Introduction to Windows and CMD

Cybersecurity

Windows Administration and Hardening Day 1

Class Objectives

By the end of today's class, you will be able to:

Leverage the Windows command prompt to execute various sysadmin responsibilities.

Use `wmic`, Task Manager, and `services.msc` to manage applications and services.

Create, manage, and view user information using command-line tool, `net`.

Manage password policies using `gpedit`.

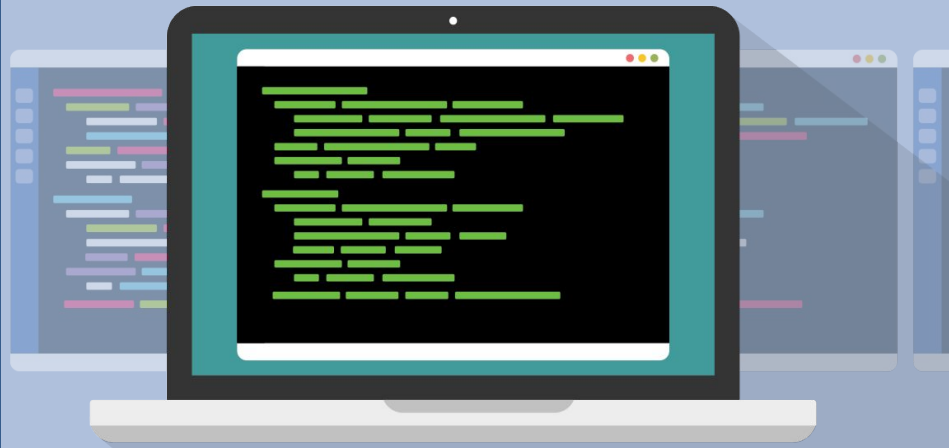
Schedule tasks using Task Scheduler.

Welcome to Windows

While many IT professionals prefer Mac OS and Linux, Windows is still the leader for desktop operating systems.

The ubiquity of Windows machines makes them the most common target for today's attackers.

Malware can specifically target vulnerabilities in unpatched and unsecure Windows machines and servers.



Windows in a Professional Context

Windows knowledge is essential for the following roles, among many others:

SOC Analyst	System Administrator	Penetration Testing	Endpoint Forensics
The SOC Analyst must monitor and detect suspicious activity on Windows machines.	The large majority of system administrators work with one or many Microsoft products and services: Windows PCs, Windows Servers, Office 365, and Exchange, etc.	Due to Windows wide usage in businesses, penetration testers must exploit Windows and Microsoft-related platforms.	Being the most commonly supported endpoint device for businesses, forensics investigators must understand how Windows works.

Windows System Administrator

Today's will cover common system administration tasks utilizing command line and GUI tools to troubleshoot a problematic Windows PC

01 Audit processes with Task Manager

02 Use the command line to gather info and create files.

03 Enforce password policies.

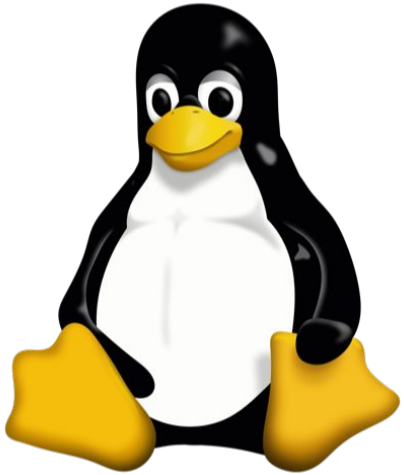
04 Manage users.

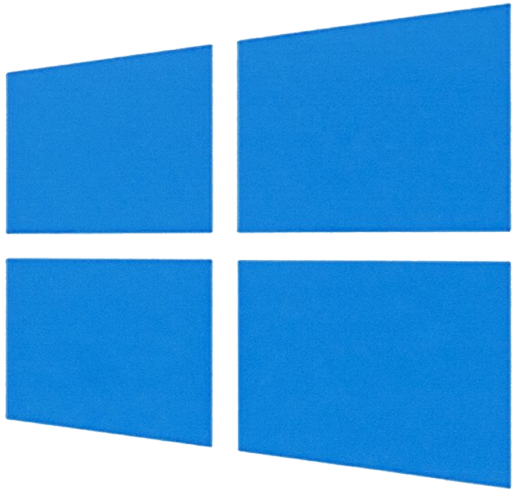
05 Automate tasks.

Learning Windows

Today, we'll learn the "Windows" way of performing basic sysadmin tasks.

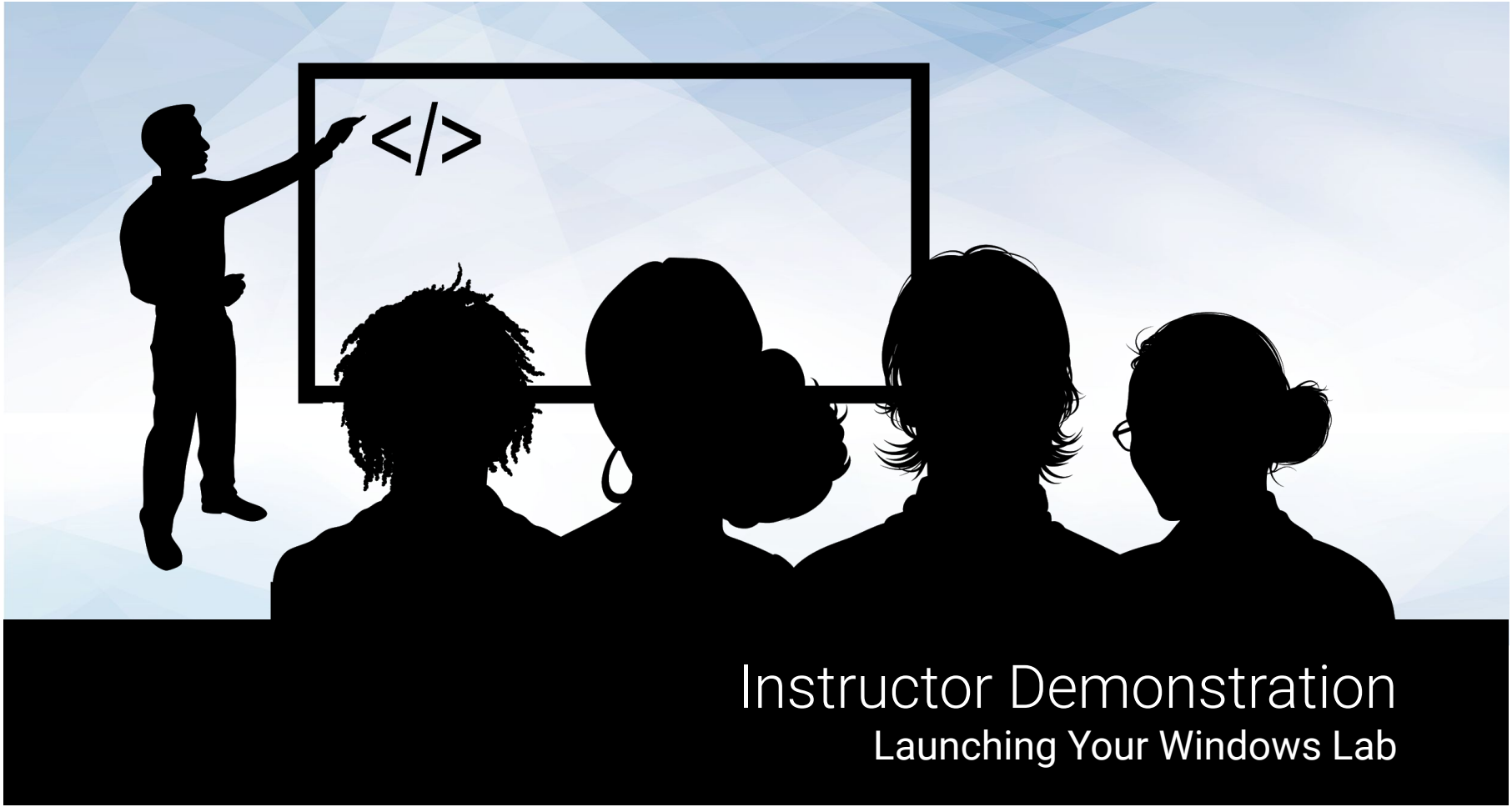
- We've already learned how to complete many of these tasks on Linux.
- While we may be moving at a quicker pace today, the topics covered will emphasize the syntax and OS differences of completing Windows tasks, since the general concepts of these tasks will remain relatively similar to Linux.





