PROJECT TASK 3

SECURE WINDOWS 10 OPERATING SYSTEM

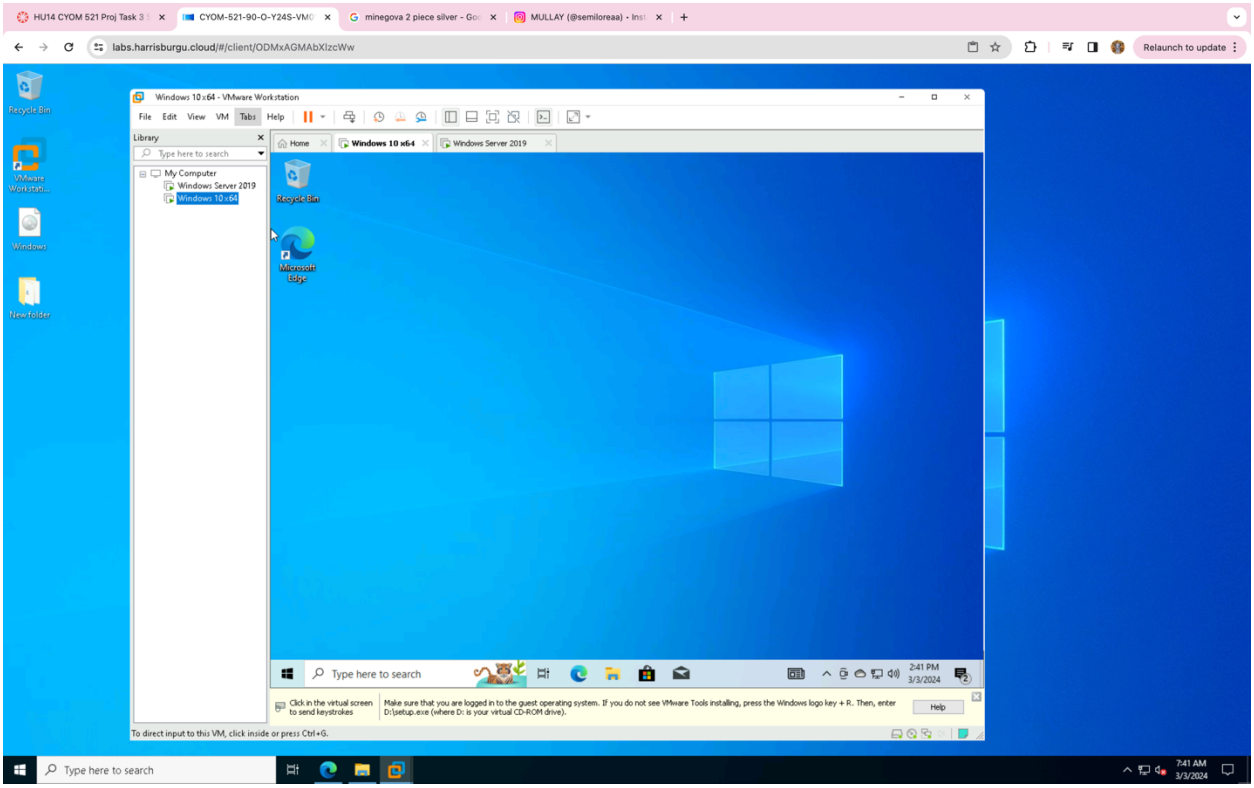
Alabi Kehinde Oluwasemilore
Information Systems Engineering and Management, Harrisburg University
CYOM 521: Cybersecurity Architect & Resiliency
Dr. Bruce Young
5/3/2024

Virtual Box Lab Setup

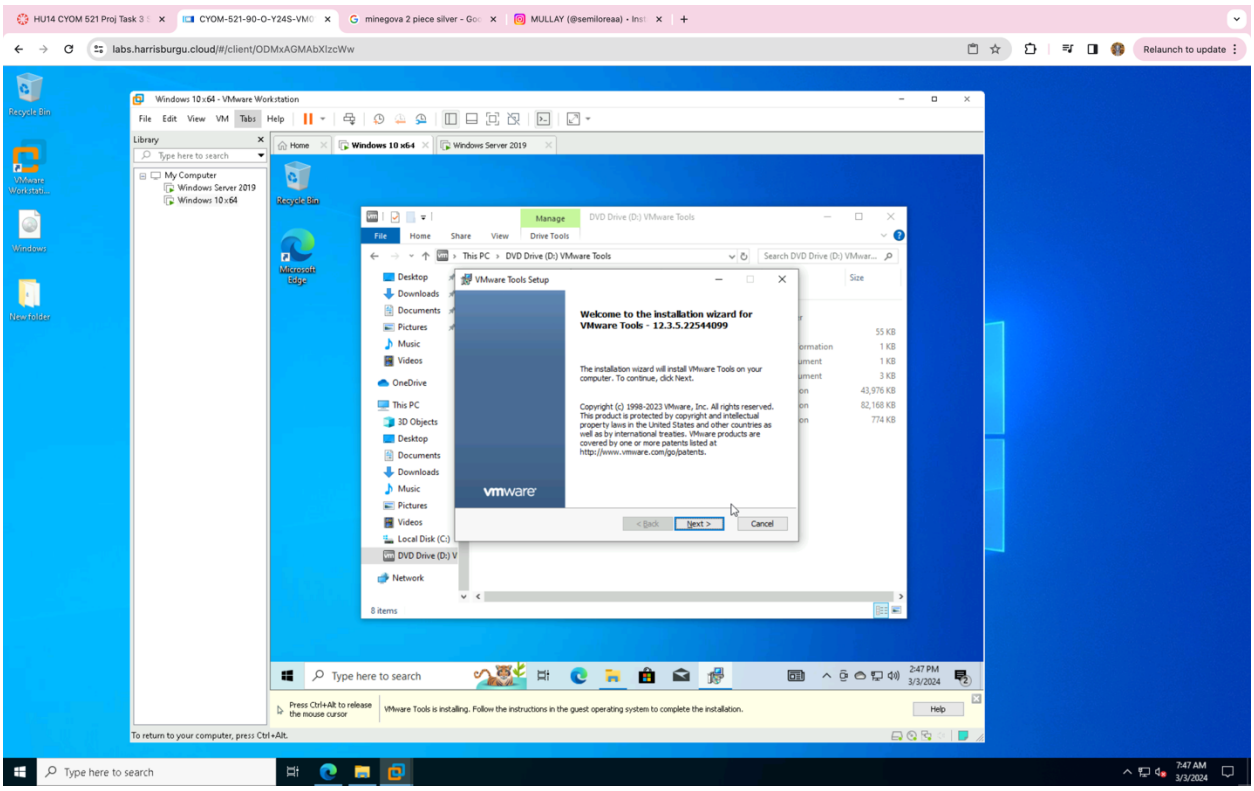
System Configuration:

- Macbook Pro 2016
- Mac OS Ventura
- 32 GB RAM
- 2.3 GHz 8-Core Intel Core i9

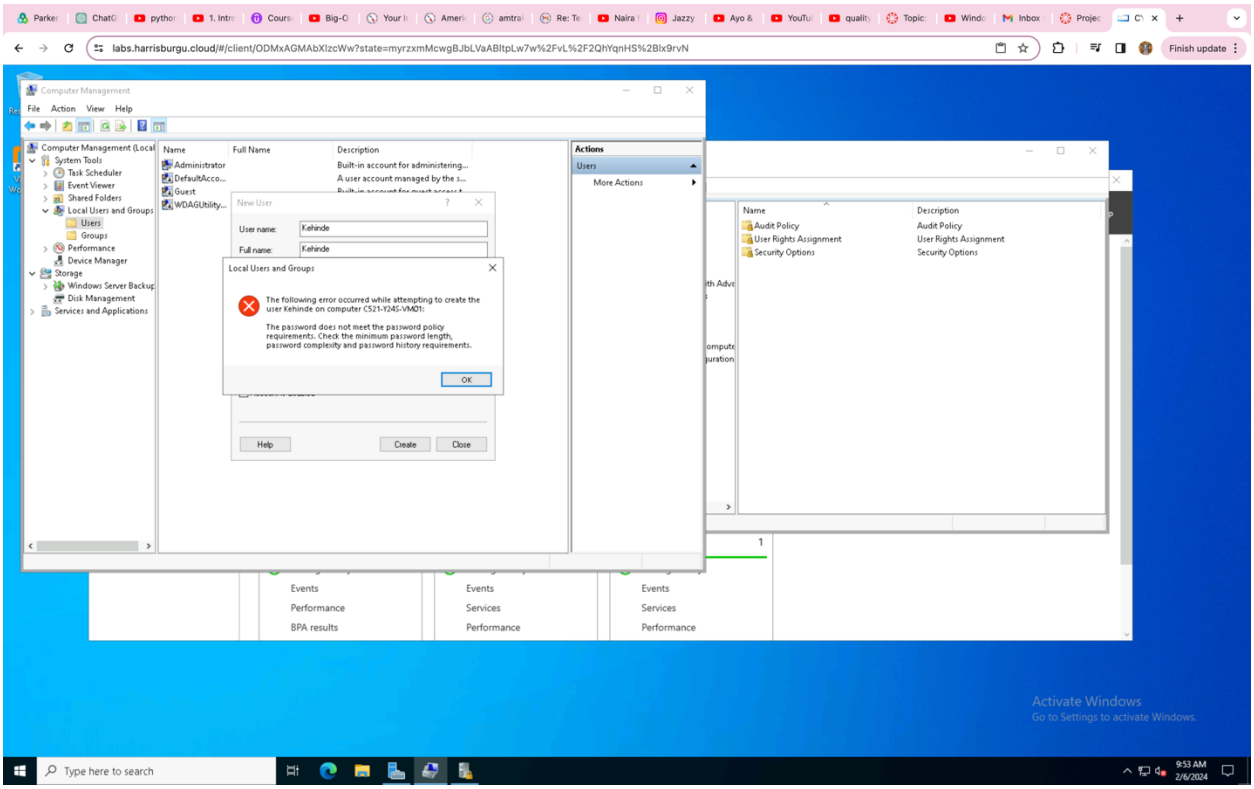
Step 1: After Windows 10 installation, click on VM and install VMware tools



