

Module 2 Windows Fundamentals 2

Task 1- Introduction

We will continue our journey exploring the Windows operating system.



In [Windows Fundamentals 1](#), we covered the desktop, the file system, user account control, the control panel, settings, and the task manager.

This module will attempt to provide an overview of some other utilities available within the Windows operating system and different methods to access these utilities.

Press the **Start Machine** button below to launch the attached virtual machine.

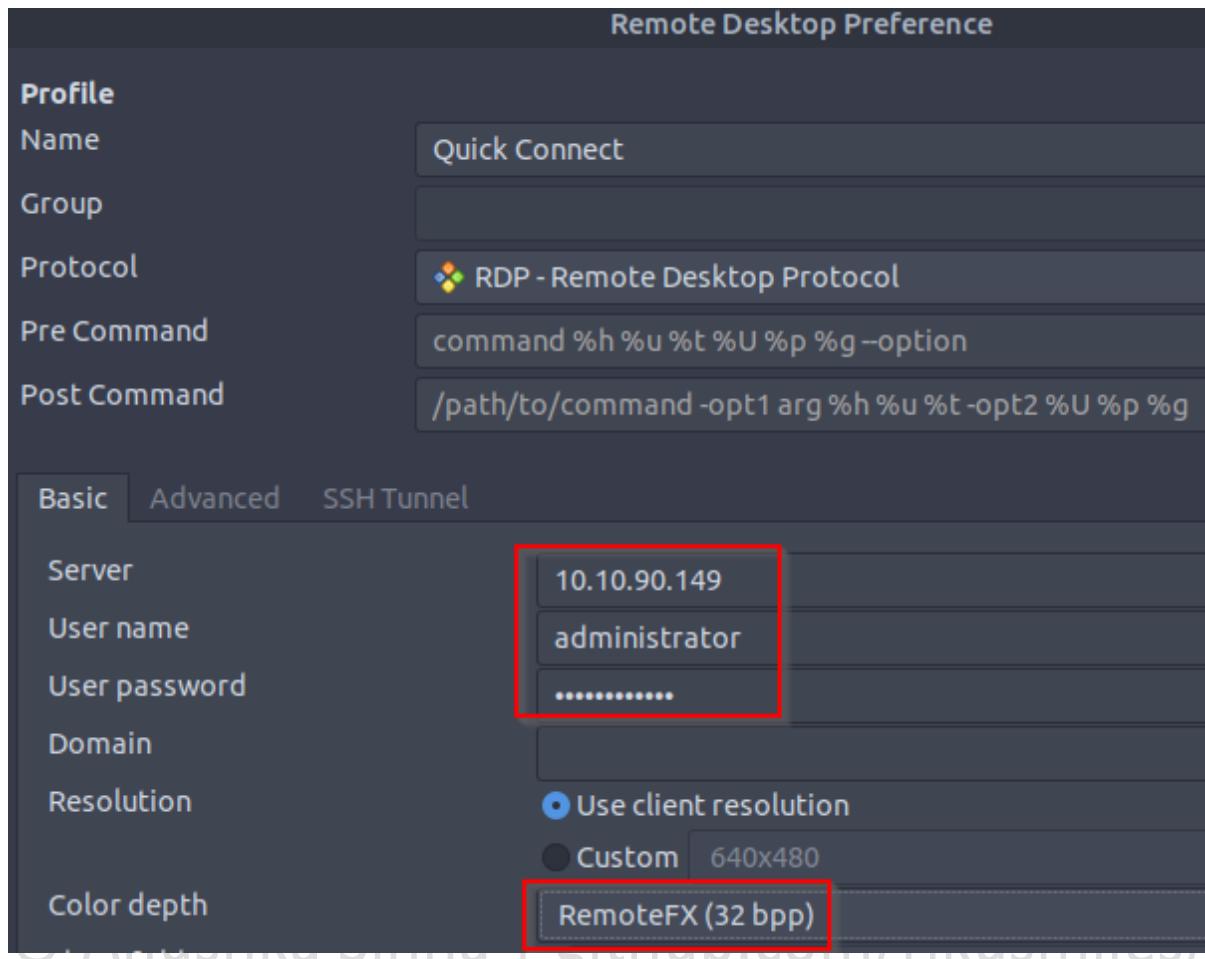
Start Machine

If you wish to access the virtual machine via Remote Desktop, use the credentials below.

Machine IP: MACHINE_IP

User: administrator

Password: letmein123!



Accept the Certificate when prompted, and you should be logged into the remote system now.

Note: The virtual machine may take up to 3 minutes to load.

Answer the questions below

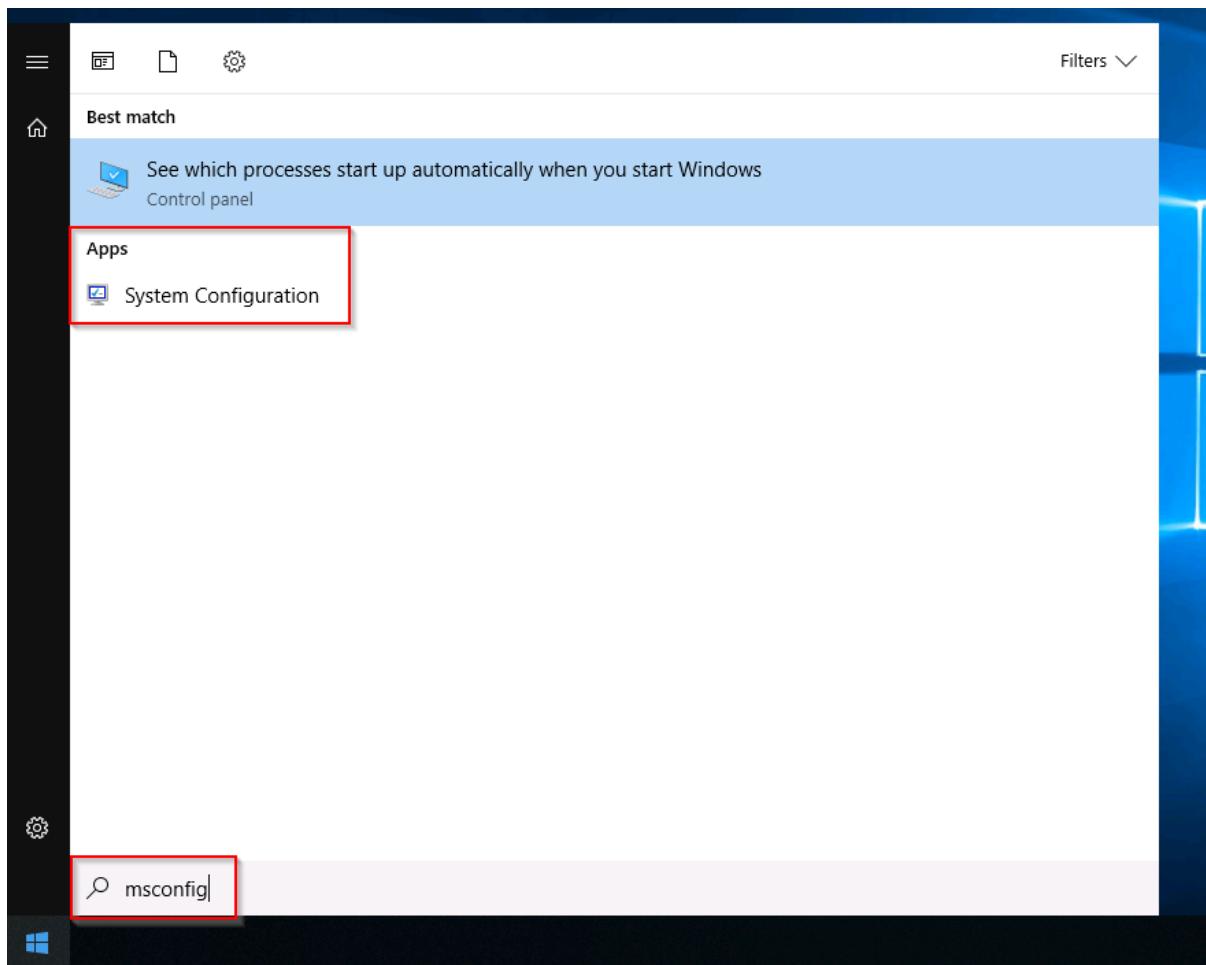
Read above and start the virtual machine.

Task 2- System Configuration

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

Reference the following document [here](#) for more information on the System Configuration utility.

