COMPLIANCE ASSESSMENT

Project Scenario

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.

Section 1: Developing a Hardening Strategy

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

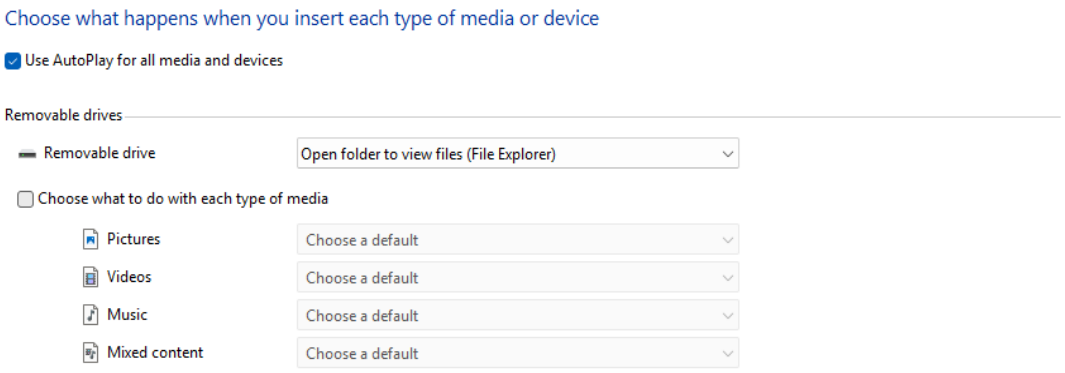
Many parts can be hardened in Windows 10, but it can be challenging to find them. You can find the way to 10 different settings:

- **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

Windows 10 Hardening

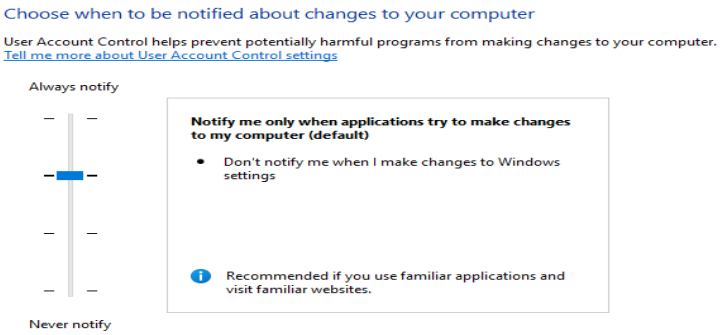
1. [AutoPlay Enable]

[Uncheck (Use AutoPlay for all media and devices) > set defaults to (Ask me every time) for Removable drive along with each type of media, Memory card, DVDs, Blu-ray discs, CDs.]



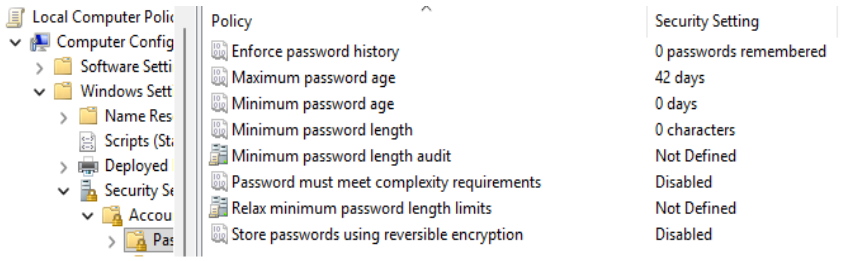
2. [Weak User account control settings]

[Set to at (Always notify)]



3. [Password Policies not configured]

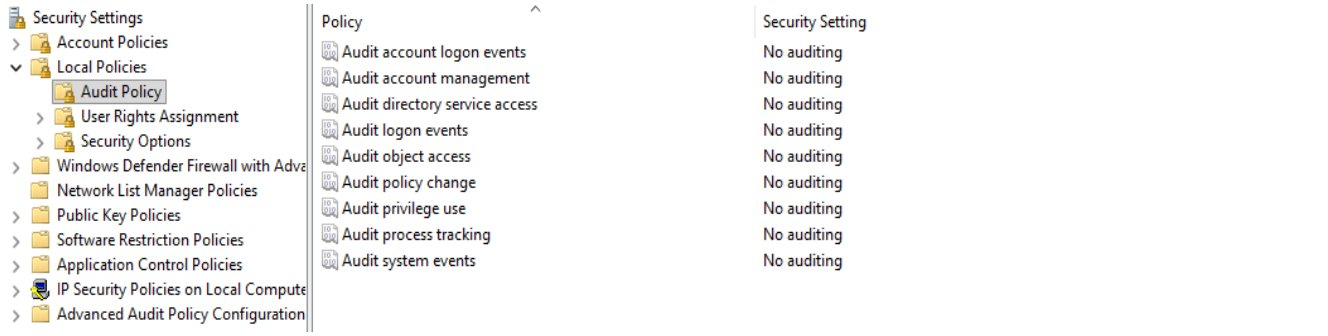
[Set Maximun password age to 90 days > Minimum password lenth to 8 characters > Minimum password lenth audit to 8 characters > Password must meet complexcity requirments to enable]



Windows 10 Hardening

4. [Audit policy (logging) not enabled]