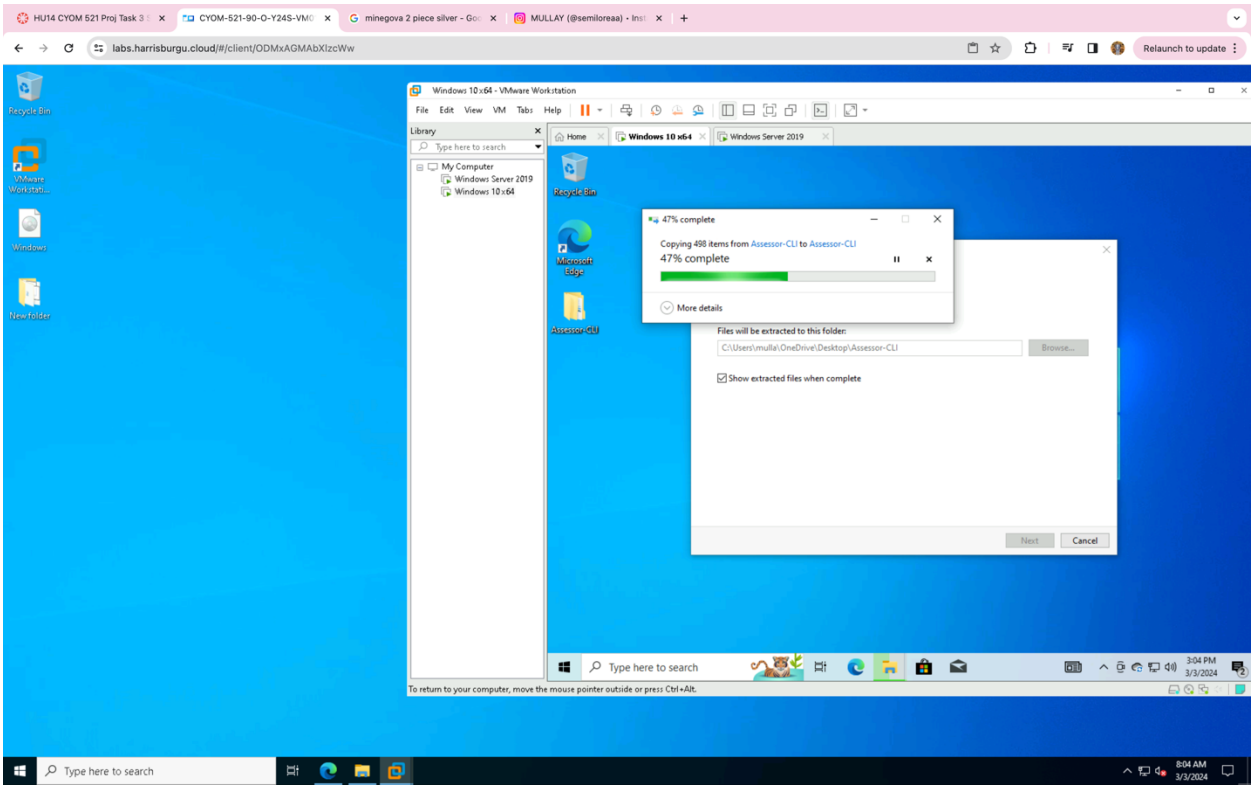
Step 2: Install VMware tools from VMware DVD drive



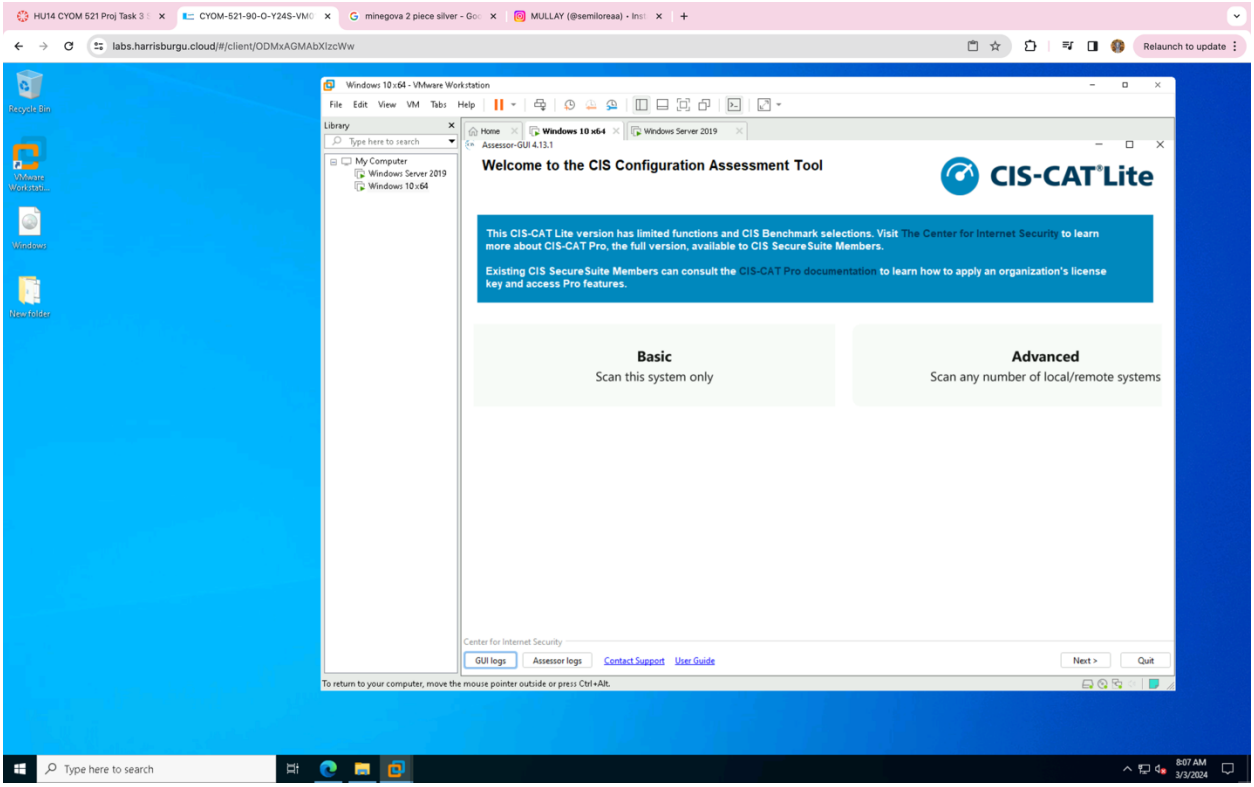
Step 3: Copy Assessor-CLI file from HPC lab to Windows 10 VM