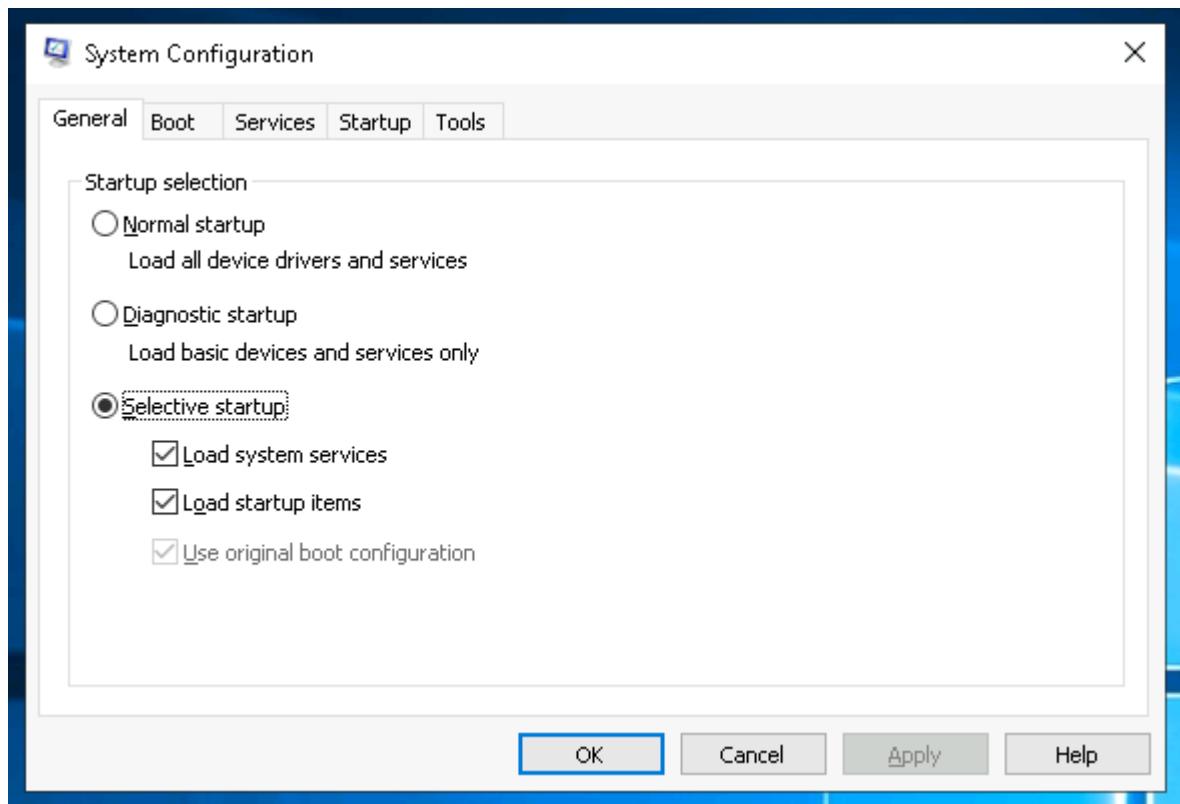
There are several methods to launch System Configuration. One method is from the Start Menu.



Note: You need local administrator rights to open this utility.

The utility has five tabs across the top. Below are the names for each tab. We will briefly cover each tab in this task.

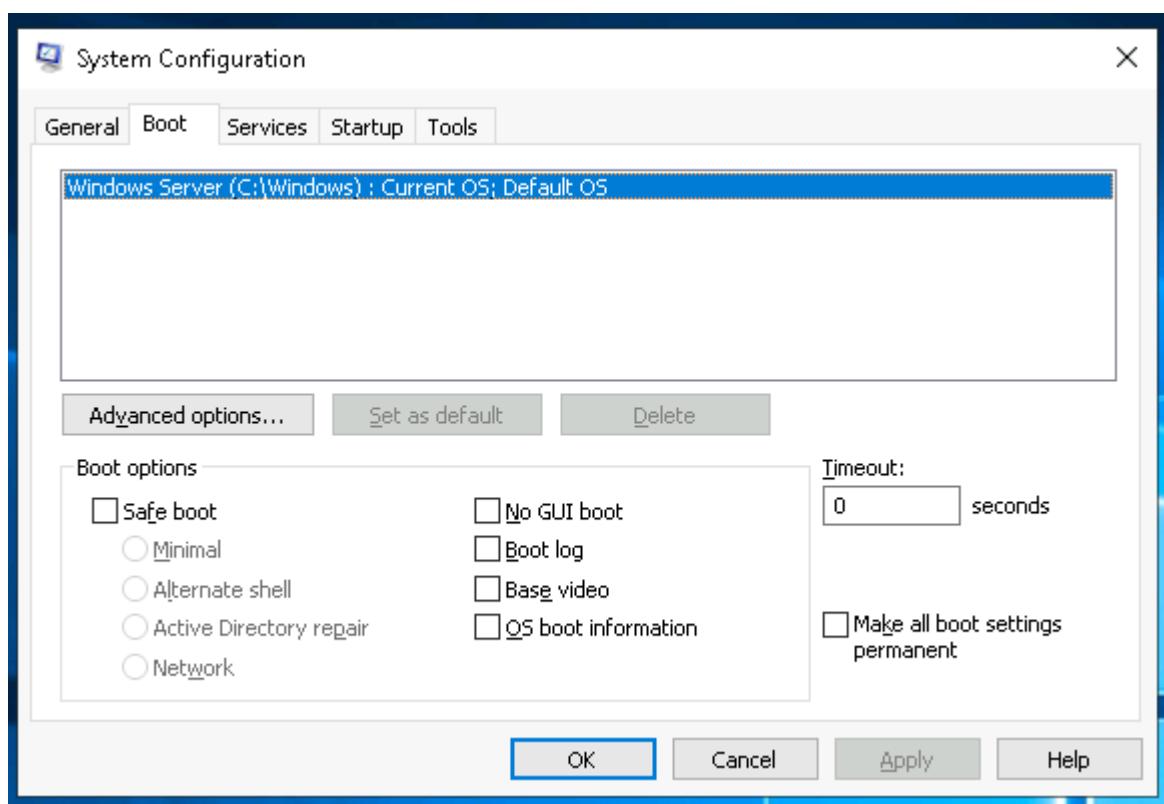
1. General
2. Boot
3. Services
4. Startup
5. Tools



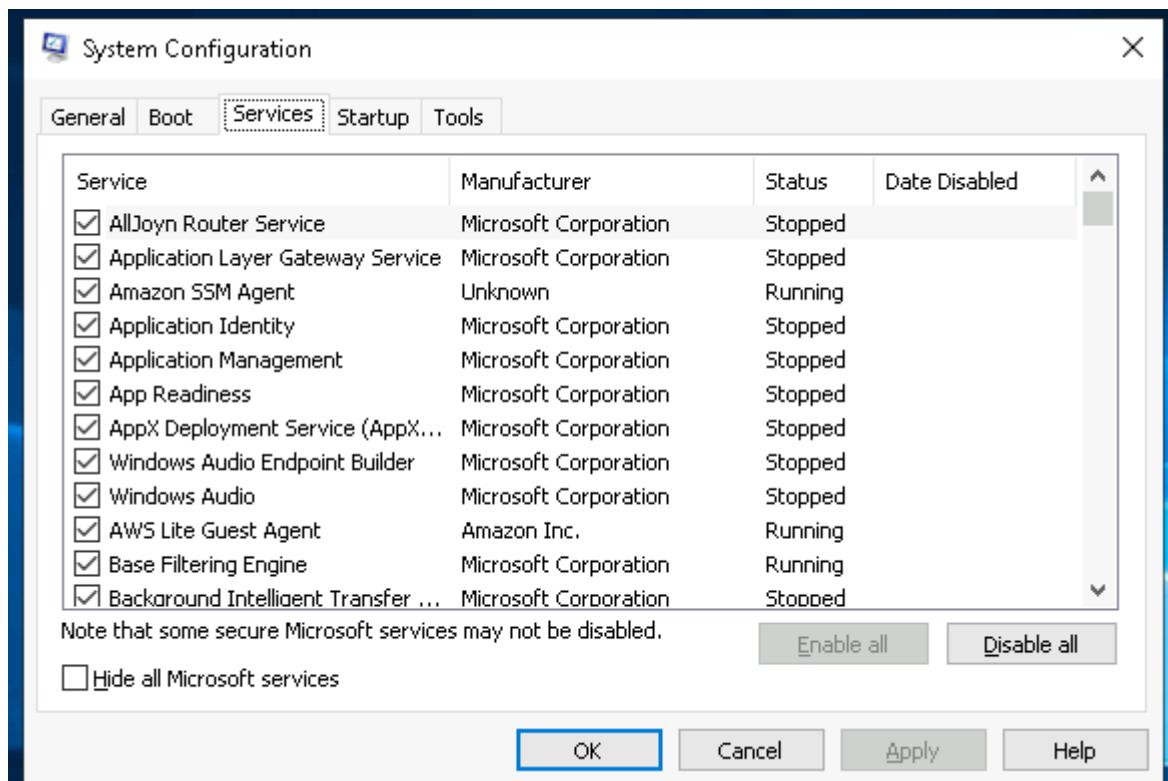
In the **General** tab, we can select what devices and services for Windows to load upon boot.

The options are: **Normal**, **Diagnostic**, or **Selective**.

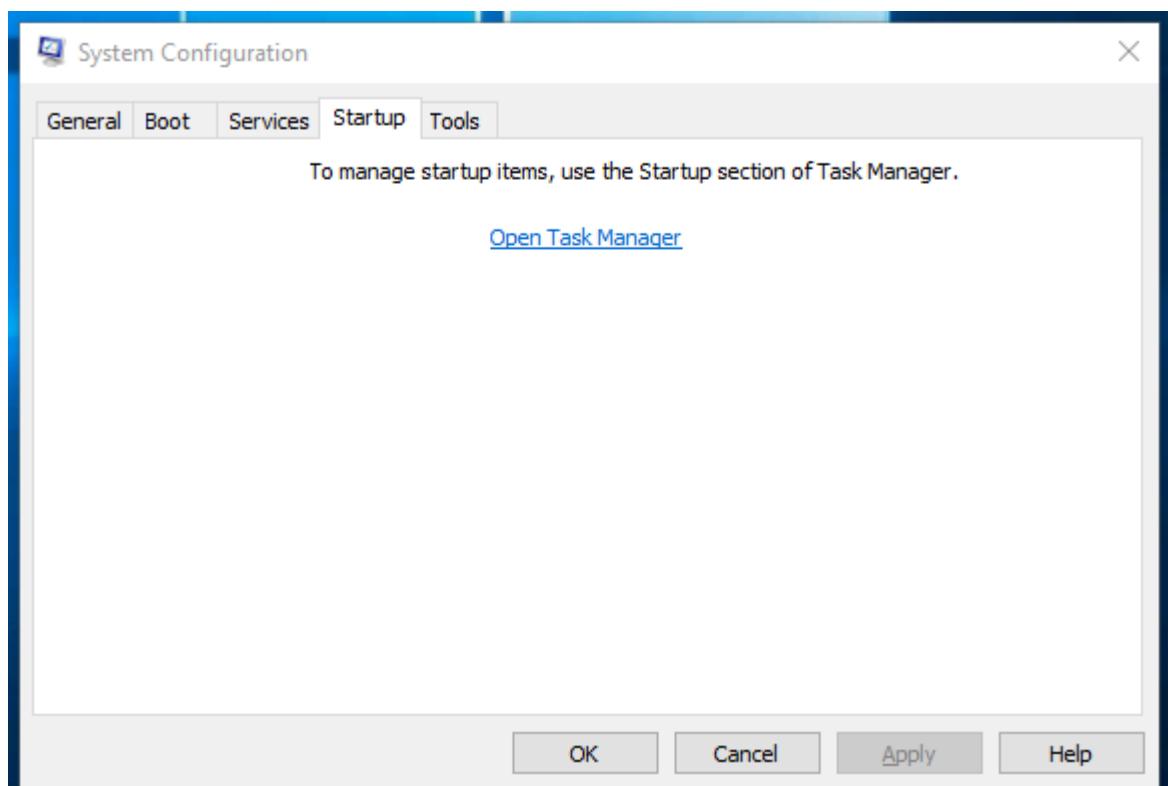
In the **Boot** tab, we can define various boot options for the Operating System.