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



5. [Guest account enabled]

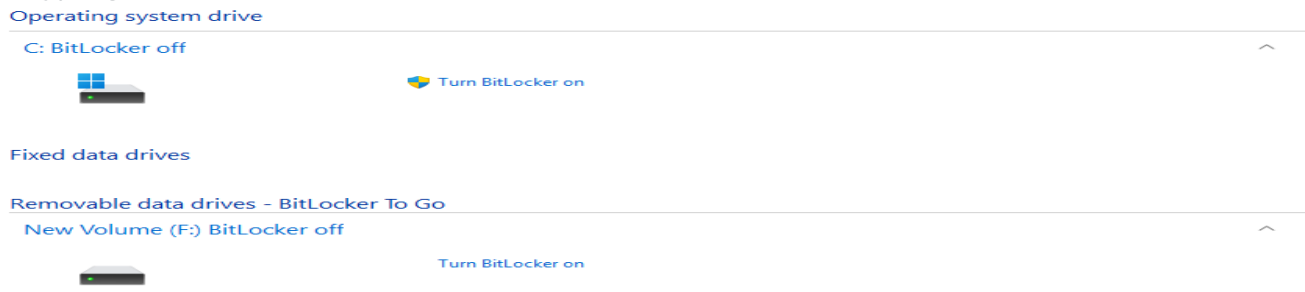
[For disable Guest account, run the command (net user guest /activ:no) in CLI]

```
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.]



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 inaccable 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.]

Section 2: Create Security Policies

