

COMPLIANCE ASSESSMENT



Overview

In the swiftly evolving digital age, Fed F1rst Control Systems stands at the cusp of a significant transformation, pushing the boundaries of cybersecurity to safeguard its technological frontier. As the organization embarks on integrating cutting-edge tools and technologies, from Windows environments to the inclusion of MacBooks, and ventures deeper into the cloud, the role of a security engineer has never been more pivotal. Amidst this backdrop, you, as a security engineer, are thrust into the heart of this transformation.

Your mission: to navigate the complexities of digital security, ensuring that every technological advancement—be it through securing desktop environments, fortifying email communications, or aligning with stringent cybersecurity standards—translates into a fortified defense against the cyber threats of tomorrow. Your efforts will not only secure Fed F1rst's digital assets but also shape the very foundation of its future in the digital realm.

Welcome to the forefront of cybersecurity at Fed F1rst Control Systems, where your expertise is the key to unlocking a secure, innovative future.

Windows 10 Hardening

In the dynamic environment of Fed F1rst Control Systems, maintaining the security integrity of desktop environments is crucial to safeguard corporate data and ensure uninterrupted business operations. As part of your responsibilities, you are required to conduct a comprehensive security review of a Windows 10 desktop. This task involves identifying vulnerabilities that could potentially compromise system security and proposing actionable remediation steps to mitigate these risks.

- *Perform a thorough security analysis focusing on key areas such as system updates, user permissions, antivirus status, firewall settings, and third-party applications*
- **Identify 6 specific security issues** *that pose a risk to the system's integrity*
- *For each identified issue, provide a detailed remediation strategy to address and resolve the vulnerability*

Windows 10/11 Hardening

Many parts can be hardened in Windows 10, but it can be challenging to find them. You can find the way to 10 different settings:

- **System Updates:** Settings > Update & Security > Windows Update
- **Antivirus Status:** Settings > Update & Security > Windows Security > Virus & threat protection
- **Firewall Settings:** Control Panel > System and Security > Windows Defender Firewall
- **AutoRun/AutoPlay:** Control Panel > Hardware and Sound > AutoPlay
- **User Account Control settings:** Control Panel > User Accounts > User Accounts > Change User Account Control settings
- **Password Policies:** Type in `gpedit.msc` in a CLI, then navigate to Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy
- **Audit Policy (logging):** Type in `secpol.msc` in a CLI, then navigate to Local Policies > Audit Policy
- **Guest Account settings:** Run the command `net user guest` in a CLI
- **Administrator Account settings:** Run the command `net user Administrator` in a CLI
- **BitLocker Drive Encryption:** Right-click on any system drive in File Explorer

Local Computer Policy	Policy	Security Setting
Computer Configuration		
Software Settings		
Windows Settings		
Name Resolution		
Scripts (Startup, Logon)		
Deployed		
Security Settings		
Account Policies		
Enforce password history	0 passwords remembered	
Maximum password age	42 days	
Minimum password age	0 days	
Minimum password length	0 characters	
Minimum password length audit	Not Defined	
Password must meet complexity requirements	Disabled	
Relax minimum password length limits	Not Defined	
Store passwords using reversible encryption	Disabled	

Windows 10 Hardening

4. [Audit policy (logging) not enabled]

[Enable (Check Success and failure) audit logging for Audit account logon events, Audit account management, Audit logon events, Audit object access, Audit policy change, Audit privilege use]

Security Settings

> Account Policies

> Local Policies

> **Audit Policy**

> User Rights Assignment

> Security Options

> Windows Defender Firewall with Advanced Security

> Network List Manager Policies

> Public Key Policies

> Software Restriction Policies

> Application Control Policies

> IP Security Policies on Local Computer

> Advanced Audit Policy Configuration

Policy

Audit account logon events

Audit account management

Audit directory service access

Audit logon events

Audit object access

Audit policy change

Audit privilege use

Audit process tracking

Audit system events

Security Setting

No auditing

No auditing

No auditing

No auditing

No auditing

No auditing

No auditing

No auditing

No auditing

No auditing

5. [Guest account enabled]

[For disable Guest account, run the command (net user guest /activ:no) in CLI]

```
C:\Windows\System32>net user guest
User name                Guest
Full Name
Comment                  Built-in account for guest access to the computer/domain
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

Password last set        12-10-2025 08:11:42
Password expires         Never
Password changeable      12-10-2025 08:11:42
Password required         No
User may change password No
```


6. [BitLocker not enabled]

[Turn on BitLocker for all sensitive drives, Control Panel > System and Security > BitLocker Drive Encryption >

- Operating system:** Turn BitLocker on > save the recovery key securely > encrypt used disk space only > new encryption mode > Check run BitLocker system check > continue > restart.
- Fixed data drives:** Turn BitLocker on > Check use a password to unlock the drive and create a password > save the recovery key securely > encrypt used disk space only > new encryption mode > start encrypting.
- Removable data drives:** Turn BitLocker on > Check use a password to unlock the drive and create a password > save the recovery key securely > encrypt used disk space only > compatible mode > start encrypting.]

Operating system drive

C: BitLocker off




Turn BitLocker on

Fixed data drives

Removable data drives - BitLocker To Go

New Volume (F:) BitLocker off



Turn BitLocker on

MacOS Hardening

As Fed F1rst Control Systems embarks on enhancing its workforce productivity tools, the decision to integrate MacBooks into the corporate ecosystem marks a significant technological advancement. Prior to deployment, it is essential to ensure these devices are configured for optimal security to protect sensitive corporate information and maintain compliance with industry standards. Your task is to identify and explain six essential security configurations that must be implemented on the MacBooks before they are distributed to employees, ensuring a secure and efficient work environment.

- **Identify six security configurations** that should be applied to MacBooks before they are deployed to employees
- For each configuration, provide a rationale explaining its importance

MacOS Hardening

1. [Requir automatic OS and security updates]

[It ensure that devices receive the latest security patches and system upgrades. It will help remediating known vulnerabilities.]

2. [Configure secure setup with firmware password]

[It protects the device at boot time, so that unauthorized users cannot start up from external media or change boot settings. It guarding against advanced attacks.]

3. [Turn on firewall]

[it monitors and restricts network traffic to prevent unauthorized access to the MacBook, providing a strong barrier against external threats.]

MacOS Hardening

4. [Enable FileVault]

[It encrypts the entire drive. It ensuring that, if a MacBook is lost or stolen, the data remains inaccessible to unauthorized parties.]

5. [Enforce strong password policies]

[Requires robust, complex passwords, regular rotation, and avoids reuse. This reduce the chance that an attacker could compromise accounts through guessing or credential stuffing.]

6. [Enable system integrity protection]

[Prevents unauthorized software or users from modifying critical system files. It protecting the operating system's core.]

Email Policy

In an era where email is a critical communication tool for businesses, it's equally a prime target for cyber threats, potentially compromising sensitive information. Fed F1rst Control Systems recognizes the importance of securing its email communications to protect against such vulnerabilities. Your task is to contribute to the development of an email policy by specifying five security-related items that should be included. These items will guide employee behavior regarding the use of corporate email systems, aiming to minimize security risks and safeguard company data.

- **Identify five security-related items** that should be included in the company's email policy
- Each item should address a specific aspect or behavior related to email use

Email Policy

1. [**Strong Password Management** : Employees must create strong, unique passwords for their email accounts and avoid reusing passwords across different systems. Passwords should include a mix of numbers, letters and special characters and be updated regularly to prevent unauthorized access.]
2. [**Email Encryption** : Emails containing confidential company data must be encrypted. Encryption ensures that even if a message is intercepted, its contents remain unreadable to unauthorized parties.]
3. [**Caution with links and attachments** : Employees should be instructed to exercise caution when opening email attachments or clicking links, especially from unknown or unexpected sources. Attachments and links can deliver malware or lead to phishing sites that harvest credentials.]
4. [**Incident reporting procedures** : Train employees to recognize phishing attempts and suspicious email behavior, and clear instructions should be provided for reporting suspicious emails, suspected phishing attempts, or other related security incidents. Employees must know who to contact and what steps to take if they encounter suspicious activity.]
5. [**Approved device and network use** : Corporate email access must be restricted to approved devices and secure network, employees are to avoid accessing corporate email on public wifi networks, unauthorized or personal devices and use secure connections or VPNs whenever possible. To prevent interception and credential theft.]

BYOD Policy

As Fed First Control Systems embraces a Bring Your Own Device (BYOD) policy to enhance flexibility and productivity, the security of corporate data on employee-owned devices becomes a critical concern. These devices, ranging from smartphones to laptops, introduce various security challenges that must be addressed to protect both the company's and employees' information. Your role is to contribute to the development of a robust BYOD policy by writing the Security section. This will ensure that employees can use their own devices without compromising the organization's digital security.

- Draft the **Security section of the BYOD policy**
- Cover Apple and Android smartphones, and Windows 11 and macOS laptops
- Include **6 security measures** relevant to these devices
- Focus on diverse security aspects such as access, data protection, and incident management

BYOD Policy

1. [**Device Authentication and access control** : All device must be secured with strong authentication mechanisms. All employees personal devices must be registered with the companye's Mobile Device Management (MDM) system before accessing corporate resource. Devices must authenticate using secure methods such as MFA or digital certificates. This enables centralized control for configaration, security monitoring, and policy enforcement.]
2. [**Data Encryption** : Full disk encryption is mandatory for all devices. For IOS/macOS FileVault and default IOS encryption settings, for android AES-based device encryption, for windows 11 BitLocker must be enabled, also all network communications with corporate system must occur over encrypted connections (HTTPS, SSL/TLS or VPN).]
3. [**Application management and whitelisting** : only approved business applications can be installed for accessing company data, rooted devices are stricthy prohibited, as these compromise device integrity and corporate data protection.]
4. [**Data backup and protection** : To prvent loss or misuse of corporate data, business related data must only be bucked up using company approved secure cloud or local solutions. Employees must promptly report any suspected data loss or exposure to the IT security team.]
5. [**Incident response and reporting** : In case of suspected data breach, malware infection, or unauthorised access employees must promptly the IT security team. The IT department will conduct investigations and take corrective actions as needed.]
6. [**Monitoring and compliance** : The company retains the right to monitor access to corporate resources and verify compliance with BYOD security standards. Non-compliance devices may be denied network access untill security issues are resolved.]

Windows Desktop Compliance

Maintaining robust security measures across all devices is crucial. As part of the organization's commitment to cybersecurity, adhering to the National Institute of Standards and Technology (NIST) guidelines is a top priority. Your task involves evaluating a Windows 10 desktop against specific *NIST SP 800-53 Rev. 5* controls. This exercise is designed to assess the desktop's compliance with established security standards, ensuring the integrity, confidentiality, and availability of the system's information.

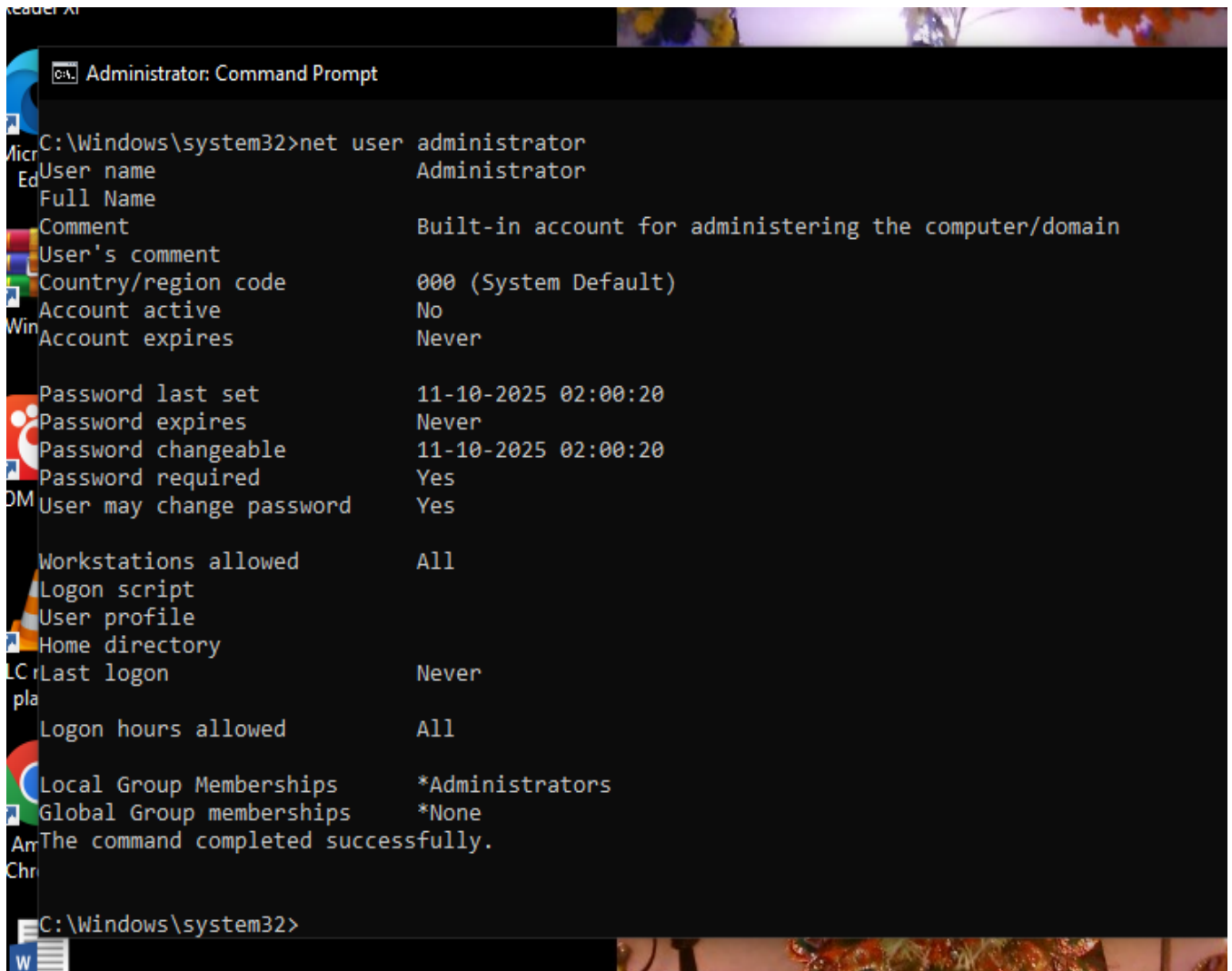
- **Review the provided 14-item list** from *NIST SP 800-53 Rev. 5*
- Evaluate a Windows 10 machine for compliance with each item
- For each item, determine if it is:
 - **Met:** The Windows 10 machine complies with the NIST guideline
 - **Not Met:** The Windows 10 machine does not comply with the NIST guideline
 - **NA (Not Applicable):** The NIST guideline does not apply to this Windows 10 machine
- Add Screenshot for each item

