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`**.

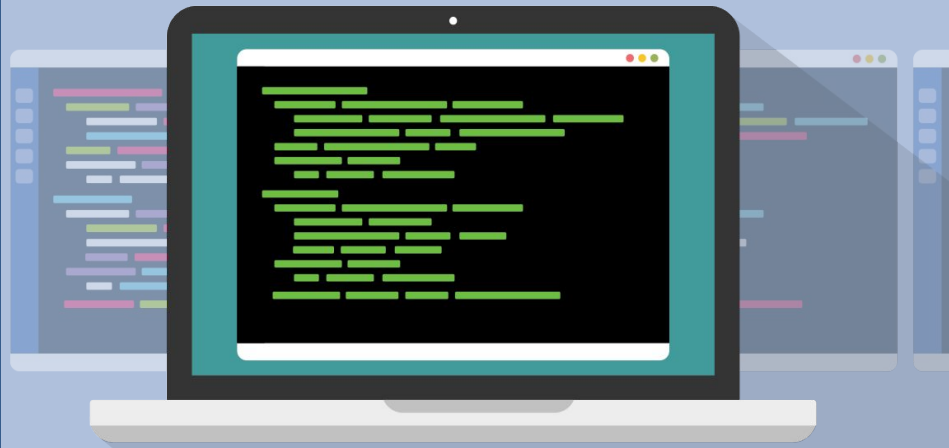
Schedule tasks using Task Scheduler.

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

Creating Compound Commands

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.



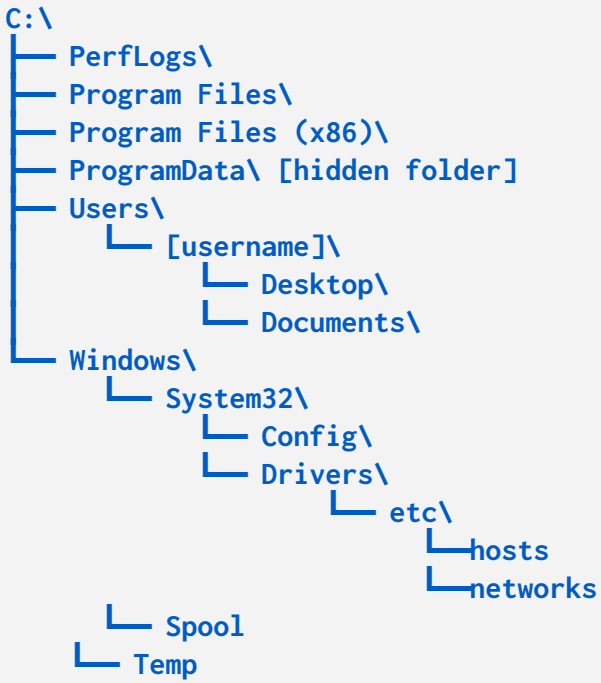
Windows in a Professional Context

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 environments: Windows PCs, Windows Servers, Office 365, and Exchange, etc.	Since Windows are the most common PC for businesses, penetration testers must exploit Windows and Microsoft-specific platforms.	Being the most commonly supported endpoint device for businesses, forensics investigators must understand how Windows works.

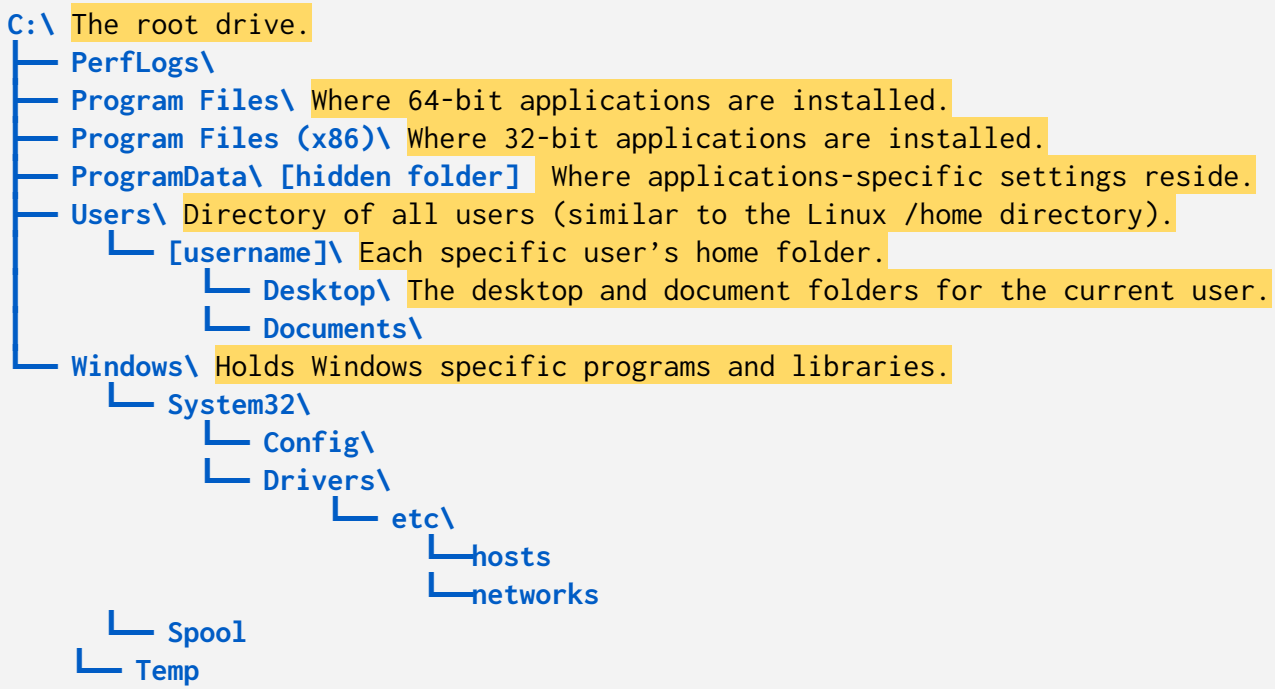
Windows Directory and File Structure

The default Windows directory structure:



Windows Directory and File Structure

The default Windows directory structure:



Command Prompt (CMD)

Today, we'll work in the Windows command prompt, **CMD**, which is comparable to Unix shells like bash.