Launching Your Windows Lab

Before we get started, we need to set up our Azure Lab environment.



Instructor Demonstration

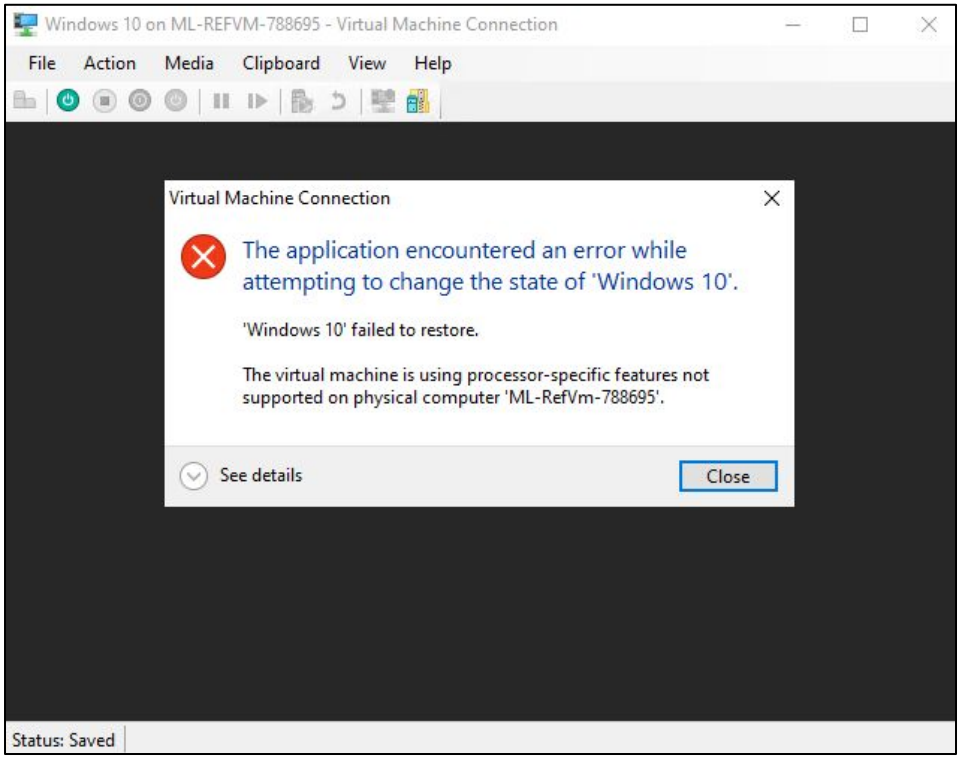
Launching Your Windows Lab

Important Note Regarding HyperV Machines

If your Hyper V machine has been sitting idle, it may go into a hibernation known as “Saved State.” This can also occur at the end of a session, so **please make sure you shut down the VMs in your lab environment at the end of class**.

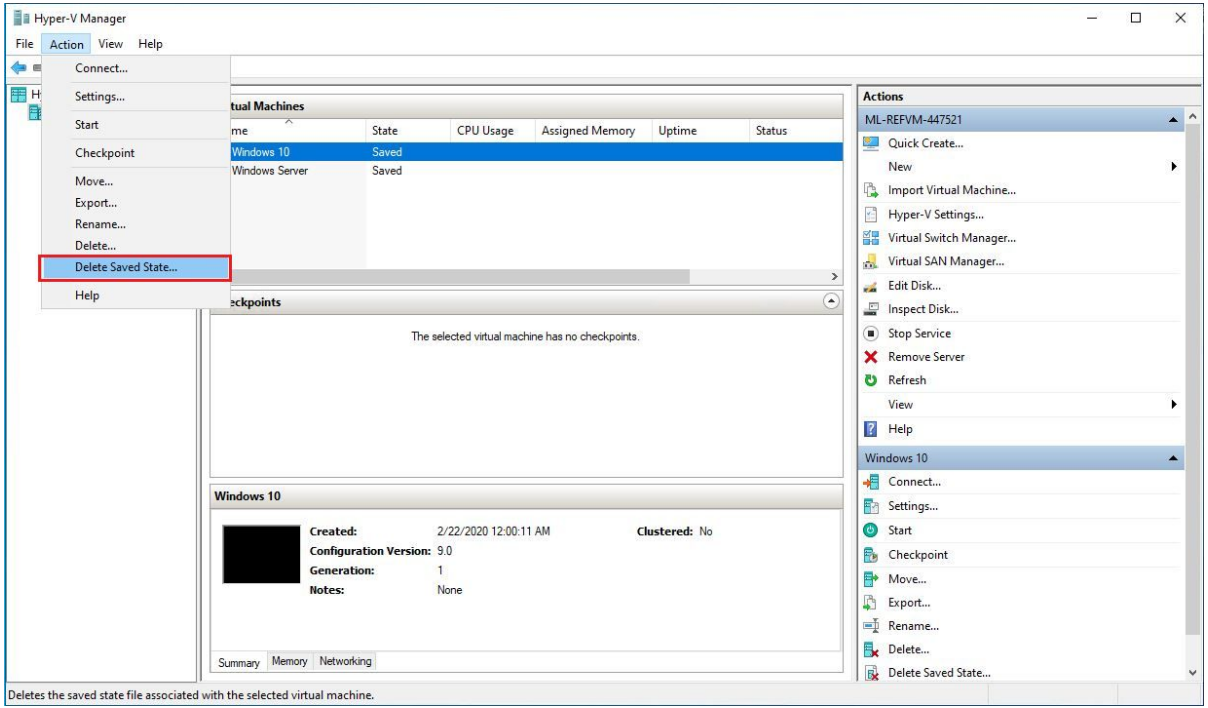
- If a machine enters a saved state during class, you may see the following error: `The application encountered an error while attempting to change the state of the 'VM-Name'.`
- If you encounter this error, the VM may not startup until you delete the saved state. Turning the VMs and the host machine off when not in-use will avoid this troubleshooting overhead.
- To delete the saved state, using the HyperV manager, go to the **Action** dropdown menu and choose “**Delete Saved State...**”

Troubleshooting HyperV Machines



If you see this error window, you will need to **delete the saved state**.

Troubleshooting HyperV Machines



To delete the saved state, using the HyperV manager, go to the Action dropdown and choose **Delete Saved State.**

Important: DO NOT click on the “Delete” option.

Introduction to Task Manager

Did you notice the excessive amount of processes that started up when you logged into the Windows 10 VM?