Step 4: Extract file

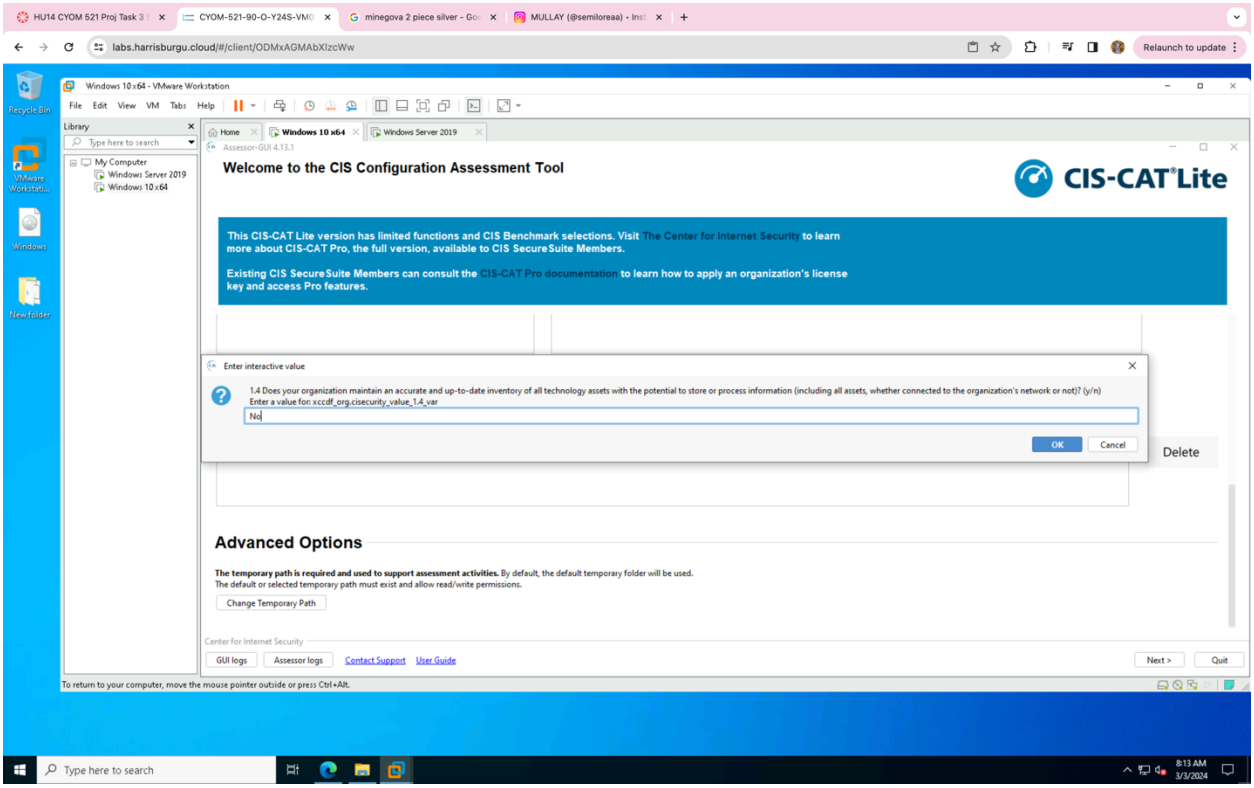


Step 5: Launch Assessor-GUI

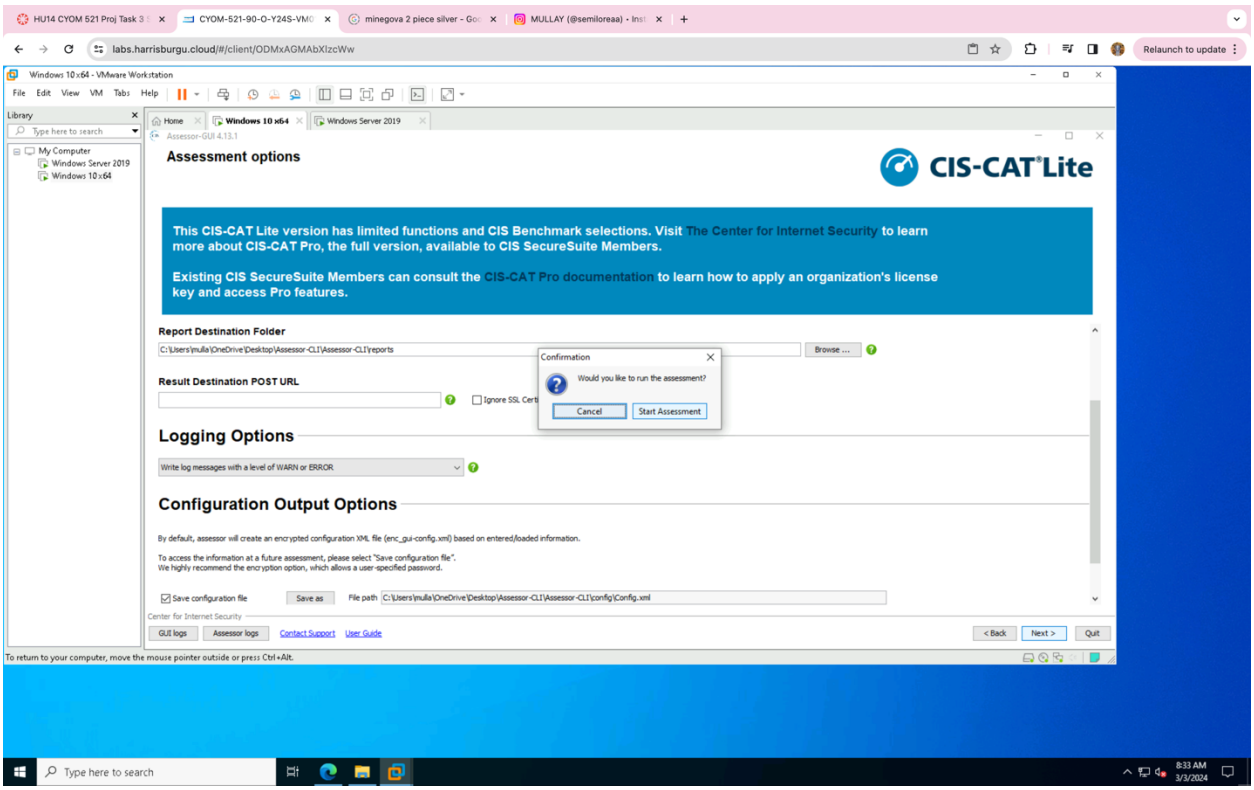