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Built-In Administrator account is disabled	Met
Windows Firewall is enabled	Met
Automatic updates are enabled	Not Met
User Account Control (UAC) is enabled	Not Met
Strong password policies are enforced	Not Met
Guest account is disabled	Met
System logging and auditing are enabled	Not Met
Windows Defender Antivirus is enabled and up to date	Met
Remote Desktop Services are configured securely	Not Met
Internet Explorer Enhanced Security Configuration (IE ESC) is enabled	NA
USB ports are disabled or restricted to authorized devices only	Not Met
Network access controls are implemented, including VLAN segmentation and port security	Not Met
Remote Registry service is disabled	Met
Windows Updates are configured to download and install updates automatically	Not Met

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Built-In Administrator account is disabled	Met

A screenshot of a Windows 10 desktop environment. In the foreground, a black Command Prompt window titled "Administrator: Command Prompt" is open. The window shows the output of the command "net user administrator", displaying details for the built-in administrator account. The desktop background is a scenic image of autumn foliage. Several application icons are visible on the left side of the taskbar, including Microsoft Edge, Word, and Chrome. The taskbar at the bottom shows the Start button and several pinned applications.

```
C:\Windows\system32>net user administrator
User name                Administrator
Full Name
Comment                  Built-in account for administering the computer/domain
User's comment
Country/region code      000 (System Default)
Account active            No
Account expires           Never

Password last set         11-10-2025 02:00:20
Password expires          Never
Password changeable       11-10-2025 02:00:20
Password required         Yes
User may change password  Yes

Workstations allowed      All
Logon script
User profile
Home directory
Last logon                Never

Logon hours allowed       All

Local Group Memberships   *Administrators
Global Group memberships  *None
The command completed successfully.

C:\Windows\system32>
```



Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Windows Firewall is enabled	Met

Windows Defender Firewall

← → ▾ ▴ > Control Panel > System and Security > Windows Defender Firewall

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks Not connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active private networks: None

Notification state: Notify me when Windows Defender Firewall blocks a new app

Guest or public networks Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state: On

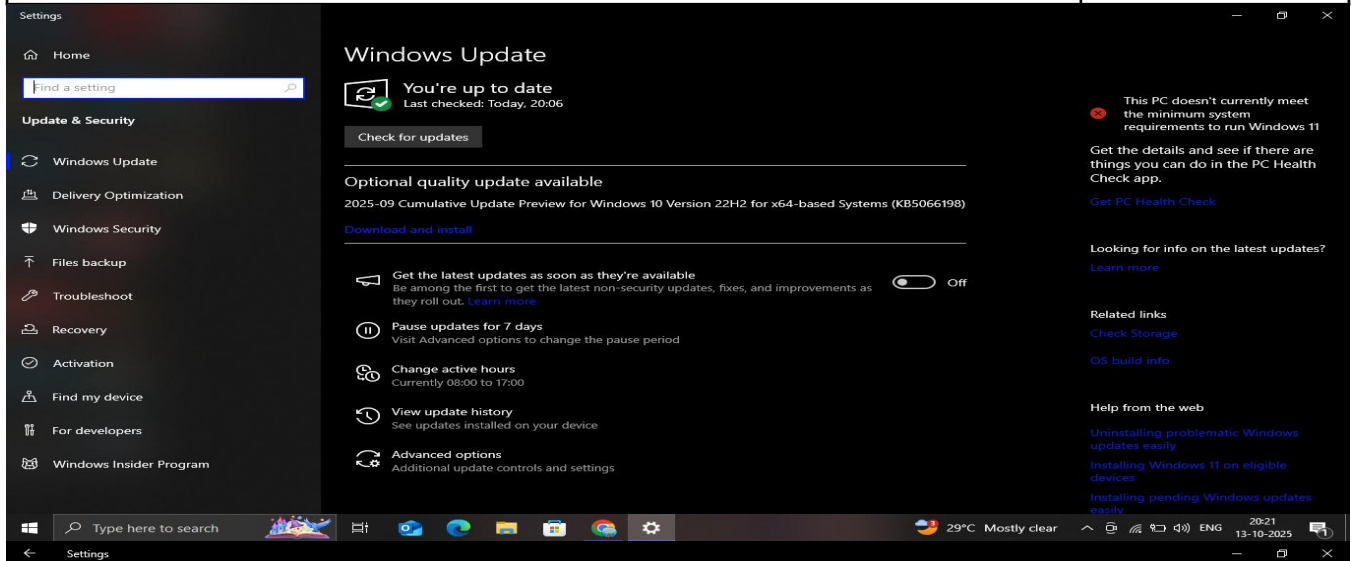
Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active public networks: ABHIJIT1

Notification state: Notify me when Windows Defender Firewall blocks a new app

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Automatic updates are enabled	Not Met



The screenshot shows the Windows Settings application, specifically the 'Windows Update' section. The left sidebar lists various settings categories, with 'Windows Update' selected. The main pane displays the 'Windows Update' status, indicating 'You're up to date' with a last check on 'Today, 20:06'. Below this, there's a 'Check for updates' button. Further down, an 'Optional quality update available' is listed for '2025-09 Cumulative Update Preview for Windows 10 Version 22H2 for x64-based Systems (KB5066198)', with a 'Download and install' link. A section titled 'Get the latest updates as soon as they're available' has a toggle switch set to 'Off'. Other options include 'Pause updates for 7 days', 'Change active hours', 'View update history', and 'Advanced options'. On the right side of the settings pane, there are links for 'Get the details and see if there are things you can do in the PC Health Check app.', 'Get PC Health Check', 'Looking for info on the latest updates?', 'Learn more', 'Related links' (including 'Check Storage' and 'OS build info'), and 'Help from the web' (including 'Uninstalling problematic Windows updates easily', 'Installing Windows 11 on eligible devices', and 'Installing pending Windows updates easily'). The taskbar at the bottom shows the search bar, task view button, and several pinned apps, along with system tray icons for weather (29°C Mostly clear), network, volume, and language (ENG), and the date/time (20:21 13-10-2025).

Advanced options

Update options

Receive updates for other Microsoft products when you update Windows

☐ Off

Download updates over metered connections (extra charges may apply)

☐ Off

Restart this device as soon as possible when a restart is required to install an update. Windows will display a notice before the restart, and the device must be on and plugged in.

☐ Off

Note: Windows Update might update itself automatically first when checking for other updates.

Configure automatic device setup after an update under the Privacy section in [Sign-in options](#)

[Get help](#)

Update notifications

Show a notification when your PC requires a restart to finish updating

☐ Off

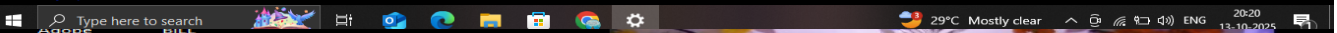
Pause updates

Temporarily pause updates from being installed on this device for up to 35 days. When you reach the pause limit, your device will need to get new updates before you can pause again.

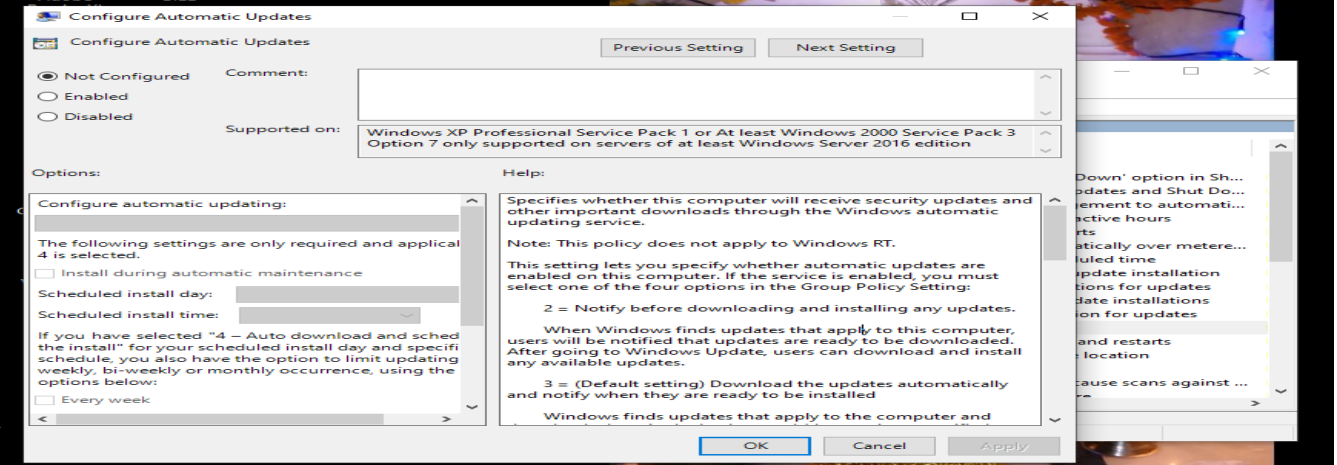
Pause until

Select date ▼

Delivery Optimization



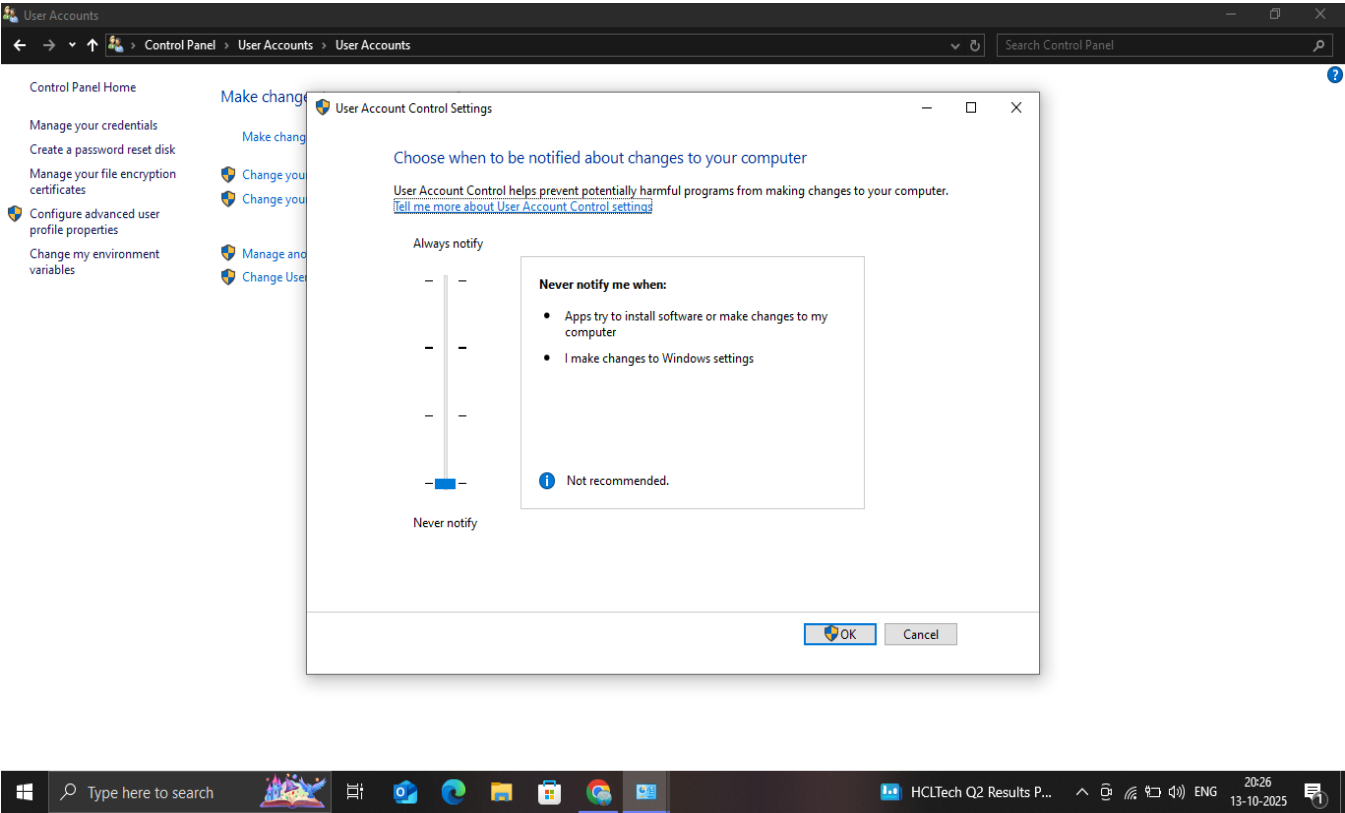
The taskbar shows the search bar, task view button, and several pinned apps (Edge, File Explorer, etc.), along with system tray icons for weather (29°C Mostly clear), network, volume, and language (ENG), and the date/time (20:20 13-10-2025).



The screenshot shows the Group Policy Editor window, specifically the 'Configure Automatic Updates' policy. The policy is currently set to 'Not Configured'. The 'Supported on:' field shows 'Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3 Option 7 only supported on servers of at least Windows Server 2016 edition'. The 'Options:' section has a dropdown menu set to '4 - Auto download and schedule the install'. The 'Help:' section provides detailed information about the policy, including a note that it does not apply to Windows RT, and explains the four options: 1 (Default setting), 2 (Notify before downloading and installing any updates), 3 (Default setting), and 4 (Auto download and schedule the install). The 'Help:' section also includes a 'Note: This policy does not apply to Windows RT.' and a 'This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:'.