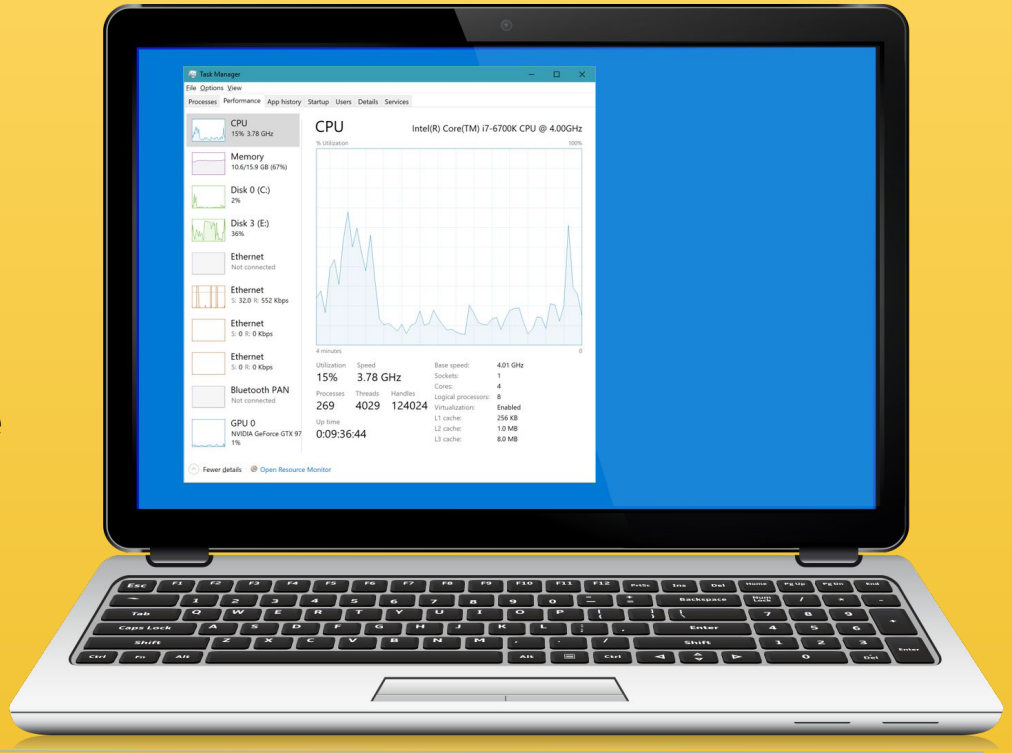
This is what an unmanaged Windows workstation may end up looking like if it’s not maintained by an organization’s system administrator.

Task Manager

Task Manager is one of the most important Windows tools for troubleshooting resource usage.

- **We'll audit and manage tasks and processes to identify errant or malicious actions taking place without users' or administrators' knowledge.**

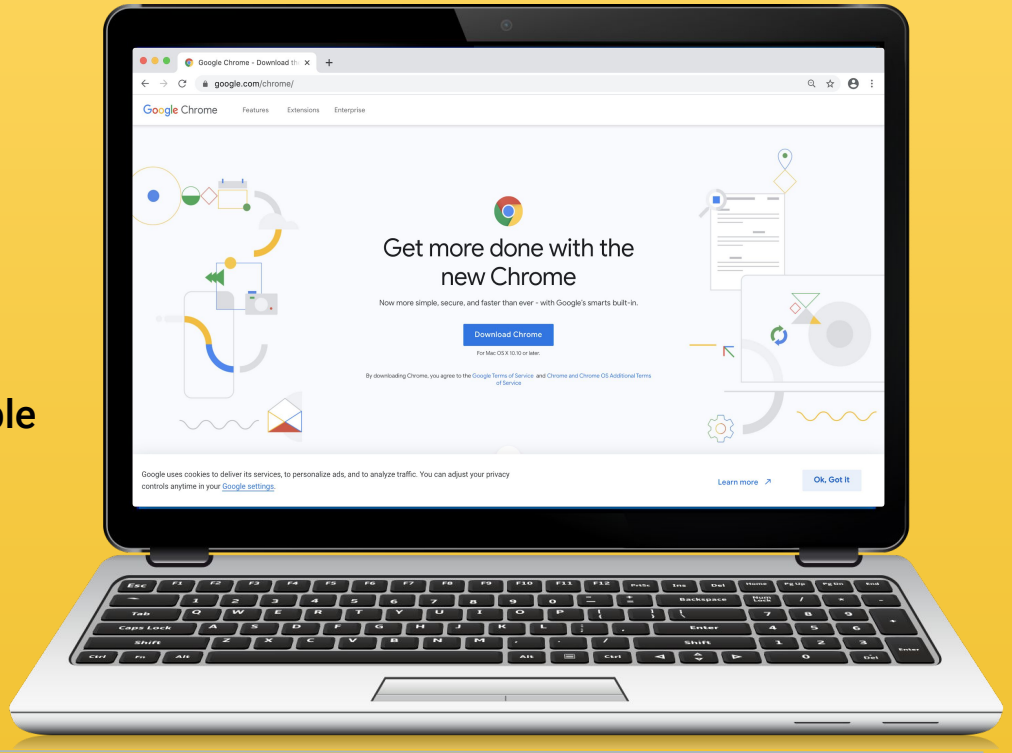
- Processes in Windows are much like the processes and PIDs that the you encountered in the Linux units.



Task Manager

Some programs, when not in use but left running, take up excessive resources or even allow for unwanted remote connections. Some examples are:

- **Google Chrome, which is well-known for its high memory usage.**
- **Teamviewer, the remote desktop application, has had critical issues that left systems extremely vulnerable AND accessible from public connections.**