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 stron, unique passwords for their email accounts and avoid reusing passwords across different systems. Passwords shouls include a mix of numbers, letters and special characters and be update regularly to prevent unauthorised 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 instracted 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 instructionns should be provided for reporting suspicious emails, suspected phishing attempts, or other related security incidents. Employee must know who to contact and what stapes to take if they encounter suspicious activity.]
5. [**Approved device and network use** : Corporate emails access must be restricted to approved devices and secure network, employees are to avoid accessing corporate email on public wifi networks, unauthorised or personal devices and use secure connections or VPNs whenever possible. To prevent interception and credential theft.]

BYOD Policy

As Fed F1rst 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.]

Section 3:
Self Assessment

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.

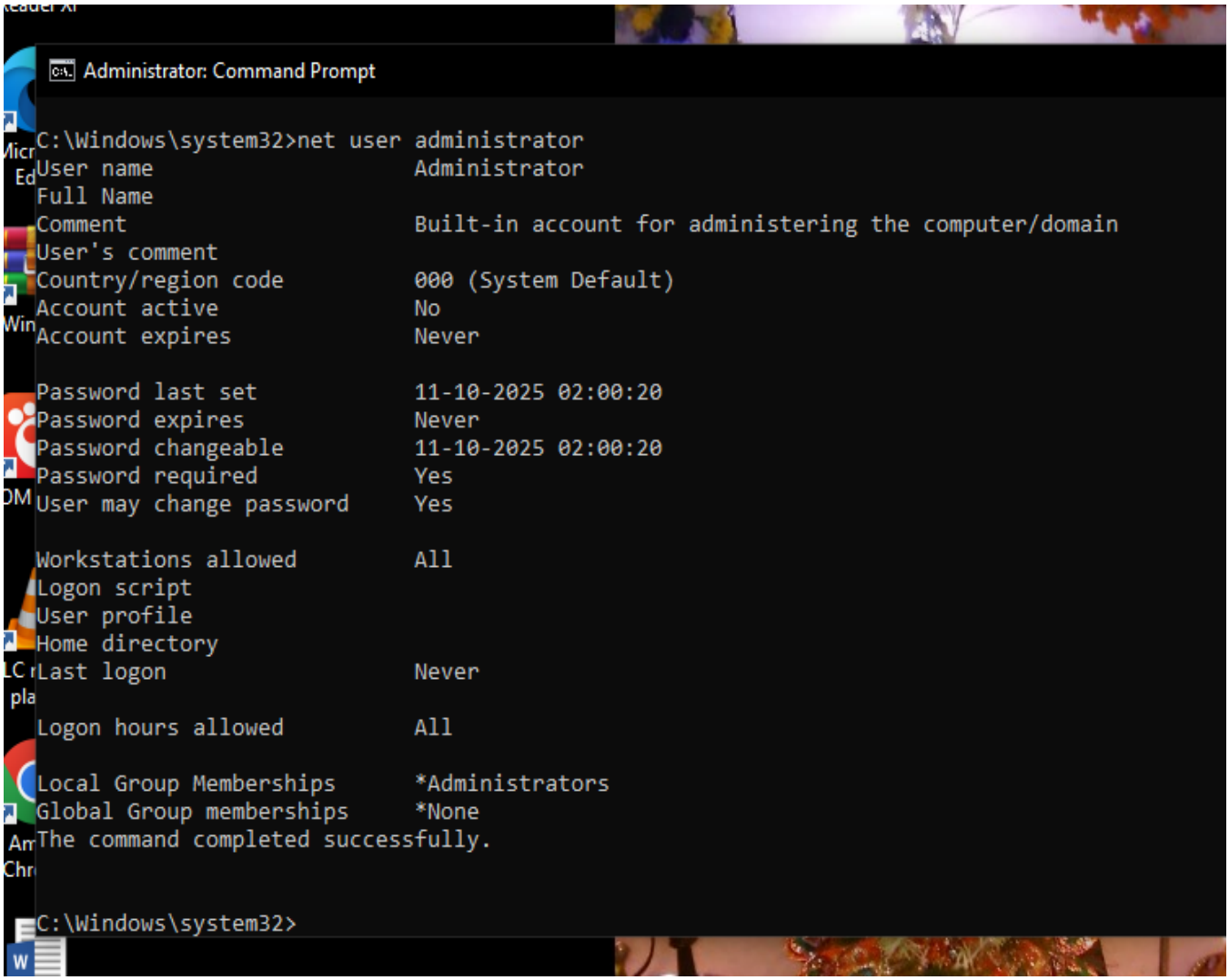
- **Review the provided 14-item list** from *NIST SP 800-53 Rev. 5*