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
User Account Control (UAC) is enabled	Not Met



Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Strong password policies are enforced	Not Met

Local Group Policy Editor

File Action View Help

Local Computer Policy

Computer Configuration

Windows Settings

Security Settings

Account Policies

Local Policies

Windows Settings

Network Settings

Public Settings

Software Settings

Application Settings

IP Security

Advanced Settings

Policy-based Settings

Administrative Settings

User Configuration

Policy

Enforce password history

Maximum password age

Minimum password age

Minimum password length

Minimum password length audit

Password must meet complexity requirements

Relax minimum password length limits

Store passwords using reversible encryption

Security Setting

0 passwords remembered

42 days

0 days

0 characters

Not Defined

Disabled

Not Defined

Disabled

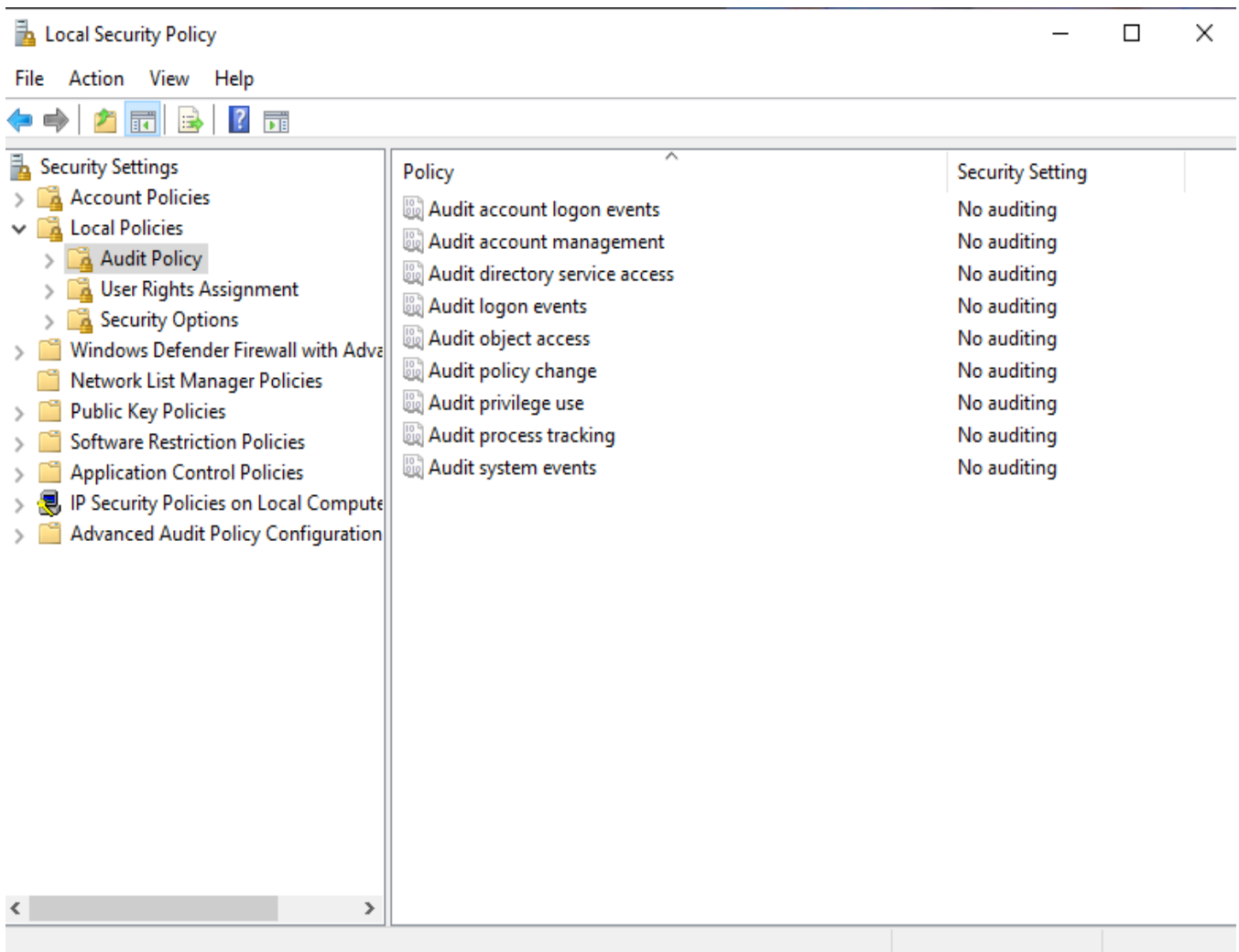
Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Guest account is disabled	Met

```
Administrator: Command Prompt
C:\Windows\system32>net user guest
User name                Guest
Full Name
Comment                  Built-in account for guest access to the computer/domain
User's comment
Country/region code      000 (System Default)
Account active            No
Account expires           Never
Password last set        13-10-2025 20:32:31
Password expires          Never
Password changeable       13-10-2025 20:32:31
Password required         No
User may change password  No
Workstations allowed      All
Logon script
User profile
Home directory
Last logon               Never
Logon hours allowed       All
Local Group Memberships  *Guests
Global Group memberships *None
The command completed successfully.
C:\Windows\system32>
```

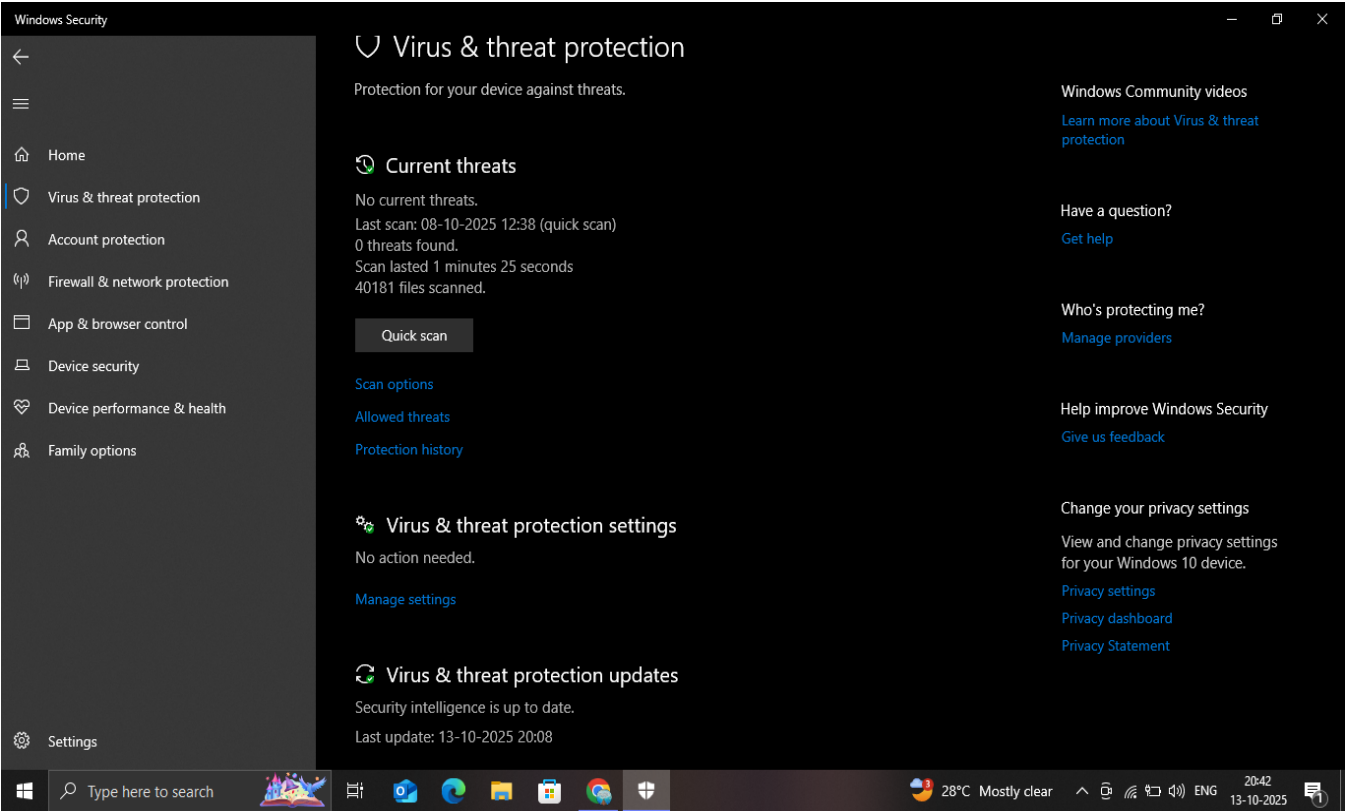
Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
System logging and auditing are enabled	Not Met



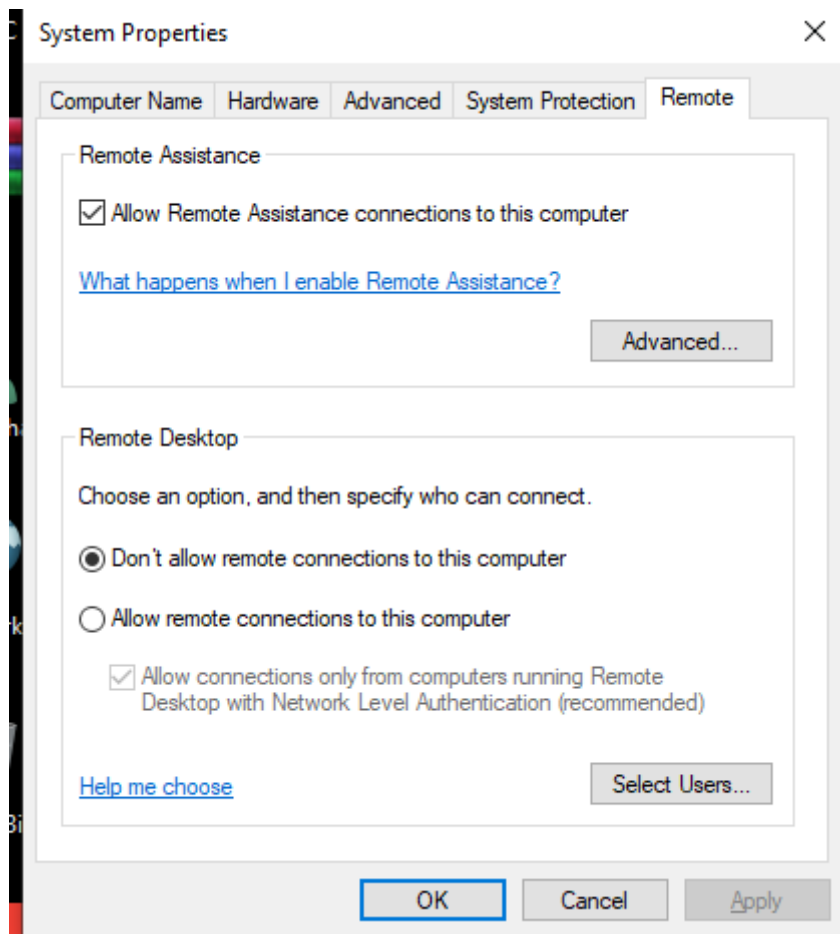
Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Windows Defender Antivirus is enabled and up to date	Met



Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Remote Desktop Services are configured securely	Not Met



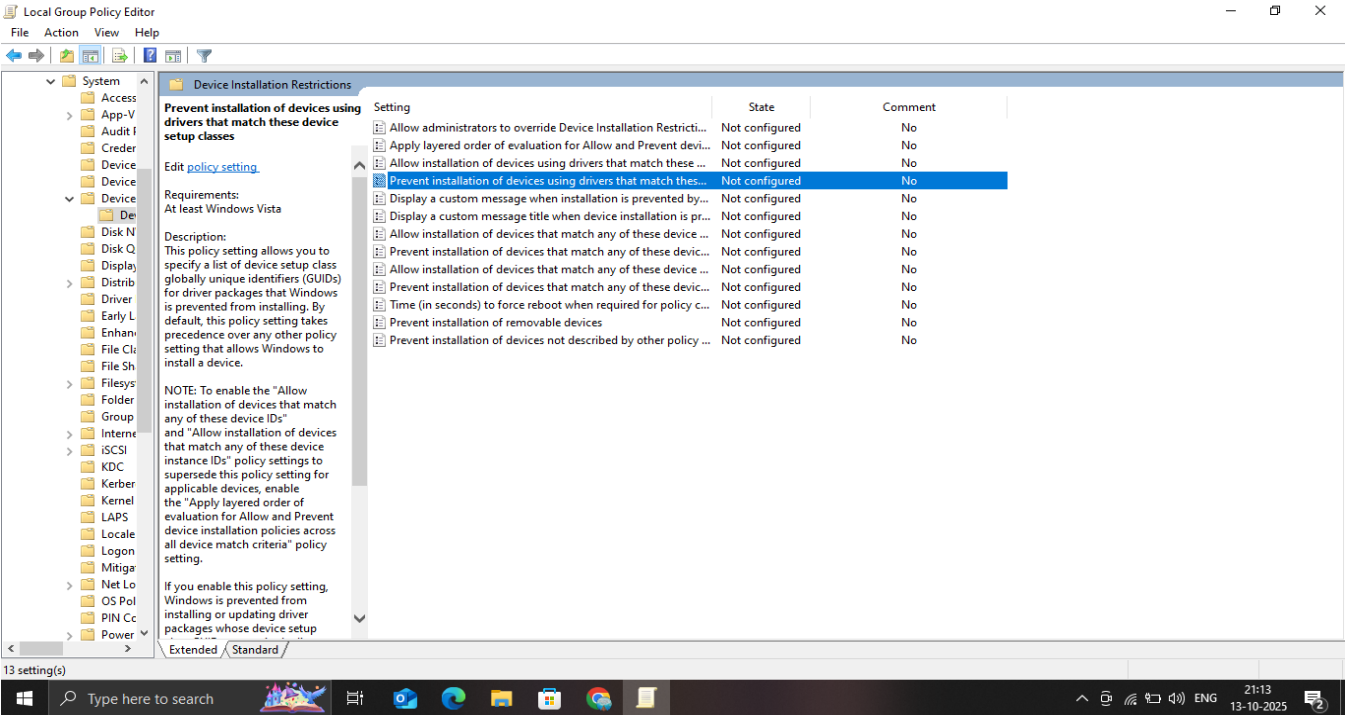
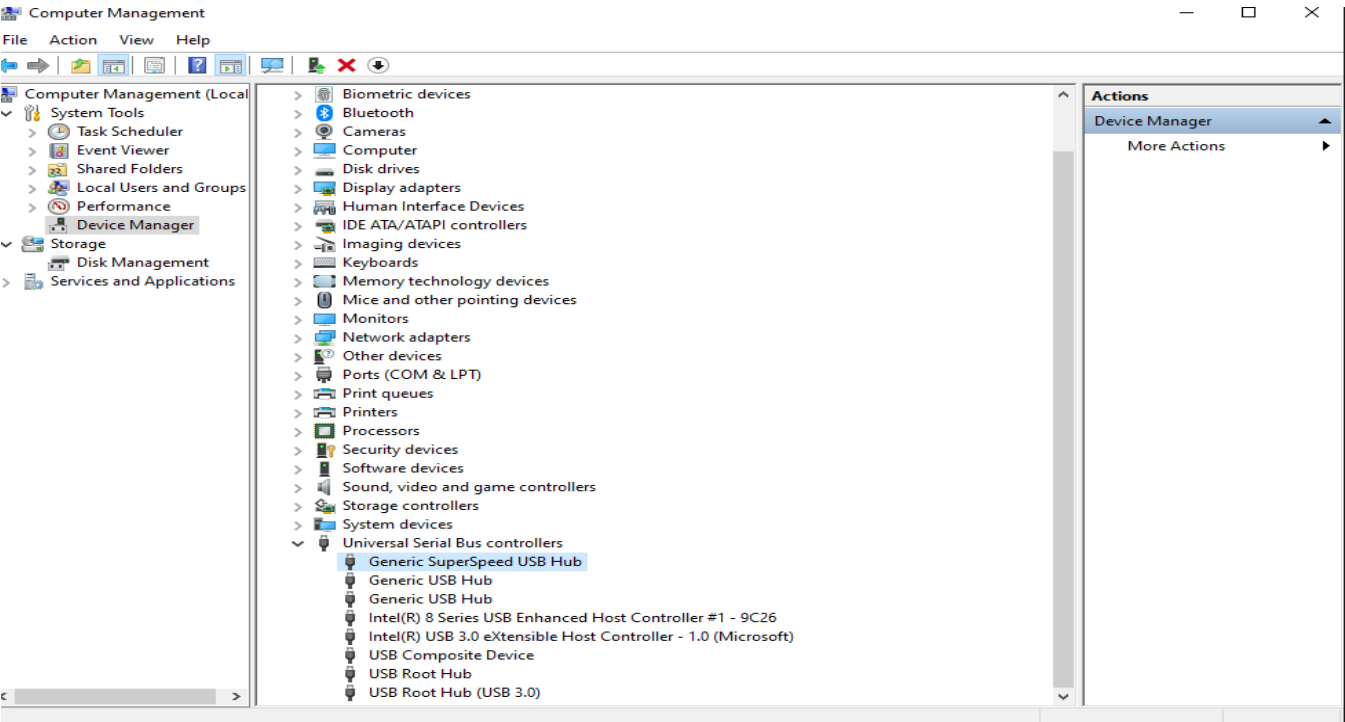
Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Internet Explorer Enhanced Security Configuration (IE ESC) is enabled	NA