The **Services** tab 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.



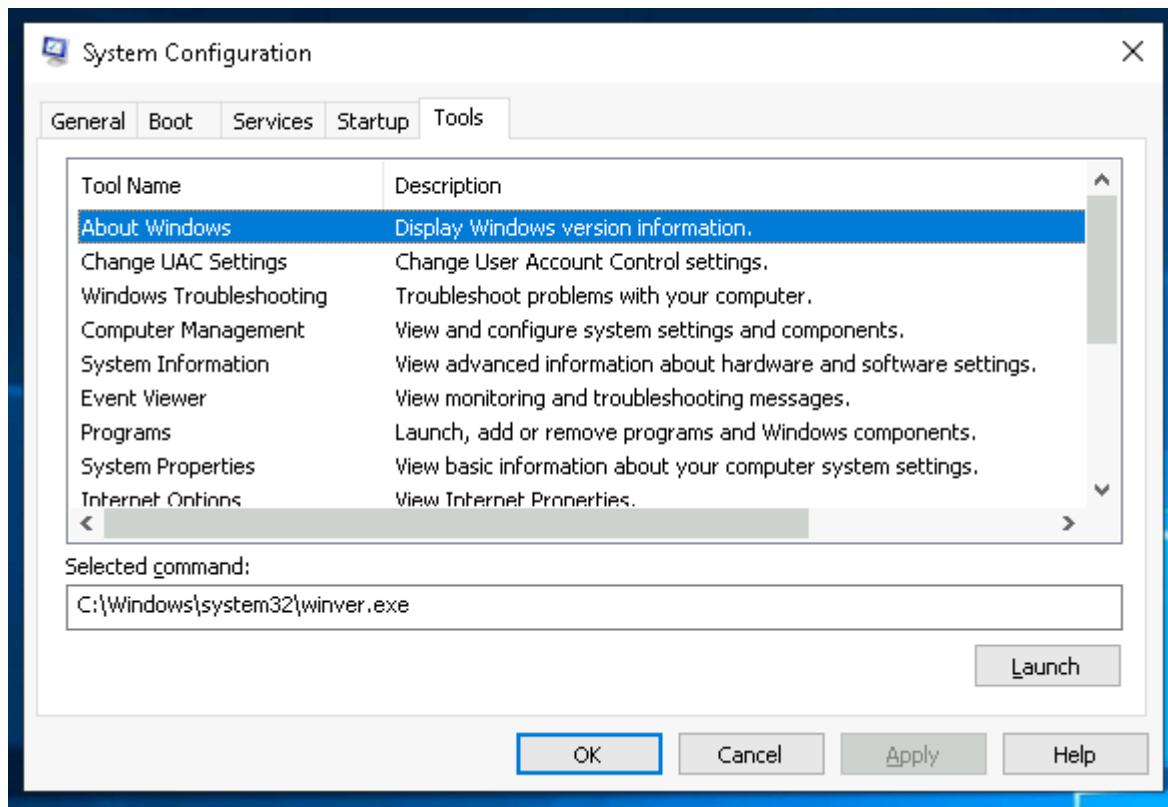
In the **Startup** tab, you won't see anything interesting in the attached VM. Below is a screenshot of the Startup tab for **MSConfig** from my local machine.



As you can see, Microsoft advises using **Task Manager** (`taskmgr`) to manage (enable/disable) startup items. The System Configuration utility is **NOT** a startup management program.

Note: If you open Task Manager for the attached VM, you will notice that Task Manager doesn't show a Startup tab.

There is a list of various utilities (tools) in the Tools tab that we 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.

Answer the questions below

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

PsShutdown

Submit

Whom is the Windows license registered to?

Winver, windows user

Submit

What is the command for Windows Troubleshooting?

C:\Windows\System32\control.exe /name Microsoft.Troubleshooting

Submit

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

The image shows a split-screen view. On the left, a browser window displays a challenge titled 'Room progress (23%)'. It asks three questions: 1) What is the name of the service that lists Systems Internals as the manufacturer? (Answer: PsShutdown, marked as correct). 2) Whom is the Windows license registered to? (Answer: Windows User, marked as correct). 3) What is the command for Windows Troubleshooting? (Answer: C:\Windows\System32\control.exe /name Microsoft.Troubleshooting, marked as correct). On the right, a Windows Server 2019 desktop is shown. A 'About Windows' dialog box is open, displaying system information. A message box at the top says 'Woop woop! Your answer is correct'. In the bottom right corner of the desktop, there is a taskbar with icons and the text '1h 44min 37s'.

Great question! You can find out who the Windows license is registered to by checking the **Registered Owner** and **Registered Organization** fields. Here are the main ways:

◆ Method 1: Using the winver command

1. Press **Win + R**.
 2. Type **winver** and press **Enter**.
 3. A dialog opens showing your Windows version, edition, and the name it is licensed to.
-

◆ Method 2: Using System Information

1. Press **Win + R**, type **msinfo32**, and press **Enter**.
 2. Look for **Registered Owner** and **Registered Organization** in the System Summary.
-

◆ Method 3: Using Command Prompt

1. Open **Command Prompt** (type cmd in Start).
2. Run:
3. slmgr /dli

or

slmgr /xpr

This shows license details, though the *owner* info is best seen in **msinfo32**.

☞ On many modern Windows 10/11 systems (especially those with digital licenses tied to a Microsoft account), the "Registered Owner" field might just say **Windows User** or be blank.

Do you want me to give you the **exact step-by-step with screenshots** for msinfo32 (that's the most reliable way for an exam or practical question)?

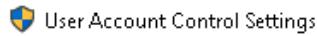
Task 3- Change UAC Settings

We're continuing with Tools that are available through the **System Configuration** panel.

User Account Control (UAC) was covered in great detail in [Windows Fundamentals 1](#).

The UAC settings can be changed or even turned off entirely (not recommended).

You can move the slider to see how the setting will change the UAC settings and Microsoft's stance on the setting.



- □

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
[Tell me more about User Account Control settings](#)

Always notify



Notify me only when apps try to make changes to my computer (default)

- Don't notify me when I make changes to Windows settings

i Recommended if you use familiar apps and visit familiar websites.

Never notify

OK

Cancel

Answer the questions below

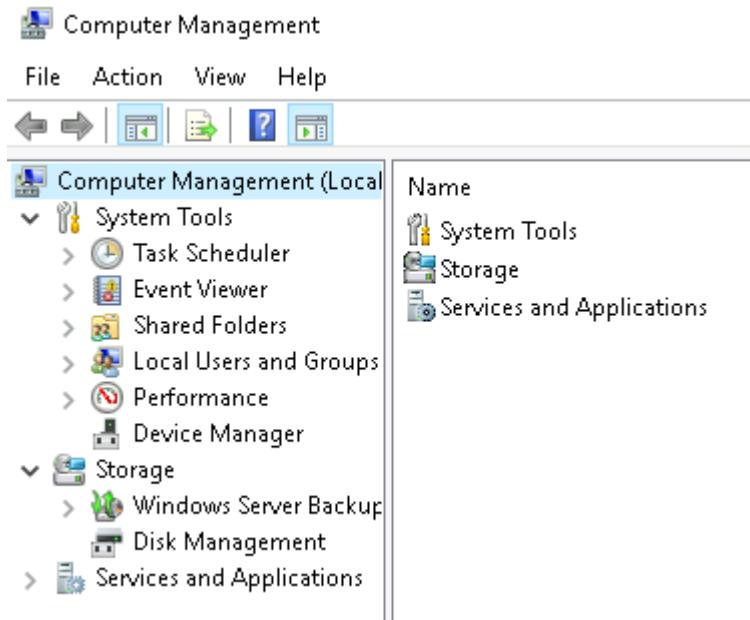
What is the command to open User Account Control Settings? (The answer is the name of the .exe file, not the full path)

UserAccountControlSettings.exe

Task 4- Computer Management

We're continuing with tools that are available through the **System Configuration** panel.

The **Computer Management** (compmgmt) utility has three primary sections: **System Tools, Storage, and Services and Applications**.

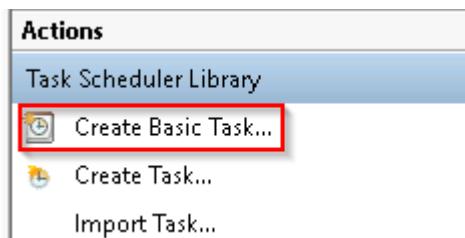


System Tools

Let's start with **Task Scheduler**. Per Microsoft, with Task Scheduler, we can create and manage common tasks that our computer will carry out automatically at the times we specify.