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)

Today, we'll work in the Windows command prompt, **CMD**, which is comparable to Unix shells like bash.

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`

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

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:

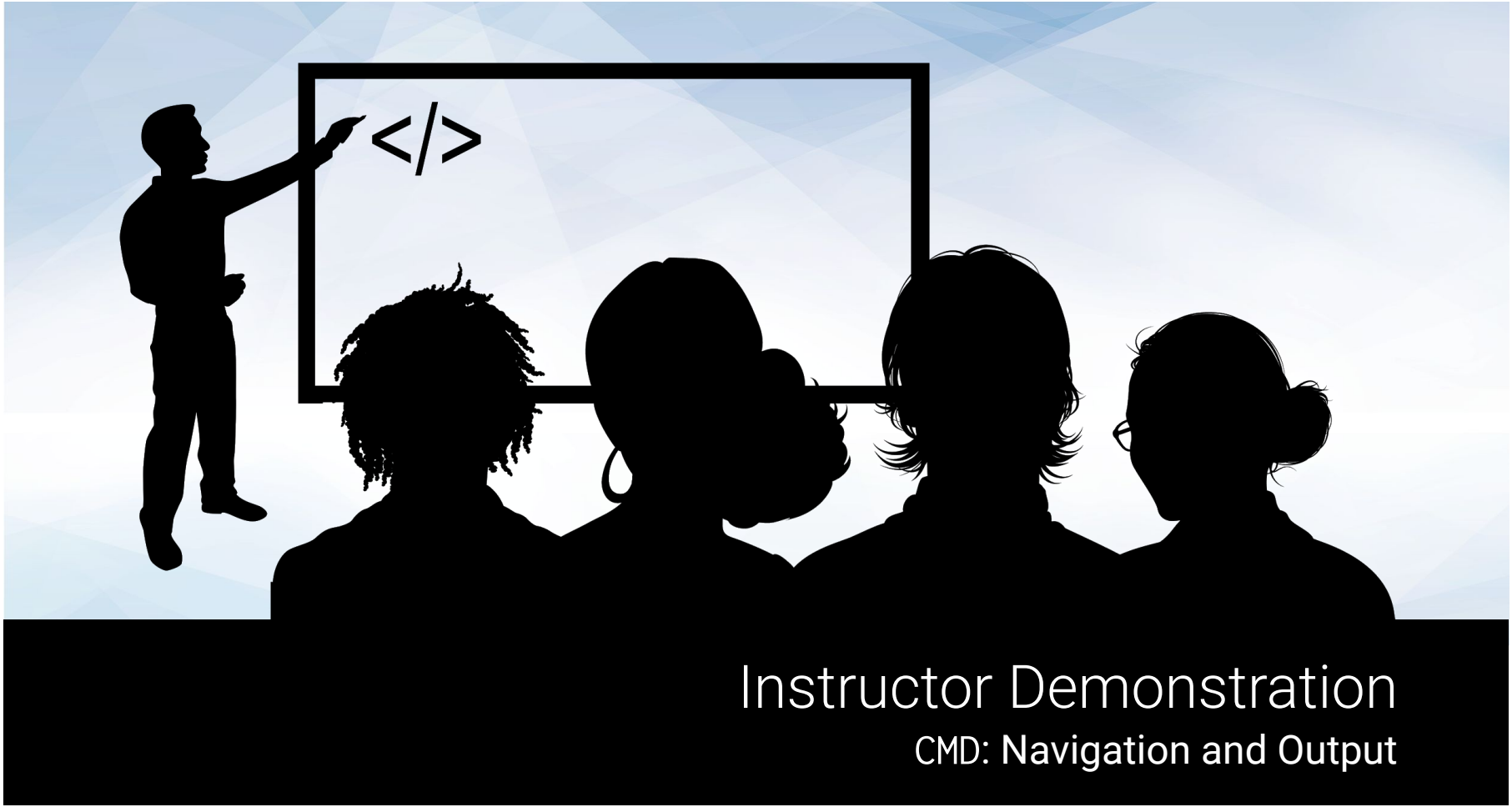
- **cd %ProgramFiles%**

We can combine ENV variables with regular directory names:

- **cd %USERPROFILE%\Desktop**

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

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



Instructor Demonstration

CMD: Navigation and Output

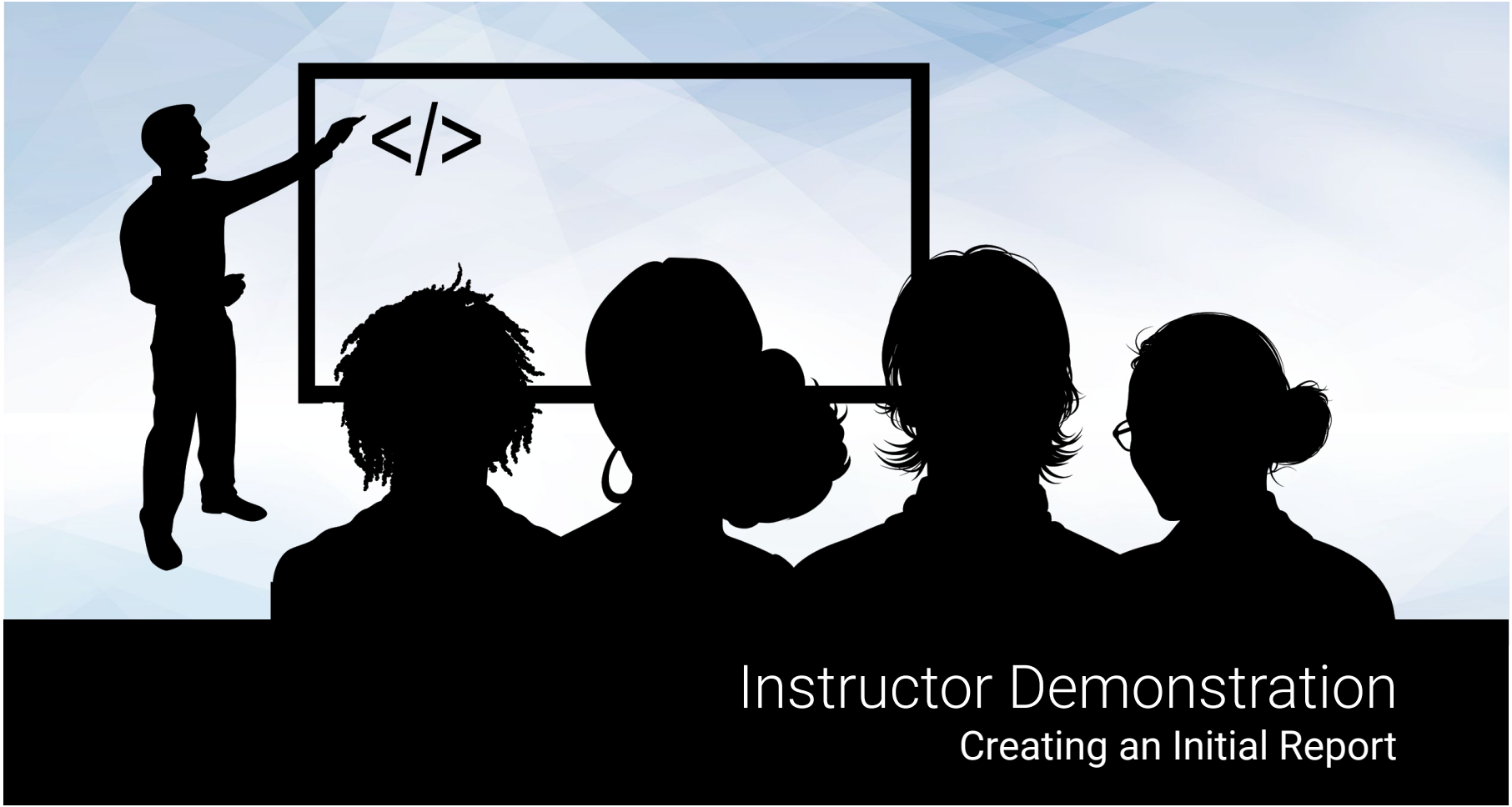
Today's Scenario

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.

- Good Corp's previous senior developer, **`sysadmin`**, was using this Windows system for a company project. They were the only developer on the project.
- Because Good Corp only uses Linux and Mac, there are no existing policies or previous setups for managing a Windows environment.
- You are helping the CIO develop a standardized Windows workstation. This will allow the next developer to get set up quickly, and ensure all future Windows workstations use a standardized Windows-specific development environment. You will create and eventually automate reports that describe specifics of this workstation.

Let’s start by **making the initial report**.

We’ll use this report in the upcoming activities and demonstrations.



Instructor Demonstration

Creating an Initial Report

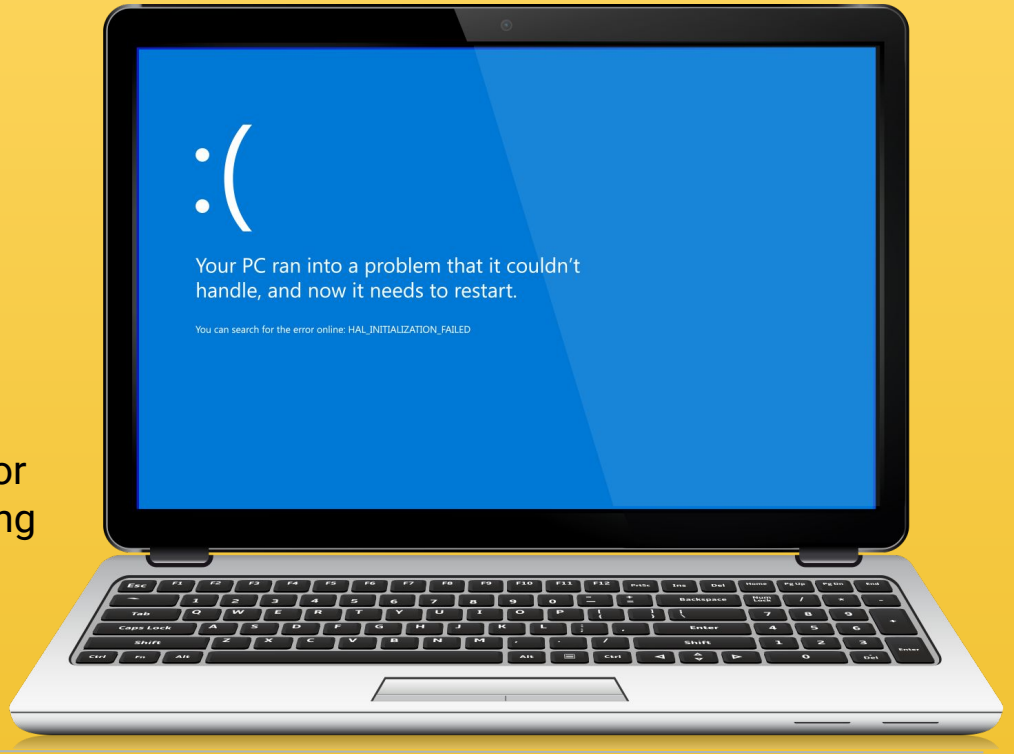
Introduction to Task Manager

Task Manager

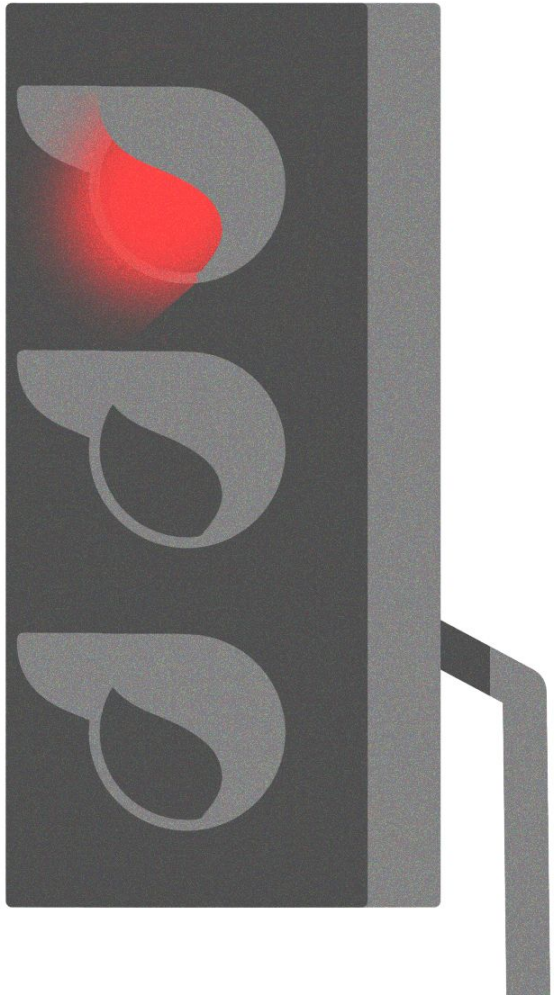
Task Manager is one of the most important Windows tools for troubleshooting resource usage.