[Screenshot]

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
USB ports are disabled or restricted to authorized devices only	Not Met



Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Network access controls are implemented, including VLAN segmentation and port security	Not Met

[Screenshot]

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Remote Registry service is disabled	Met

Services

File Action View Help

Services (Local)

Services (Local)

Remote Registry

Description:
Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log On As
Portable Device Enumerator...	Enforces gr...		Manual (Trig...	Local Syste...
Power	Manages p...	Running	Automatic	Local Syste...
Print Spooler	This service ...	Running	Automatic	Local Syste...
Printer Extensions and Notif...	This service ...		Manual	Local Syste...
PrintWorkflow_4bd15a	Provides su...		Manual (Trig...	Local Syste...
Problem Reports Control Pa...	This service ...		Manual	Local Syste...
Program Compatibility Assi...	This service ...	Running	Manual	Local Syste...
Quality Windows Audio Vid...	Quality Win...		Manual	Local Service
Radio Management Service	Radio Mana...	Running	Manual	Local Service
Recommended Troublesho...	Enables aut...		Manual	Local Syste...
Remote Access Auto Conne...	Creates a co...		Manual	Local Syste...
Remote Access Connection...	Manages di...	Running	Automatic	Local Syste...
Remote Desktop Configurati...	Remote Des...		Manual	Local Syste...
Remote Desktop Services	Allows user...		Manual	Network S...
Remote Desktop Services U...	Allows the r...		Manual	Local Syste...
Remote Procedure Call (RPC)	The RPCSS s...	Running	Automatic	Network S...
Remote Procedure Call (RP...	In Windows...		Manual	Network S...
Remote Registry	Enables rem...	Disabled	Local Service	
Retail Demo Service	The Retail D...		Manual	Local Syste...
Routing and Remote Access	Offers routi...		Disabled	Local Syste...
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network S...
Samsung UPD Utility Service		Running	Automatic	Local Syste...
Secondary Logon	Enables star...		Manual	Local Syste...
Secure Socket Tunneling Pr...	Provides su...	Running	Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local Syste...
Security Center	The WSCSV...	Running	Automatic (...)	Local Service
Sensor Data Service	Delivers dat...		Manual (Trig...	Local Syste...
Sensor Monitoring Service	Monitors va...		Manual (Trig...	Local Service
Sensor Service	A service fo...		Manual (Trig...	Local Syste...

Extended / Standard /

Windows Taskbar

Type here to search

27°C Mostly clear

21:21 13-10-2025

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Windows Updates are configured to download and install updates automatically	Not Met

Settings

Home

Find a setting

Update & Security

Windows Update

Delivery Optimization

Windows Security

Files backup

Troubleshoot

Recovery

Activation

Find my device

For developers

Windows Insider Program

Windows Update

You're up to date

Last checked: Today, 20:06

Check for updates

Optional quality update available

2025-09 Cumulative Update Preview for Windows 10 Version 22H2 for x64-based Systems (KB5066198)

Download and install

Get the latest updates as soon as they're available

Be among the first to get the latest non-security updates, fixes, and improvements as they roll out. [Learn more](#)

Off

Pause updates for 7 days

Visit Advanced options to change the pause period

Change active hours

Currently 08:00 to 17:00

View update history

See updates installed on your device

Advanced options

Additional update controls and settings

This PC doesn't currently meet the minimum system requirements to run Windows 11

Get the details and see if there are things you can do in the PC Health Check app.

Get PC Health Check

Looking for info on the latest updates?

Learn more

Related links

Check Storage

OS build info

Help from the web

Uninstalling problematic Windows updates easily

Installing Windows 11 on eligible devices

Installing pending Windows updates easily

Note: Windows Update might update itself automatically first when checking for other updates.

Configure automatic device setup after an update under the Privacy section in [Sign-in options](#)

Get help

Advanced options

Update options

Receive updates for other Microsoft products when you update Windows

Off

Download updates over metered connections (extra charges may apply)

Off

Restart this device as soon as possible when a restart is required to install an update. Windows will display a notice before the restart, and the device must be on and plugged in.

Off

Update notifications

Show a notification when your PC requires a restart to finish updating

Off

Pause updates

Temporarily pause updates from being installed on this device for up to 35 days. When you reach the pause limit, your device will need to get new updates before you can pause again.

Pause until

Select date

Delivery Optimization

Configure Automatic Updates

Configure Automatic Updates

Previous Setting

Next Setting

Not Configured

Comment:

Enabled

Supported on:

Disabled

Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3 Option 7 only supported on servers of at least Windows Server 2016 edition

Options:

Help:

Configure automatic updating:

The following settings are only required and applicable if 4 is selected.

Install during automatic maintenance

Scheduled install day:

Scheduled install time:

If you have selected "4 - Auto download and schedule the install" for your scheduled install day and specific schedule, you also have the option to limit updating weekly, bi-weekly or monthly occurrence, using the options below:

Every week

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading and installing any updates.

When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.

3 = (Default setting) Download the updates automatically and notify when they are ready to be installed

Windows finds updates that apply to the computer and

OK

Cancel

Apply

Windows Desktop Compliance

Ensuring the Windows 10 desktop at Fed First Control Systems meets all *NIST SP 800-53 Rev. 5* controls is vital for maintaining a strong security posture. After identifying controls that are not met, the next step is to outline straightforward remediation actions. Simplifying the remediation process by focusing on concise, one-line solutions will facilitate a more efficient path to compliance. This approach enables you to quickly address vulnerabilities and enhance the system's security with minimal complexity.

- Review the list of *NIST SP 800-53 Rev. 5* controls previously identified as "Not Met"
- For **each control not met**, provide a short remediation solution. This should be a direct action that can be taken to address the gap
- Ensure the solution is specific enough to be actionable and relevant to a Windows 10 environment

Windows Desktop Compliance

Write your remediation solutions below. **You should write one solution to one row, adding rows as necessary.**

[Automatic updates are not enabled]: [Press Windows + I > Update & Security > Windows Update > Click Advanced options > Automatically download updates, even over metered data connections" is ON
Windows + R and type gpedit.msc > Computer Configuration > Administrative Templates > Windows Components > Windows Update > Configure Automatic Updates > Enabled > Click Apply and OK]

[User Account Control (UAC) is not enabled]: [Control Panel > User Accounts > User Accounts > Change User Account Control settings > Alwaysse notify]

[Strong password policies are not configured]: [Type in `gpedit.msc` in a CLI, then navigate to Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy > Set Maximum password age to 90 days > Minimum password lenth to 8 characters > Minimum password lenth audit to 8 characters > Password must meet complexcity requirments to enable]

[System logging and auditing are not configured]: [Type in `secpol.msc` in a CLI, then navigate to Local Policies > Audit Policy > Enable (Check Success and failure) audit logging for Audit account logon events, Audit account management, Audit logon events, Audit object access, Audit policy change, Audit privilege use]

[Remote Desktop Services are not configured securely]: [Press Windows + R, type sysdm.cpl > Remote tab > Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)]

[USB ports are not disabled or restricted to authorized devices only]: [Disable All USB Ports : Device Manager > Universal Serial Bus controllers > right-click > Disable Device
Restrict USB Ports : Windows + R, type gpedit.msc > Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions > Enable "Prevent installation of devices not described by other policy settings".
Enable "Allow installation of devices that match any of these device IDs
]

[Windows Updates are not configured to download and install updates automatically]: [Settings > Update & Security > Windows Update > Advanced options > select Automatic (recommended)

Open gpedit.msc > Computer Configuration > Administrative Templates > Windows Components > Windows Update > Configure Automatic Updates > Enable > Apply]

Linux Compliance

As part of Fed F1rst Control Systems' ongoing commitment to cybersecurity excellence, aligning with the Cybersecurity Maturity Model Certification (CMMC) framework is essential. This task is designed to evaluate the security posture of a provided CentOS/Ubuntu/Kali Virtual Machine (VM) against a set of 15 CMMC controls. Your objective is to assess each item's compliance, ensuring that the VM meets the stringent requirements set forth for protecting sensitive information. This exercise is crucial for identifying gaps in security practices and ensuring that the VM is fortified against potential cyber threats.

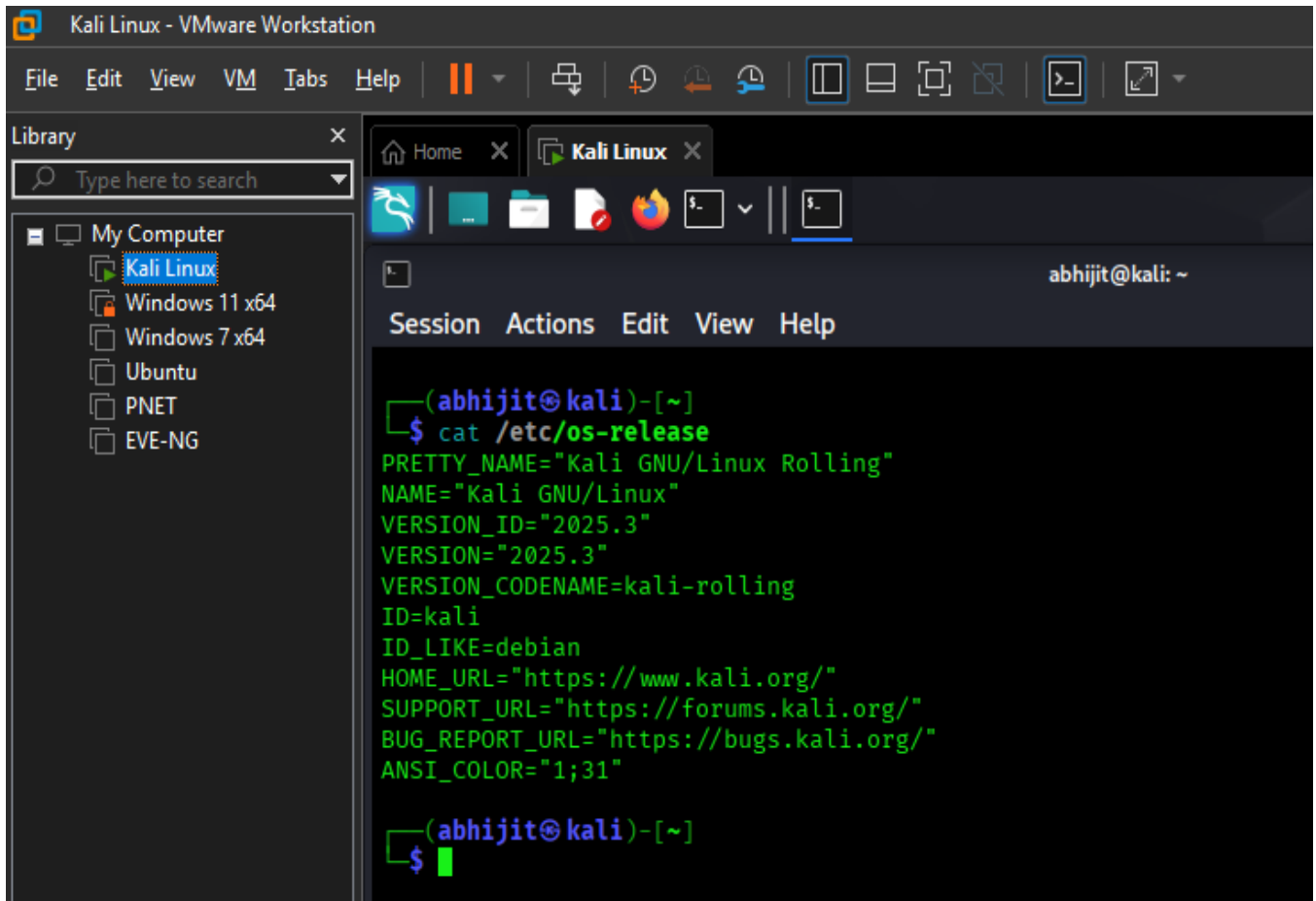
- Review the provided 15-item list of CMMC controls
- Assess a Linux VM for compliance with each listed control
- For each control, determine if it is:
 - **Met:** The Kali Linux VM complies with the CMMC control
 - **Not Met:** The Kali Linux VM does not comply with the CMMC control
 - **NA (Not Applicable):** The CMMC control does not apply to this CentOS VM

