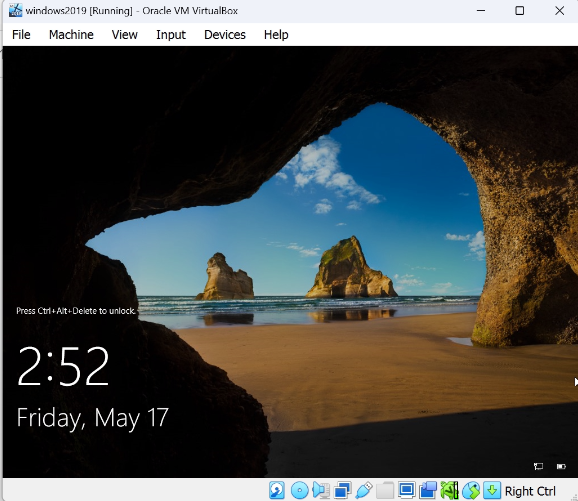
# Workshop 1 -- CSY2085 – Server Administration and Security

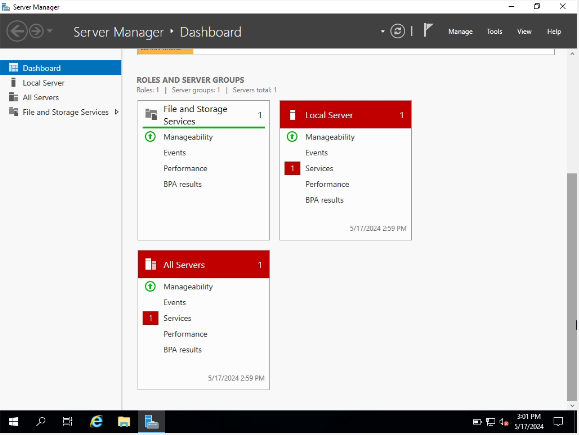
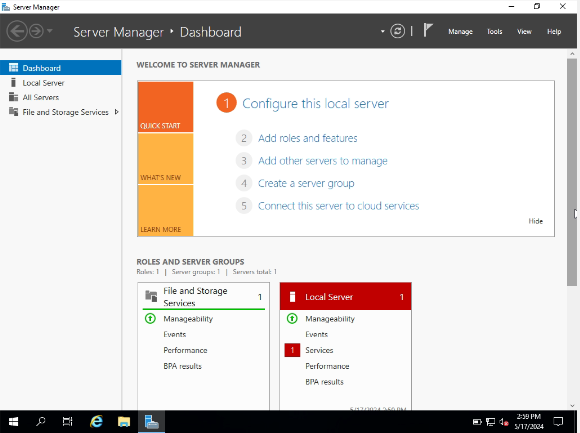
STUDENT NAME: Muhammad Raza