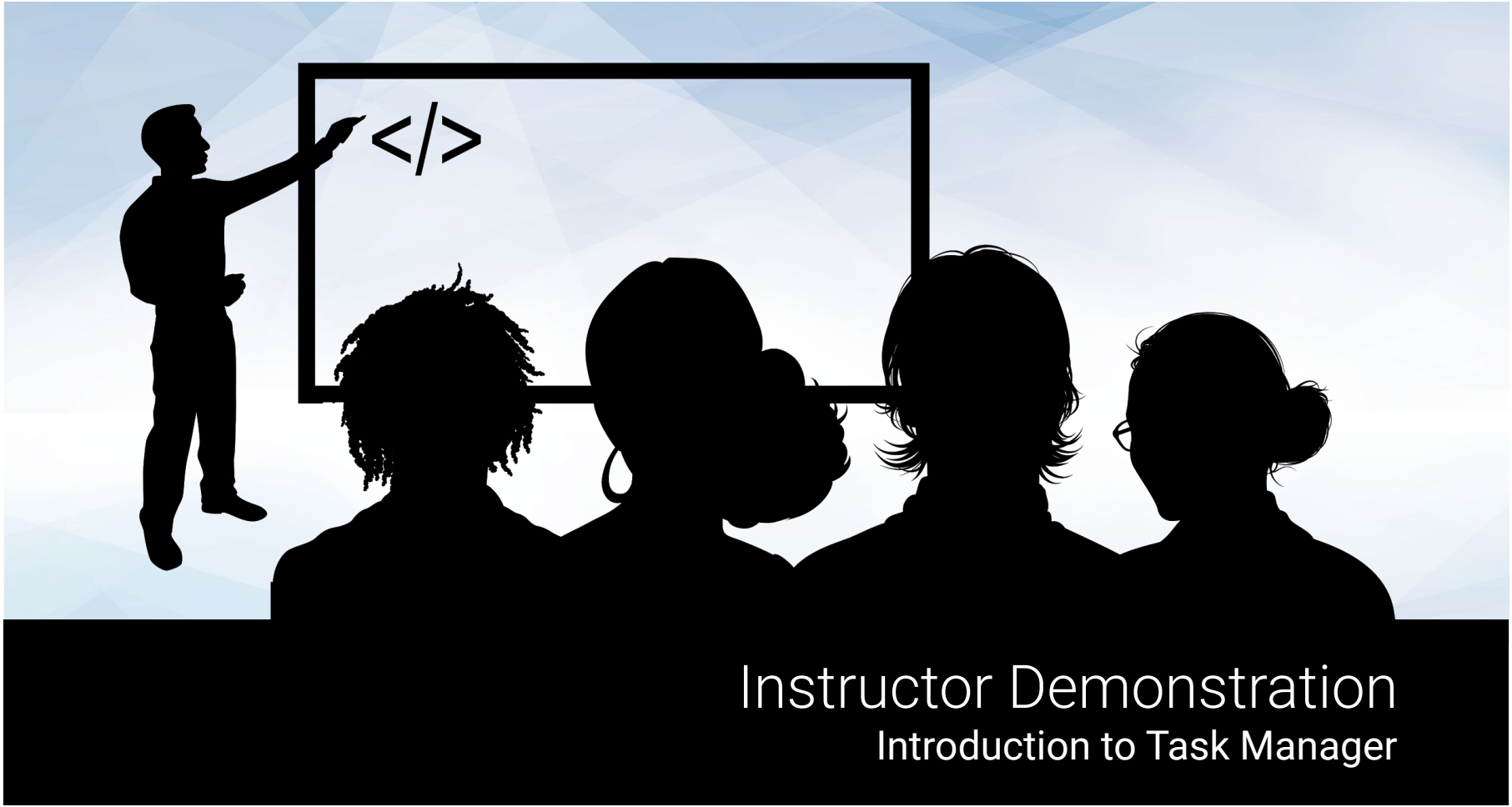
- **We'll audit and manage tasks and processes to identify errant or malicious actions taking place without users' or administrators' knowledge.**

- When left open, some programs can take up unnecessary resources or cause memory leak, eventually leading to system crashes — the blue screen of death.