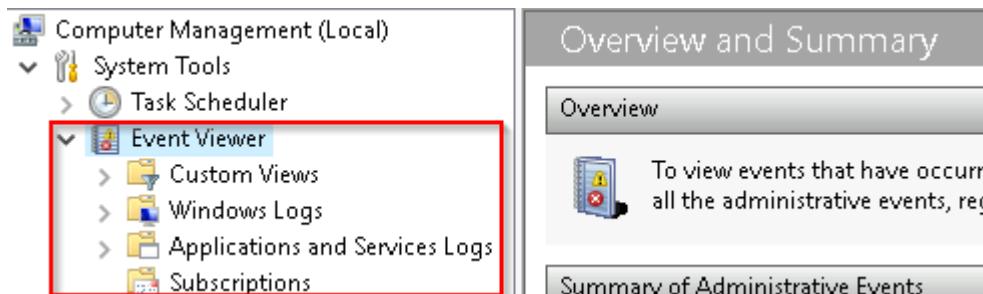
A task can run an application, a script, etc., and tasks can be configured to run at any point. A task can run at log in or at log off. Tasks can also be configured to run on a specific schedule, for example, every five mins.

To create a basic task, click on Create Basic Task under **Actions** (right pane).



Next is **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.



Event Viewer has three panes.

1. The pane on the left provides a hierarchical tree listing of the event log providers. (as shown in the image above)
2. The pane in the middle will display a general overview and summary of the events specific to a selected provider.
3. The pane on the right is the actions pane.

There are five types of events that can be logged. Below is a table from docs.microsoft.com providing a brief description for each.

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**. Below is a table from docs.microsoft.com providing a brief description for each.

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.

For more information about Event Viewer and Event Logs, please refer to the Windows Event Log [room](#).

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

Share Name	Folder Path	Type	# Client Connections	Description
ADMIN\$	C:\Windows	Windows	0	Remote Admin
C\$	C\	Windows	0	Default share
IPC\$		Windows	0	Remote IPC

In the above image, under Shares, are the default share of Windows, C\$, and default remote administration shares created by Windows, such as ADMIN\$.

As with any object in Windows, you can right-click on a folder to view its properties, such as Permissions (who can access the shared resource).

Under **Sessions**, you will see a list of users who are currently connected to the shares. In this VM, you won't see anybody connected to the shares.

All the folders and/or files that the connected users access will list under **Open Files**.

The **Local Users and Groups** section you should be familiar with from [Windows Fundamentals 1](#) because it's lusrmgr.msc.

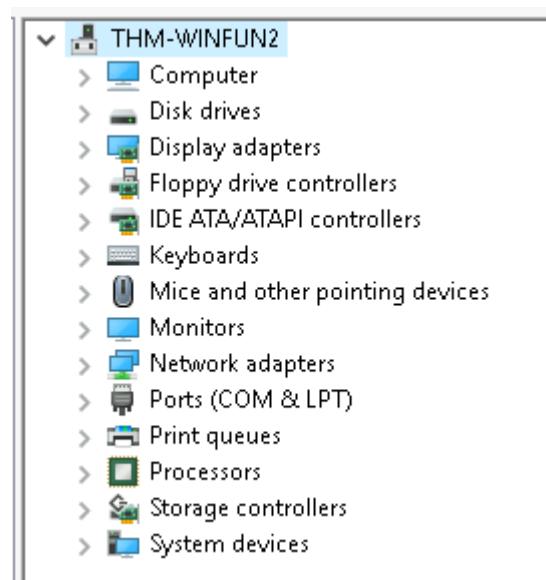
In **Performance**, you'll see a utility called **Performance Monitor** (perfmon).

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.

System Summary

\\THM-WINFUN2			
Memory			
% Committed Bytes In Use	44.807		
Available MBytes	980.000		
Cache Faults/sec	0.000		
Network Interface		AWS PV Network Device _0	
Bytes Total/sec	360.000		
PhysicalDisk		_Total	0 C: 1
% Idle Time	99.967	99.935	99.999
Avg. Disk Queue Length	0.001	0.001	0.000
Processor Information		_Total	0, _Total 0,0
% Interrupt Time	0.000	0.000	0.000
% Processor Time	0.001	0.001	0.001
Parking Status	0.000	0.000	0.000

Device Manager allows us to view and configure the hardware, such as disabling any hardware attached to the computer.



github.com/rikusmiles/

Storage

Under Storage is **Windows Server Backup** and **Disk Management**. We'll only look at Disk Management in this room.

Note: Since the virtual machine is a Windows Server operating system, there are utilities available that you will typically not see in Windows 10.

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
— (C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	19.46 GB	9.13 GB	47%
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	549 MB	115 MB	21%

Disk 0 Basic 20.00 GB Online	System Reserved 549 MB NTFS Healthy (System, Active, Primary Partition)	(C:) 19.46 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary Partition)
--	--	--

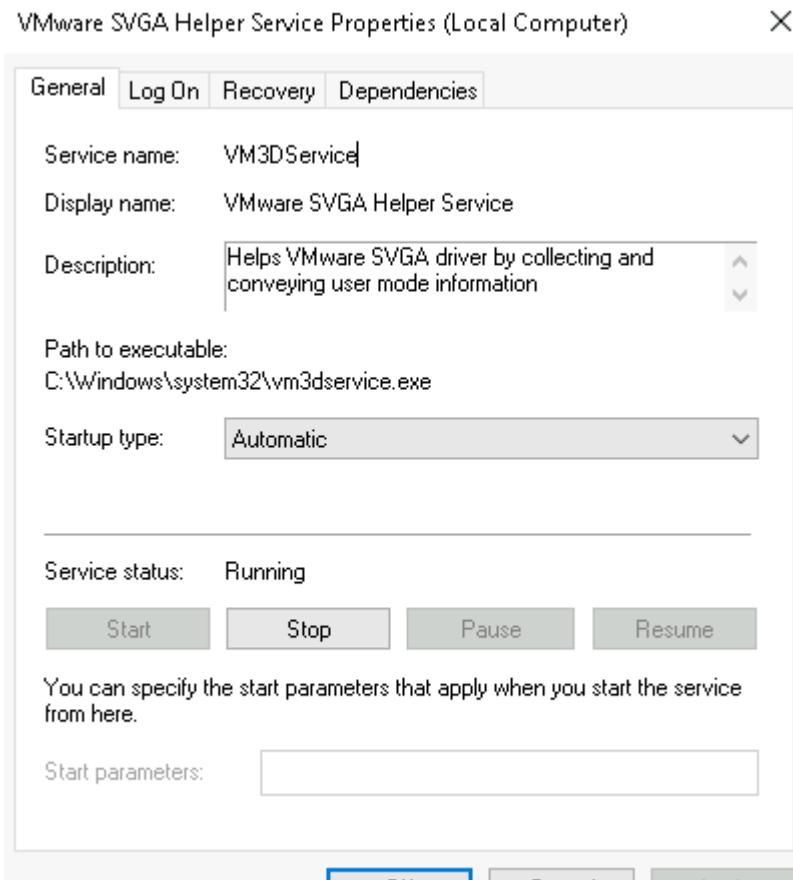
Disk Management is a system utility in Windows that enables you to perform advanced storage tasks. Some tasks are:

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

Services and Applications

Name	Type	Description
Routing and Remote ...	Routing and Remote Access	Routing and Remote Access
Services		Starts, stops, and configures Windows services.
WMI Control	Extension Snap-in	Configures and controls the Windows Management Instrumentation (WMI) service.

Recall from the previous task; a service is a special type of application that runs in the background. Here you can do more than enable and disable a service, such as view the Properties for the service.



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

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.

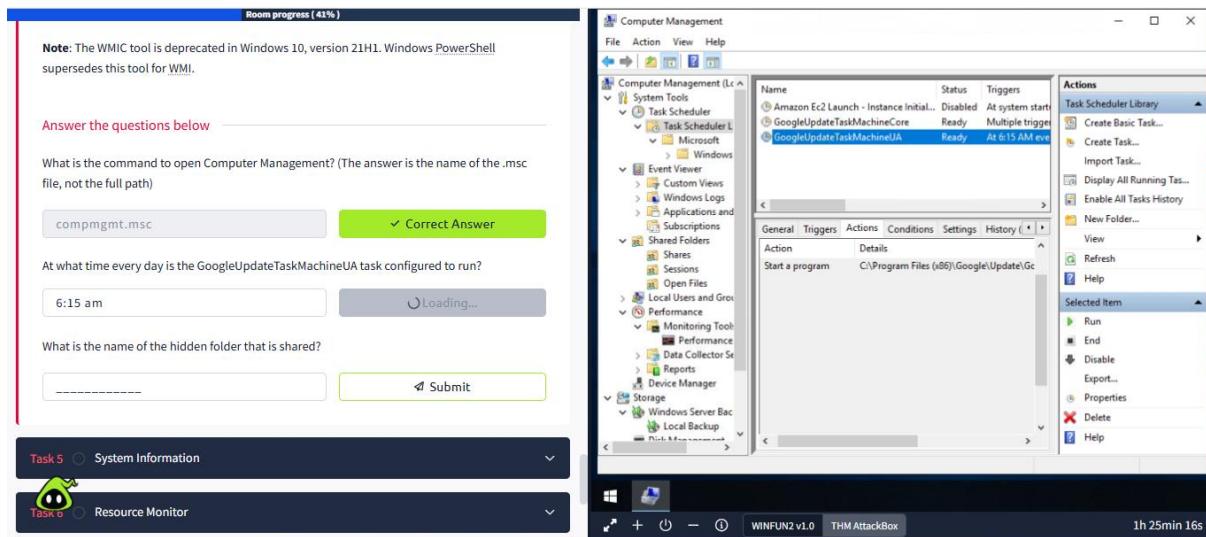
Answer the questions below

What is the command to open Computer Management? (The answer is the name of the .msc file, not the full path)

Compmgmt.msc

Submit

At what time every day is the GoogleUpdateTaskMachineUA task configured to run?



◆ Method 1: Task Scheduler

1. Press **Win + R**, type `taskschd.msc`, and hit **Enter**.
2. In the left pane, go to:
3. Task Scheduler Library > Google > Update
4. Look for **GoogleUpdateTaskMachineUA** in the middle pane.
5. Double-click it → Go to the Triggers tab → You'll see the **time of day** it is set to run.