Linux Compliance

Linux CMMC Requirements	Met/Not Met
Current on security updates	Met
Ensure separate partition exists for /var	Not Met
Disable Automounting of drives	Not Met
Ensure AIDE is installed	Met
Ensure daytime services are not enabled	Met
Ensure echo services are not enabled	Met
Ensure tftp server is not enabled	Met
Ensure CUPS is not enabled	Met
Ensure DHCP Server is not enabled	Met
Ensure FTP Server is not enabled	Met
Ensure Samba is not enabled	Met
Ensure TCP Wrappers is installed	Met
Ensure DCCP is disabled	Met
Ensure iptables is installed	Met
Ensure audit log storage size is configured	Not Met
Ensure audit logs are not automatically deleted	Not Met

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Current on security updates	Met

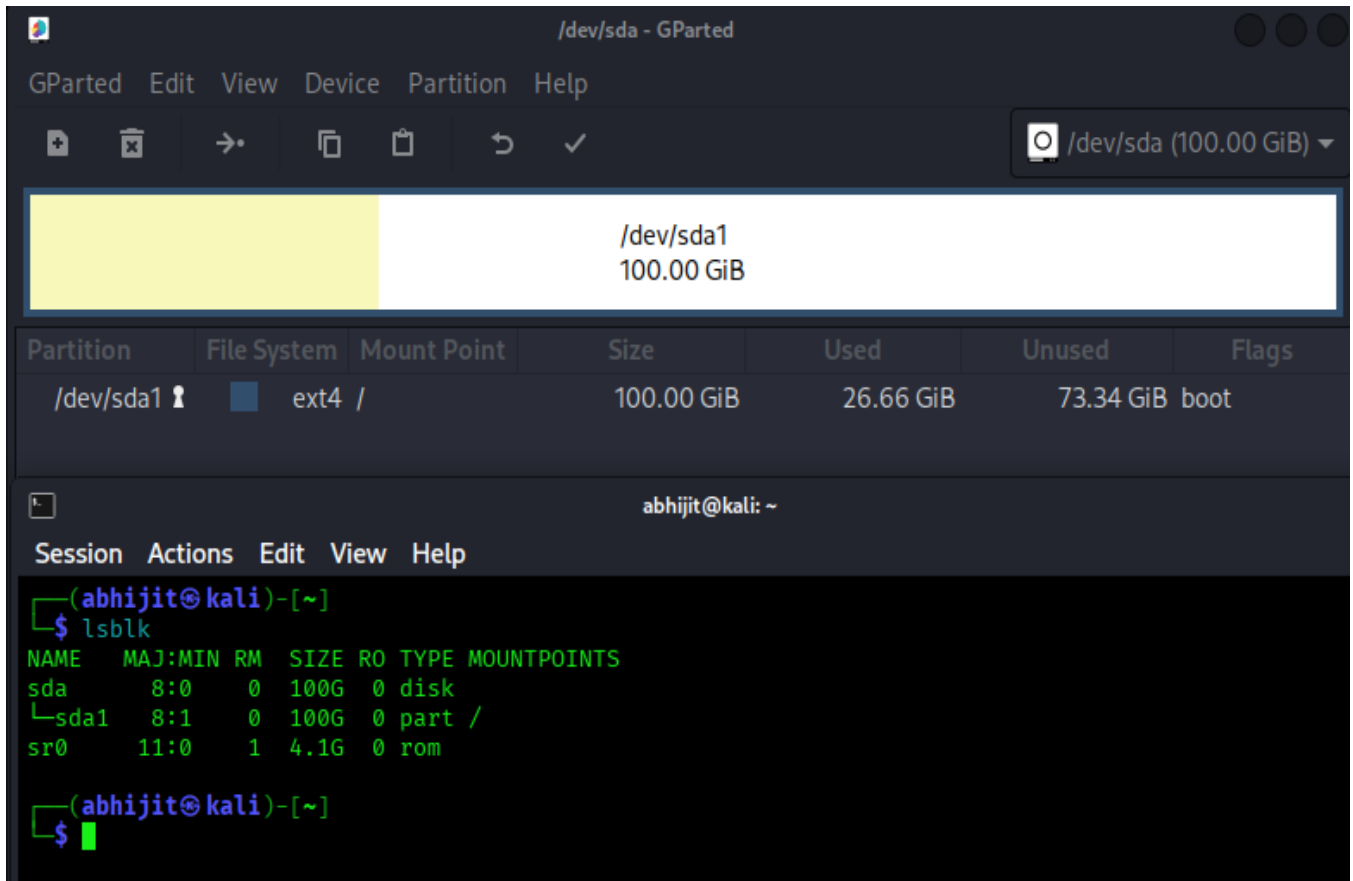


The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The interface includes a menu bar (File, Edit, View, VM, Tabs, Help), a toolbar with various VM controls, and a Library pane on the left listing virtual machines: My Computer, Kali Linux (selected), Windows 11 x64, Windows 7 x64, Ubuntu, PNET, and EVE-NG. The main window displays the Kali Linux desktop environment. A terminal window is open, showing the command `cat /etc/os-release` and its output:

```
(abhiжит@kali)-[~]  
$ cat /etc/os-release  
PRETTY_NAME="Kali GNU/Linux Rolling"  
NAME="Kali GNU/Linux"  
VERSION_ID="2025.3"  
VERSION="2025.3"  
VERSION_CODENAME=kali-rolling  
ID=kali  
ID_LIKE=debian  
HOME_URL="https://www.kali.org/"  
SUPPORT_URL="https://forums.kali.org/"  
BUG_REPORT_URL="https://bugs.kali.org/"  
ANSI_COLOR="1;31"  
  
(abhiжит@kali)-[~]  
$
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure separate partition exists for /var	Not Met



The screenshot displays two windows from a Kali Linux environment. The top window is GParted, titled '/dev/sda - GParted', showing a single partition /dev/sda1 of 100.00 GiB. Below the visual representation is a table with the following data:

Partition	File System	Mount Point	Size	Used	Unused	Flags
/dev/sda1	ext4	/	100.00 GiB	26.66 GiB	73.34 GiB	boot

The bottom window is a terminal titled 'abhijit@kali: ~'. It shows the command 'lsblk' being executed, with the following output:

```
(abhijit@kali)-[~]  
$ lsblk  
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS  
sda    8:0    0 100G 0 disk  
└─sda1  8:1    0 100G 0 part /  
sr0    11:0    1  4.1G 0 rom
```

The terminal prompt is currently at the root directory (~).

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Disable Automounting of drives	

[Screenshot]

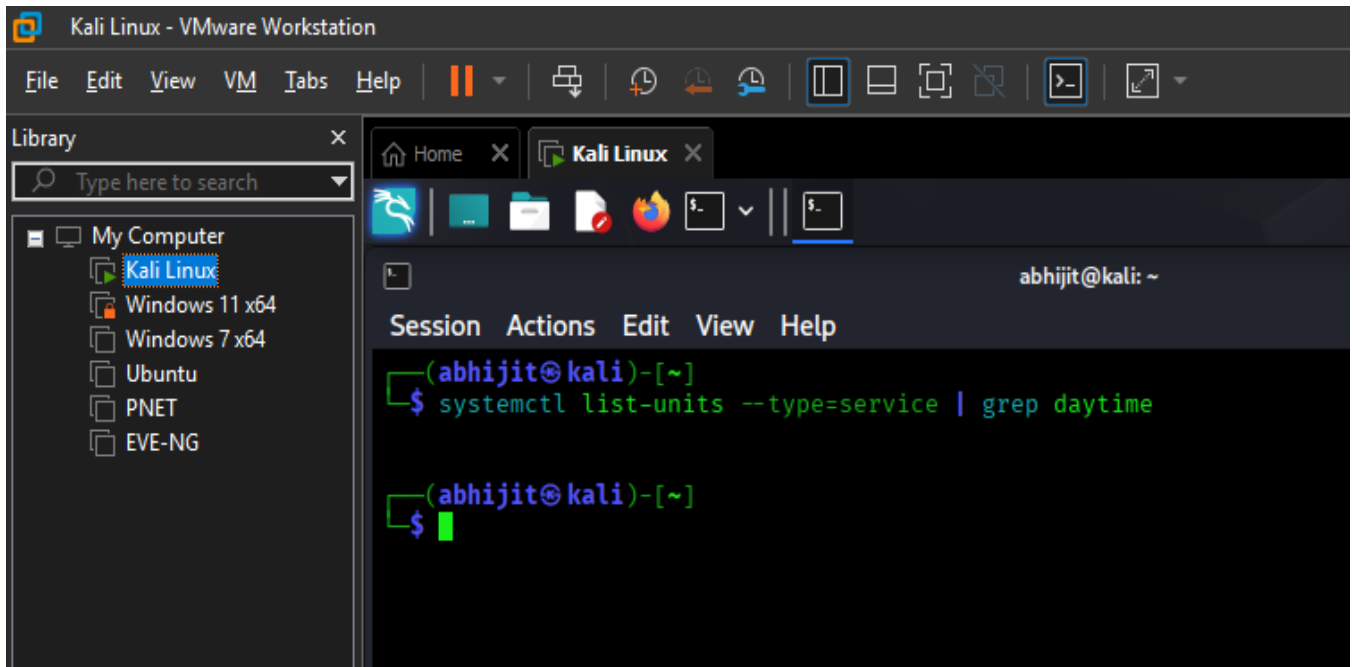
Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure AIDE is installed	Met

```
abhijit@kali: ~  
Session Actions Edit View Help  
(abhijit@kali)-[~]  
$ aide -v  
AIDE 0.19.2  
  
Compile-time options:  
use pcre2: mandatory  
use pthread: mandatory  
use zlib compression: yes  
use POSIX ACLs: yes  
use SELinux: yes  
use xattr: yes  
use POSIX 1003.1e capabilities: yes  
use e2fsattrs: yes  
use cURL: no  
use Nettle crypto library: yes  
use GNU crypto library: no  
use Linux Auditing Framework: yes  
use locale: no  
syslog ident: aide  
syslog logopt: LOG_CONS  
syslog priority: LOG_NOTICE  
default syslog facility: LOG_LOCAL0  
  
Default config values:  
config file: <none>  
database_in: <none>  
database_out: <none>  
  
Available compiled-in attributes:  
acl: yes  
xattrs: yes  
selinux: yes
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure daytime services are not enabled	Met

