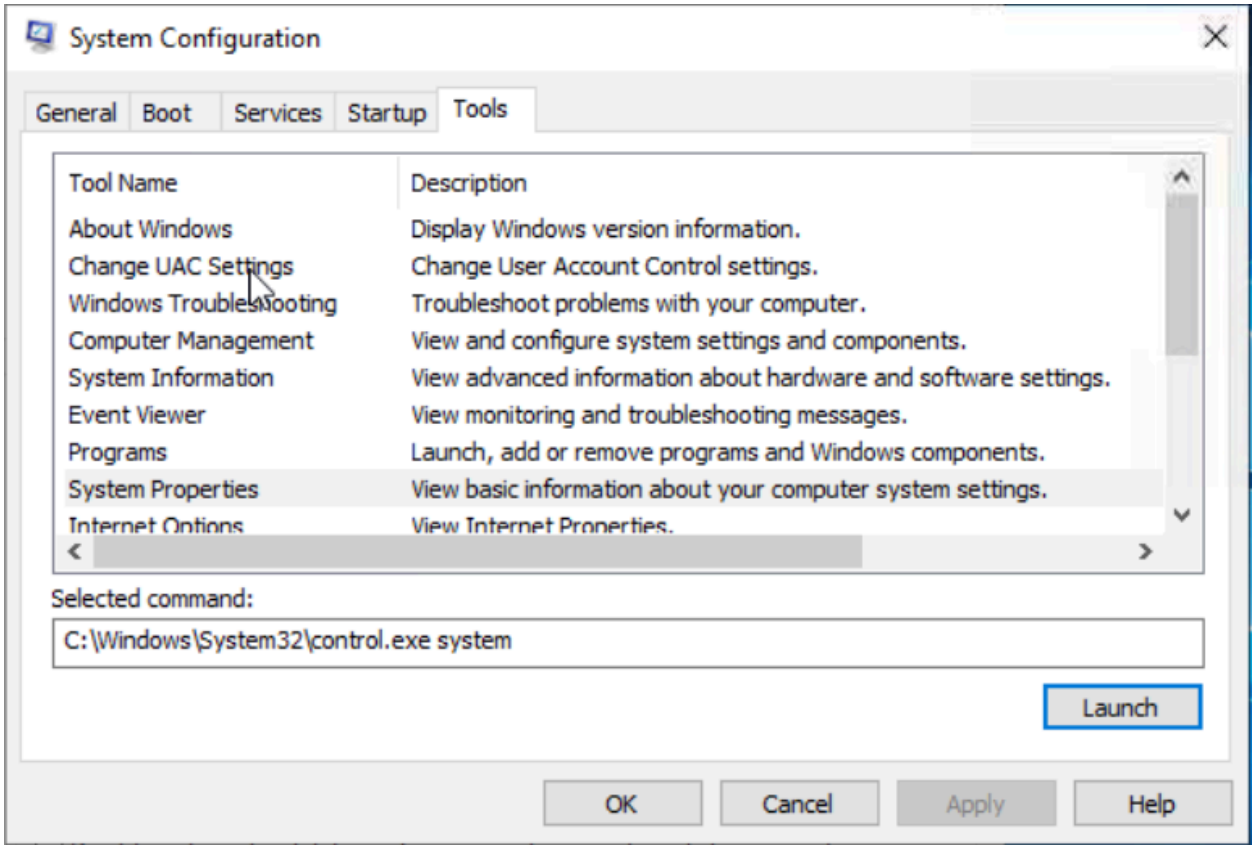
3. What is the command for Windows Troubleshooting?

   On the tools tab, clicking on the Windows Troubleshooting tool gives the selected command: ***C:\Windows\System32\control.exe /name Microsoft.Troubleshooting***



4. What command will open the Control Panel? (The answer is the name of .exe, not the full path)

   Answer: control.exe



Task 2: Changing UAC settings

User Account Control (UAC) helps prevent malware from damaging a PC and helps organizations deploy a better-managed desktop. With UAC, apps and tasks always run in the security context of a non-administrator account, unless an administrator specifically authorizes administrator-level access to the system. UAC can block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings.

- From my understanding, it is similar to Linux's **sudo** command

The UAC slider in the UAC settings has four security levels, each of which controls how Windows alerts you when apps or users try to make changes at the system level. They fall into four standard categories as explained below:

- **Always notify**: This is the highest security. Windows notifies you whenever any apps or you yourself try to make changes, and the desktop dims (Secure Desktop).
- **Notify for apps**: Windows notifies only when apps try to make changes, but not when you change Windows settings. This option is enabled by default.
- **Notify without dimming**: Same as above (Notify for apps), but this time the screen does not dim.
- **Never notify**: Notifications are turned off. Windows won't warn you about any changes made by you or any apps.