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





Instructor Demonstration

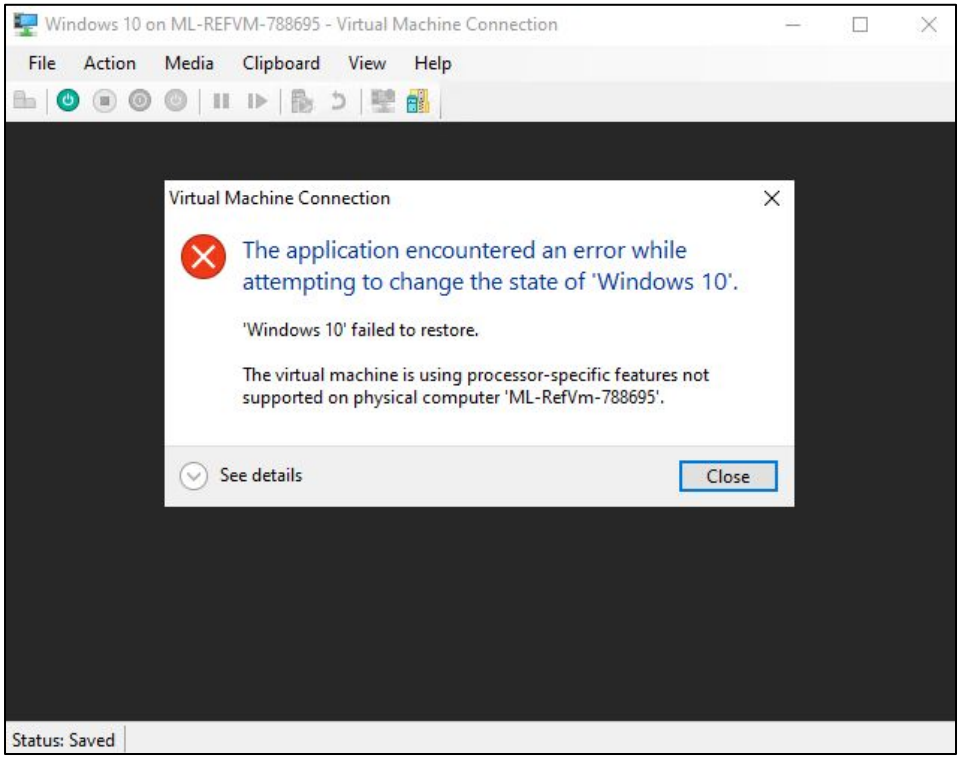
Introduction to Task Manager

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**.

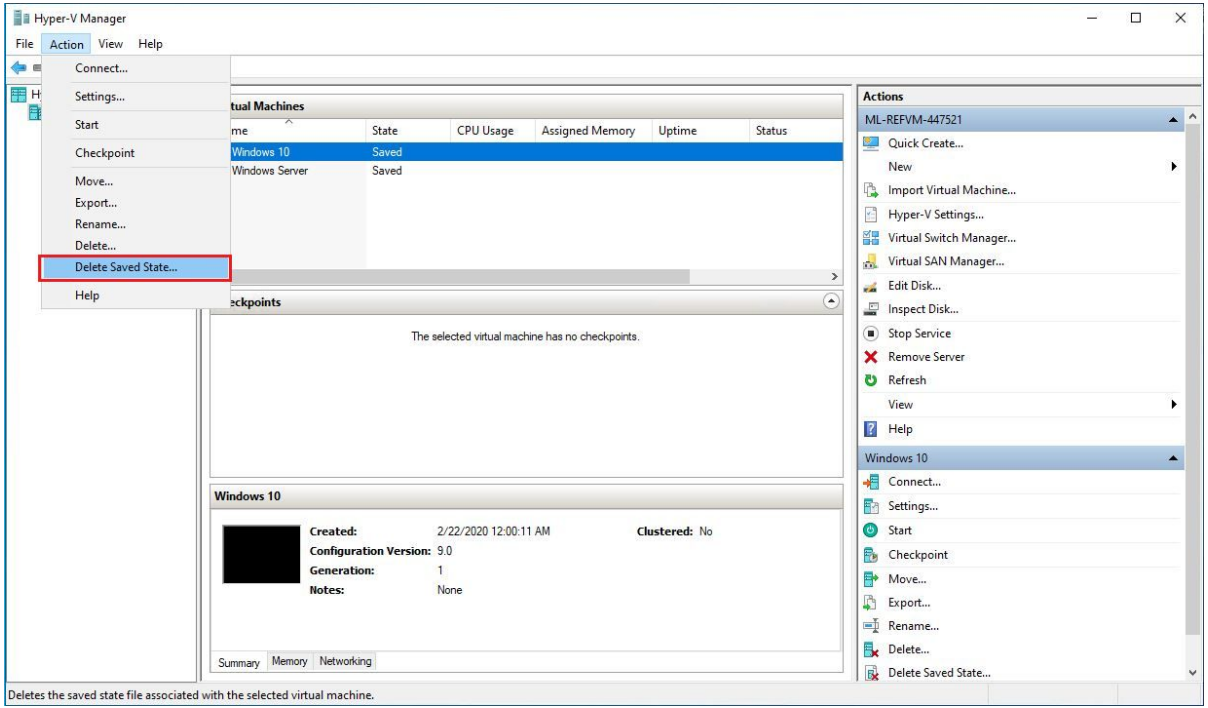
- If a machine enters a saved state during class, you may see the following error: `The application encountered an error while attempting to change the state of the 'VM-Name'.`
- If you encounter this error, the VM may not startup until you delete the saved state. Turning the VMs and the host machine 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



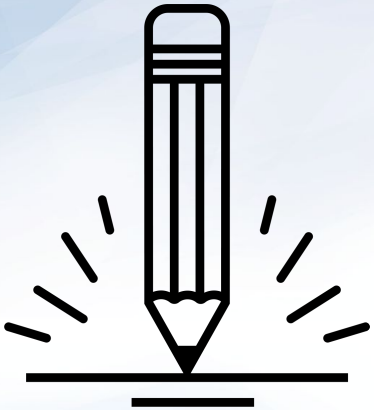
If you see this error window, you will need to **delete the saved state**.

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.



Activity: Task Manager and CMD

In this activity, you will use the command line to generate a baseline report of a Window system.

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 by CPU usage and end a high CPU utilization task.

03 Navigate to the desktop.

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.

`[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.

`[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.