- Evaluate a Windows 10 machine for compliance with each item
- For each item, determine if it is:
  - **Met:** The Windows 10 machine complies with the NIST guideline
  - **Not Met:** The Windows 10 machine does not comply with the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

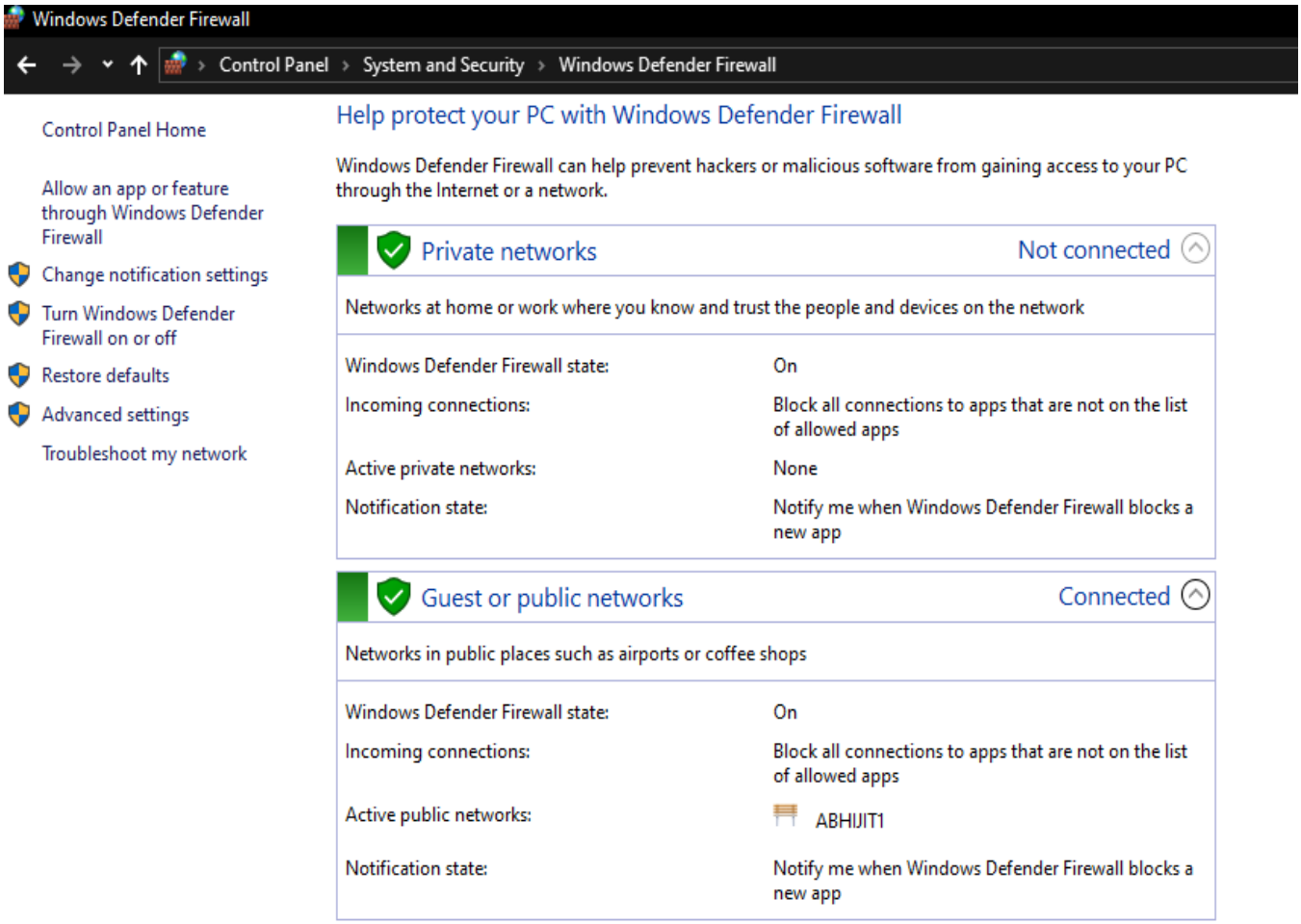
Windows Desktop Compliance

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



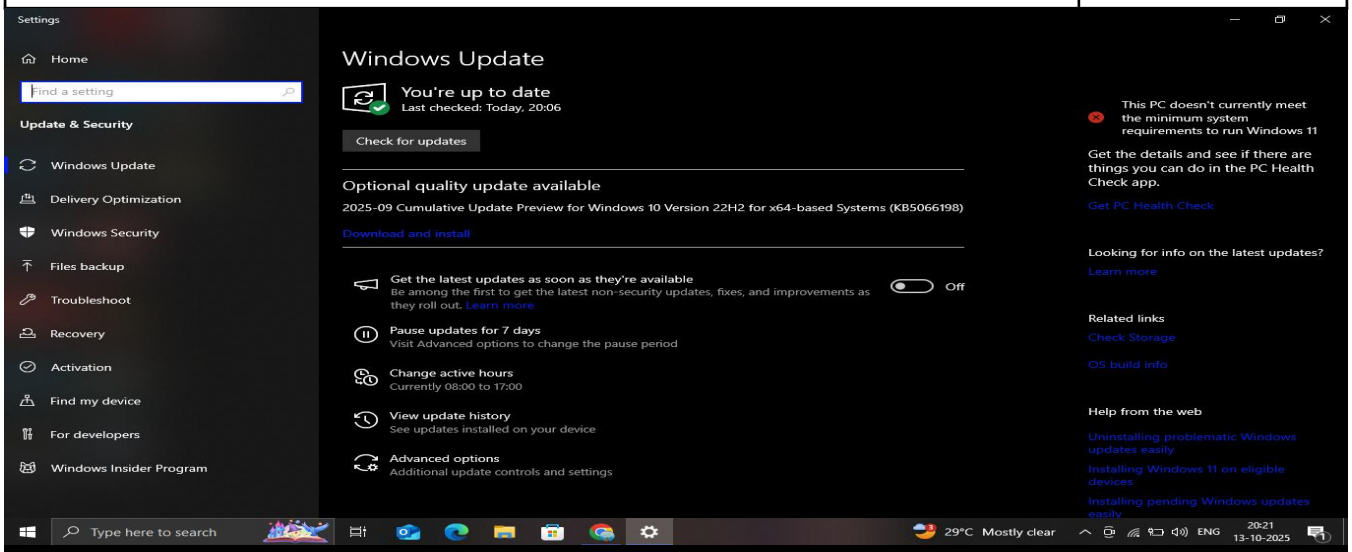