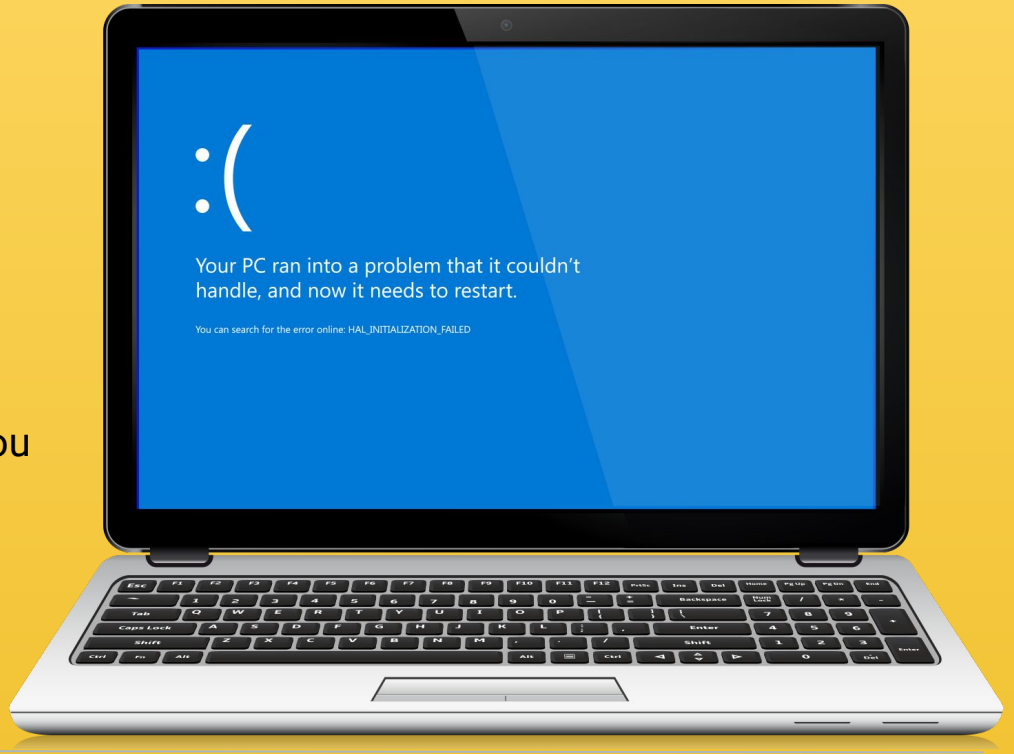


Task Manager

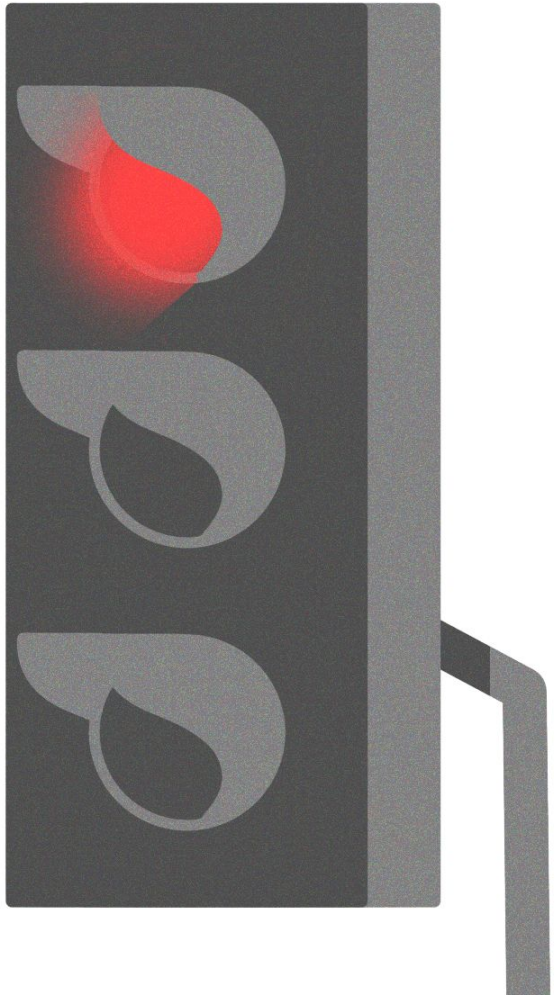
Task Manager is one of the most important Windows tools for troubleshooting resource usage.

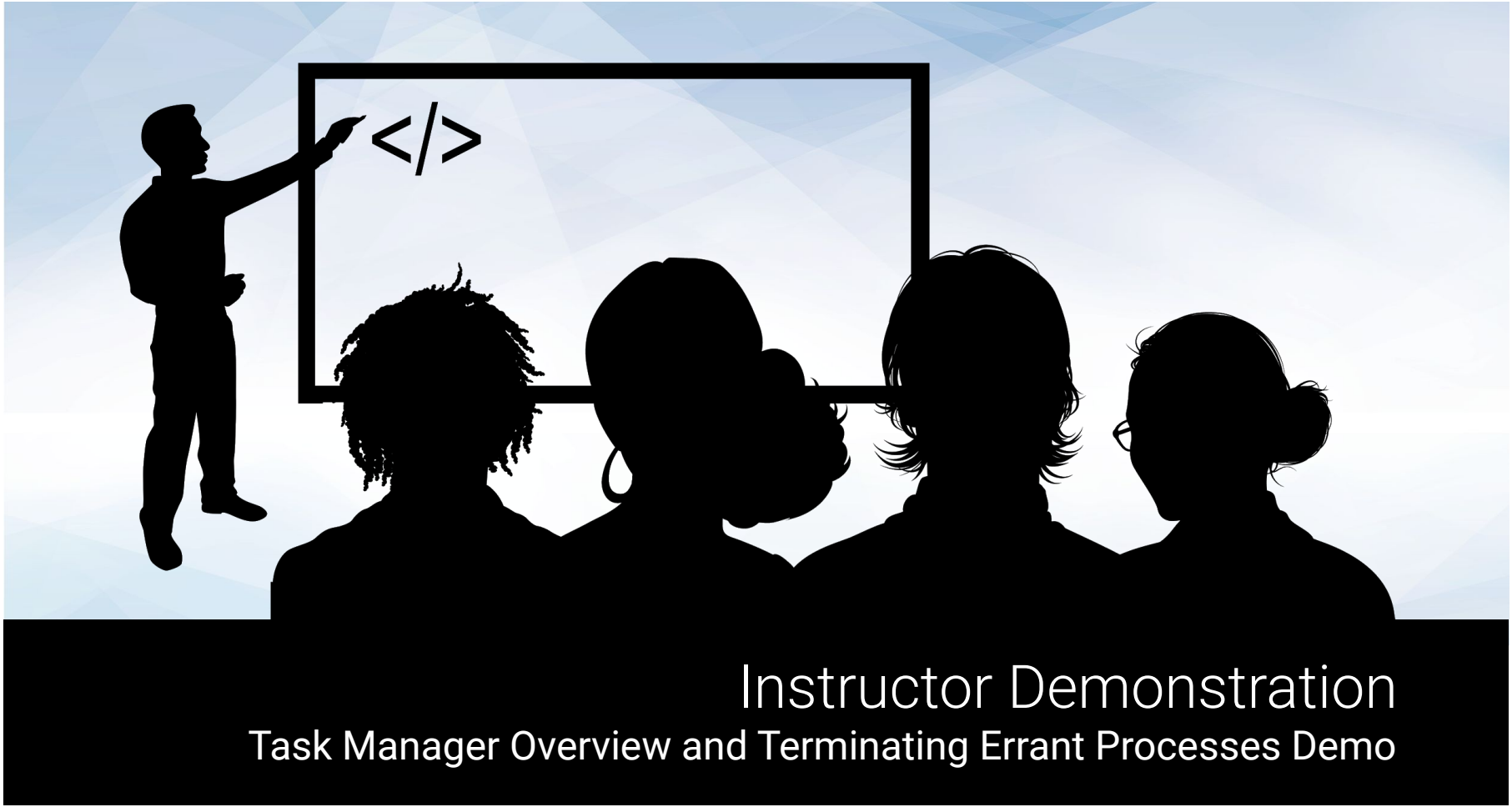
- **Some processes can even cause memory leaks that can result in system instability and abrupt system crashes.**

- When a Windows system crashes, you are often stuck with what what is known as the **blue screen of death**.



Let’s open up Task Manager, check out the processes, and end an errant process.





Instructor Demonstration

Task Manager Overview and Terminating Errant Processes Demo

Disabling Startup Applications (Task Manager)

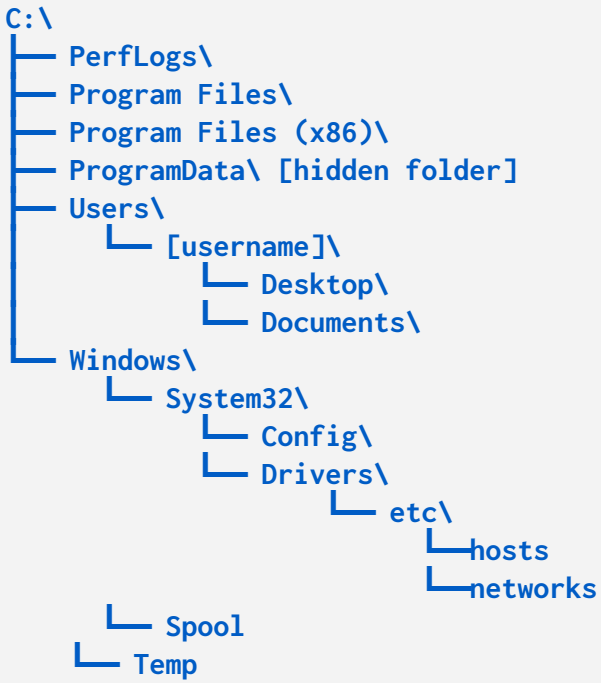
Managing startup applications is important for system and security administration:

- Startup applications can slow boot time due to their execution priority.
- These applications may use excessive resources while in the background, causing random system slowdowns.
- Applications might use the network in the background. They might, for example, initiate their own automatic updates, hogging network bandwidth.
- Startup applications may require special permissions to function. These can pose security risks if, for example, they are compromised through malware.