Step 5: Conduct system scan

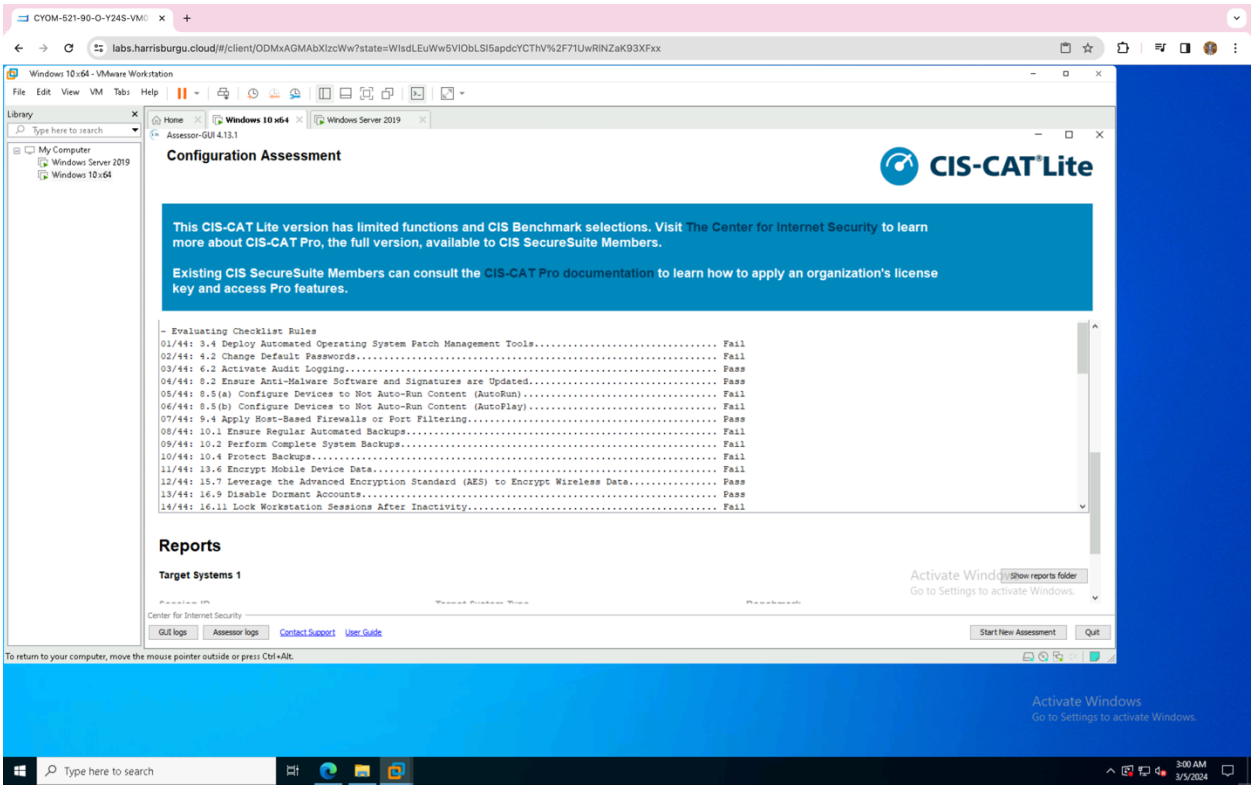
-Answer questions related to hardening in risk assessment process