Submit

What is the name of the hidden folder that is shared?

Good question — Windows has some **hidden administrative shares** that aren't visible in File Explorer but are created automatically for administration.

◆ Common Hidden Shared Folders

- **C\$** → The root of the C: drive is shared as **C\$** (hidden).
- **ADMIN\$** → Points to the Windows installation folder (usually C:\Windows).
- **IPC\$** → For interprocess communication (not a normal folder).
- Any other drives (D:, E:, etc.) also get hidden shares like **D\$, E\$, etc.**

The “\$” at the end means the share is **hidden** (not listed in the network browser).

◆ How to find out on your PC

1. Command Prompt method

Open cmd and type:

2. net share

This lists all shared folders, including hidden ones like C\$, ADMIN\$, and IPC\$.

3. Computer Management method

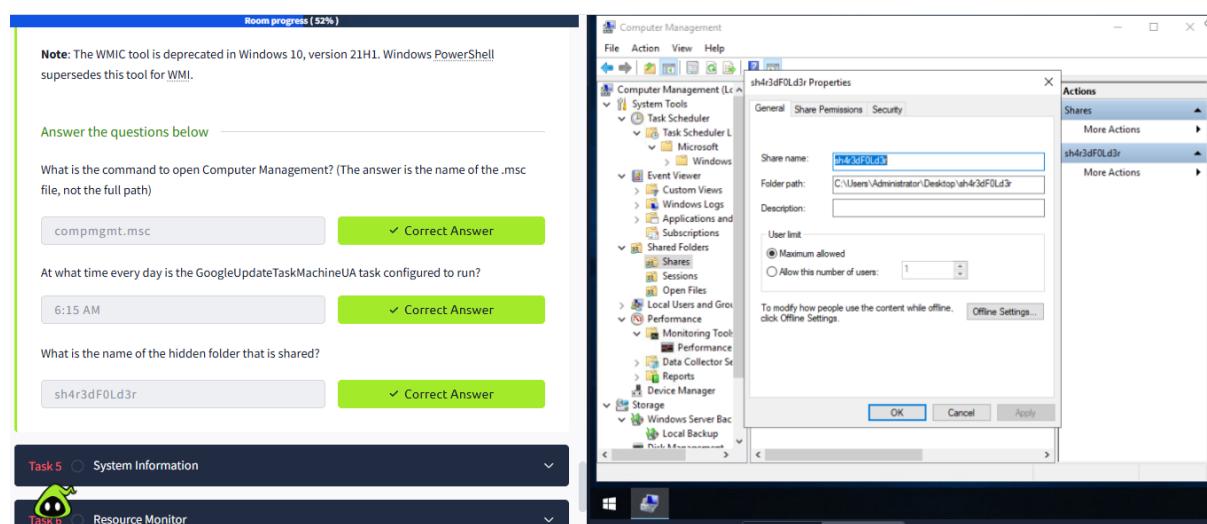
- Press **Win + R**, type compmgmt.msc, hit Enter.
- Go to **Shared Folders > Shares**.
- You'll see all current shares, including hidden ones.

The most typical answer to:

“What is the name of the hidden folder that is shared?” is:

C\$

Do you want me to also explain why Windows automatically creates these hidden shares (like for **remote administration and backups**)? That often comes up in exams.



Task 5- System Information

We're continuing with Tools that are available through the **System Configuration** panel.

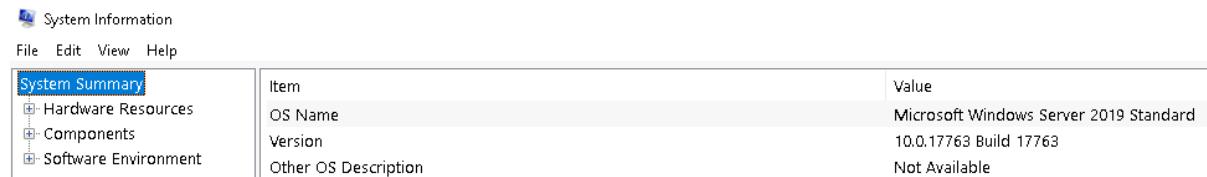
What is the **System Information** (msinfo32) tool?

Per Microsoft, "Windows includes a tool called Microsoft System Information (Msinfo32.exe). This 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."

The information in **System Summary** is divided into three sections:

- **Hardware Resources**
- **Components**
- **Software Environment**

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

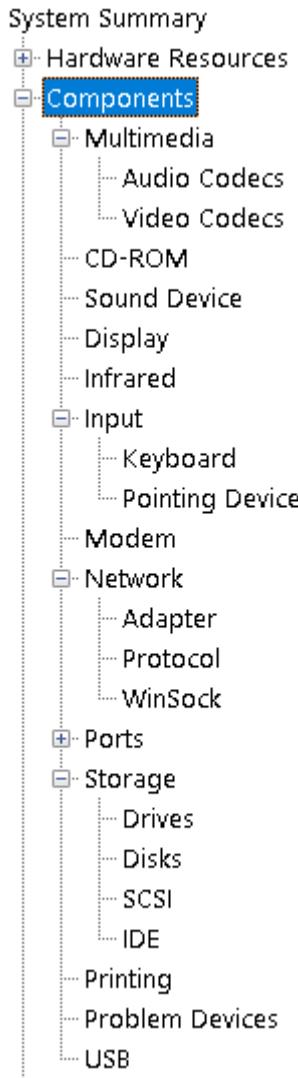


Item	Value
OS Name	Microsoft Windows Server 2019 Standard
Version	10.0.17763 Build 17763
Other OS Description	Not Available

The information displayed in **Hardware Resources** is not for the average computer user. If you want to learn more about this section, refer to the official Microsoft [page](#).

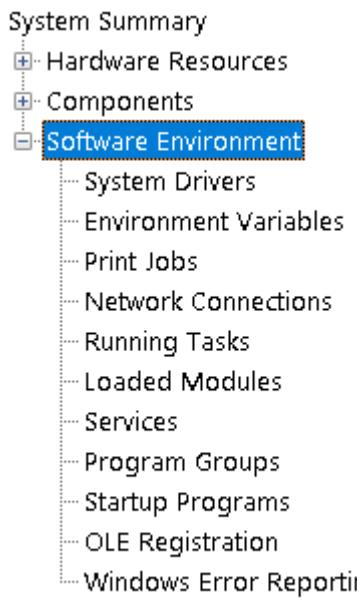


Under **Components**, you can see specific information about the hardware devices installed on the computer. Some sections don't show any information, but some sections do, such as **Display** and **Input**.



Sinha | github.com/rikusmiles/

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**.



Recall from the [Windows Fundamentals 1 room](#) (The Windows\System32 Folder task) where **Environment Variables** was briefly touched on.

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*".

Click on Environment Variables to see the assigned values for the virtual machine.