Introduction to Command Prompt, CMD

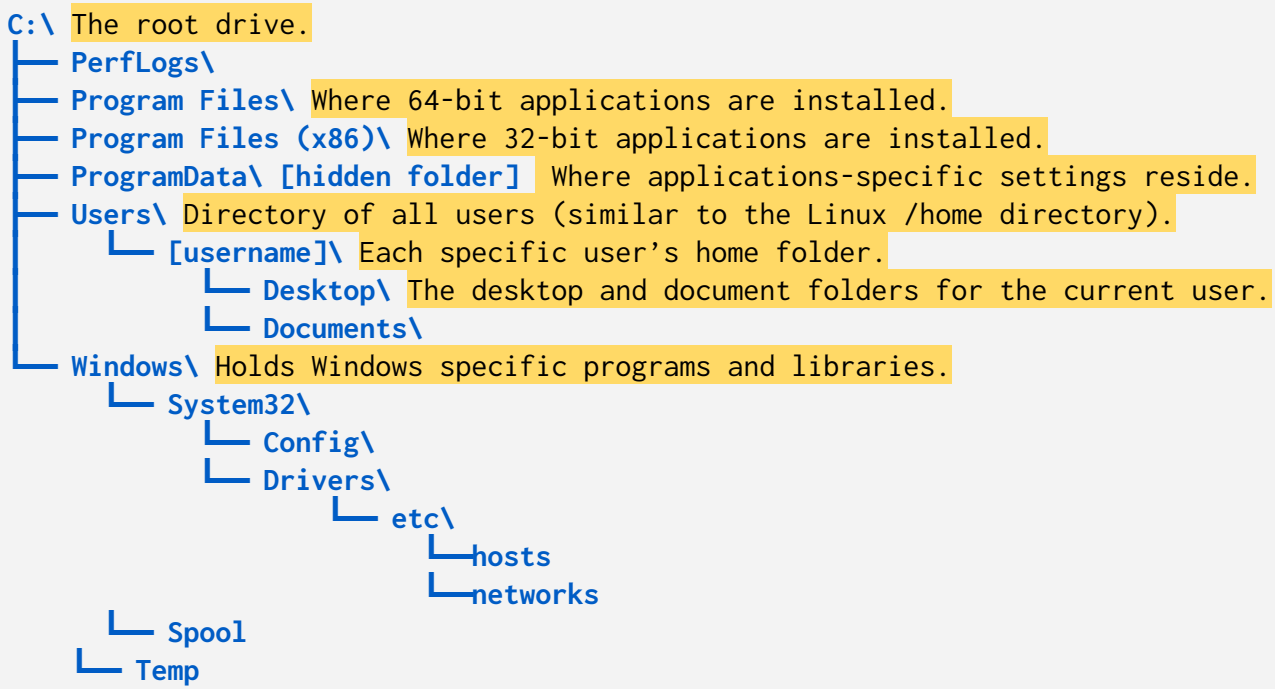
Windows Directory and File Structure

The default Windows directory structure:



Windows Directory and File Structure

The default Windows directory structure:



Remember environment variables from the bash programming unit?

In Windows, they work the same way—preset by the system and usable in the command line and scripts.

Common ENV Variables

Environment variables (envvars) are special values that contain information about the system, such as the user's home directory or the system's program files directory.

Environment Variables	Default Value
%CD%	Current directory
%DATE%	Current date
%OS%	Windows
%ProgramFiles%	C:\Program Files
%ProgramFiles(x86)%	C:\Program Files (x86)
%TIME%	Current time
%USERPROFILE%	C:\Users{username}
%SYSTEMDRIVE%	C:\
%SYSTEMROOT%	C:\Windows

Envvars can be used for the following:

- Shortening long directory paths.
- Grabbing the current time.
- Finding the location of your system files.

Common ENV Variables

Linux variables are designated with a **$**, while Windows ENV variables are enclosed with **%** signs.

Environment Variables	Default Value
%CD%	Current directory
%DATE%	Current date
%OS%	Windows
%ProgramFiles%	C:\Program Files
%ProgramFiles(x86)%	C:\Program Files (x86)
%TIME%	Current time
%USERPROFILE%	C:\Users{username}
%SYSTEMDRIVE%	C:\
%SYSTEMROOT%	C:\Windows

For example, to navigate to the 64-bit Program Files folder, we run:

- **cd %ProgramFiles%**

We can combine ENV variables with regular directory names:

- **cd %USERPROFILE%\Desktop**

This would send us to the desktop of the current user.

Common ENV Variables

We can combine environment variables with regular directory names:

Environment Variables	Default Value
%CD%	Current directory
%DATE%	Current date
%OS%	Windows
%ProgramFiles%	C:\Program Files
%ProgramFiles(x86)%	C:\Program Files (x86)
%TIME%	Current time
%USERPROFILE%	C:\Users{username}
%SYSTEMDRIVE%	C:\
%SYSTEMROOT%	C:\Windows

```
cd %USERPROFILE%\Desktop
```

- USERPROFILE% is a variable assigned to the value of the current user's home directory. In this case, C:\Users\sysadmin.
- This is the same as $HOME in Linux.

Command Prompt (CMD)

Windows command prompt CMD, or cmd.exe, is the command line interface for Windows, comparable to a Unix shell, such as bash for Linux.

CMD Command	Action	Linux Counterpart
`cd or chdir`	Change directory	`cd`
`dir`	List contents of directory	`ls`
`md or mkdir`	Create directory	
`copy`	Copy file	`cp`
`move`	Move (cut and paste) files	`mv`
`del or erase`	Delete files and directories	
`rd or rmdir`	Remove a directory if empty	
`find`	Search a file for specified string	
`exit`	Closes `CMD`	
`type`	Show contents of specified file	`cat`

Command Prompt (CMD)

Windows command prompt CMD, or cmd.exe, is the command line interface for Windows, comparable to a Unix shell, such as bash for Linux.

Note

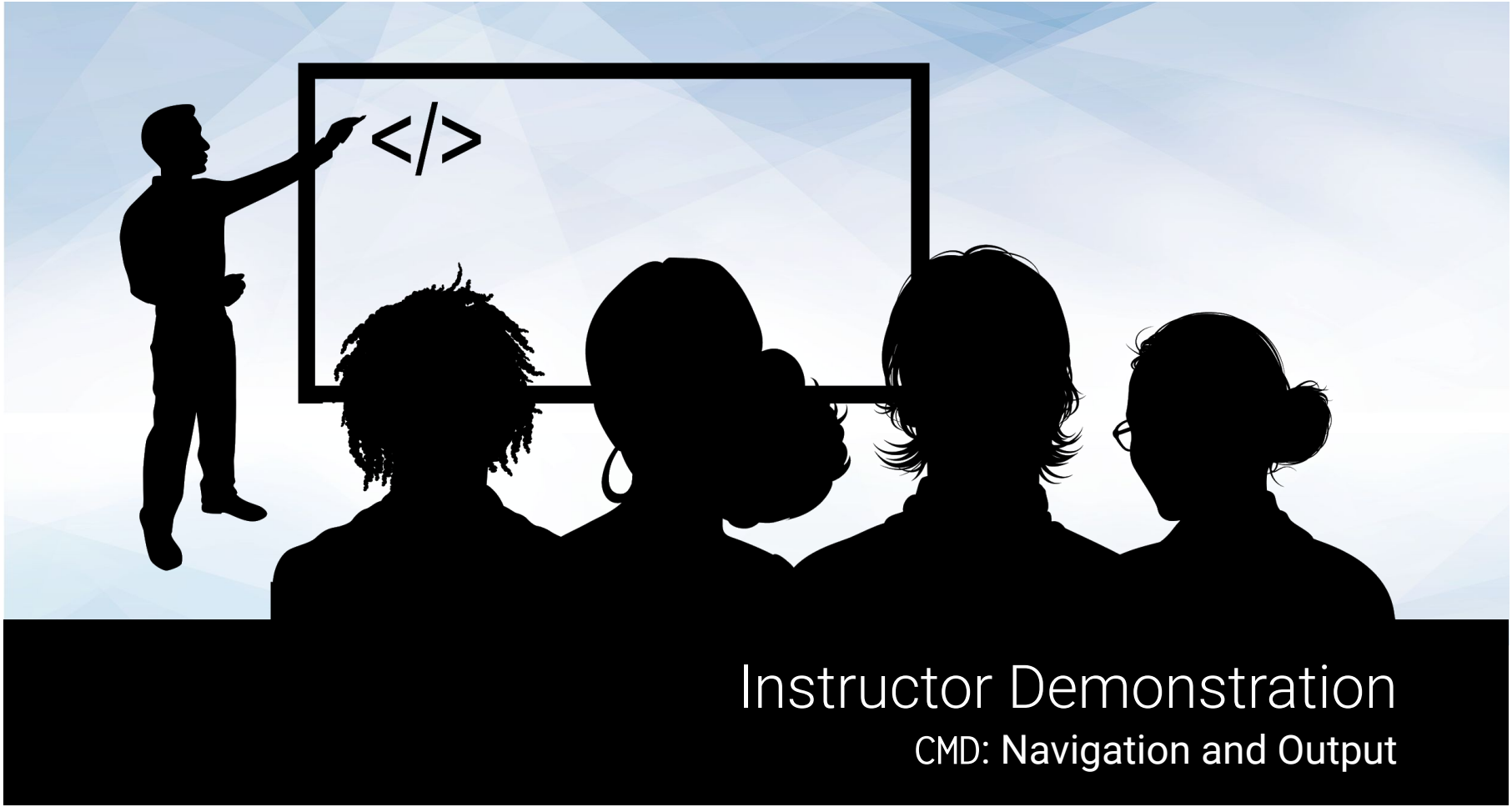
Command prompts are not case sensitive with files and directories. I.e.,