-Start Assessment



Step 5: Assessment results



Step 5: Prioritize failed security checks based on severity and potential impact

1. Change default passwords
2. Protect backups
3. Ensure regular automated backups
4. Perform complete system backups
5. Deploy Automated Operating System Patch Management Tools
6. Configure devices to not auto-run content (Autorun)
7. Configure devices to not auto-run content (Autoplay)

Step 6: Remediation process for each of the 7 failed items

Change default passwords:
Description: Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

Default passwords are the passwords that ship with computers, applications, routers, and other equipment. Default passwords are a very common way for computer systems, devices, and applications to be hacked. Lists of default passwords for operating systems, applications, and devices are readily available on the internet for anyone to download and try on enterprise systems. Therefore, they need to be changed from the defaults to something that is not easily guessable.

Default passwords can be easily guessed by individuals external to an organization, which can result in the theft of sensitive enterprise data. For example, if the password for a wireless router is guessed, an attacker will be able to add and remove network devices, which will allow them to read sensitive enterprise information. To be able to guess a router's default password, it's often sufficient to identify the make and model. Attacks may be able to figure this out by physically seeing the device, or remotely based on a router's SSID or MAC address. Cheatsheets are also available online with the default passwords for wireless routers common to small and home offices. If a password for an application or utility is guessed, the offending party will be able to access the information contained by that program.

Since Windows does not have default passwords, the automated CAM check for 4.2 focuses on the having "values consistent with administrative level accounts" portion of the sub-control. CAM is checking for a required minimum password length. By default, the required minimum in CAM is 14 (which is consistent with the Windows Benchmark), but this setting can be adjusted in the assessor-cli.properties file as appropriate for your organization.

The minimum password length can be set via local group policy as follows: Open the Local Group Policy Editor, navigate to Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy > Minimum password length. Similar settings are available at the Domain level as well.

Show Assessment Evidence:

Script:	sce/cam/windows_10/4_2.ps1
Result:	Fail
Exit Value:	102

Output:
- CAM Sub-Control 4.2
- Fail - Minimum password length is 0 which does not meet the required minimum of 14

References: CIS Controls V7.0: **Control 4: Controlled Use of Administrative Privileges**

Protect backups:
Description: Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

Backups can help an enterprise recover from a variety of disaster situations, be they the cause of malicious actors or accidents. Yet backups can be physically and digitally targeted by attackers looking to hurt an enterprise. Backups that are connected to a network can be altered or deleted by malware, and physical backup drives can be stolen or suffer fires, floods, and other natural disasters. Backups need to be protected from these threats in order to be useful when the time comes. Digital mitigations include authenticating users before access and encrypting backups. Physical mitigations include keeping backup drives locked away from thieves, and also outside of the same fire zone. This means that if a fire or flood were to strike an organization's physical location, the backups would not be affected. This is sometimes accomplished by using third-party backup services to store data offsite. These backups need to be protected as well.

There are two primary groups of threats to backups: digital and physical. Digital threats include local and remote attempts to access backups without being properly authenticated. Additional issues include altering or deleting backups. Physical threats include theft of physical backups or natural disasters (e.g., fires, floods).

The automated Controls Assessment Module check for 10.4 verifies that if Windows 10 File History is on, the drive that the File History data is being backed up to is encrypted with native Windows encryption (either hardware/device encryption or BitLocker software encryption). Similarly, if Windows System Image backups are turned on, this check verifies that the destination drive for those backups is encrypted with native Windows encryption. If either/both of these two backup methods are enabled, the check will fail if the corresponding backup drives are not encrypted. If neither backup method is enabled, the check will also fail.

In order to pass this check, enable either Windows 10 File History, Windows System Image backups, or both. For whichever of these backup methods that you enable, ensure that the corresponding backup drive destinations are encrypted with native Windows encryption.

File History can be turned on in the Windows 10 Backup settings, in the "Back up using File History" section, ensure an appropriate destination drive is selected (or select one with "Add a drive"), then make sure the "Automatically back up my files" toggle is set to "On". In the "More options" menu, individual folders can be included or excluded from the File History backups.

A Windows System Image backup can be initiated in Control Panel > System and Security > Backup and Restore (Windows 7), and then clicking on "Create a system image" on the left side.

To turn on Bitlocker, navigate to Control Panel > System and Security > BitLocker Drive Encryption, and select Turn on BitLocker.