System Information

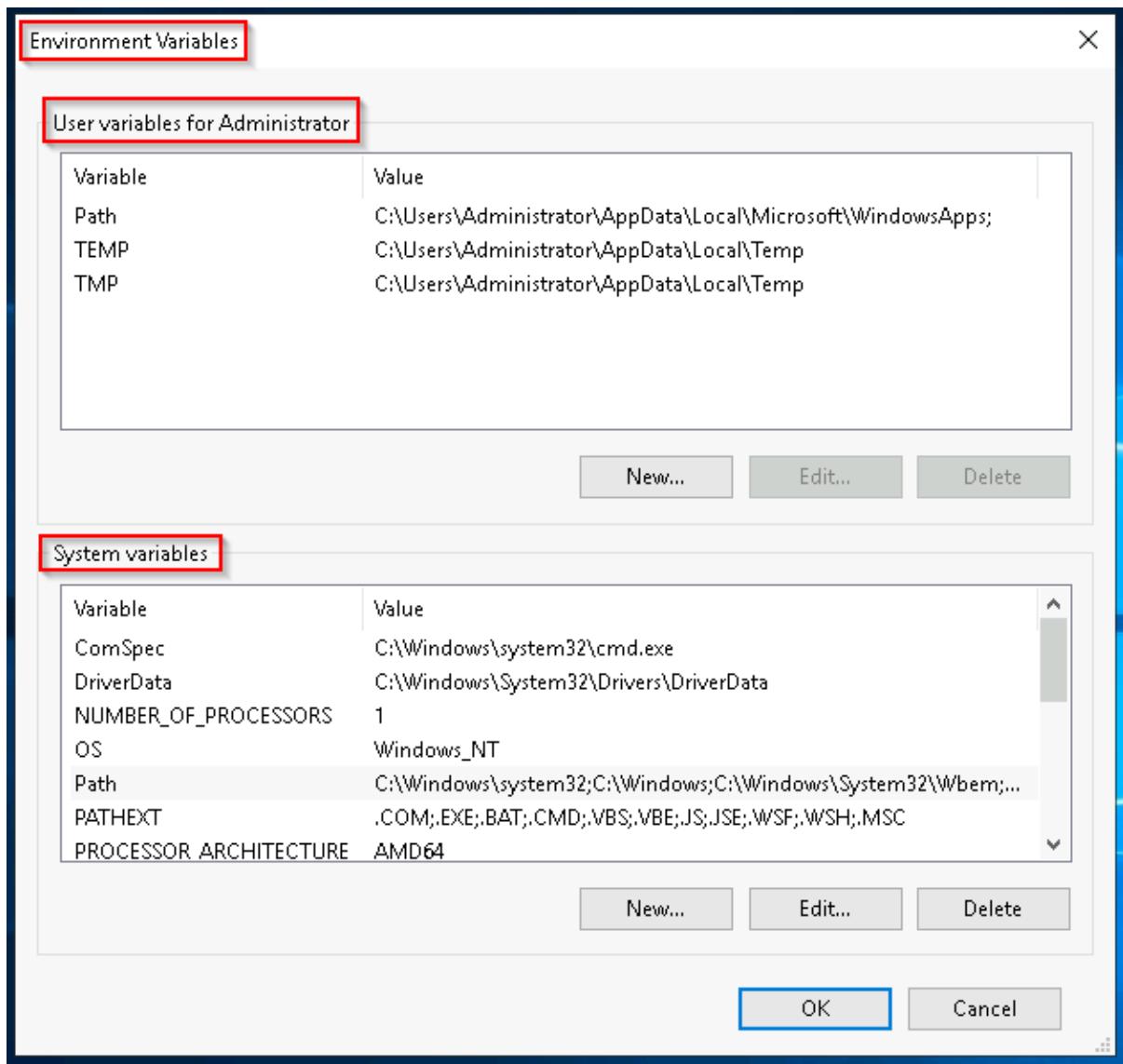
File Edit View Help

Variable	Value	User Name
DriverData	C:\Windows\System32\Drivers\DriverData	<SYSTEM>
NUMBER_OF_PROCESSORS	1	<SYSTEM>
OS	Windows_NT	<SYSTEM>
Path	%SystemRoot%\system32;%SystemRoot%\\Sys...<SYSTEM>	
Path	%USERPROFILE%\AppData\Local\Microsoft\Win... NT AUTHORITY\SYSTEM	
Path	%USERPROFILE%\AppData\Local\Microsoft\Win... NT AUTHORITY\LOCAL ...	
Path	%USERPROFILE%\AppData\Local\Microsoft\Win... NT AUTHORITY\NETW...	
Path	%USERPROFILE%\AppData\Local\Microsoft\Win... THM-WINFUN2\Admini...	
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.ISE;.WSF;.WS...	<SYSTEM>
PROCESSOR_ARCHITECTURE	AMD64	<SYSTEM>
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 63 Stepping 2, GenuineI...	<SYSTEM>
PROCESSOR_LEVEL	6	<SYSTEM>
PROCESSOR_REVISION	3f02	<SYSTEM>
PSModulePath	%ProgramFiles%\WindowsPowerShell\Modules;...<SYSTEM>	
TEMP	%SystemRoot%\TEMP	<SYSTEM>
TEMP	%USERPROFILE%\AppData\Local\Temp	NT AUTHORITY\SYSTEM
TEMP	%USERPROFILE%\AppData\Local\Temp	NT AUTHORITY\LOCAL ...
TEMP	%USERPROFILE%\AppData\Local\Temp	NT AUTHORITY\NETW...
TEMP	%USERPROFILE%\AppData\Local\Temp	THM-WINFUN2\Admini...
TMP	%SystemRoot%\TEMP	<SYSTEM>
TMP	%USERPROFILE%\AppData\Local\Temp	NT AUTHORITY\SYSTEM
TMP	%USERPROFILE%\AppData\Local\Temp	NT AUTHORITY\LOCAL ...
TMP	%USERPROFILE%\AppData\Local\Temp	NT AUTHORITY\NETW...
TMP	%USERPROFILE%\AppData\Local\Temp	THM-WINFUN2\Admini...
USERNAME	SYSTEM	<SYSTEM>
windir	%SystemRoot%	<SYSTEM>

Find what:

Search selected category only Search category names only

Another method to view environment variables is Control Panel > System and Security > System > Advanced system settings > Environment Variables **OR** Settings > System > About > system info > Advanced system settings > Environment Variables.



The detour is over. Let's redirect our attention back to msinfo32 and pick up where we left off.

Towards the very bottom of this utility, there is a search bar. Please give it a go. Select Components and search for IP address.

Components		Adapter Type	Not Available
Multimedia	Product Type	Microsoft Kernel Debug Network Adapter	
Audio Codecs	Installed	Yes	
Video Codecs	PNP Device ID	ROOT\KDNIC\0000	
CD-ROM	Last Reset	5/20/2021 11:07 AM	
Sound Device	Index	0	
Display	Service Name	kdnic	
Infrared	IP Address	Not Available	
Input	IP Subnet	Not Available	
Keyboard	Default IP Gateway	Not Available	
Pointing Device	DHCP Enabled	Yes	
Modem	DHCP Server	Not Available	
Network	DHCP Lease Expires	Not Available	
Adapter	DHCP Lease Obtained	Not Available	
Protocol	MAC Address	Not Available	
WinSock	Driver	c:\windows\system32\drivers\kdnic.sys (6.1.0.0, 23.50 KB (24,064 bytes), 9/15/...	
Ports	Name	[00000001] Intel(R) 82574L Gigabit Network Connection	
Storage	Adapter Type	Not Available	
Drives	Product Type	Intel(R) 82574L Gigabit Network Connection	
Disks	Installed	Yes	
SCSI	PNP Device ID	Not Available	
IDE	Last Reset	5/20/2021 11:07 AM	
Printing	Index	1	
Problem Devices	Service Name	e1iexpress	
USB			
Software Environment			

Find what: Search selected category only

Answer the questions below

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

Msinfo32.exe

Submit

What is listed under System Name?

THM-WINFUN2

Room progress (64%)

Find what: Search selected category only

Answer the questions below

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

✓ Correct Answer

What is listed under System Name?

✓ Correct Answer

Under Environment Variables, what is the value for ComSpec?

Submit

Task 6 Resource Monitor

Command Prompt

System Information

Item	Value
OS Name	Microsoft Windows Server 2019 Standard
Version	10.0.17763 Build 17763
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	THM-WINFUN2
System Manufacturer	Xen
System Model	HVM domU
System Type	x86-based PC
System SKU	
Processor	Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.80GHz
BIOS Version/Date	Xen 4.11.amazon, 8/24/2006
SMBIOS Version	2.7
Embedded Controller Version	255.255
Platform Role	Legacy
Current Boot State	Unconnected

Find what: Search selected category only

Task 6 Resource Monitor

Command Prompt

Submit

Under Environment Variables, what is the value for ComSpec?

%SystemRoot%\system32\cmd.exe

Task 6- Resource Monitor

We're continuing with Tools that are available through the **System Configuration** panel.

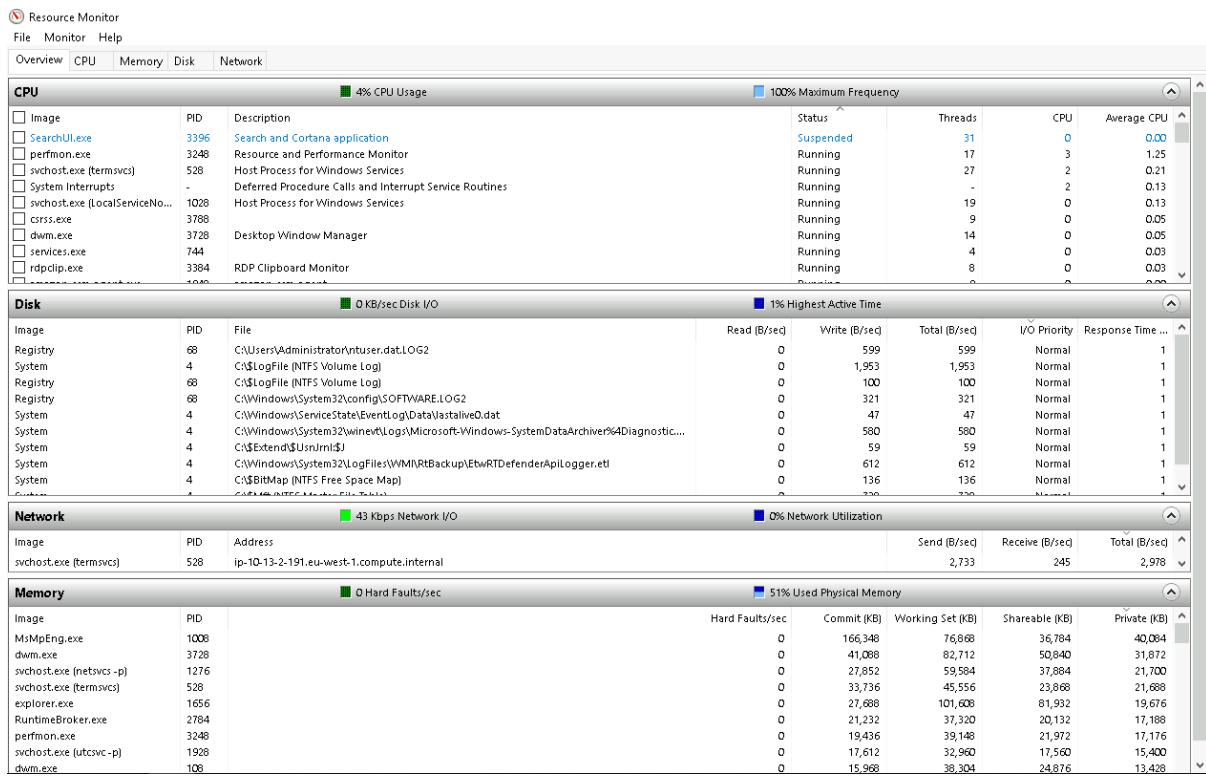
What is **Resource Monitor** (resmon)?

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.*"

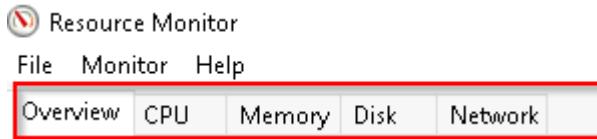
As some of the other tools mentioned in this room, this utility is geared primarily to advanced users who need to perform advanced troubleshooting on the computer system.