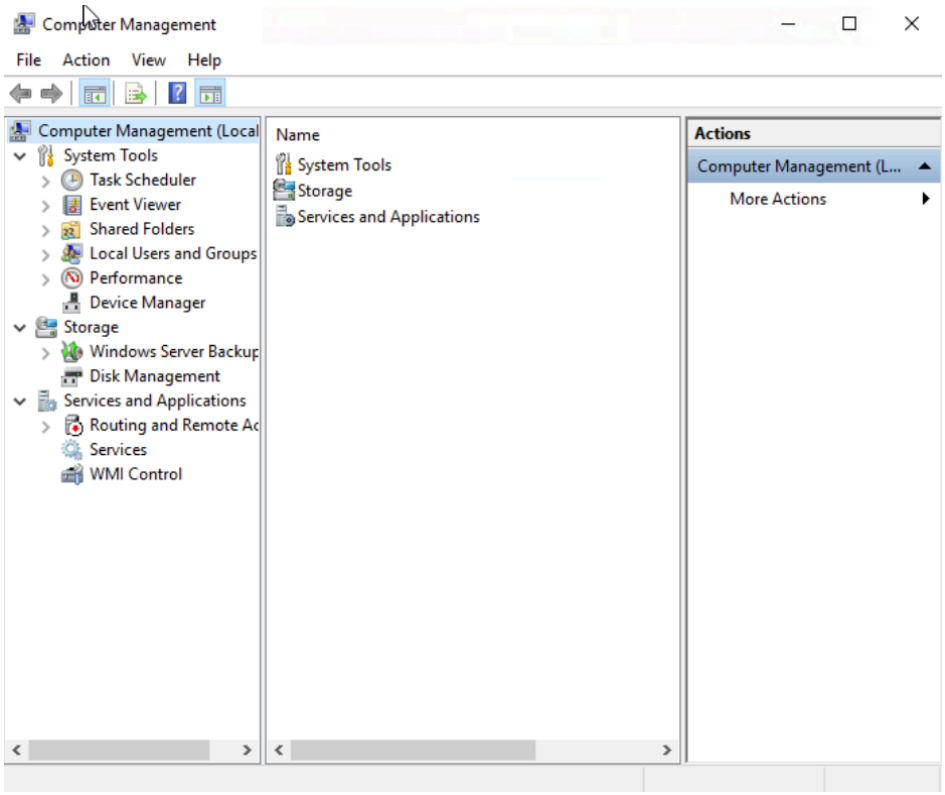
Questions

What is the command to open User Account Control Settings? (The answer is the name of the .exe file, not the full path)

Answer: **UserAccountControlSettings.exe**

Task 3: Computer Management

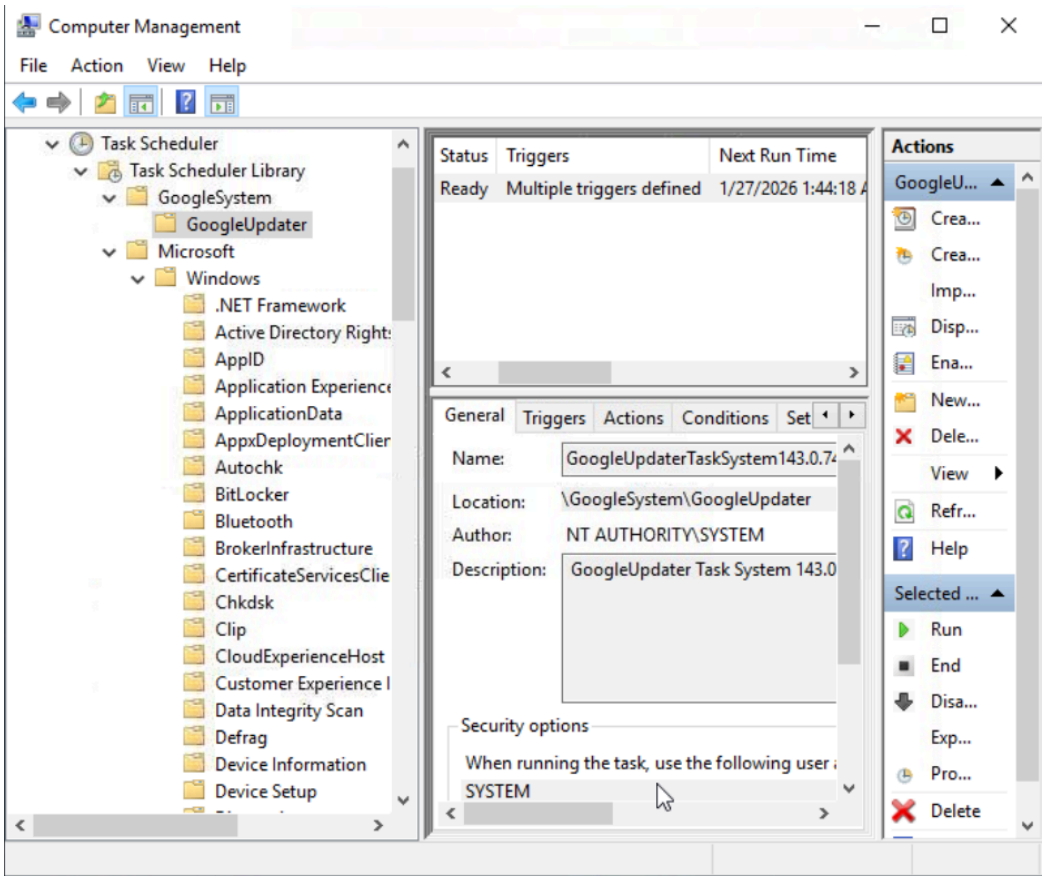
The Computer Management (compmgmt) utility is used to view & configure system settings and components. It has three primary sections: **System Tools, Storage, and Services and Applications.**