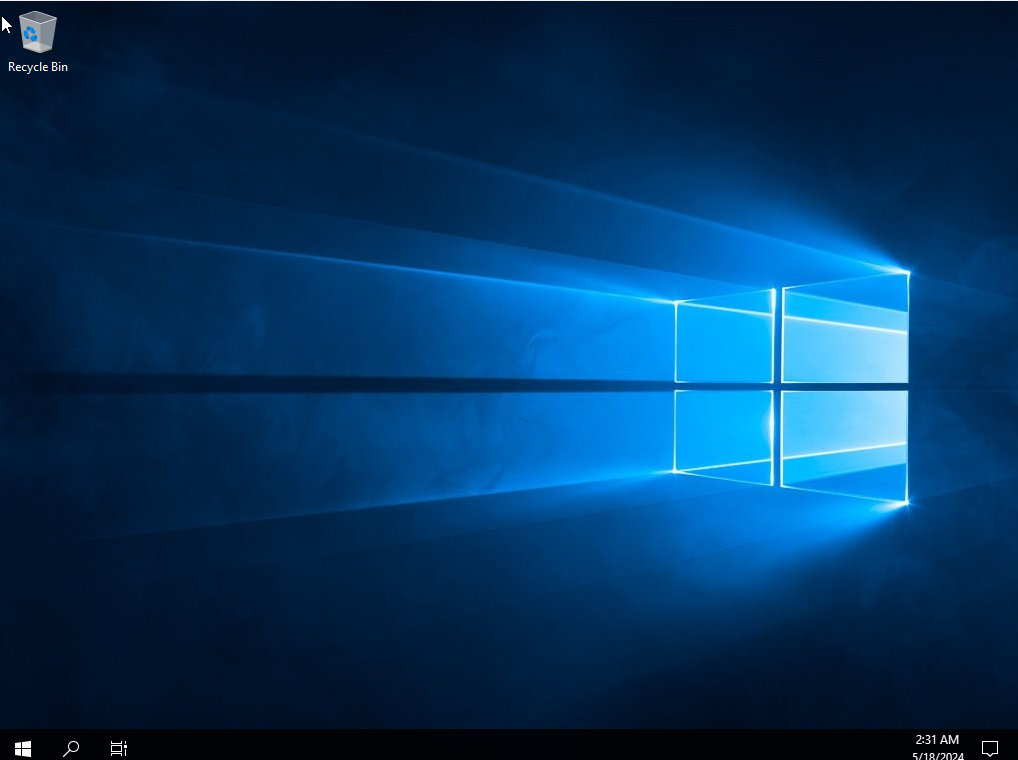
STUDENT NUMBER: 21426838

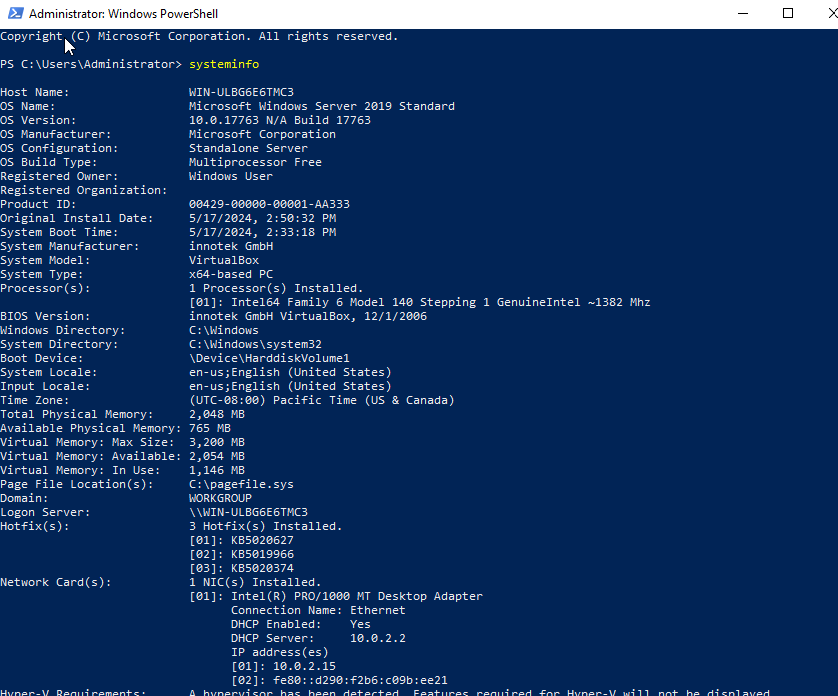
1. Task 1 - Installing and Windows Server 2019 using VMware Player