In the Overview tab, Resmon has four sections:

- **CPU**
- **Disk**
- **Network**
- **Memory**

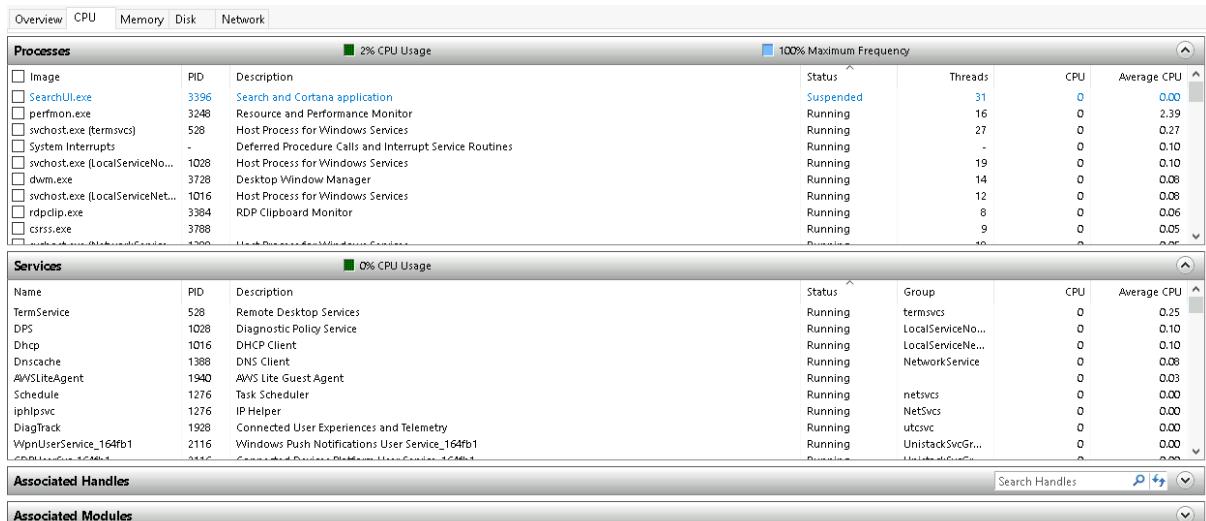


The same four sections have corresponding tabs across the top. See below.

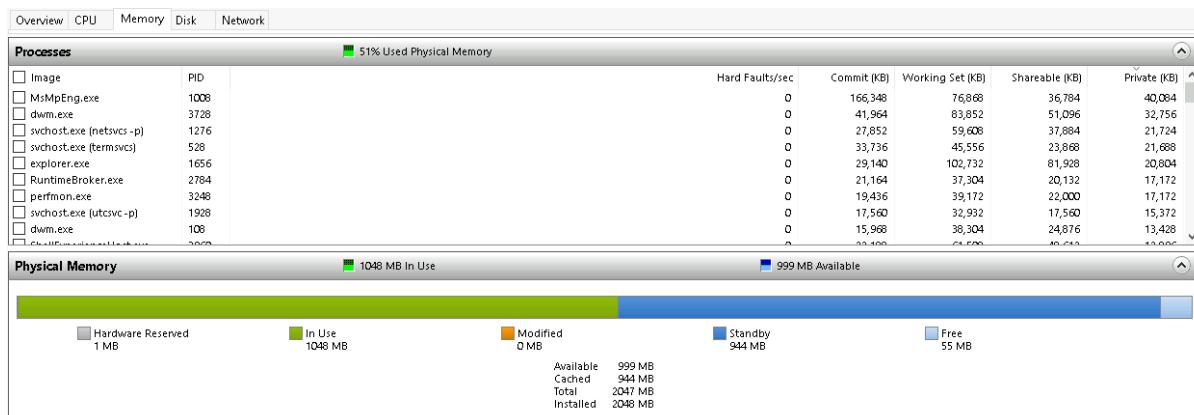


Note that each tab has additional information for each. An image is shown below for each tab.

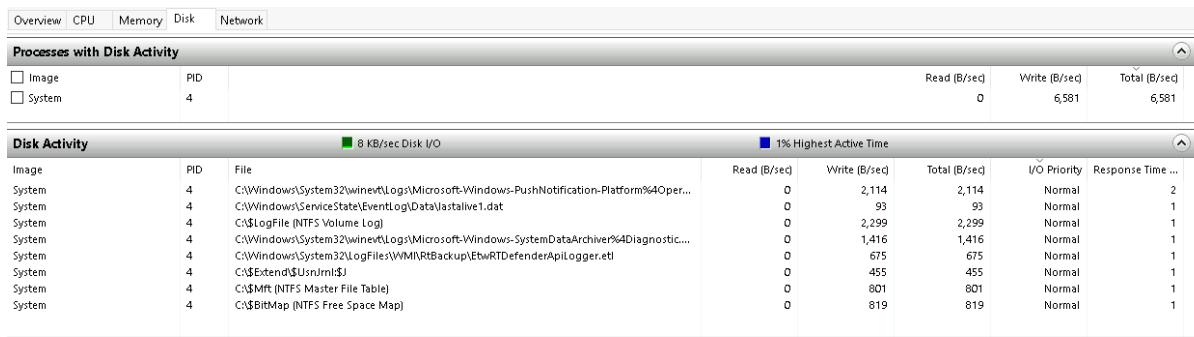
CPU



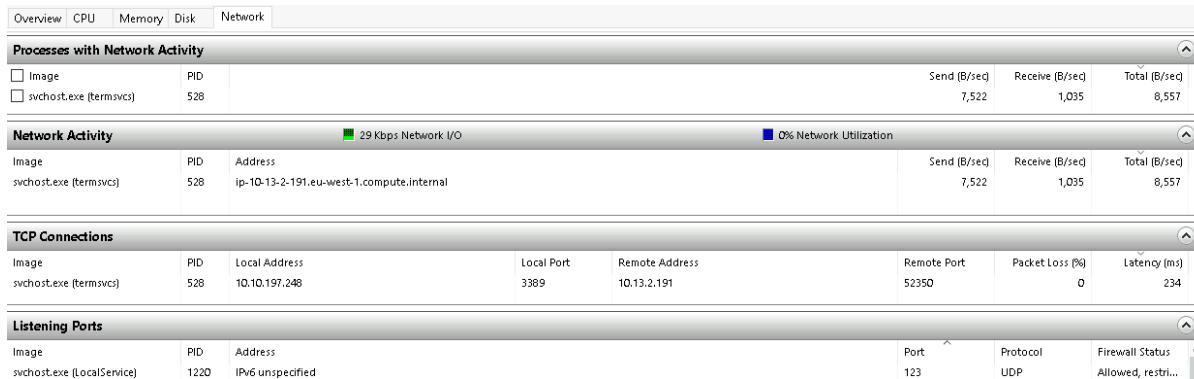
Memory



Disk



Network



Although not captured in any of the images above, Resource Monitor has a pane at the far right. This pane shows a graphical view in real-time for each section.

Note: The information displayed in Resource Monitor will be different for you compared to the images above.

Answer the questions below

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

Resmon.exe

Submit

Excellent observation 🙌 — you've spotted a real design difference in Windows tools.

Here's why:

◆ **.msc files**

- **MSC = Microsoft Saved Console.**
- They are *snap-in consoles* for the **Microsoft Management Console (MMC)** framework.
- Example:
 - compmgmt.msc → opens Computer Management
 - services.msc → opens Services
 - eventvwr.msc → opens Event Viewer

These are like *containers* that plug into the MMC shell.

◆ **.exe files**

- **EXE = Executable programs.**
- Tools that were designed as **standalone applications** use .exe.
- Example:
 - resmon.exe → Resource Monitor
 - taskmgr.exe → Task Manager
 - notepad.exe → Notepad

These don't run *inside* MMC; they are their own apps with custom GUIs.

◆ **Why the difference?**

- Tools like **Computer Management** or **Services** are built as **MMC snap-ins**, so they use .msc.

- Tools like **Resource Monitor** were built as **dedicated executables**, not MMC snap-ins
 - so they use .exe.
-

✓ So the short answer:

- **compmgmt.msc** works because it's an MMC console file.
 - **resmon.exe** works because Resource Monitor was built as a standalone program, not as an MMC snap-in.
-

Do you want me to give you a **list of the most useful .msc vs .exe tools** (like a cheat sheet)? It's a common exam topic.

Perfect  — here's a **Windows cheat sheet** of the most useful tools, split into **.msc (MMC snap-ins)** and **.exe (executables)**.

MMC Snap-Ins (.msc)

These are management consoles that run inside the Microsoft Management Console framework.

- compmgmt.msc → Computer Management
- services.msc → Services
- eventvwr.msc → Event Viewer
- secpol.msc → Local Security Policy
- gpedit.msc → Local Group Policy Editor
- devmgmt.msc → Device Manager
- diskmgmt.msc → Disk Management
- perfmon.msc → Performance Monitor
- taskschd.msc → Task Scheduler
- lusrmgr.msc → Local Users and Groups
- certmgr.msc → Certificate Manager
- fsmgmt.msc → Shared Folders

(Some are Pro/Enterprise only, e.g., gpedit.msc and secpol.msc aren't in Home.)

Executables (.exe)

These are standalone programs with their own GUI, not part of MMC.

- resmon.exe → Resource Monitor
- taskmgr.exe → Task Manager
- msinfo32.exe → System Information
- dxdiag.exe → DirectX Diagnostic Tool
- control.exe → Control Panel
- notepad.exe → Notepad
- regedit.exe → Registry Editor
- mspaint.exe → Paint
- calc.exe → Calculator
- cmd.exe → Command Prompt
- powershell.exe → Windows PowerShell
- explorer.exe → File Explorer

Quick Rule of Thumb:

- If it's a **system management console**, it's usually .msc.
- If it's a **standalone app/tool**, it's .exe.

Would you like me to also build you a **one-page PDF “Windows Run Commands Quick Reference”** with both lists side by side (good for exams/interviews)?

Task 7- Command Prompt

We're continuing with Tools that are available through the **System Configuration** panel.

The command prompt (cmd) can seem daunting at first, but it's really not that bad once you understand how to interact with it.

In early operating systems, the command line was the sole way to interact with the operating system.

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.

In this task, we'll only cover a few commands that a computer user can run in the command prompt to obtain information about the computer system.

Let's start with a few simple commands, such as `hostname` and `whoami`.