`cd "Program files"` is the same as `cd "PROGRAM FILES"`

Use quotes around the name of a file or directory that contains spaces.

CMD Command	Action	Linux Counterpart
`cd or chdir`	Change directory	`cd`
`dir`	List contents of directory	`ls`
`md or mkdir`	Create directory	
`copy`	Copy file	`cp`
`move`	Move (cut and paste) files	`mv`
`del or erase`	Delete files and directories	
`rd or rmdir`	Remove a directory if empty	
`find`	Search a file for specified string	
`exit`	Closes `CMD`	
`type`	Show contents of specified file	`cat`

In the next walkthrough, we will create and manage files within Windows **CMD**.



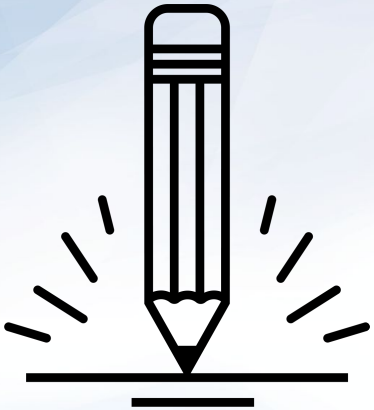
Instructor Demonstration

CMD: Navigation and Output

Today's Activity Scenario

You will be playing the role of a junior Windows system administrator for the data analytics company Good Corp Inc. We'll be using the Windows CMD to output various details of a Windows workstation into a report file.

- A senior software developer who recently left the company left behind a Windows workstation that was never centrally managed by IT.
- Your CIO has requested that you do the following on the Windows workstation:
  - Use Task Manager to clean up running and startup processes.
  - Use cmd to create a simple text file in the %USERPROFILE%\Desktop directory called report.txt to begin appending Windows system information to.



Activity: Task Manager and CMD

In this activity, you will use CMD and Task Manager to complete to

Please use the Windows 10 Hyper-V VM.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Activity Review: Task Manager and CMD

This activity covered Windows sysadmin duties such as auditing tasks and using basic commands like **`echo`** and **`type`**. You had to:

01 Launch Task Manager.

02 Sort processes and end processes with high CPU utilization.

03 Navigate to the desktop using environment variables.

04 Create a reports folder.

05 Append terminal output that use **`echo`** and **`env`** variables into a **`reports.txt`** file.

Windows Management Instrumentation Command (`wmic`)

wmic

Windows Management Instrumentation Command (`wmic`) is a tool used to query system information and diagnostics, such as OS and hard disk info.

Sysadmins can also use `wmic` to launch, terminate, install, and uninstall processes.

`wmic` Structure and Conventions

`wmic [global switches] [alias] [verbs] [properties]`

`[global switches]` are global commands called on by `wmic`.

- For example: **`wmic /APPEND:report.txt os get caption`** will append the Windows build number to **`report.txt`** file. This will add the output content to the file and not overwrite the file.

`wmic` Structure and Conventions

```
wmic [global switches] [alias] [verbs] [properties]
```

`[alias]` is the Windows component that `wmic` queries. Common aliases include:

- **`os`** (*operating system*): Contains properties specific to the operating system, such as the Windows edition name and build number.
- **`Logicaldisk`**: Contains properties specific to the disk drives, such as drive name, filesystem, free space, size, and volume serial number.

`wmic` Structure and Conventions

`wmic [global switches] [alias] [verbs] [properties]`

`[verbs]` are actions we want to complete with the `wmic` command.

- For example, if we are using **`wmic os`** to find operating system information, we can then use the **`get`** verb, followed by the various **`[properties]`** we want to find.

`wmic` Structure and Conventions

```
wmic [global switches] [alias] [verbs] [properties]
```

Common `[properties]` to retrieve using `get`:

- **`get caption`**: Returns a one-line description of the given alias.
- **`get /value`**: Gets *all* of the properties and values of an alias and lists each on separate line.

Applying `wmic`

Let’s walk through a few examples:

```
wmic os get /value
```

```
wmic os get caption, buildnumber
```

```
wmic /APPEND:report.txt os get caption
```

```
wmic logicaldisk get caption, filesystem, freespace, size, volumeserialnumber
```

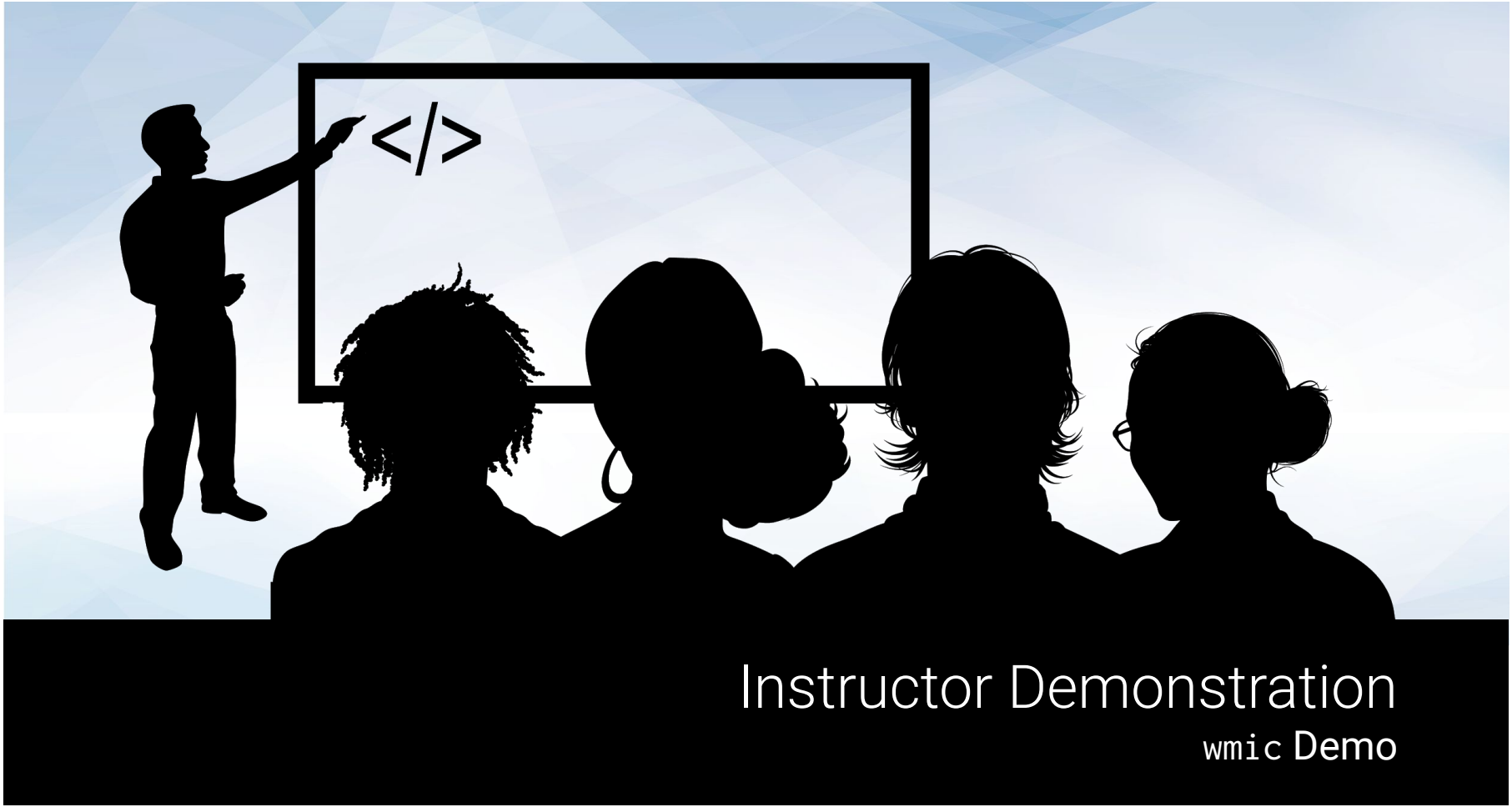
```
wmic /APPEND:report.txt logicaldisk get caption, filesystem, freespace
```