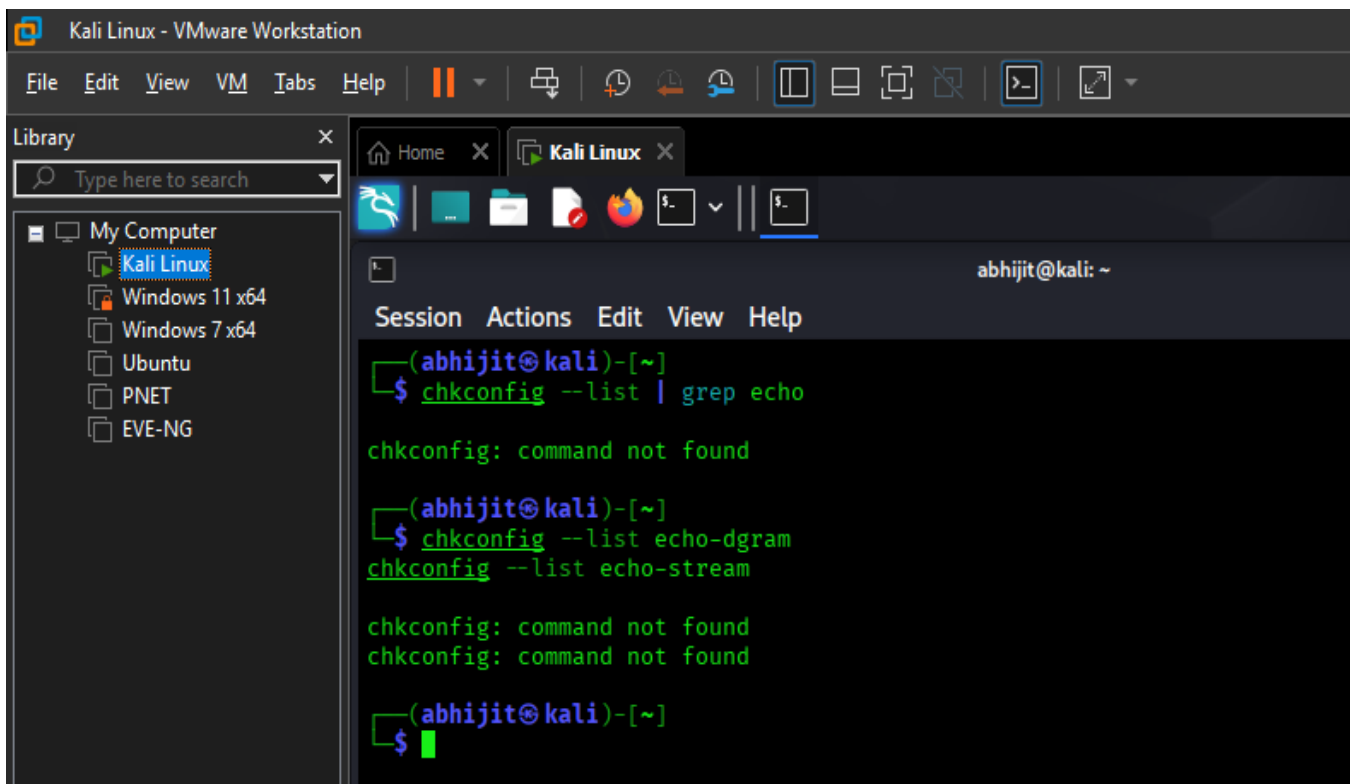


The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The interface includes a menu bar (File, Edit, View, VM, Tabs, Help), a toolbar with various icons, and a left-hand library pane. The library pane shows a tree view under 'My Computer' with 'Kali Linux' selected. The main window displays a terminal session with the following content:

```
abhijit@kali: ~  
Session Actions Edit View Help  
(abhijit@kali)-[~]  
$ systemctl list-units --type=service | grep daytime  
  
(abhijit@kali)-[~]  
$
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure echo services are not enabled	Met

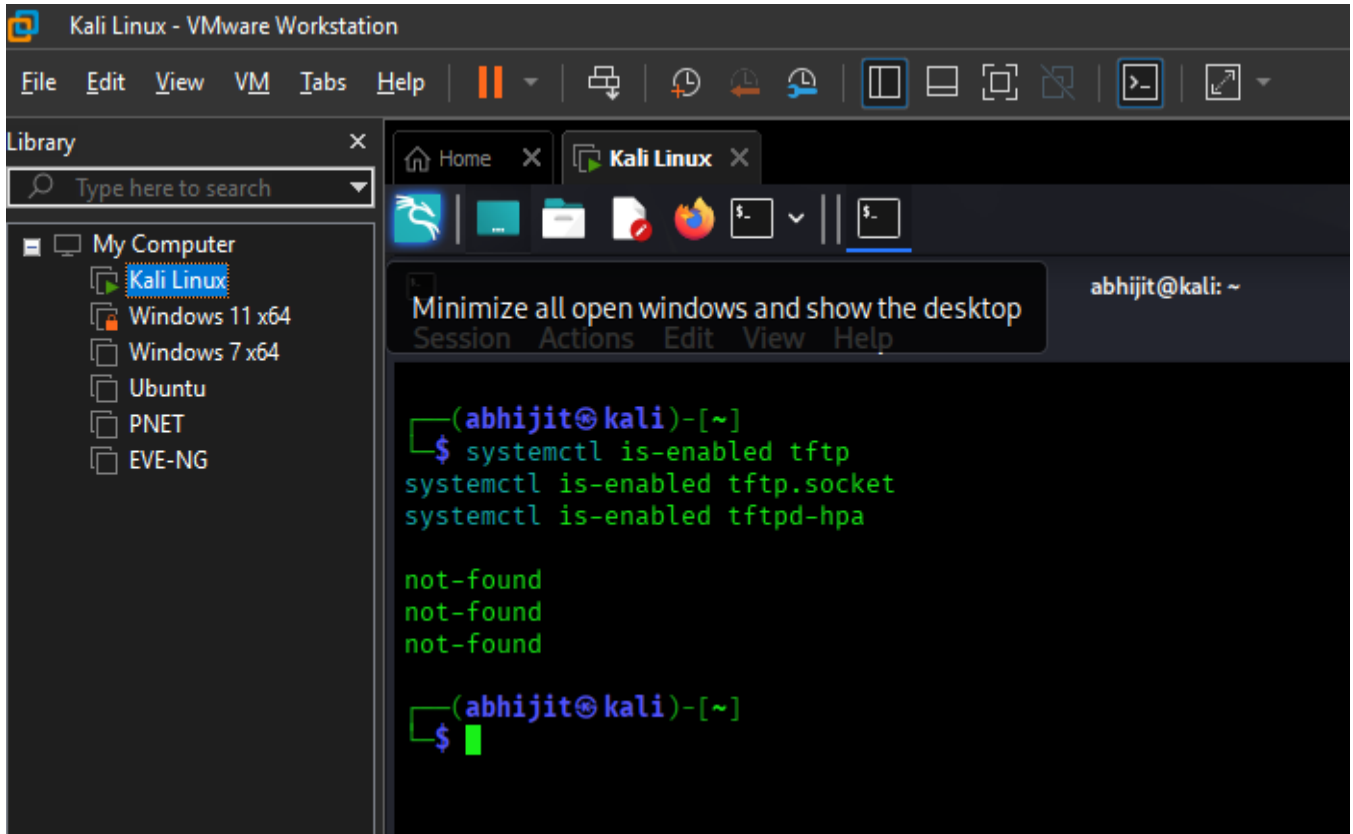


The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The terminal window displays the following commands and output:

```
(abhijit@kali)-[~]  
$ chkconfig --list | grep echo  
  
chkconfig: command not found  
  
(abhijit@kali)-[~]  
$ chkconfig --list echo-dgram  
chkconfig --list echo-stream  
  
chkconfig: command not found  
chkconfig: command not found  
  
(abhijit@kali)-[~]  
$
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure tftp server is not enabled	Met

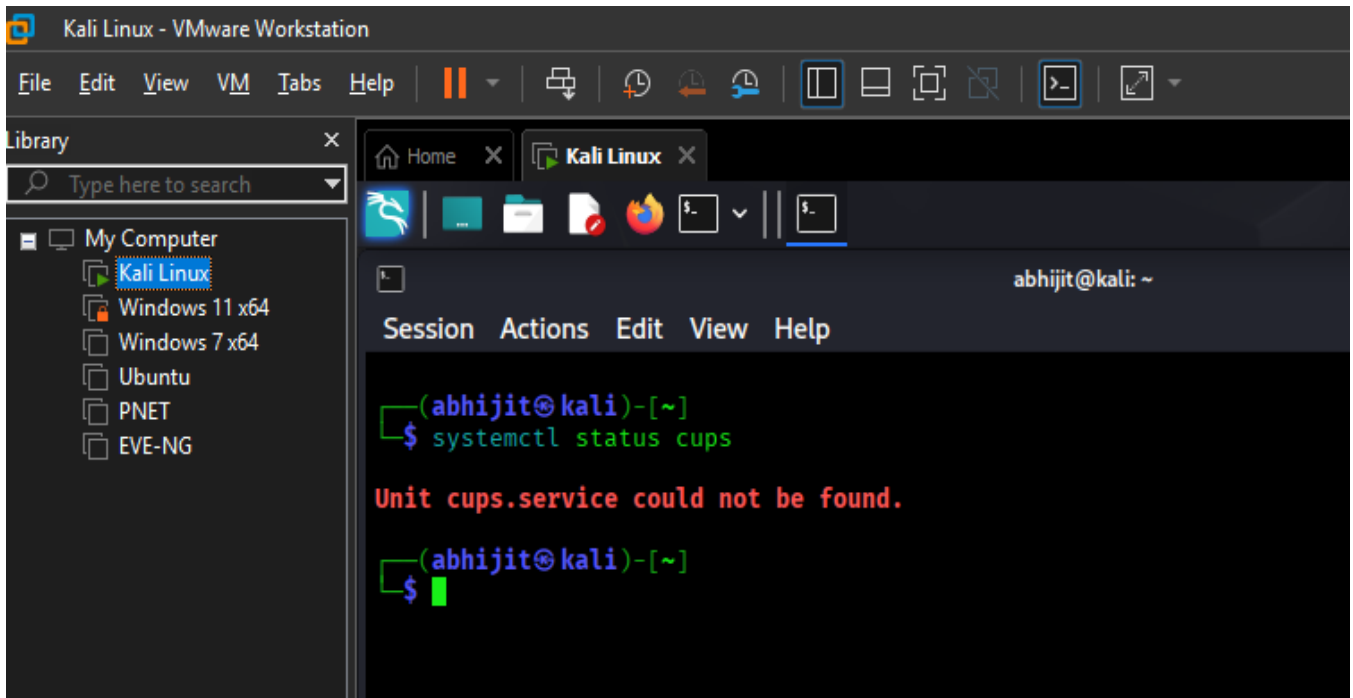


The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The interface includes a menu bar (File, Edit, View, VM, Tabs, Help), a toolbar with various icons, and a left-hand library pane. The library pane lists several virtual machines: My Computer, Kali Linux (selected), Windows 11 x64, Windows 7 x64, Ubuntu, PNET, and EVE-NG. The main window displays the Kali Linux desktop environment. A terminal window is open, showing the user 'abhijit' at the 'kali' prompt. The user has entered three commands to check the status of the tftp service: `systemctl is-enabled tftp`, `systemctl is-enabled tftp.socket`, and `systemctl is-enabled tftpd-hpa`. All three commands return the output 'not-found'. The terminal prompt is now ready for the next command.

```
(abhijit@kali)-[~]  
$ systemctl is-enabled tftp  
not-found  
$ systemctl is-enabled tftp.socket  
not-found  
$ systemctl is-enabled tftpd-hpa  
not-found  
(abhijit@kali)-[~]  
$
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure CUPS is not enabled	Met

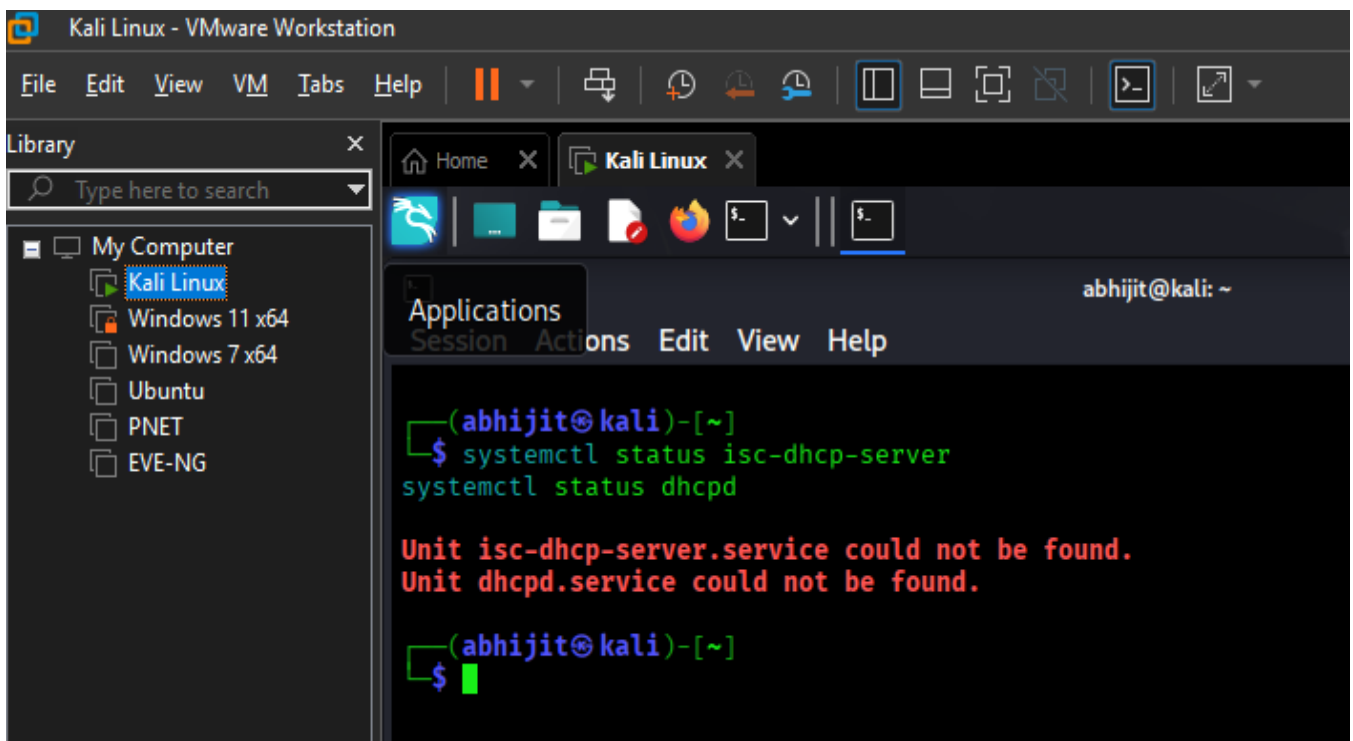


The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The interface includes a menu bar (File, Edit, View, VM, Tabs, Help), a toolbar with various icons, and a left-hand library pane. The library pane shows a tree view under 'My Computer' with entries for 'Kali Linux', 'Windows 11 x64', 'Windows 7 x64', 'Ubuntu', 'PNET', and 'EVE-NG'. The 'Kali Linux' entry is selected. The main window displays a terminal session with the prompt '(abhiжит@kali)-[~]'. The user has entered the command 'systemctl status cups', and the output is 'Unit cups.service could not be found.'.

```
(abhiжит@kali)-[~]  
$ systemctl status cups  
  
Unit cups.service could not be found.  
  