Show Assessment Evidence:

Script:	sce/cam/windows_10/10_4.ps1
Result:	Fail
Exit Value:	102

Output:

- CAM Sub-Control 10.4
- Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsBackup\SystemImageBackup LastSuccessfulBackupDrive does not exist
- Could not identify the last successful Windows System Image backup drive.
- File History is not being used.
- Fail - Could not identify drives for either Windows System Image backup or File History backups. It is likely that neither backup method is being used.

Errors:

- Get-Item : Cannot find path 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\fhsvc\Parameters\Configs' because it
- does not exist.
- At C:\Users\mulla\OneDrive\Desktop\Assessor-CLI\Assessor-CLI\sce\cam\windows_10\10_4.ps1:45 char:16
- + ... leHistory = Get-Item "Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentCont ...
- + ~~~~~~
- + CategoryInfo : ObjectNotFound: (HKEY_LOCAL_MACH...ameters\Configs:String) [Get-Item], ItemNotFoundExcep
- tion

- + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetItemCommand

References: CIS Controls V7.0: **Control 10: Data Recovery Capabilities**

Ensure regular automated backups

Description: Ensure that all system data is automatically backed up on a regular basis.

A backup is a duplicate of a computer system's data. If an attacker breaches a network or computer system, their first step will often be to change system configurations to ensure access to the attacker is permanently available. Additionally automated malware infections will often delete or prevent an organization's valid access to data. Attackers will sometimes make subtle alterations to data that can jeopardize an organization's effectiveness at a later date. It's also common for computer systems to fail and simply stop working when attacked. This can be especially true of backend information systems that remain out of sight from customers. These systems may simply grow old and need to be replaced. Other accidents can happen like fires and floods. Systems fail and a plan needs to be in place to make sure that a business can recover from whatever incident occurs. Automated backups taken on a regular basis are a primary part of an enterprise disaster recovery plan.

Backups protect against the effects of many types of malware, including newer variants such as ransomware and destructive malware. Additionally, backups help to harden an organization against accidents, natural disasters, and hardware failures.

The automated CAM check for 10.1 verifies that Windows 10 File History is turned on for at least one user. In the Windows 10 Backup settings, in the "Back up using File History" section, ensure an appropriate destination drive is selected (or select one with "Add a drive"), then make sure the "Automatically back up my files" toggle is set to "On". In the "More options" menu, individual folders can be included or excluded from the File History backups.

Show Assessment Evidence:

Script:	sce/cam/windows_10/10_1.ps1
Result:	Fail
Exit Value:	102
Output:	- CAM Sub-Control 10.1 - Fail - File History backups are not configured.
Errors:	- Get-Item : Cannot find path 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\fhsvc\Parameters\Configs' because it does not exist. - At C:\Users\mulla\OneDrive\Desktop\Assessor-CLI\Assessor-CLI\sce\cam\windows_10\10_1.ps1:10 char:16 - + ... leHistory = Get-Item "Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentCont ...

- + ~~~~~~
- + CategoryInfo : ObjectNotFound: (HKEY_LOCAL_MACH...ameters\Configs:String) [Get-Item], ItemNotFoundExcep
- tion
- + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetItemCommand

References: CIS Controls V7.0: **Control 10: Data Recovery Capabilities**

Perform complete system backups

Description: Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

A backup is a duplicate of a computer system's data, but different types and degrees of backups exist. A backup is commonly viewed as a small collection of a system's overall data. Often times a few important folders containing photos, receipts, contracts, or tax information are stored elsewhere. This information may be stored on another computer system, external hard drive, removable media, or cloud service. This strategy is insufficient for protecting an organization. Flavors of backups include incremental, differential, or complete. A complete system image is a snapshot of all data and settings on a system.

If a system is breached by an attacker, infected with malware, or involved in an accident (e.g., fire, flood), it often takes a long time to bring a system or network back online. This would include reinstalling and configuring all of the enterprise applications used for business tasks. Complete system backups rectify this issue by backing up not just important folders, but by backing up the entire computer, which can be pushed to new systems. Although this approach is a more complex solution, it makes recovery from a disaster or computer incident much quicker and enables you to get your business operational again. Backups protect against many types of malware, including ransomware and destructive malware. Additionally, backups help to harden your organization against accidents and natural disasters.

The automated CAM check for 10.2 verifies that a successful Windows System Image backup was generated within a specified timeframe. By default, CAM uses 7 days for this time frame, but this setting can be adjusted in the assessor-cli.properties file as appropriate for your organization.

A Windows System Image backup can be initiated in Control Panel > System and Security > Backup and Restore (Windows 7), and then clicking on "Create a system image" on the left side.

Show Assessment Evidence:

Script:	sce/cam/windows_10/10_2.ps1
Result:	Fail
Exit Value:	102
Output:	• CAM Sub-Control 10.2 • Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsBackup\SystemImageBackup LastSuccessfulBackupTime does not exist

- Fail - No record exists of a successful Windows System Image Backup

References:

CIS Controls V7.0: **Control 10: Data Recovery Capabilities:**

Deploy Automated Operating System Patch Management Tools

Description: Deploy automated software update tools to ensure that the operating systems are running the most recent security updates provided by the software vendor.

Security patches are updates to a computer system's operating system or installed software and are a basic part of IT maintenance. The patches the OS developers provide may contain new features, but also contain fixes to recently discovered security vulnerabilities. Operating systems go "stale" and need to be updated. Without a constant stream of security patches, computer systems are more vulnerable to malware that can read sensitive company data, or simply destroy it. Accordingly, patching systems is one of the primary ways an enterprise can protect itself from attackers.