1. System tools

a. **Task Scheduler**: used to 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.

To view the scheduled tasks that are present on the system, click Task Scheduler Library. This will display all the scheduled tasks of the system. You can click on any of them to view their details. The screenshot below shows a scheduled task named SystemInfoDailyLog configured to run every day at 10:00 AM. Here, you will see the program or command that will run when the task is triggered.



b. Event Viewer: 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.

There are five types of events that can be logged.

The following table describes the five event types used in event logging.

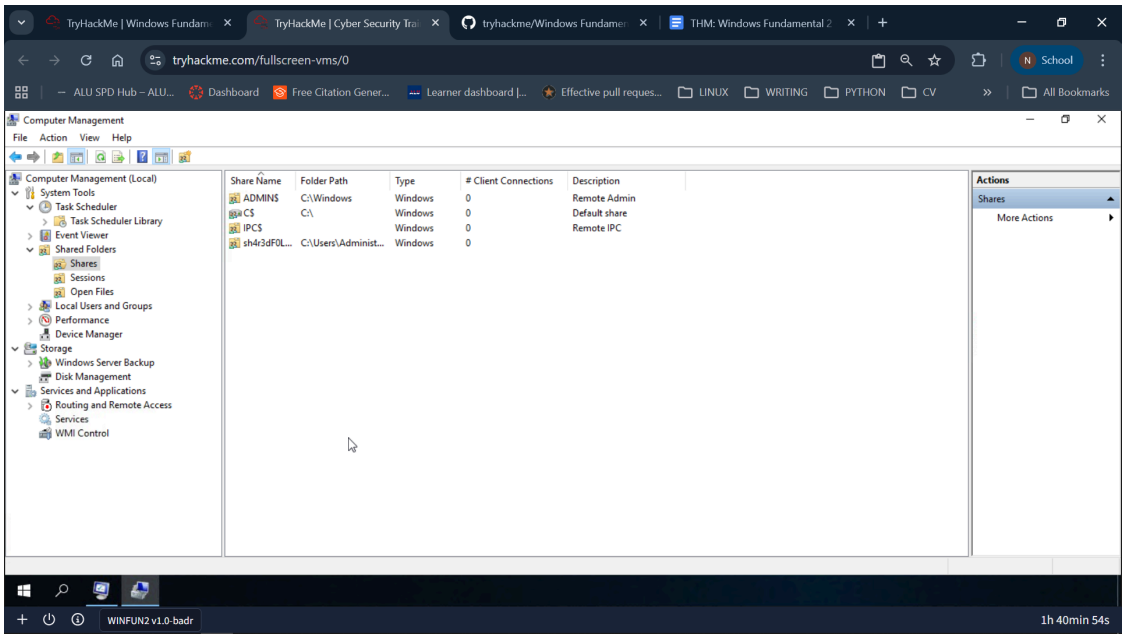
Event type	Description
Error	An event that indicates a significant problem such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error event is logged.
Warning	An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning event is logged. If an application can recover from an event without loss of functionality or data, it can generally classify the event as a Warning event.
Information	An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, it may be appropriate to log an Information event. Note that it is generally inappropriate for a desktop application to log an event each time it starts.
Success Audit	An event that records an audited security access attempt that is successful. For example, a user's successful attempt to log on to the system is logged as a Success Audit event.
Failure Audit	An event that records an audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt is logged as a Failure Audit event.