The command **hostname** will output the computer name.

```
C:\Users\Administrator>hostname  
THM-WINFUN2
```

The command **whoami** will output the name of the logged-in user.

```
C:\Users\Administrator>whoami  
thm-winfun2\administrator
```

Next, let's look at some commands that are useful when troubleshooting.

A command used often is `ipconfig`. This command will show the network address settings for the computer.

```
C:\Users\Administrator>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet:  
  
Connection-specific DNS Suffix . : eu-[REDACTED].internal  
Link-local IPv6 Address . . . . . : fe80::6486:c81a:3db5:a0ed%7  
IPv4 Address. . . . . : 10.10.[REDACTED]  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.10.[REDACTED]  
  
C:\Users\Administrator>
```

Each command will have a help manual to explain the expected syntax to execute the command properly, along with any additional parameters that can be added to the command to expand its execution.

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 /?

```
C:\Users\Administrator>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all | 
                /renew [adapter] | /release [adapter] | 
                /renew6 [adapter] | /release6 [adapter] | 
                /flushdns | /displaydns | /registerdns | 
                /showclassid adapter | 
                /setclassid adapter [classid] | 
                /showclassid6 adapter | 
                /setclassid6 adapter [classid] ]

where
    adapter           Connection name
                    (wildcard characters * and ? allowed, see examples)

    Options:
        /?             Display this help message
        /all           Display full configuration information.
```

Note: To clear the command prompt screen, the command is cls.

The next command is netstat. Per the help manual, this command will display protocol statistics and current TCP/IP network connections.

```
C:\Users\Administrator>netstat

Active Connections

  Proto  Local Address          Foreign Address          State
  TCP    10.10.■■■■■:3389    ip-10-13-■■■■■:38150  ESTABLISHED

C:\Users\Administrator>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]
```

In the above image, the line within the red box shows us an example syntax for the command.

The structure tells us the **netstat** command can be run alone or with parameters, such as -a, -b, -e, etc.

When any of the parameters are appended to the root command, **netstat** in this case, the output changes. Play with a few to see for yourself.

The net command is 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.

```
C:\Users\Administrator>net
The syntax of this command is:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

For the net command, to display the help manual /? will not work. In this case, you need to use different syntax, which is net help.

```
C:\Users\Administrator>net help
The syntax of this command is:

NET HELP
command
-or-
NET command /HELP

Commands available are:

NET ACCOUNTS          NET HELPMSG           NET STATISTICS
NET COMPUTER           NET LOCALGROUP        NET STOP
NET CONFIG             NET PAUSE             NET TIME
NET CONTINUE           NET SESSION           NET USE
NET FILE               NET SHARE             NET USER
NET GROUP              NET START             NET VIEW
NET HELP

NET HELP NAMES explains different types of names in NET HELP syntax lines.
NET HELP SERVICES lists some of the services you can start.
NET HELP SYNTAX explains how to read NET HELP syntax lines.
NET HELP command | MORE displays Help one screen at a time.
```

So, if you wish to see the help information for net user , the command is net help user.

```
C:\Users\Administrator>net help user
The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
    username {password | *} /ADD [options] [/DOMAIN]
    username [/DELETE] [/DOMAIN]
    username [/TIMES:{times | ALL}]
    username [/ACTIVE: {YES | NO}]

NET USER creates and modifies user accounts on computers. When used
without switches, it lists the user accounts for the computer. The
user account information is stored in the user accounts database.
```

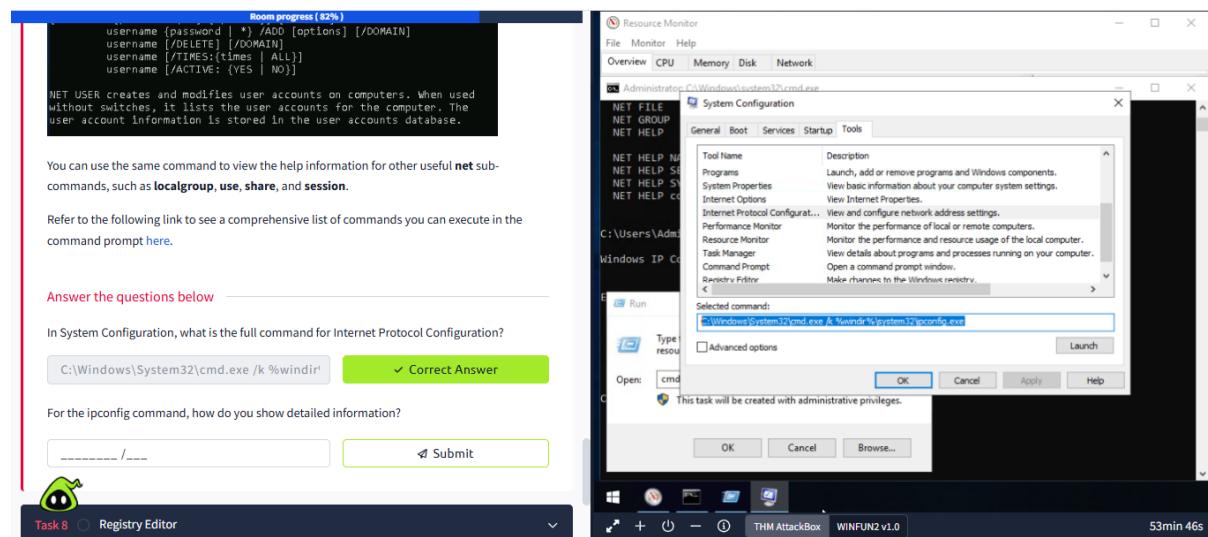
You can use the same command to view the help information for other useful **net** sub-commands, such as **localgroup**, **use**, **share**, and **session**.

Refer to the following link to see a comprehensive list of commands you can execute in the command prompt [here](#).

Answer the questions below

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

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



Great question Let's break this down carefully.

When you say **System Configuration**, you probably mean the tools you can open from **Run (Win + R)** or via msconfig to manage settings. The phrase *Internet Protocol Configuration* usually refers to the **ipconfig** command.

◆ Full command for Internet Protocol Configuration

The executable is:

ipconfig.exe

This shows your IP address, subnet mask, default gateway, and other network info.

◆ How to find it

1. Open **Command Prompt** (cmd.exe).
2. Type:
3. where ipconfig

Output will show the full path, e.g.:

C:\Windows\System32\ipconfig.exe

4. You can also verify in **System Configuration** → **Tools** tab:

- Scroll the list until you see **Internet Protocol Configuration**.
 - In the **Selected command** box at the bottom, you'll see the **full command** (C:\Windows\System32\ipconfig.exe).
-

 So the final answer:

C:\Windows\System32\ipconfig.exe

Do you want me to also give you the **other commands listed in System Configuration > Tools tab** (like Event Viewer, System Info, etc.)? That way you'll have the full set for exam prep.

Submit

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

ipconfig /all

Task 8- Registry Editor

We're continuing with Tools that are available through the **System Configuration** panel.

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.

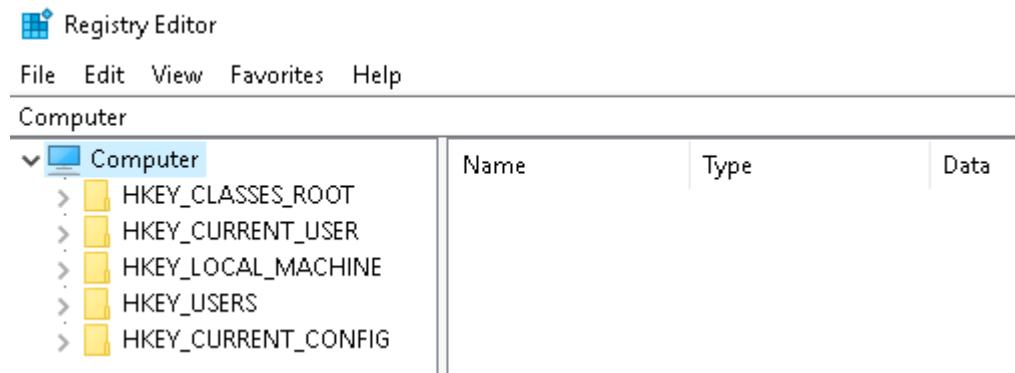
The registry contains information that Windows continually references during operation, such as:

- 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.

Warning: The registry is for advanced computer users. Making changes to the registry can affect normal computer operations.

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



Refer to the following Microsoft documentation [here](#) to learn more about the Windows Registry.

Answer the questions below

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

regedt32.exe

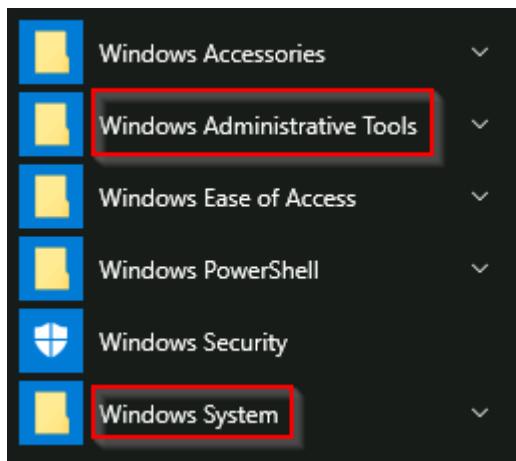
The screenshot shows a browser window with a question about opening the Registry Editor using the command "regedt32.exe". Below the question is a terminal window titled "C:\Users\Administrator>" showing the command "C:\Windows\System32\regedt32.exe" entered and ready to be run.

Task 9- Conclusion

Recall that the tasks covered in this room were some of the tools that can launch from MSConfig.

Throughout the room, commands and shortcuts were shared for the utilities. This means you don't have to launch **MSConfig** to run these utilities.

You can also run some of these utilities directly from the Start Menu. See below where some of these utilities can be found.



Some of the tools listed in **MSConfig** that weren't mentioned in this room were either covered in Windows Fundamentals 1 or were left for you to explore on your own.

References:

Tryhackme Labs