(abhiжит@kali)-[~]  
$
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure DHCP Server is not enabled	Met

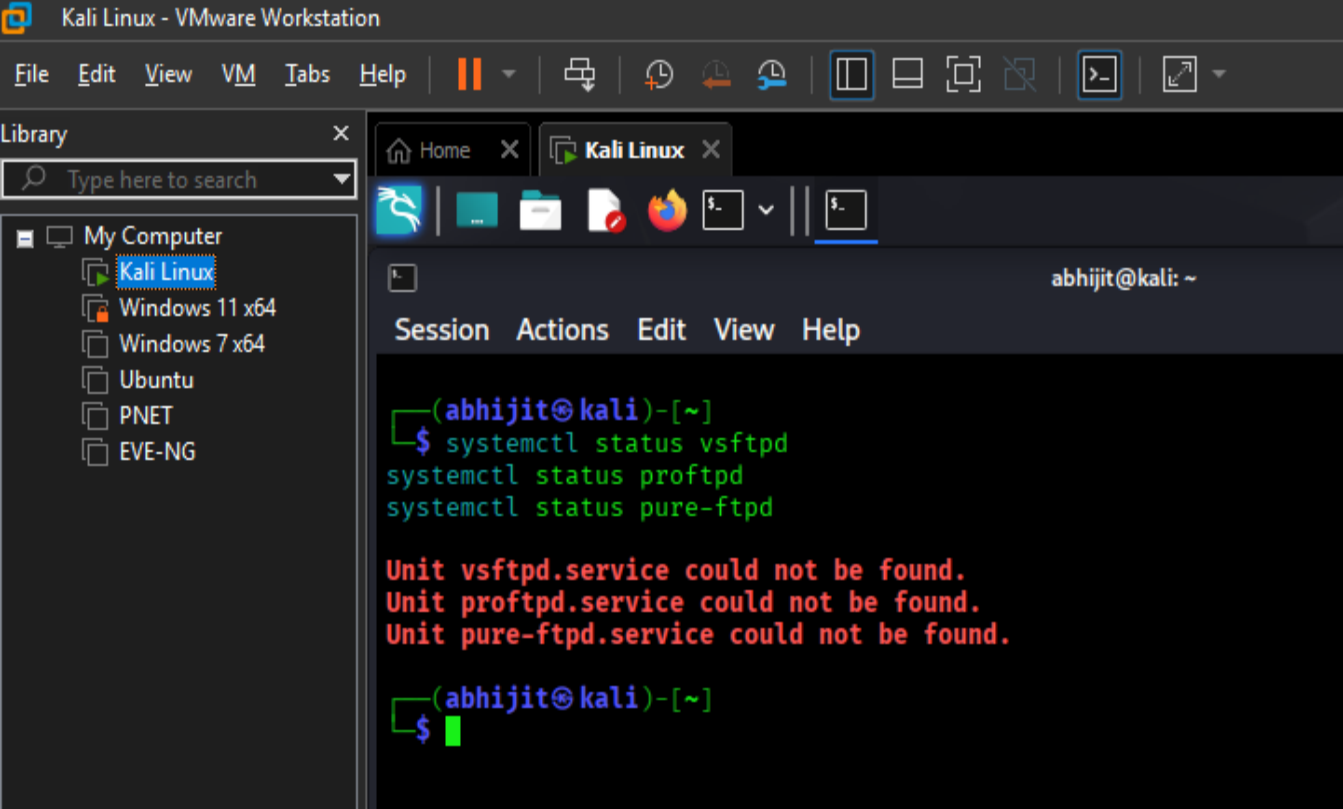


The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The interface includes a menu bar (File, Edit, View, VM, Tabs, Help), a toolbar with various icons, and a sidebar with a library of virtual machines. The main window displays a terminal session with the following commands and output:

```
(abhijit@kali)-[~]  
$ systemctl status isc-dhcp-server  
systemctl status dhcpd  
  
Unit isc-dhcp-server.service could not be found.  
Unit dhcpd.service could not be found.  
  
(abhijit@kali)-[~]  
$
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure FTP Server is not enabled	Met



The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The interface includes a menu bar (File, Edit, View, VM, Tabs, Help), a toolbar with various icons, and a sidebar with a library of virtual machines. The main window displays a terminal session for the user 'abhijit' on the host 'kali'. The terminal shows the command `systemctl status vsftpd` and its output, which indicates that the service could not be found. The same command is run for `proftpd` and `pure-ftpd`, both of which also report that the services could not be found. This confirms that no FTP server is enabled on the system.

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
  Kali Linux
  Windows 11 x64
  Windows 7 x64
  Ubuntu
  PNET
  EVE-NG

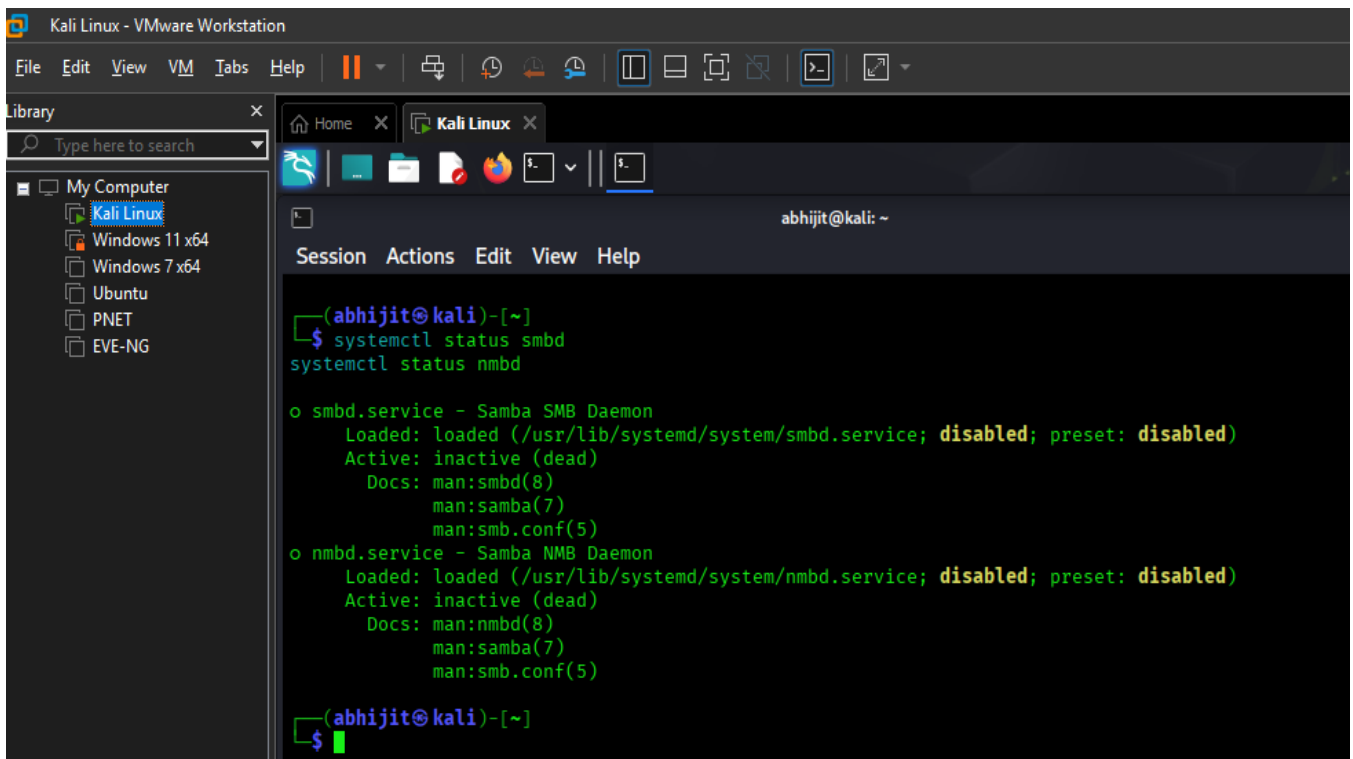
(abhijit@kali)-[~]
$ systemctl status vsftpd
systemctl status proftpd
systemctl status pure-ftpd

Unit vsftpd.service could not be found.
Unit proftpd.service could not be found.
Unit pure-ftpd.service could not be found.

(abhijit@kali)-[~]
$
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure Samba is not enabled	Met



The screenshot shows a Kali Linux terminal window within a VMware Workstation. The terminal displays the output of the `systemctl status smbd` and `systemctl status nmbd` commands. Both services are shown as loaded but inactive (dead), and their status is reported as **disabled**. The terminal output is as follows:

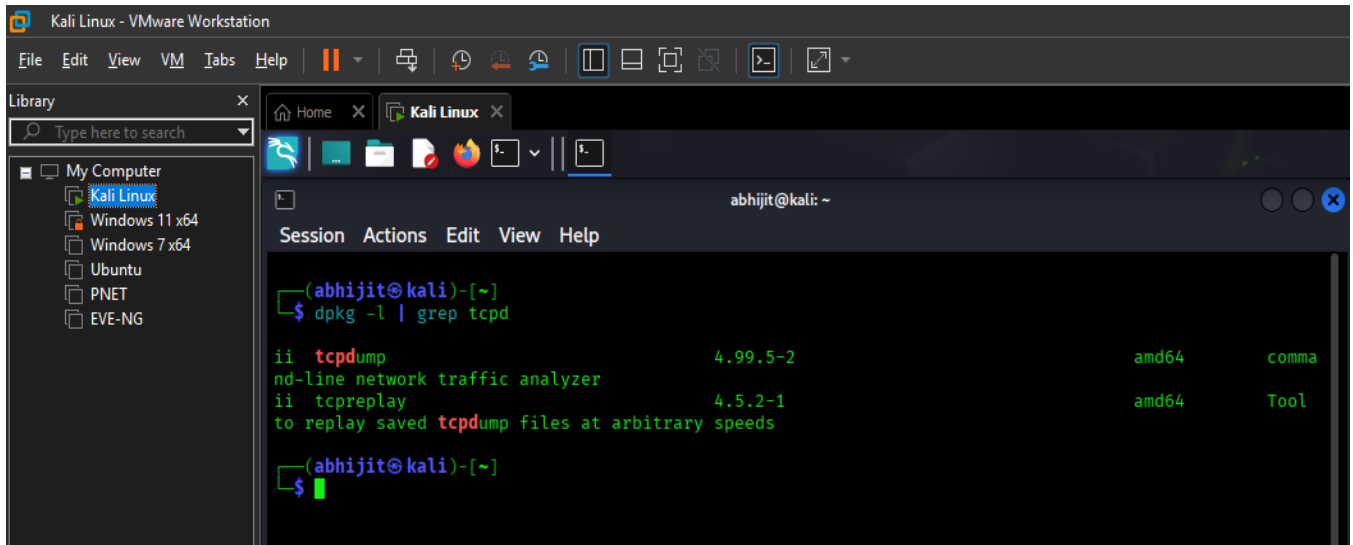
```
(abhiжит@kali)-[~]
$ systemctl status smbd
systemctl status nmbd

o smbd.service - Samba SMB Daemon
  Loaded: loaded (/usr/lib/systemd/system/smbd.service; disabled; preset: disabled)
  Active: inactive (dead)
  Docs: man:smbd(8)
        man:samba(7)
        man:smb.conf(5)
o nmbd.service - Samba NMB Daemon
  Loaded: loaded (/usr/lib/systemd/system/nmbd.service; disabled; preset: disabled)
  Active: inactive (dead)
  Docs: man:nmbd(8)
        man:samba(7)
        man:smb.conf(5)

(abhiжит@kali)-[~]
$
```


Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure TCP Wrappers is installed	Met

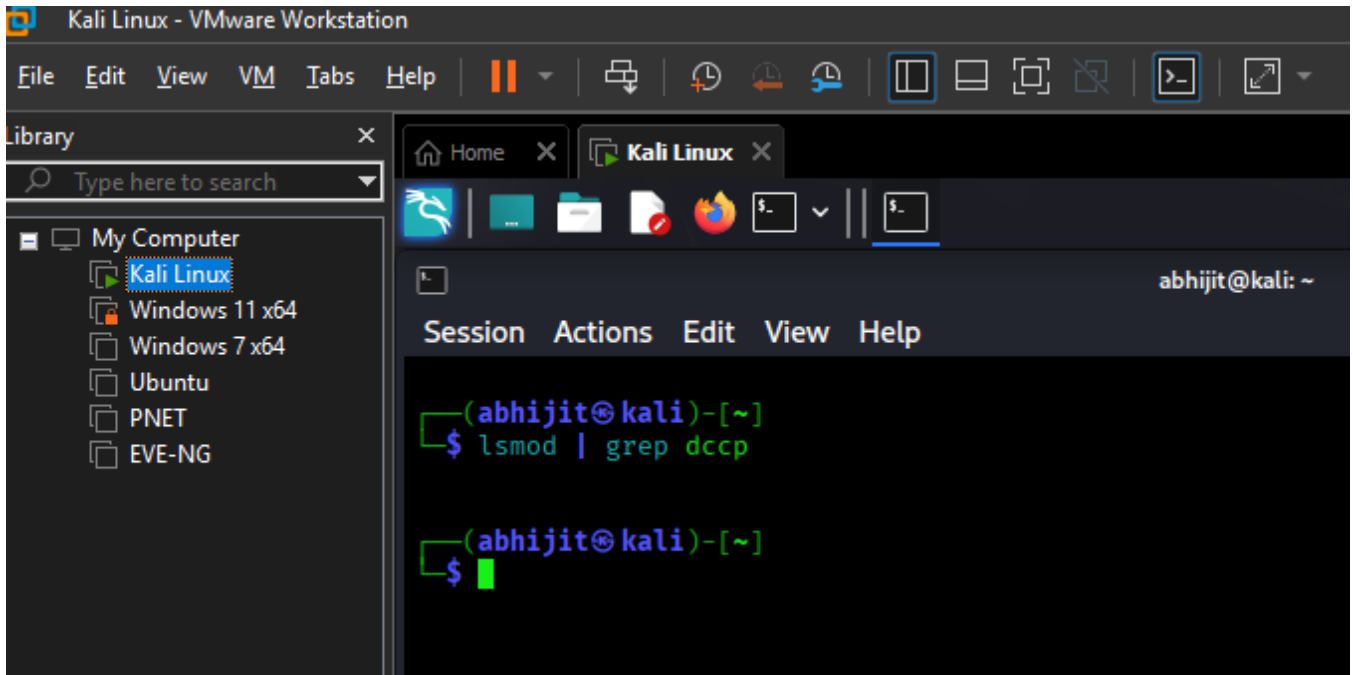


The screenshot shows a Kali Linux terminal window within a VMware Workstation. The terminal displays the output of the command `dpkg -l | grep tcpd`. The output lists two packages: `tcpdump` (version 4.99.5-2) and `tcpreplay` (version 4.5.2-1). The `tcpdump` package is described as a "nd-line network traffic analyzer" and is marked as "comma". The `tcpreplay` package is described as a "to replay saved tcpdump files at arbitrary speeds" and is marked as "Tool".