`wmic` Demo

In the next demo, we will move through different programs, understand their importance in a sysadmin context, and get and append them to our report.

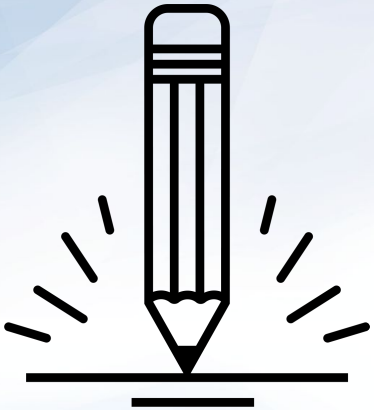
We'll retrieve the following properties from the startup alias:

- **Name/Caption** : the name of each startup application.
- **Command**: the execution path of this startup process.
- **User**: the user that the startup application runs as on boot.



Instructor Demonstration

`wmic` Demo



Activity: Creating a Report with `wmic` Output

In this activity, you will continue baselining the Windows system using `wmic` queries.

Please use the Windows 10 Hyper-V VM.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

Activity Review: Creating a Report with `wmic` Output

Completing this activity required the following steps:

01 Use the **`wmic [alias] get /value`** call to see all available alias options.

02 Test various alias options.

03 Examine the reports contents with type **`report.txt`**.

04 Find SID, and important directories and files.

05 Retrieve user logon information.

06 Retrieve Windows update information and startup application list.

07 Enumerate a list of startup services.

Activity Review: Creating a Report with wmic Output

We encountered the following aliases in this exercise:

- The **`useraccount`** alias retrieves information about user accounts.
- The **`netlogin`** alias retrieves user logon metrics.
- The **`qfe`** alias retrieves information about Windows updates installed on the system.
- The **`startup`** alias retrieves information about startup applications on the system.
- The **`where`** clause narrows down results to match a specified property.

Countdown timer

15:00

(with alarm)

Users and Password Policies

Next, we'll use the command-line tool **`net`** to manage user accounts, groups, and password policies.

Using `net`

We'll be using the following **`net`** utilities:

- **`net user`** for adding, removing and managing users.
- **`net localgroup`** for adding, removing, and managing local groups.
- **`net accounts`** for viewing password and logon requirements for users to enforce password security policies.

Using `net`

`net` lets us set the following password policies:

Time before a password expires.

Minimum number of characters required for password.

Minimum number of days before a password can be changed.

Number of times a password must be unique before it can be reused again.

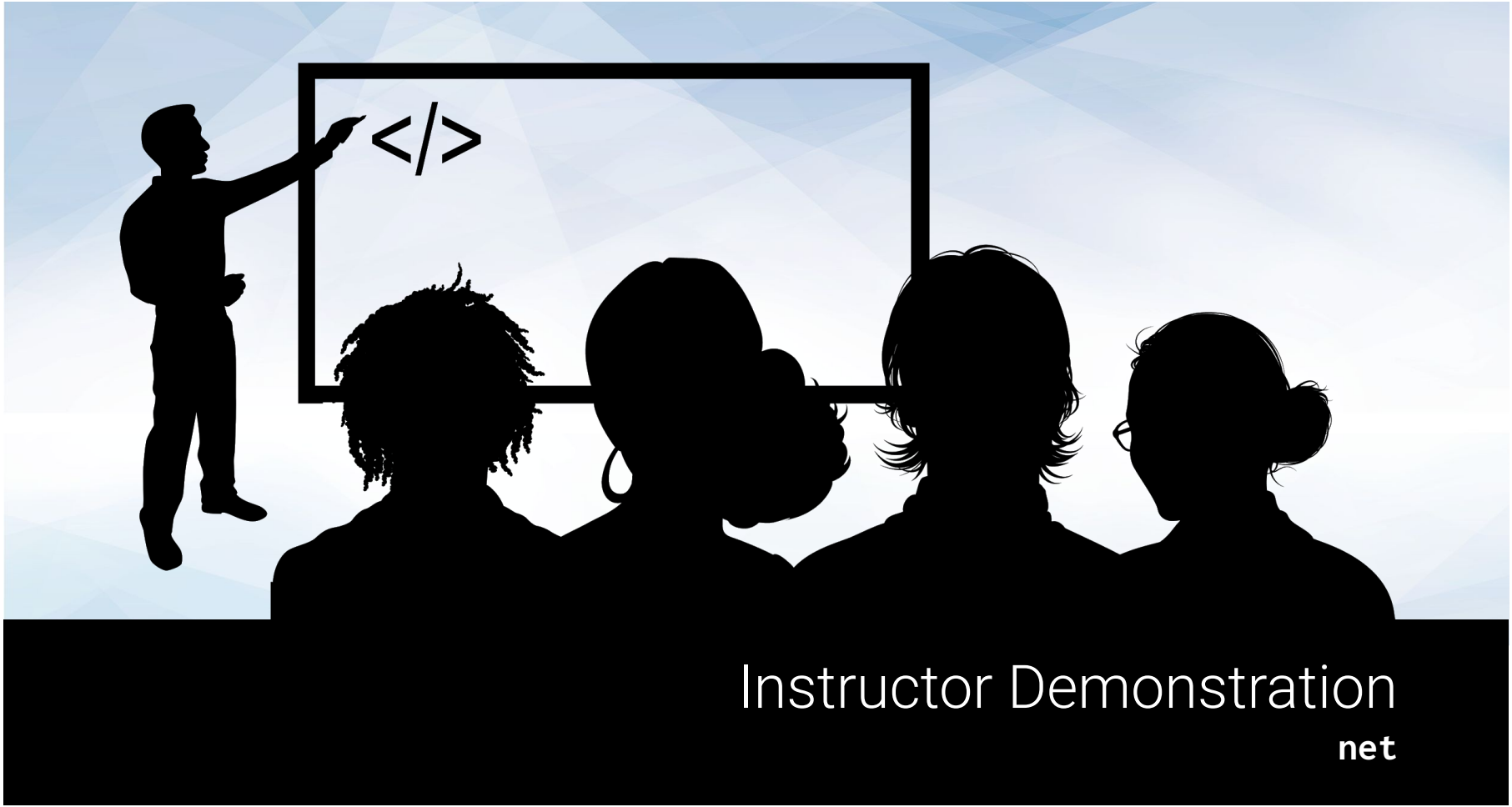
- E.g., if using the PW **`apples2apples`**, you'll have to change it to two new passwords before you can use **`apples2apples`** again.