The standard logs are visible under **Windows Logs**:

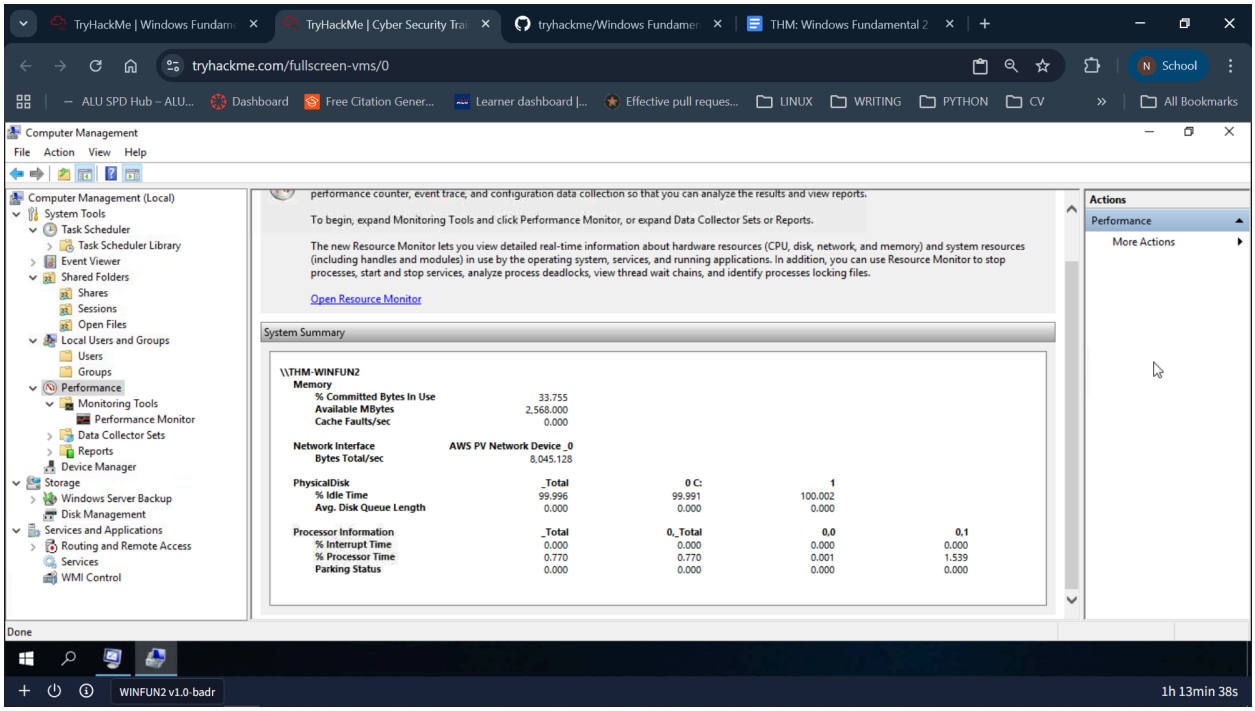
The event log contains the following standard logs as well as custom logs:

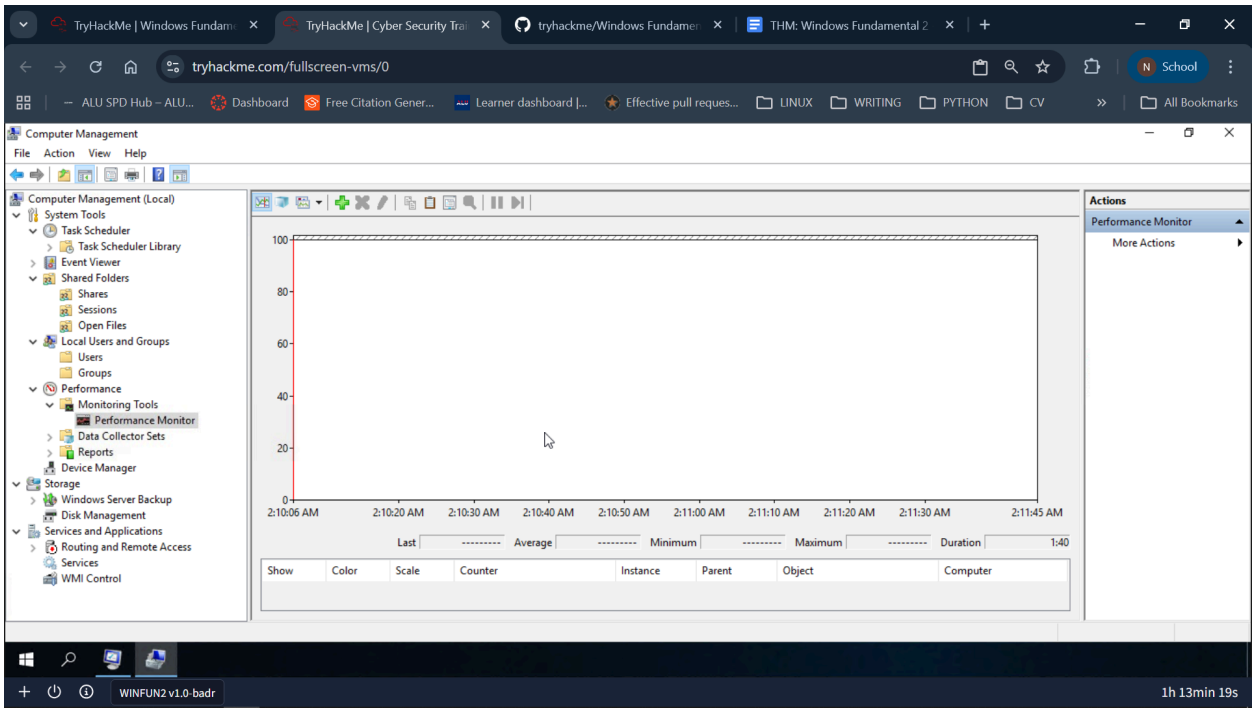
Log	Description
Application	Contains events logged by applications. For example, a database application might record a file error. The application developer decides which events to record.
Security	Contains events such as valid and invalid logon attempts, as well as events related to resource use such as creating, opening, or deleting files or other objects. An administrator can start auditing to record events in the security log.
System	Contains events logged by system components, such as the failure of a driver or other system component to load during startup.
CustomLog	Contains events logged by applications that create a custom log. Using a custom log enables an application to control the size of the log or attach ACLs for security purposes without affecting other applications.

c. **Shared Folders:** where you will see a complete list of shares and folders shared that others can connect to.



d. **Performance:** There is a utility called Performance Monitor (perfmon). Perfmon is used to view performance data either in real-time or from a log file. This utility is useful for troubleshooting performance issues on a computer system, whether local or remote.





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 and Applications

WMI Control configures and controls the Windows Management Instrumentation (WMI) service.

- Windows Management Instrumentation (WMI) is the infrastructure for management data and operations on Windows-based operating systems. It is used to automate administrative tasks on remote computers and supply management data to other parts of the operating system and products.

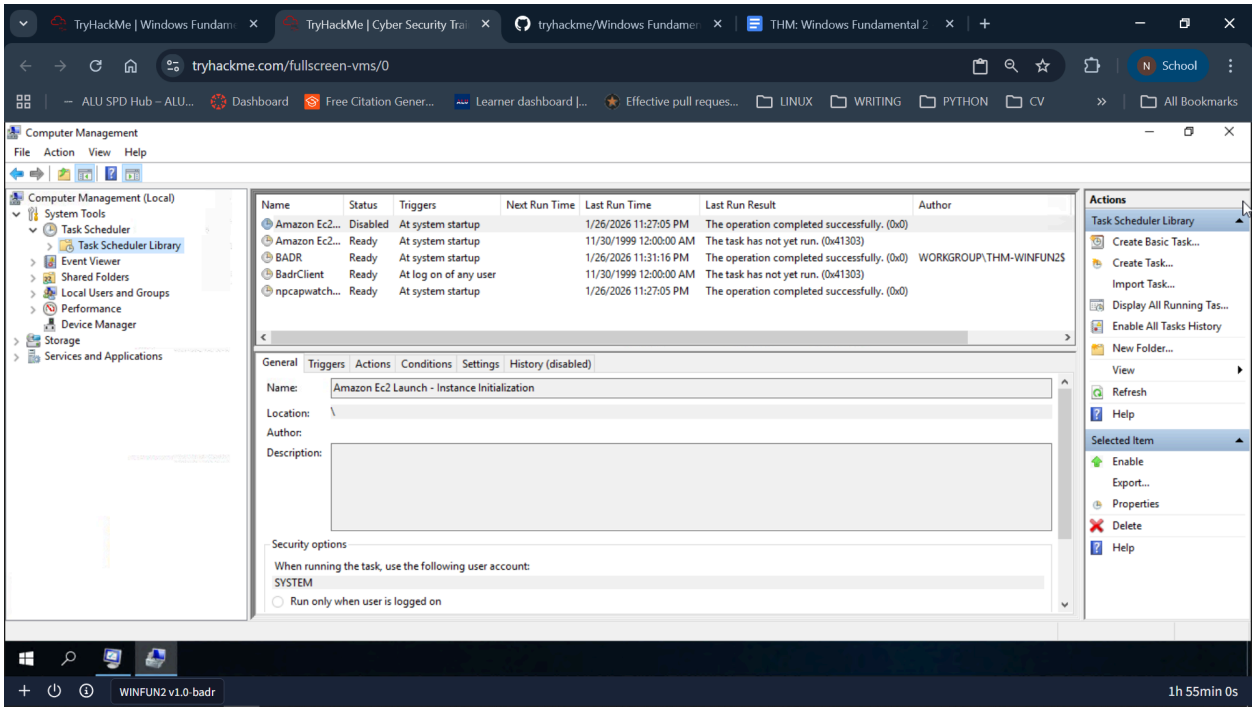
- Per Wikipedia, "WMI allows scripting languages (such as VBScript or Windows PowerShell) to manage Microsoft Windows personal computers and servers, both locally and remotely. Microsoft also provides a command-line interface to WMI called Windows Management Instrumentation Command-line (WMIC)."
- Note: The WMIC tool is deprecated in Windows 10, version 21H1. Windows PowerShell supersedes this tool for WMI.