```
(abhihit@kali)-[~]  
$ dpkg -l | grep tcpd  
  
ii  tcpdump                4.99.5-2          amd64      comma  
nd-line network traffic analyzer  
ii  tcpreplay              4.5.2-1           amd64      Tool  
to replay saved tcpdump files at arbitrary speeds  
  
(abhihit@kali)-[~]  
$
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure DCCP is disabled	Met

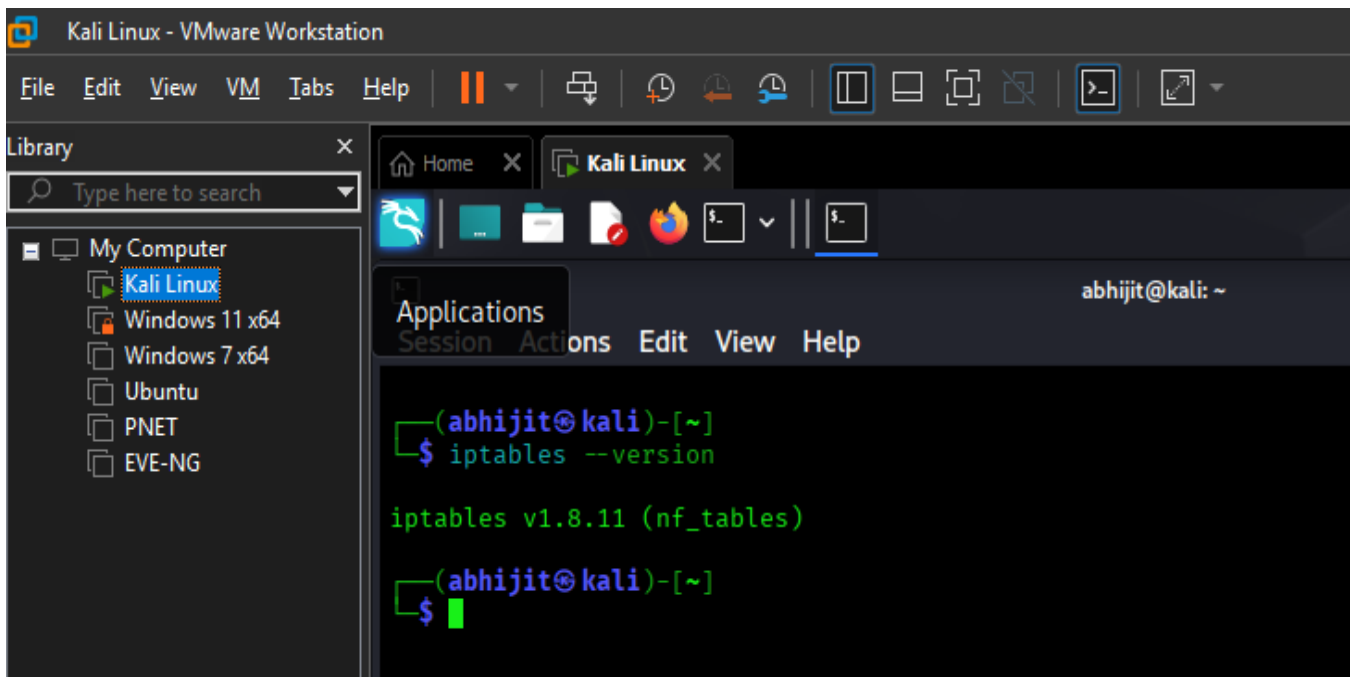


The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The interface includes a menu bar (File, Edit, View, VM, Tabs, Help), a toolbar with various icons, and a left-hand library pane listing virtual machines: My Computer, Kali Linux (selected), Windows 11 x64, Windows 7 x64, Ubuntu, PNET, and EVE-NG. The main window displays the Kali Linux desktop environment with a terminal window open. The terminal shows the user 'abhijit' at the 'kali' machine in the '~' directory. The command 'lsmod | grep dccp' has been entered, and the output is currently blank, indicating that the DCCP module is not loaded.

```
(abhijit@kali)-[~]  
$ lsmod | grep dccp  
  
(abhijit@kali)-[~]  
$
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure iptables is installed	Met



The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The interface includes a menu bar (File, Edit, View, VM, Tabs, Help), a toolbar with various VM controls, and a left-hand library pane. The main window displays a terminal session with the following content:

```
(abhijit@kali)-[~]  
$ iptables --version  
  
iptables v1.8.11 (nf_tables)  
  
(abhijit@kali)-[~]  
$
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure audit log storage size is configured	Not Met

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
  Kali Linux
  Windows 11 x64
  Windows 7 x64
  Ubuntu
  PNET
  EVE-NG

root@kali: /etc

(root@kali)-[/]
# pwd
/

(root@kali)-[/]
# ls
bin    dev    home   initrd.img.old  lib32  lost+found  mnt  proc  run  srv  tmp  var  vmlinuz.old
boot   etc    initrd.img  lib        lib64  media      opt  root  sbin sys  usr  vmlinuz

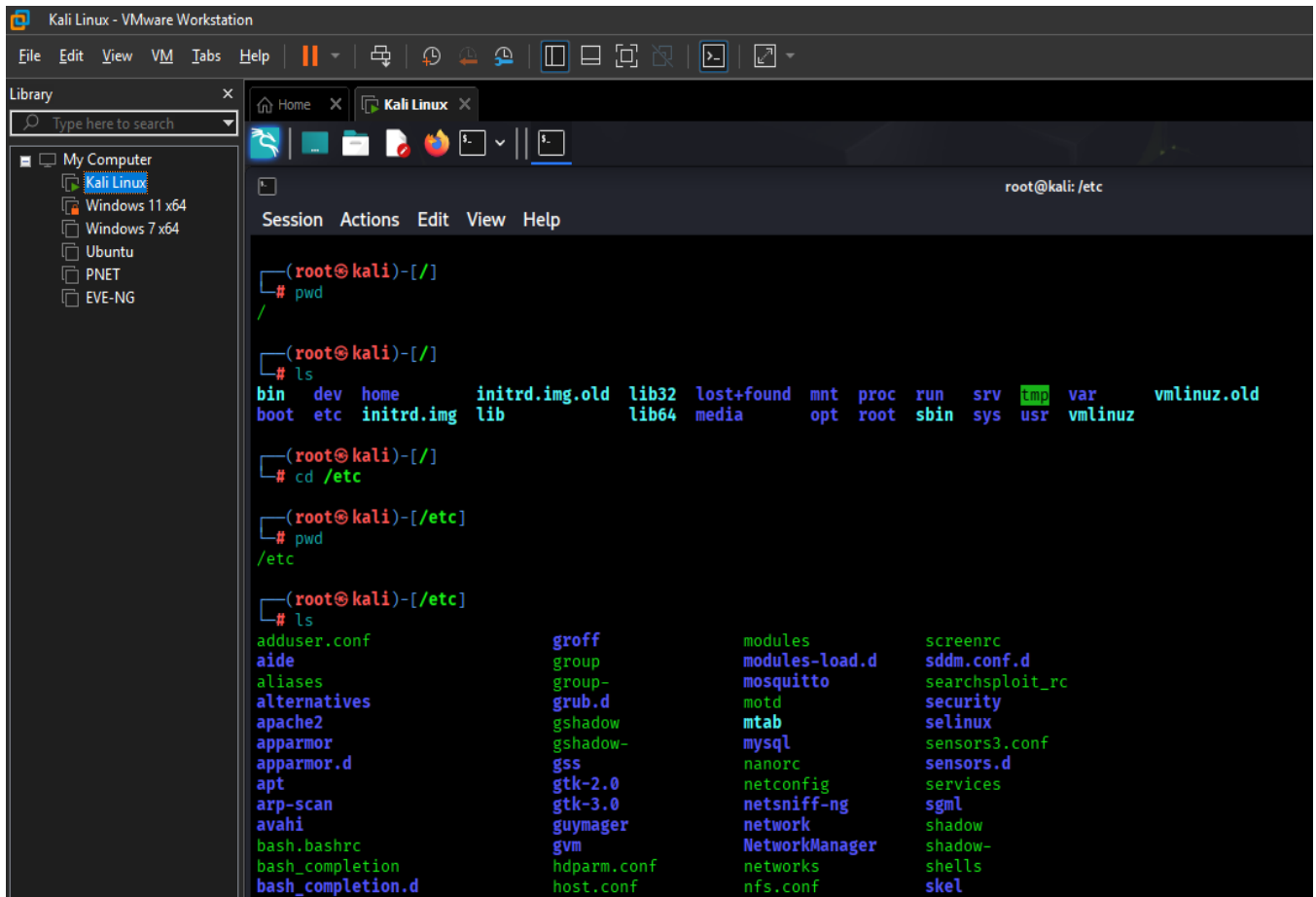
(root@kali)-[/]
# cd /etc

(root@kali)-[/etc]
# pwd
/etc

(root@kali)-[/etc]
# ls
adduser.conf  groff          modules        screenrc
aide          group          modules-load.d sddm.conf.d
aliases       group-         mosquitto      searchsploit_rc
alternatives  grub.d        motd           security
apache2       gshadow       mtab           selinux
apparmor      gshadow-     mysql          sensors3.conf
apparmor.d    gss          nanorc         sensors.d
apt           gtk-2.0       netconfig      services
arp-scan      gtk-3.0       netsniff-ng    sgml
avahi         guymager      network        shadow
bash.bashrc   gvm           NetworkManager shadow-
bash_completion hdparm.conf  networks       shells
bash_completion.d host.conf    nfs.conf       skel
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure audit logs are not automatically deleted	Not Met



The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The terminal window is open, showing the root user at the kali machine. The user has navigated to the /etc directory and listed its contents. The terminal output is as follows:

```
(root@kali)-[/]
# pwd
/

(root@kali)-[/]
# ls
bin    dev    home   initrd.img.old  lib32  lost+found  mnt  proc  run  srv  tmp  var  vmlinuz.old
boot  etc    initrd.img  lib      lib64  media      opt  root  sbin sys  usr  vmlinuz

(root@kali)-[/]
# cd /etc

(root@kali)-[/etc]
# pwd
/etc

(root@kali)-[/etc]
# ls
adduser.conf  groff      modules      screenrc
aide           group      modules-load.d  sddm.conf.d
aliases       group-     mosquitto     searchsploit_rc
alternatives  grub.d     motd          security
apache2       gshadow    mtab          selinux
apparmor      gshadow-   mysql         sensors3.conf
apparmor.d    gss        nanorc        sensors.d
apt           gtk-2.0    netconfig     services
arp-scan      gtk-3.0    netsniff-ng   sgml
avahi         guymager   network       shadow
bash.bashrc   gvm        NetworkManager  shadow-
bash_completion  hdparm.conf  networks      shells
bash_completion.d  host.conf    nfs.conf       skel
```


Windows Server Build Sheet

As part of Fed F1rst Control Systems' security policy implementation, it is crucial to establish a standardized build process for Windows web servers hosted in the public cloud. A well-defined build sheet ensures consistency, security, and adherence to best practices across all server deployments. In this task, you will create a list of 10 essential items, along with examples, that should be included in a build sheet for a Windows web server hosted in the public cloud.

- **Identify 10 critical items** that should be included in a build sheet for a Windows web server hosted in the public cloud
- Provide a brief **description OR an example** for each item

Windows Server Build Sheet

1. [Operating system version and hardening]

[Specify the exact windows server version like Windows server 2022 and include hardening steps such as disabling unnecessary services and enabling only required windows roles and features like IIS, .NET]

2. [Patch management]

[Ensure the operating system is up to date with the latest security updates. Document patch baseline requirements and patch automation setup like using AWS patch manager or Azure update management.]

3. [Cloud instance configuration]

[Document the instance type, storage allocation and networking setup for the cloud provider. For instance, AWS EC2 t3.medium, 100GB SSD, VPC subnet with public IP and security group allowing HTTP/HTTPS only.]

4. [Identity and access management]

[Prepare a list for required user accounts, groups and their permissions. Enforce least-privilege access through IAM policies, local group policy, and strong password policies, only admins and designated support personnel have RDP access.]

5. [Firewall and network security]

[To restrict inbound/outbound traffic, define firewall rules, NSGs (Azure) or security groups. Only allow HTTP/HTTPS port and block all other ports, AWS security group restricts SSH/RDP to trusted IPs only]

Windows Server Build Sheet

6. [Web Server configuration]

[Document settings for Internet Information Services (IIS), including IIS modules, application pools setup HTTPS enforcement and minimum TLS version configuration.]

7. [Logging and monitoring]

[For alerting and auditing include configuration of windows event logging, IIS logs and integration with a central SIME like ELK or cloud-native monitoring solutions like AWS CloudWatch, Azure Monitor.]

8. [Backup and Recovery]

[Configure automated backup procedures for critical OS, data and IIS configuration, including retention policies and regular backup testing like scheduled daily image backups via cloud provider's backup service.]

9. [Secure remote access]

[Define permitted remote access protocols and restrictions. Describe how administrators should connect securely such as enforcing MFA for RDP, using bastion hosts/jumpboxes, and disabling direct exposure of management ports.]

10. [Baseline application deployment]

[Describe standard procedures for deploying applications and required web roles like web deploy tool used for application deployment. List any required software packages, runtime versions like .NET and configurations, as well as a reference to a deployment automation script or tools like install Microsoft .NET 6.0, configure IIS to host ASP.NET apps.]

Enhancing Cloud Security with CASB

With Fed F1rst Control Systems increasingly leveraging cloud technologies for their operations, the integration of Cloud Access Security Brokers (CASB) into their security framework is more crucial than ever. Given your understanding of CASBs from the course, you're in a unique position to assess how their capabilities can specifically enhance Fed F1rst's security posture.

- Identify **5 specific benefits** of CASBs that would directly enhance the cloud security posture of Fed F1rst Control Systems
- Provide a concise, clear description for each benefit

Enhancing Cloud Security with CASB

1. [Enhanced visibility into cloud usage]

[CASBs provide comprehensive insight into what cloud services are being used, who is accessing them and where data is traveling and how, for both managed and unmanaged devices. It allows to monitor both sanctioned and unsanctioned services and identify shadow IT risks, monitor data flow, ensure only authorized usage of approved cloud applications.]

2. [Data Loss Prevention DLP]

[CASBs integrate advanced DLP mechanisms to prevent accidental or intentional data leakage, ensuring sensitive information remains secure during cloud storage and sharing, enforce policies to detect, prevent, and remediate unauthorized sharing, exfiltration or exposure of sensitive data.]

3. [Threat protection and Malware Detection]

[CASBs offer protection against malware, suspicious logins and risk behavior using analytics and automated remediation to detect and respond to anomalous activity and malware threats within cloud environment.]

4. [regulatory Compliance and Governance]

[CASBs support compliance with industry standards such as GDPR and HIPAA by enforcing policy controls, providing audit trails and generating compliance reports for cloud usage. It helps to meet regulatory requirements with robust evidence of policy enforcement and controlled data access.]

5. [Access Control and Identity security]

[CASBs allow the implementation of context-aware access controls, adjusting permissions based on user role, device health, location, and real-time risk level. Will gain granular and flexible user authentication, minimizing risk from compromised accounts or unsafe devices while supporting remote work.]