## Task 2 – Verifying the Installation



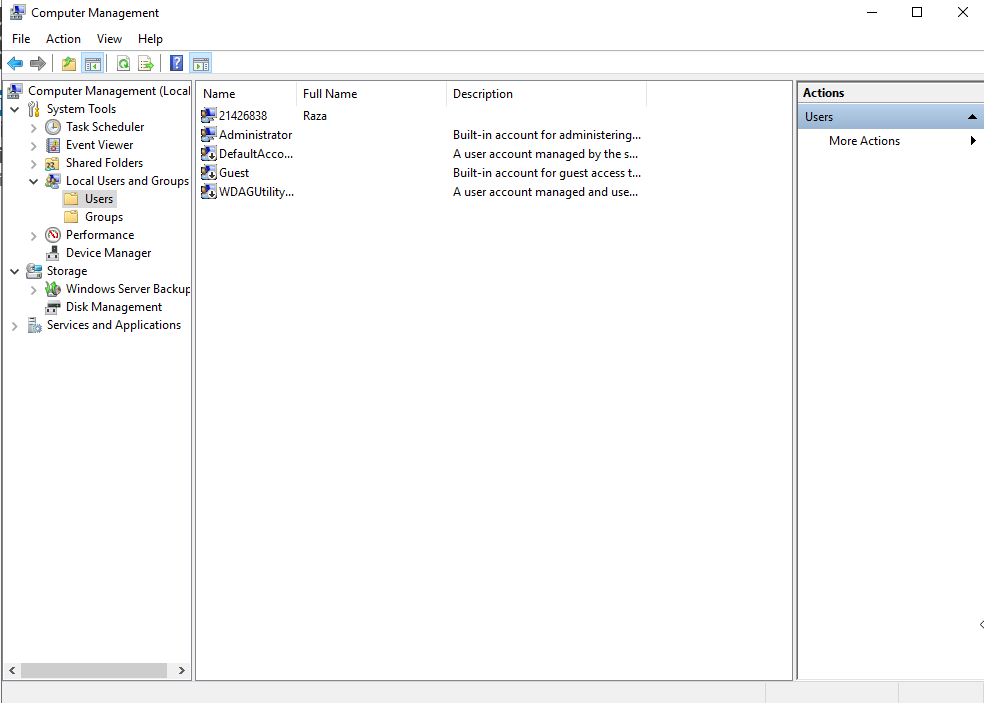
1. Now capture your full screen Windows Server desktop and paste the screenshot into the space below:  
     
   ****
2. Maximize this PowerShell window so that it is as large as it can be. Click within this window window and type the command "**systeminfo**" and press the Return or Enter key.

****

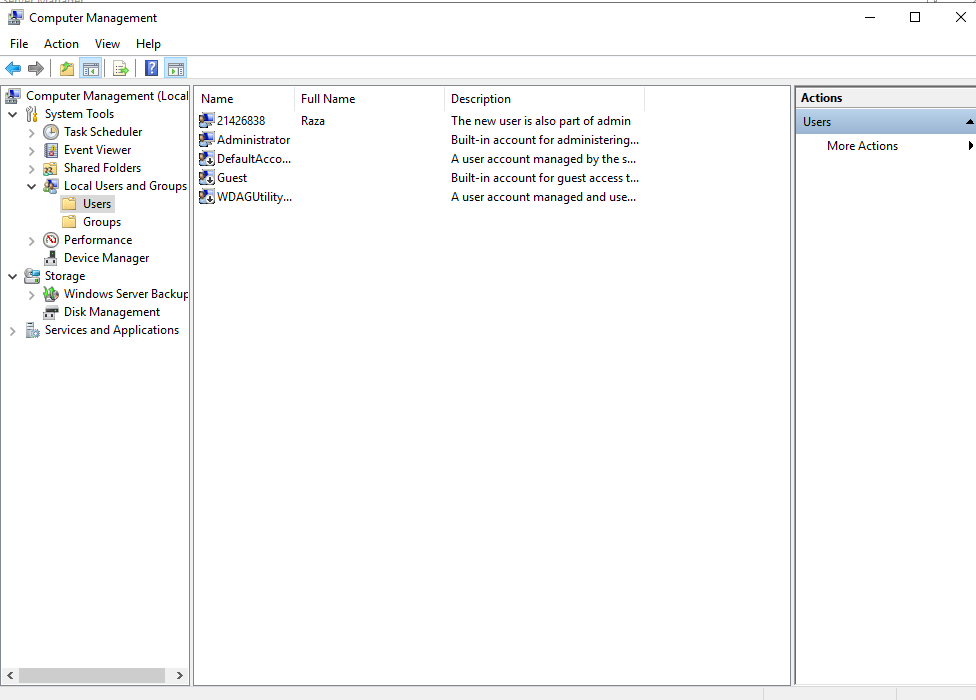
**What useful information can you deduct from the output of this command?**

1. **Operating System Details:** You can see the version of Windows installed, including the edition (like Home, Professional, Enterprise) and the build number.
2. **System Manufacturer and Model:** This tells you who manufactured the computer and what model it is.
3. **BIOS Version and Date:** Knowing the BIOS version can be useful for troubleshooting or determining if a system update is available.
4. **Processor(s) Information:** It provides details about the CPU(s) installed, such as the manufacturer, model, and clock speed.
5. **Installed Physical Memory (RAM):** This tells you how much RAM is installed on the system.
6. **Network Adapter(s):** It lists information about all network adapters present in the system, including their MAC addresses and IP configurations.
7. **System Up Time:** It shows how long the system has been running since the last reboot, which can be useful for diagnosing uptime-related issues.
8. **System Locale, Time Zone, and Language:** These settings can be important for troubleshooting certain types of issues or for ensuring that the system is configured correctly.
9. **Hotfixes and Patches:** It lists all installed updates, patches, and hotfixes, which can be crucial for ensuring system security and stability.
10. **System Boot Time:** It indicates when the system was last booted, which can be helpful for troubleshooting startup-related issues or determining system availability.