Questions:

1. When is the *npcapwatchdog* scheduled task set to run at?

   Answer: At system startup

   I checked the task scheduler library to look up the *npcapwatchdog* task.



Task 5: System Information(msinfo32.exe)

The information in System Summary is divided into three sections:

- Hardware Resources
- Components
- Software Environment

Under the software Environment, we have Environment variables:

Per Microsoft, "*Environment variables store information about the operating system environment. This information includes details such as the operating system path, the number of processors used by the operating system, and the location of temporary folders.*

The environment variables store data that is used by the operating system and other programs. For example, the WINDIR environment variable contains the location of the Windows installation directory. Programs can query the value of this variable to determine where Windows operating system files are located".

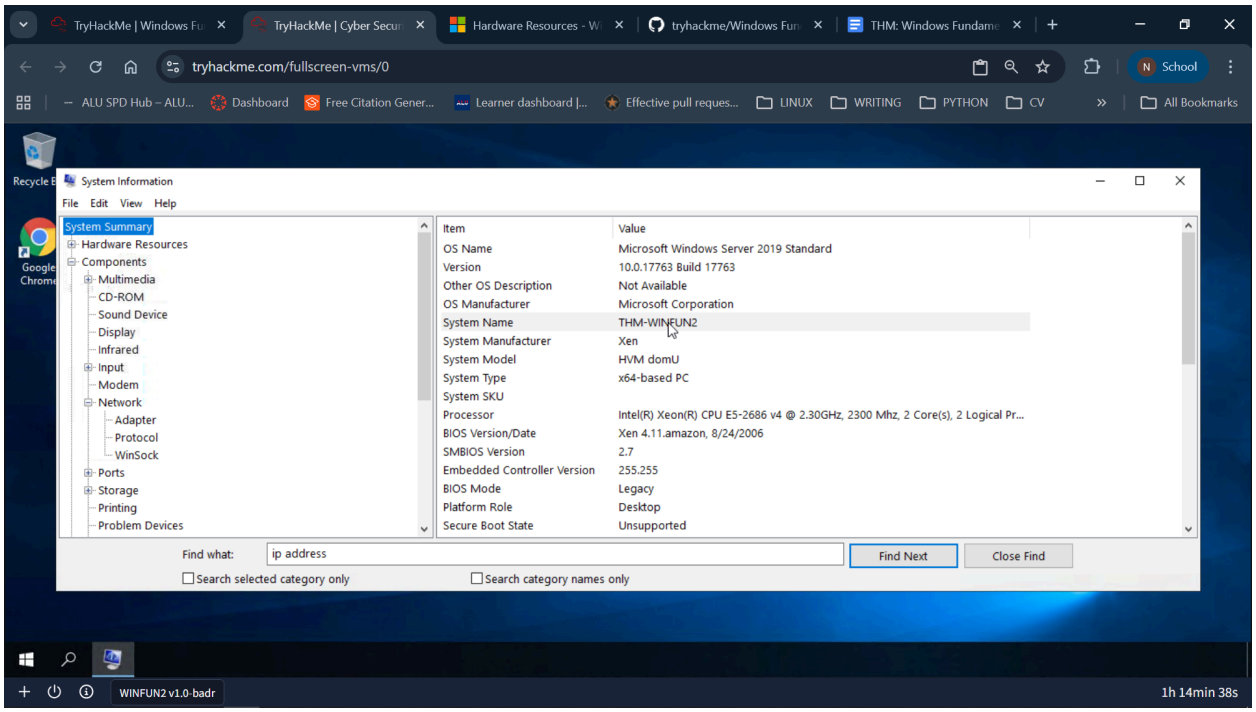
Questions:

1. What is the command to open System Information? (The answer is the name of the .exe file, not the full path)

   Answer: msinfo32.exe

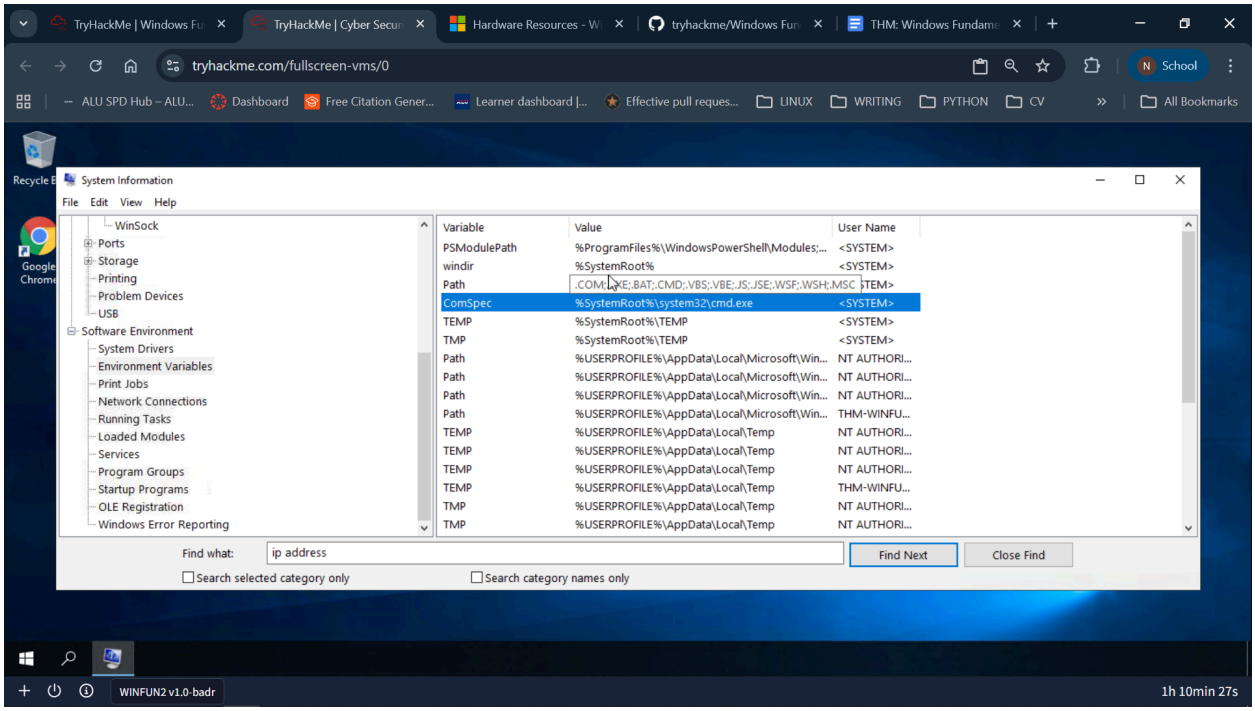
2. What is listed under System Name?