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
```

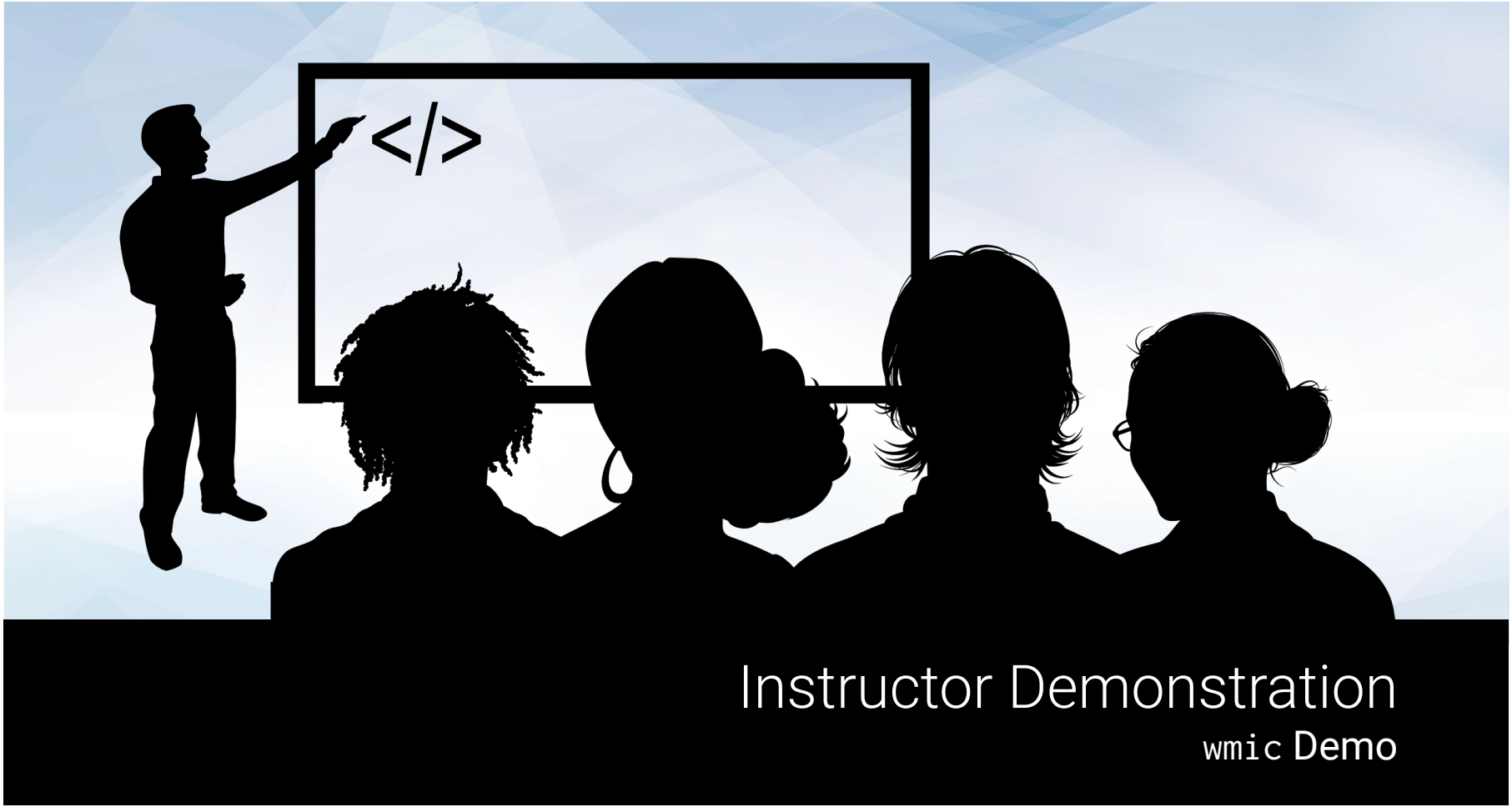
```
wmic logicaldisk get caption, filesystem, freespace, size, volumeserialnumber
```

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

`wmic` Demo

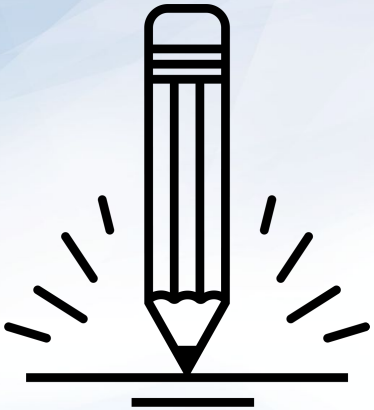
In the next demo, we will move through different programs, understand their importance in a sysadmin context, and get and append them to our report.

- 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.



Instructor Demonstration

`wmic` Demo



Activity: Creating a Report with `wmic` Output

In this activity, you will continue baselining the 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.

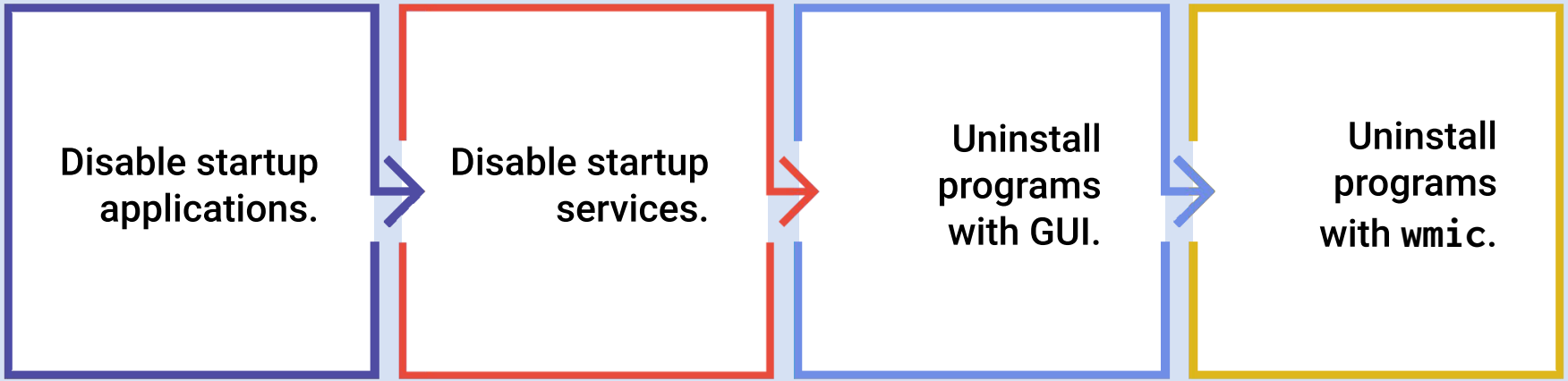
06 Retrieve Windows update information and startup application list.

07 Enumerate a list of startup services.

Removing Unwanted Programs and Services

Removing Unwanted Programs and Services

We will continue our sysadmin tasks by using the GUI and command line to complete the following:



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.

Disabling Startup Applications (Task Manager)

Let’s manage and audit these startup applications with the GUI Task Manager:

Our CIO read the latest report and noticed that the peer-to-peer file sharing application uTorrent was installed. Your CIO asked you to disable it from starting up automatically, as it poses a security risk by exposing your public IP address.

Let’s walk through the following steps:

- Launch Task Manager.
- Navigate to the *Startup* tab.
- Find uTorrent.
- Disable it.

Disabling Startup Services (`services.msc`)