Windows Desktop Compliance

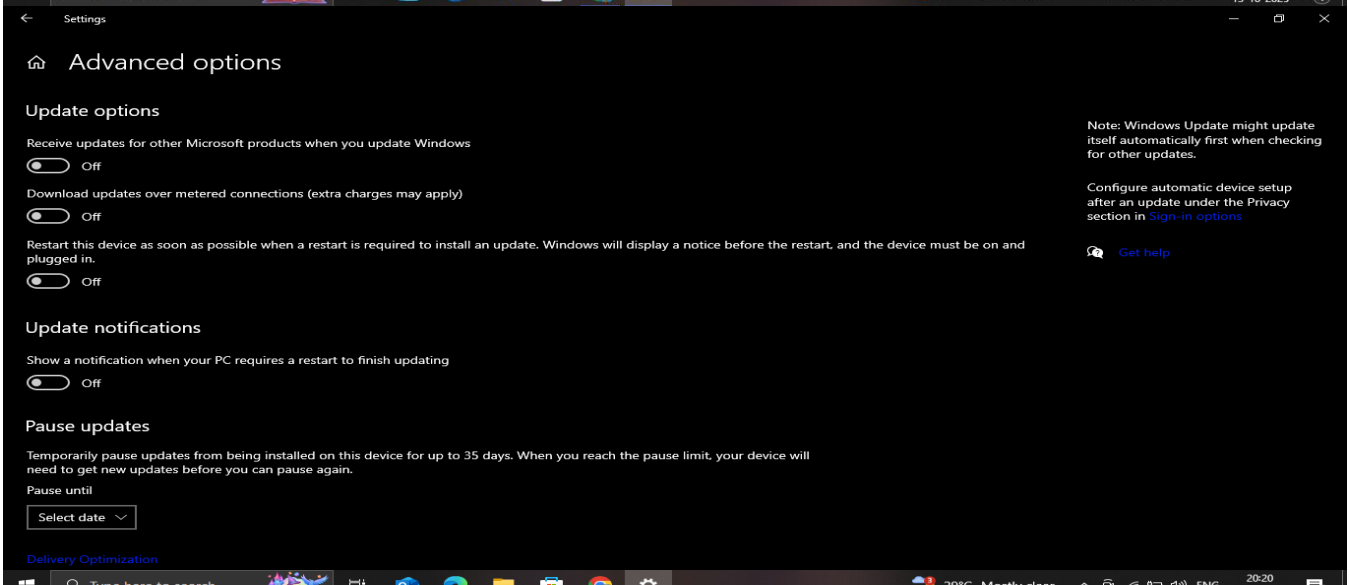
Windows 10 Regulatory Requirement	Met/Not Met
Windows Firewall is enabled	Met

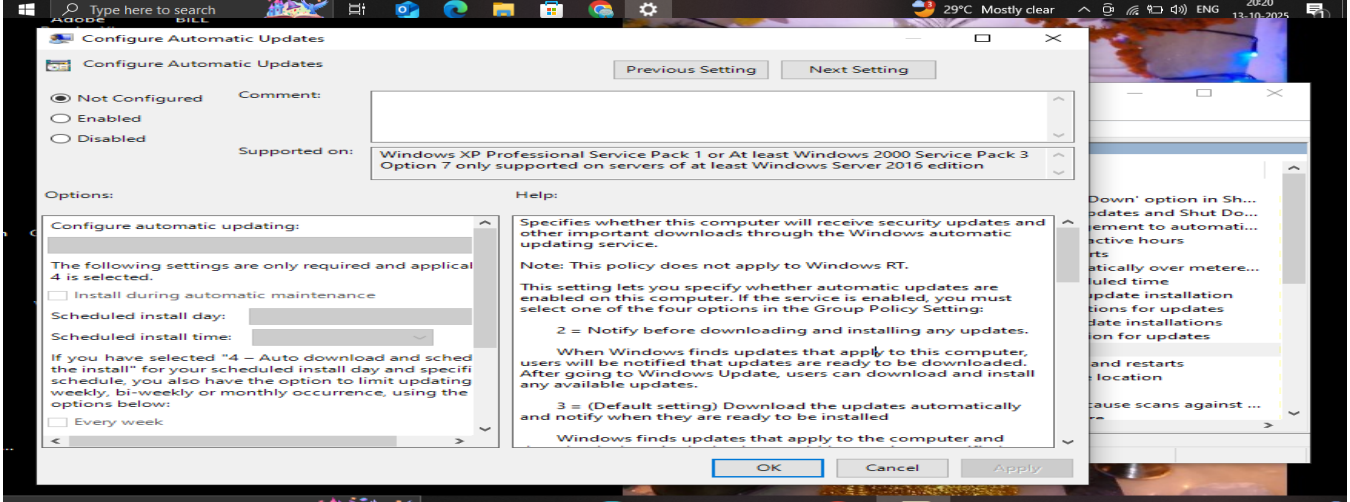


Windows Desktop Compliance

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

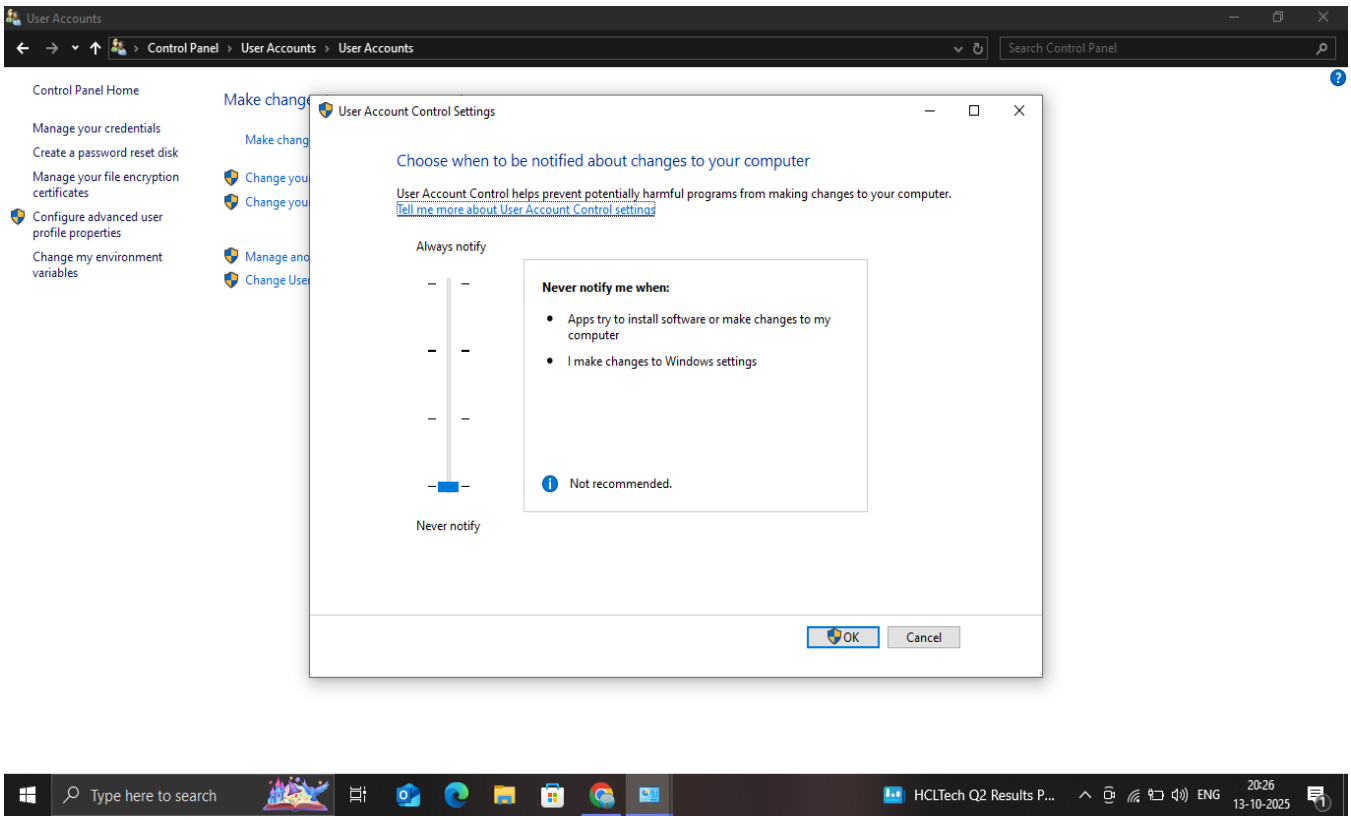






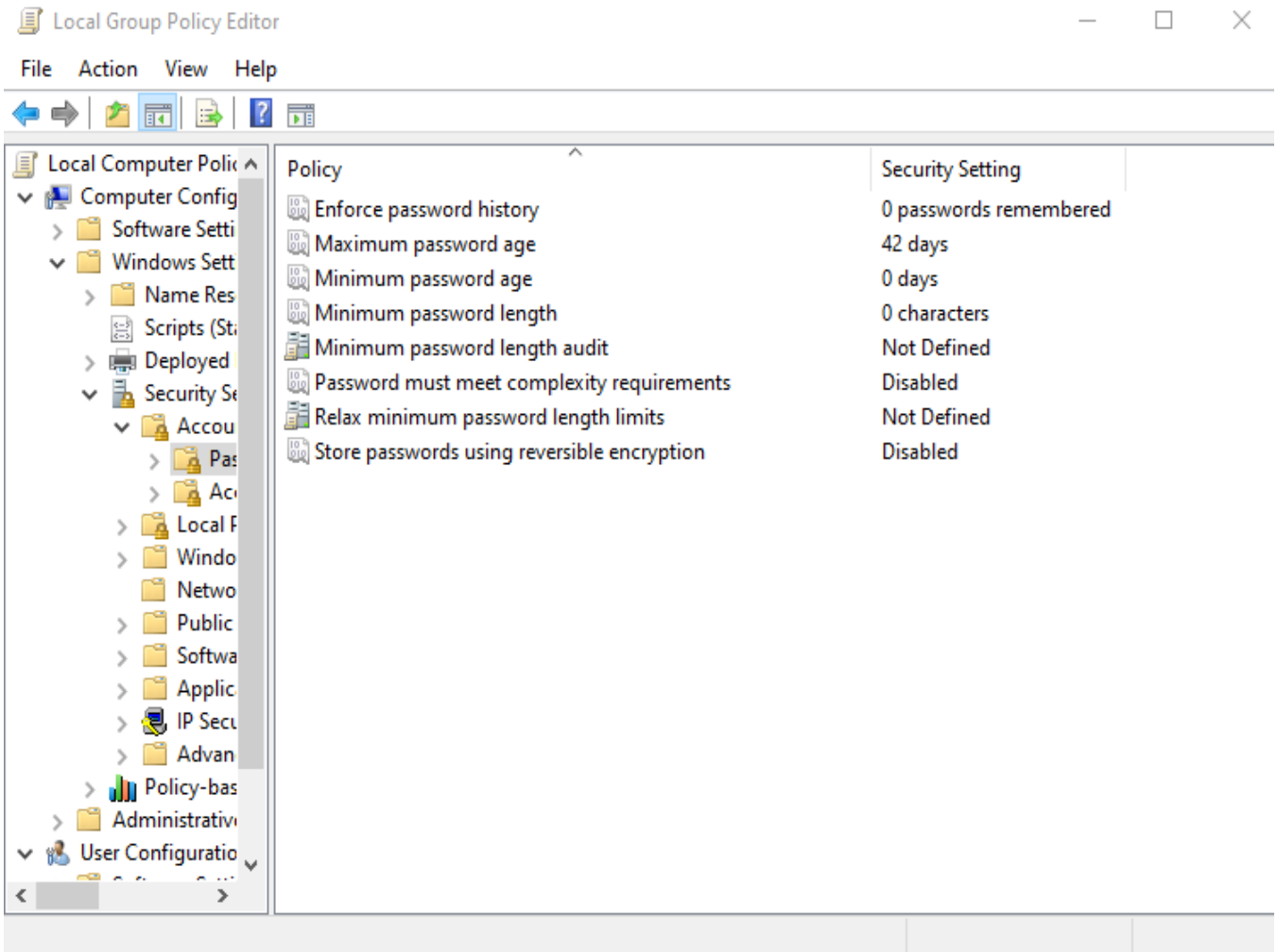
Windows Desktop Compliance