   Answer: **THM-WINFUN2**



3. Under Environment Variables, what is the value for ComSpec?

   Answer: **%SystemRoot%\system32\cmd.exe**



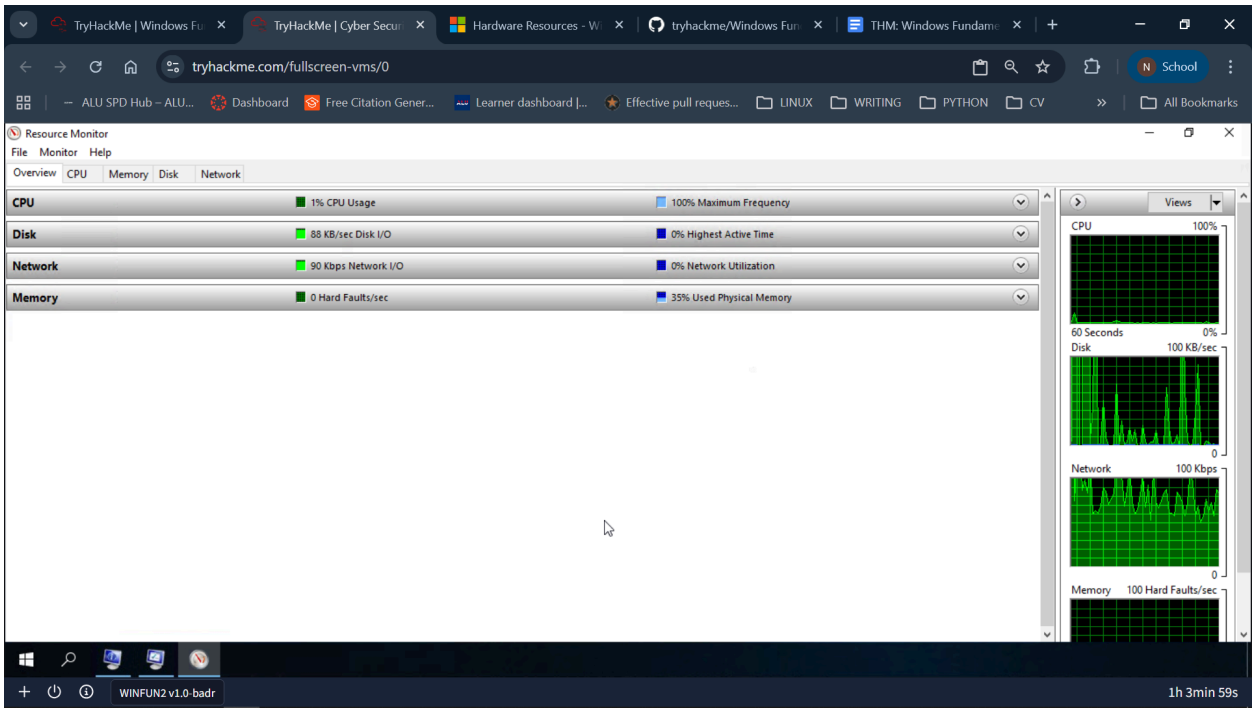
Task 6: Resource Monitor (resmon.exe)

Per Microsoft, *"Resource Monitor 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. It also includes a process analysis feature that can help identify deadlocked processes and file locking conflicts so that the user can attempt to resolve the conflict instead of closing an application and potentially losing data."*

This utility is geared primarily to advanced users who need to perform advanced troubleshooting on the computer system.

In the Overview tab, Resmon has four sections:

- CPU
- Disk
- Network
- Memory



Task 7: Command prompt

A user can run the following commands in command prompt to obtain information about the computer system:

1. **hostname -** outputs the computer name.
2. **whoami** - outputs the name of the logged-in user.
3. **ipconfig** - shows the network address settings for the computer.
4. **/? -** A command to retrieve the help manual for a command is.

   For example, to see the help manual for ipconfig, you can use the following command: **ipconfig /?**

5. **netstat -** displays protocol statistics and current TCP/IP network connections.
6. **net** - primarily used to manage network resources. This command supports sub-commands.

   If you type net without a sub-command, the output will show the syntax for the root command showing a few of the sub-commands you can use.

Questions:

1. In System Configuration, what is the full command for Internet Protocol Configuration?

   Answer: C:\Windows\System32\cmd.exe /k %windir%\system32\ipconfig.exe

2. For the ipconfig command, how do you show detailed information?

   Answer: ipconfig /all

Task 7: Registry Editor

The Windows Registry (per Microsoft) 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, such as:

- Profiles for each user
- Applications installed on the computer and the types of documents that each can create
- Property sheet settings for folders and application icons
- What hardware exists on the system
- The ports that are being used.

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

- **NB: Making changes to the registry can affect normal computer operations.**

Questions

What is the command to open the Registry Editor? (The answer is the name of the .exe file, not the full path)

Answer: regedt32.exe

Conclusion

Conclusion

This report explored key components of the Windows operating system through the Windows Fundamentals (Part 2) module on TryHackMe, with the aim of gaining a deeper understanding of how Windows is configured, managed, and troubleshot. By examining utilities such as System Configuration, Advanced System Settings, User Account Control, Computer Management, System Information, Resource Monitor, Command Prompt, and

the Windows Registry, I developed a clearer picture of how Windows operates beneath the surface.

Each task highlighted the importance of built-in administrative tools in diagnosing system issues, monitoring performance, managing security, and understanding system behaviour. Features such as crash dump configuration, scheduled tasks, environment variables, and registry settings demonstrated how Windows maintains stability, performance, and control across both user and system levels. Additionally, practical command-line usage reinforced how system information can be efficiently retrieved without relying solely on graphical interfaces.

Overall, this module significantly enhanced my technical familiarity with Windows internals. As a long-time Windows user, this hands-on exploration bridged the gap between everyday usage and administrative-level understanding, providing a strong foundation for further learning in system administration, troubleshooting, and cybersecurity.