The automated CAM check for 3.4 requires both the download of updates and the installation of those updates to be automatic and without user intervention. Therefore, it will fail even if automatic update downloads are on, but the user can decide whether to install those updates.

CAM is checking the following registry settings:

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate
DisableWindowsUpdateAccess
(Fail if this setting is set to 1)

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU NoAutoUpdate
(Fail if this setting is set to 1)

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU AUOptions
(Fail if this setting is not set to 4)

The AUOptions value can be set via local group policy as follows: Open the Local Group Policy Editor, navigate to Computer Configuration > Administrative Templates > Windows Components > Windows Update > Configure Automatic Updates. Ensure that Enabled is selected, and Configure automatic updating is set to 4 – Auto download and schedule the install. The other settings there (such as the specific schedule for updates) can be set as appropriate for your organization and are not assessed by CAM. Similar settings are available at the Domain level as well.

Show Assessment Evidence:

Script:	sce/cam/windows_10/3_4.ps1
Result:	Fail
Exit Value:	102

Output:

- CAM Sub-Control 3.4
- Registry::HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate DisableWindowsUpdateAccess does not exist
- Registry::HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate \AU NoAutoUpdate does not exist
- Registry::HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate \AU AUOptions does not exist
- FAIL - Automatic Updates are not set to automatically download and automatically schedule an installation

References: CIS Controls V7.0: **Control 3: Continuous Vulnerability Management**

Configure devices to not auto-run content (Autorun)

Description: Configure devices to not auto-run content from removable media.

Removable media includes USB sticks, memory cards, and external hard drives, just to name a few examples. These devices are commonly used to store photos, videos, and enterprise data. Removable media is also one method used by attackers to install malicious software on computer systems. This attack method can be used to infect traditional enterprise workstations, but also computer systems without a WiFi or Internet connection. Banning the use of removable media is often impractical for businesses. If software on a USB device is allowed to automatically run, it could install malware with limited to no user interaction.

This Sub-Control was specifically included due to the emerging technique of dropping USB drives embedded with malware in parking lots or other areas where employees are likely to pick them up and plug them into their computers.

CAM's check for 8.5 is divided into two separate checks - one for AutoRun and one for AutoPlay. This is the AutoRun check.

CAM is checking the following registry settings to see if at least one of them is set to disable AutoRun:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer NoAutoRun
(Pass if this setting is set to 1)

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer NoAutoRun
(Pass if this setting is set to 1)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
NoDriveTypeAutoRun
(Pass if this setting is set to 0xff)

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
NoDriveTypeAutoRun
(Pass if this setting is set to 0xff)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer NoDriveAutoRun
(Pass if this setting is set to 0x3FFFFFF)

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer NoDriveAutoRun
(Pass if this setting is set to 0x3FFFFFF)

Note that while the Machine settings or Current User settings are accepted by CAM, the Machine settings are preferred because they would turn AutoRun off for all users on the machine.

AutoRun can be turned off via local group policy as follows: Open the Local Group Policy Editor, navigate to Computer Configuration > Administrative Templates > Windows Components > AutoPlay Policies > Set the default behavior for AutoRun. Ensure that Enabled is selected, and then select "Do not execute any autorun commands" in the drop down menu. Similar settings are available at the Domain level as well.

Show Assessment Evidence:

Script:	sce/cam/windows_10/8_5_a_autorun.ps1
Result:	Fail
Exit Value:	102
Output:	CAM Sub-Control 8.5 Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer NoAutoRun does not exist Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer NoDriveTypeAutoRun does not exist Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer NoDriveAutoRun does not exist Fail - AutoRun is on

References: CIS Controls V7.0: **Control 8: Malware Defenses**

Configure devices to not auto-run content (Autoplay)
Description: Configure devices to not auto-run content from removable media.

Removable media includes USB sticks, memory cards, and external hard drives, just to name a few examples. These devices are commonly used to store photos, videos, and enterprise data. Removable media is also one method used by attackers to install malicious software on computer systems. This attack method can be used to infect traditional enterprise workstations, but also computer systems without a WiFi or Internet connection. Banning the use of removable media is often impractical for businesses. If software on a USB device is allowed to automatically run, it could install malware with limited to no user interaction.

This Sub-Control was specifically included due to the emerging technique of dropping USB drives embedded with malware in parking lots or other areas where employees are likely to pick them up and plug them into their computers.

CAM's check for 8.5 is divided into two separate checks - one for AutoRun and one for AutoPlay. This is the AutoPlay check.

CAM is checking the following registry setting to see if it is set to disable AutoPlay:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers
DisableAutoPlay
(Pass if this setting is set to 1)

In the Windows Settings, go to AutoPlay Settings. Move the "Use AutoPlay for all media and devices" toggle to Off. Note: this is a per user setting.

Show Assessment Evidence:

Script:	sce/cam/windows_10/8_5_b_autoplay.ps1
Result:	Fail
Exit Value:	102
Output:	CAM Sub-Control 8.5 Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers DisableAutoPlay 0 Fail - AutoPlay is on

References: CIS Controls V7.0: **Control 8: Malware Defenses**