`net` Demo Scenario

Your CIO is curious about the groups and password policies on the Windows workstation. We need to retrieve more information from this workstation using the `net` command-line utility.

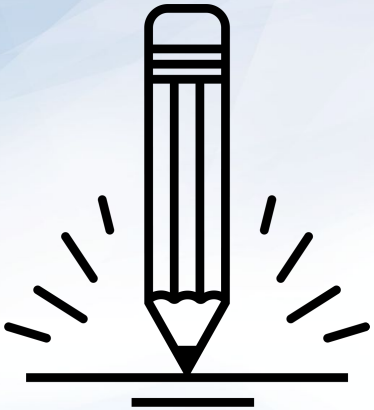
We'll use the **`net`** tool to do the following:

- Enumerate users to see net output.
- Enumerate sysadmin's groups and password policies.
- Enumerate local groups with net localgroup.
- Enumerate the Windows workstation's current password policies with net accounts.



Instructor Demonstration

net



Activity: Users, Groups and Password Policies

In this activity, you will use the **`net`** utility to retrieve more information about the Windows workstation.

Please use the Windows 10 Hyper-V VM.

Suggested Time:
10 Minutes

Activity Review: Users, Groups, and Password Policies

Completing this activity required completing the following steps:

01 Enumerate users with **`net`**.

02 Enumerate **`sysadmin`**'s groups and password policies

03 Enumerate local groups with **`net localgroup`**.

04 Enumerate current password policies with **`net accounts`**.

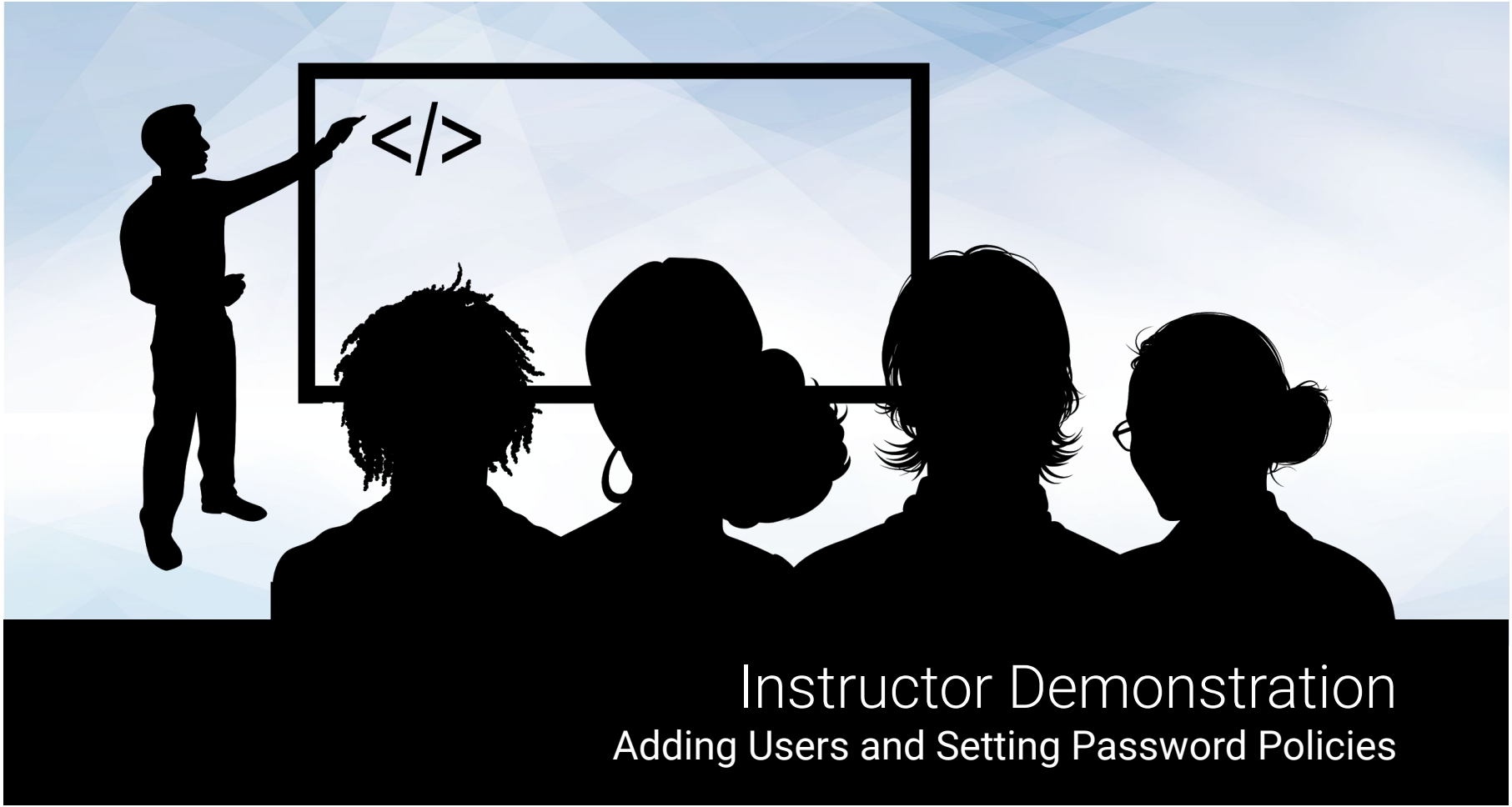
Creating Users and Setting Password Policy

Password Policies

We've discussed the importance of password policies in earlier Linux units. Now we'll establish password policies for new users in Windows.

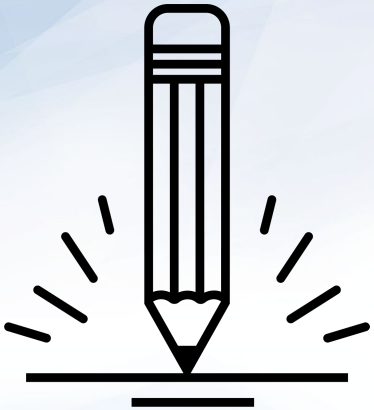
In the next demonstration, we'll use the following scenario:

- A new regular user (Bob) and new administrator (Andrea) need to be added to the workstation.
- We'll use `net user` to create user accounts for Andrea, the new senior developer, and Bob, the new sales representative.
- We will create these users and set their password policies to ensure they adhere to company wide policies.



Instructor Demonstration

Adding Users and Setting Password Policies



Activity: Create Users and Set Passwords

In this activity, you will create users and set password policies for two new users.

Please use the Windows 10 Hyper-V VM.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

Task Scheduling

Task Scheduling

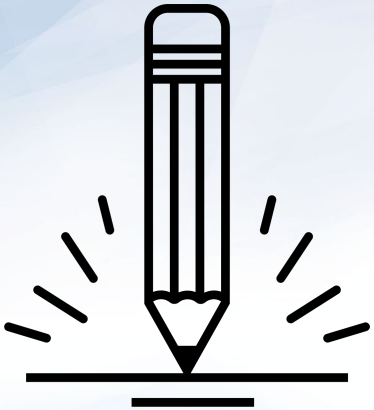
Task Scheduler is a GUI tool that allows system administrators to automate the execution of scripts and applications on a Windows system.

- Similar to cron jobs, tasks can be set to execute at specific times, or a certain amount of time after a user logs in.
- Properly managing systems with scheduled tasks allows us to automate security and system administration actions, such as checking for updates for endpoint security software, sending important logs to systems such as SIEMs, and scheduling system maintenance scripts.

Task Scheduling Demo Setup

In this demo, we will use the administrative user, Andrew, to create scheduled tasks that will automate the reports we've been working on.

- The CIO wants us to schedule reports to be created on a daily basis.
- We will use Task Scheduler to create a task that runs each day.



Activity: Task Scheduling

In this activity, we will use Task Scheduler to schedule reports to be created on a daily basis.

Please use the Windows 10 Hyper-V VM.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

Important!

Make sure to shutdown your HyperV VMs and Lab Machine

Any Questions?