## Task 3 – Creating User Accounts

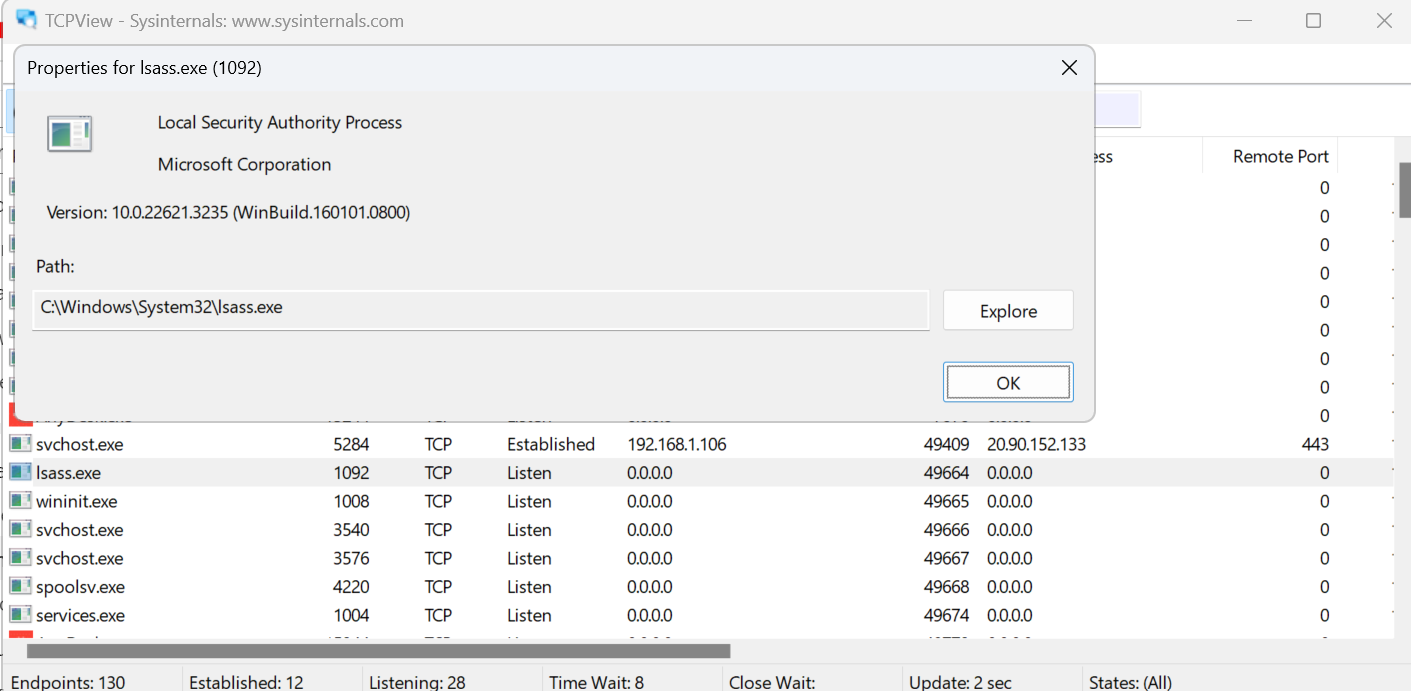


1. Do a bit of research of how to do this and paste a screenshot of your result below (the screenshot should show that the new user is now also a member of "Administrators". Capture the screen showing this information and paste it below:

****

## Task 4 – Identify Running Processes

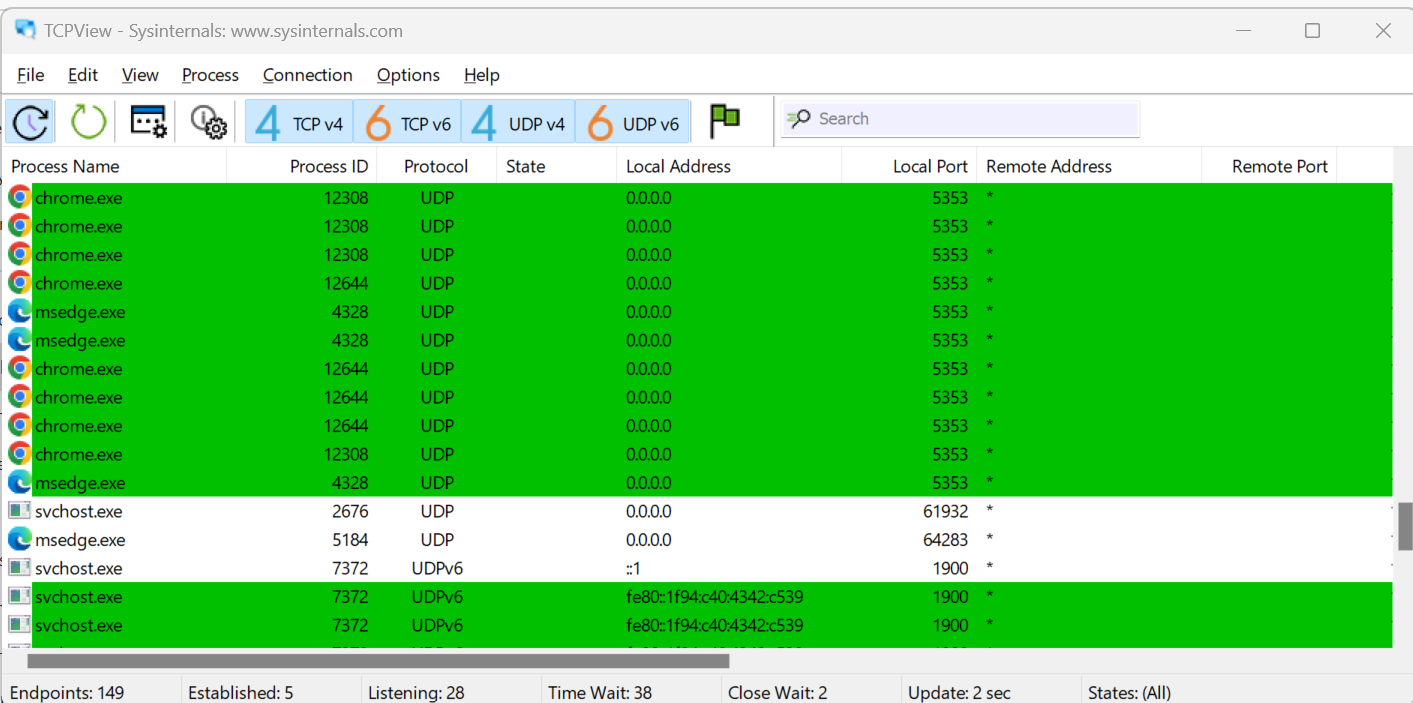
1. Double-click **lsass.exe**. What is lsass.exe? In what folder is it located?

****

**The folder is located in Windows\System32 folder.**

1. Explore a user-started process. Open a web browser, such as Microsoft Edge. What did you observe in the TCPView window?

**In TCPView, I observed a new entry corresponding to the web browser process (e.g., Microsoft Edge). The entry displayed the local address and port through which the browser is communicating, along with any remote addresses it's connected to. Additionally, it showed the state of the connection, such as established or listening.**



1. Close the web browser. What did you observe in the TCPView window?

Upon closing the web browser, the corresponding entry in TCPView disappeared from the list of active connections. The local address and port associated with the browser process were no longer visible, indicating the termination of communication. Additionally, any remote addresses connected to the browser were also removed from the display.

1. Reopen the web browser. **Research 3 of the processes listed in TCPView**. Record your findings.

**Researching the processes listed in TCPView, I found:**

**1. MicrosoftEdge.exe:** This process is the main executable for the Microsoft Edge web browser, responsible for rendering web pages and managing browser functionality.

**2. svchost.exe:** This is a generic host process name for services that run from dynamic-link libraries (DLLs). It hosts services related to Windows components and often manages network-related tasks**.**

**3. dllhost.exe:** This process hosts DLL-based COM objects. It's commonly used by various system components and applications to execute tasks in a separate process, enhancing stability and security.