Windows services are usually GUI-less processes that run on startup and in the background.

Our CIO is concerned with the service **Downloaded Maps Manager**.

- Downloaded Maps Manager, a telemetry-based service automatically installed with Windows 10, downloads offline maps when map applications are in use.
- Disabling this service is our first step in disabling all telemetry and data gathering applications on this computer.

Let's walk through the following:

- Launch **`services.msc`.**
- Find the Downloaded Maps Manager service.
- Click on *Properties* in the drop-down menu, select *Disable*, then *Apply* and *OK*.

Uninstall Programs (GUI)

Now the CIO wants us to entirely remove any components of Adobe Flash Player on the system.

- Adobe Flash Player is well-known among the cybersecurity community as one of the most vulnerable browser plugins.
- Because of Flash Player's many security issues, many browsers have officially disabled it by default.

Remove this program by doing the following:

- *Windows Setting* window → *Apps*
- Find Adobe Flash Player 32 NPAPI in the list.
- Click *Uninstall*.

Uninstall Programs (CMD/wmic)

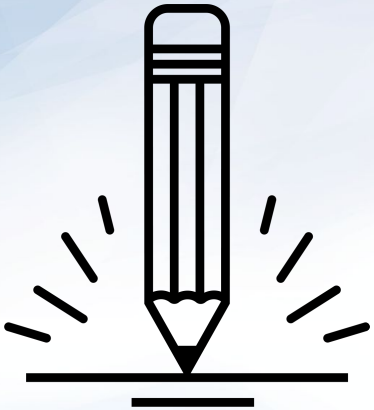
We'll use the command line with `wmic`, the `where` clause, and a `call` method:

- `wmic product get name,version`
- `wmic product where (name="QuickTime 7") call uninstall`

QuickTime Player has similar vulnerabilities to Flash Player. Let's get rid of it too.

Let's remove additional Apple products:

- `wmic product where name="Apple Application Support" call uninstall`
- `wmic product where name="Apple Software Update" call uninstall`



Activity: Remove Unwanted Programs and Services

In this activity, we will remove from the system some of the applications and services mentioned in our report.

Please use the Windows 10 Hyper-V VM.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

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.

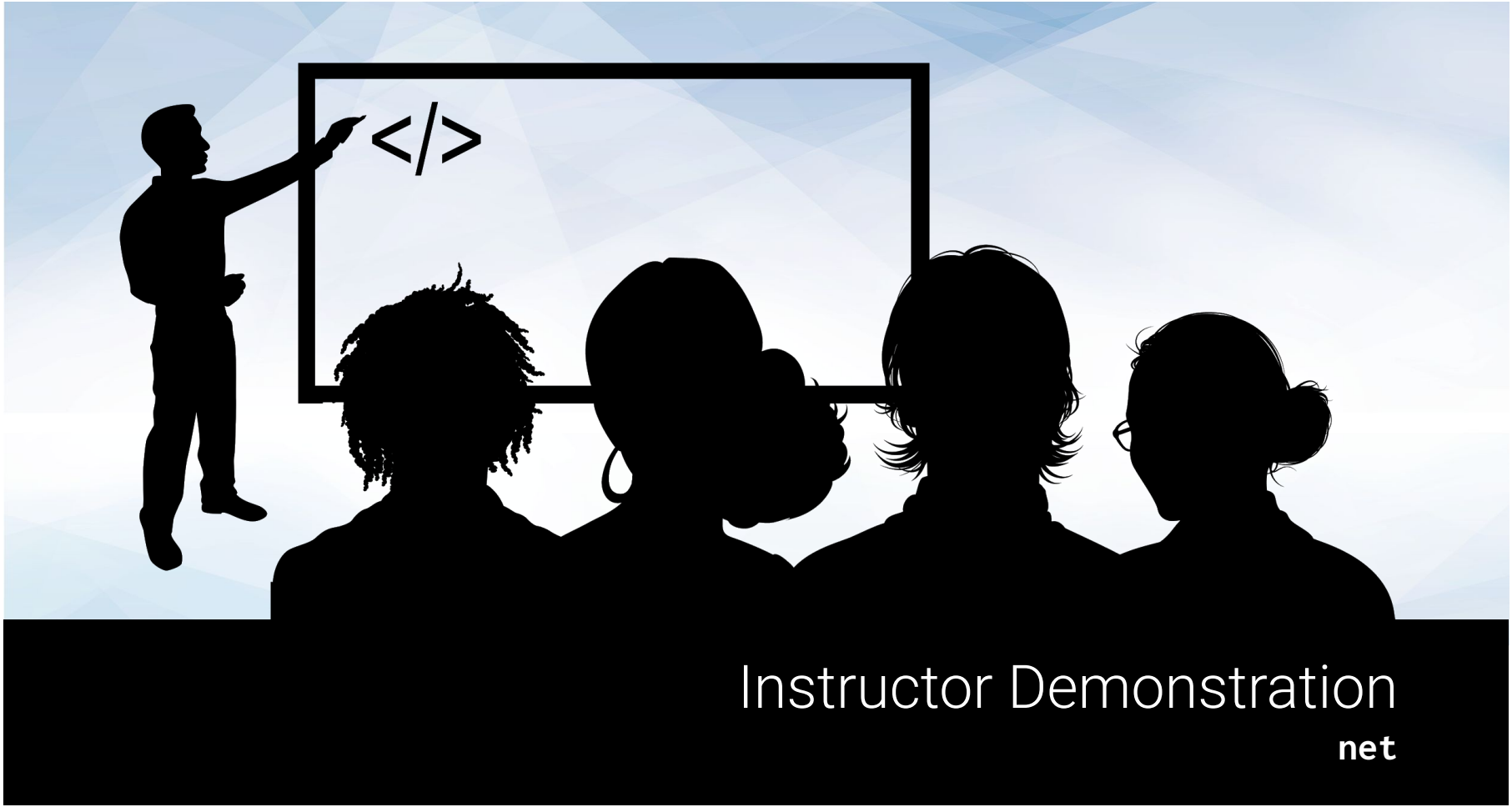
- E.g., if using the PW **`apples2apples`**, you'll have to change it to two new passwords before you can use **`apples2apples`** again.

`net` Demo Set Up

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.

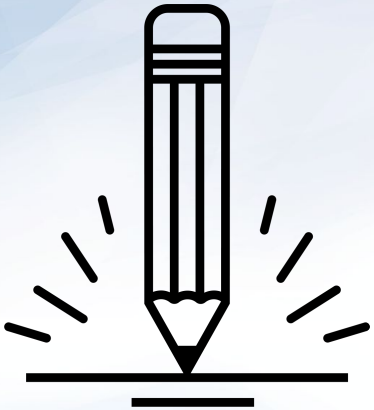
We'll use the **`net`** tool to do the following:

- Learn about users on the system.
- Learn about **`sysadmin`**'s group and password policies.
- Learn about local groups.
- Learn about the current password policies.
- Append all of this information to the report.



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`**.

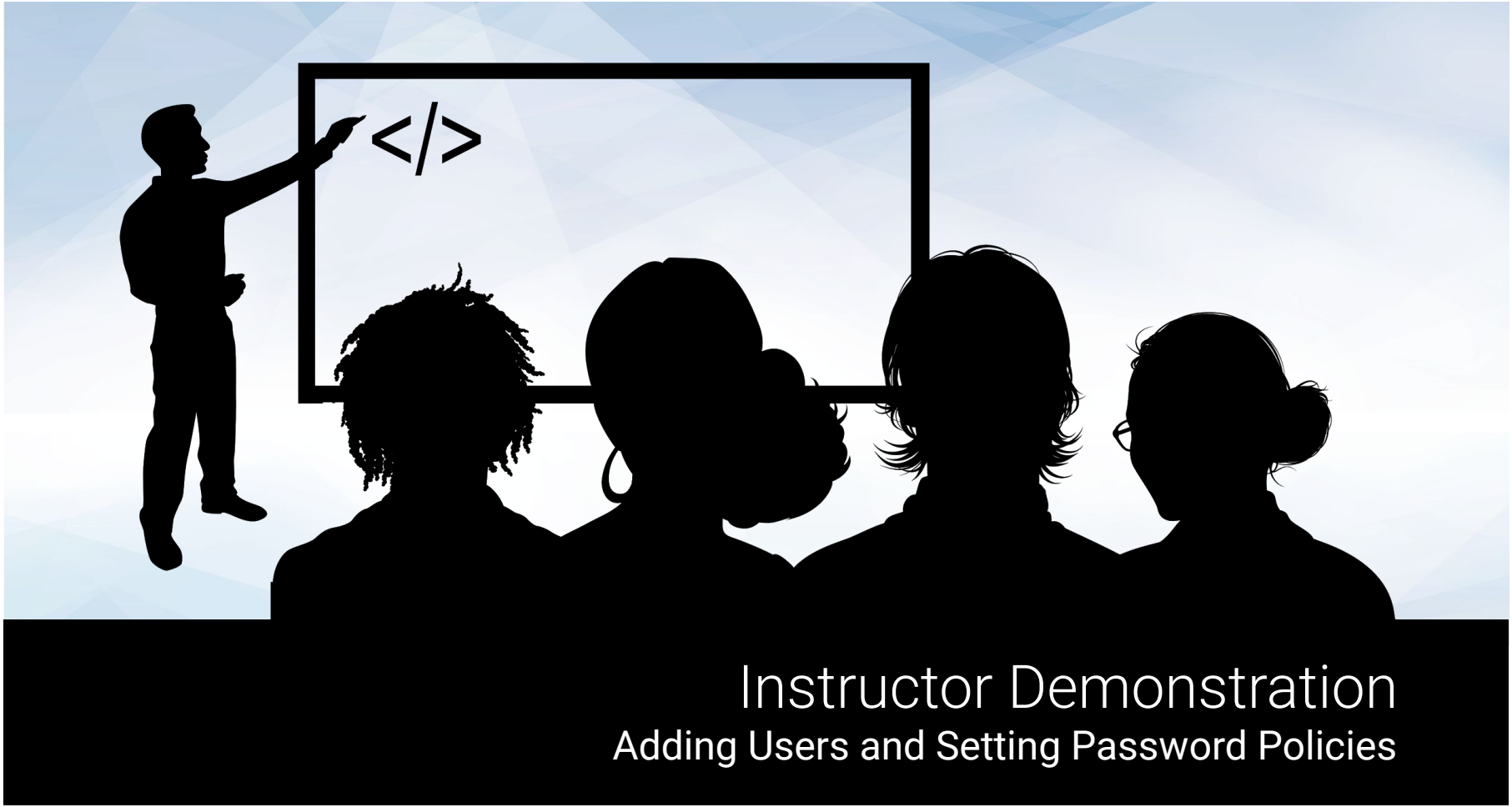
Creating Users and Setting Password Policy

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.

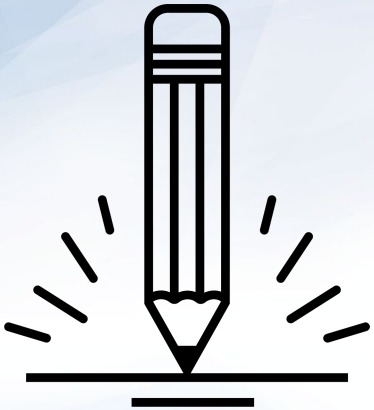
Consider the following scenario:

- A new regular user (Bob) and new administrator (Andrew) need to be added to the workstation.
- We'll use `net user` to create user accounts for Andrew, 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

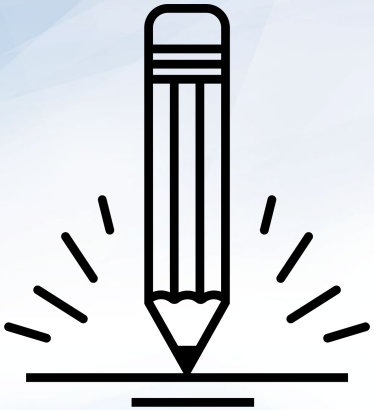
Task Scheduler is a GUI tool that allows system administrators to automate the execution of scripts and applications on a Windows system.

- 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.

Any Questions?