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



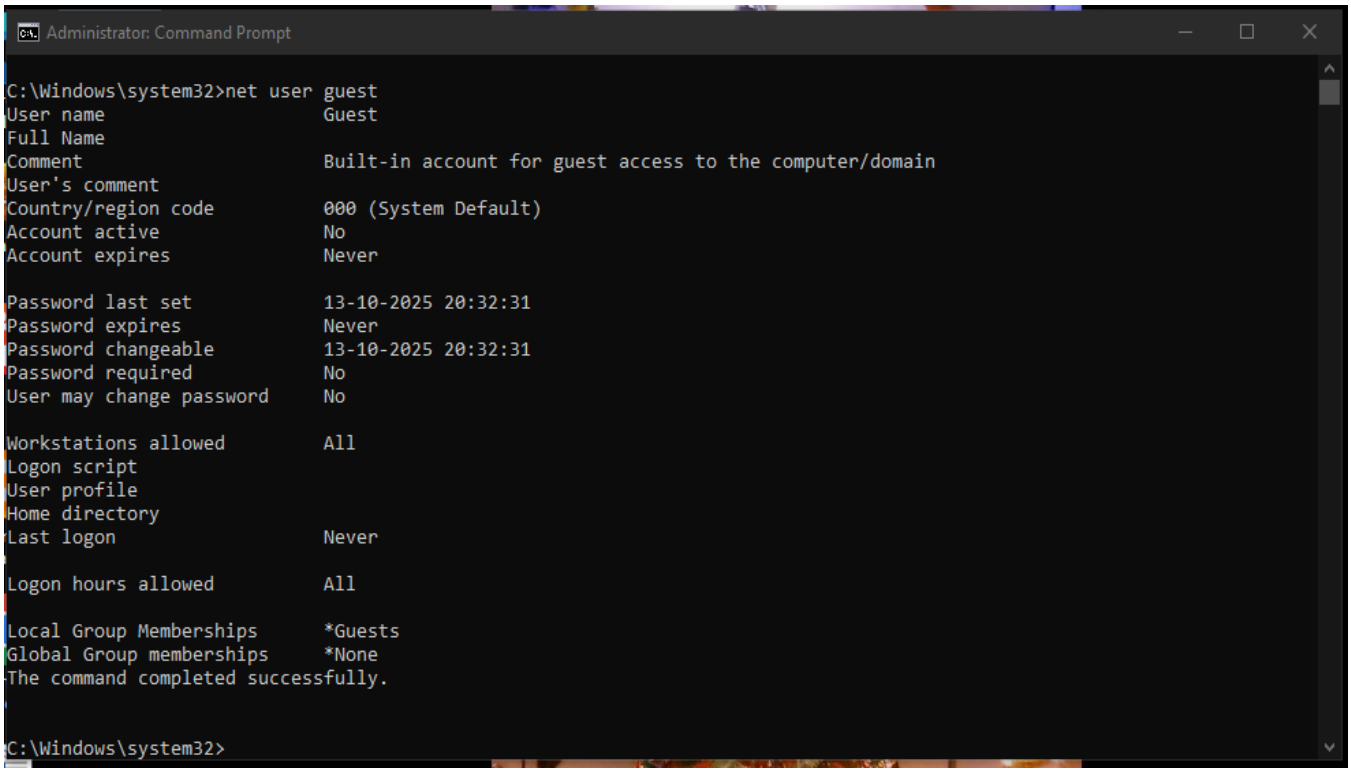
Windows Desktop Compliance

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



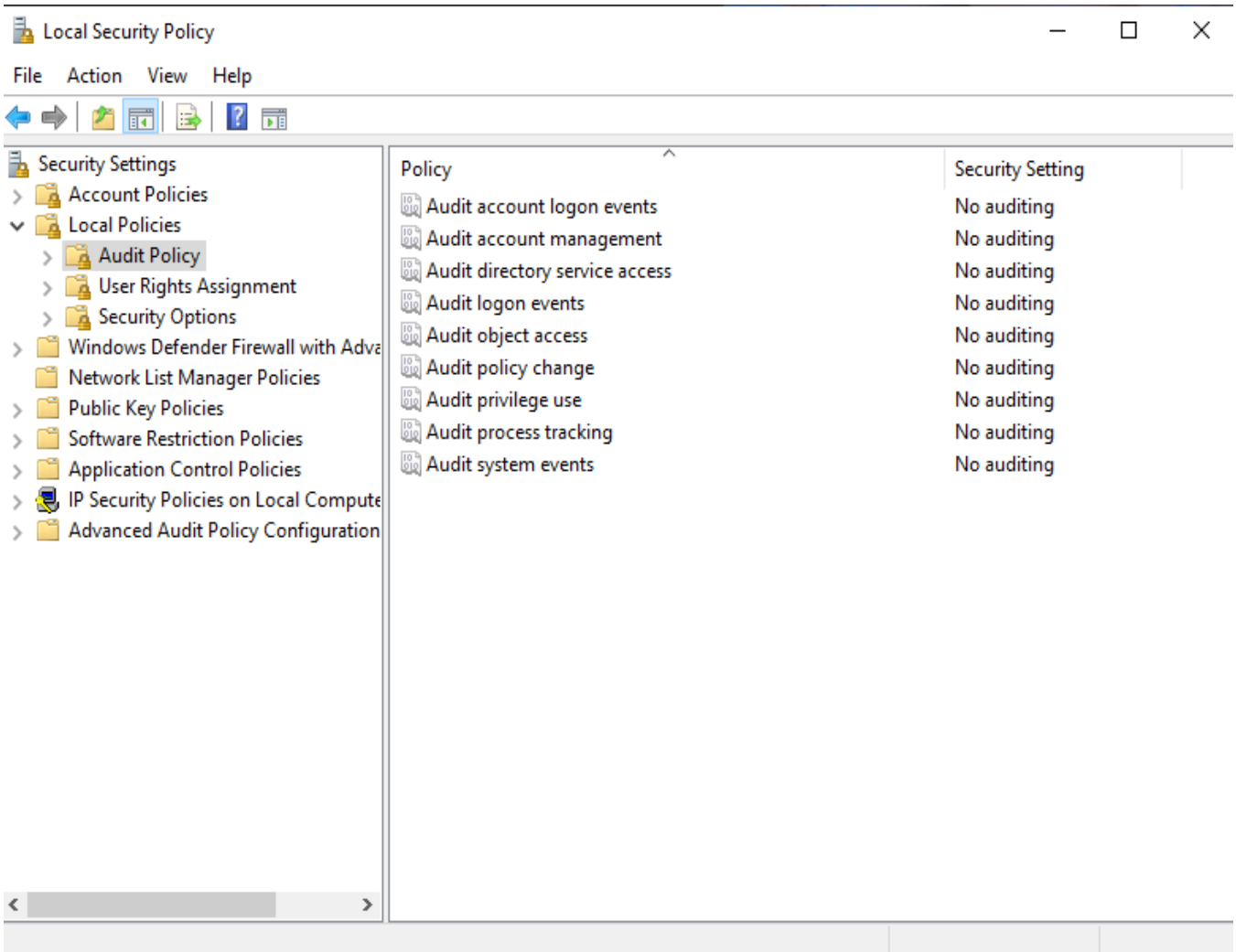
Windows Desktop Compliance

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



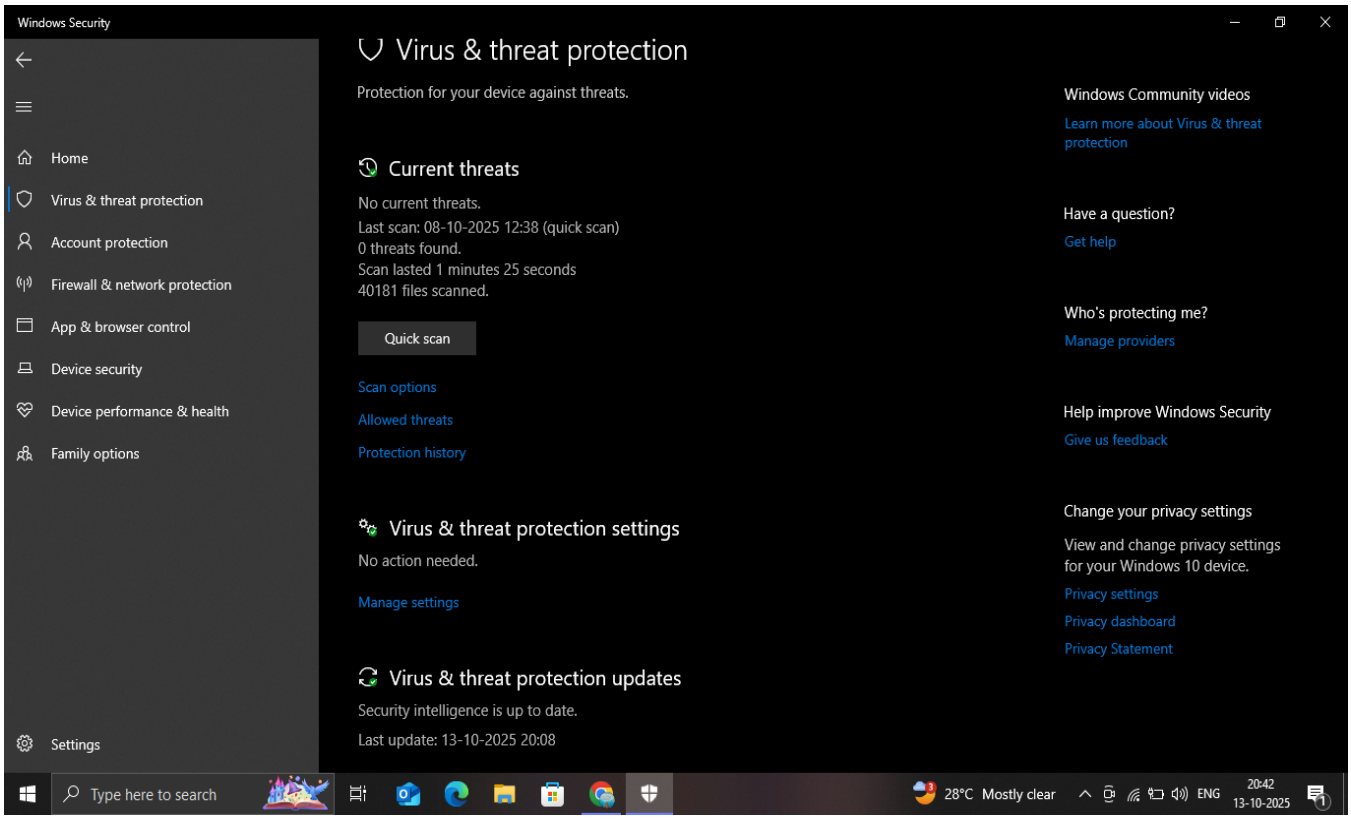
Windows Desktop Compliance

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



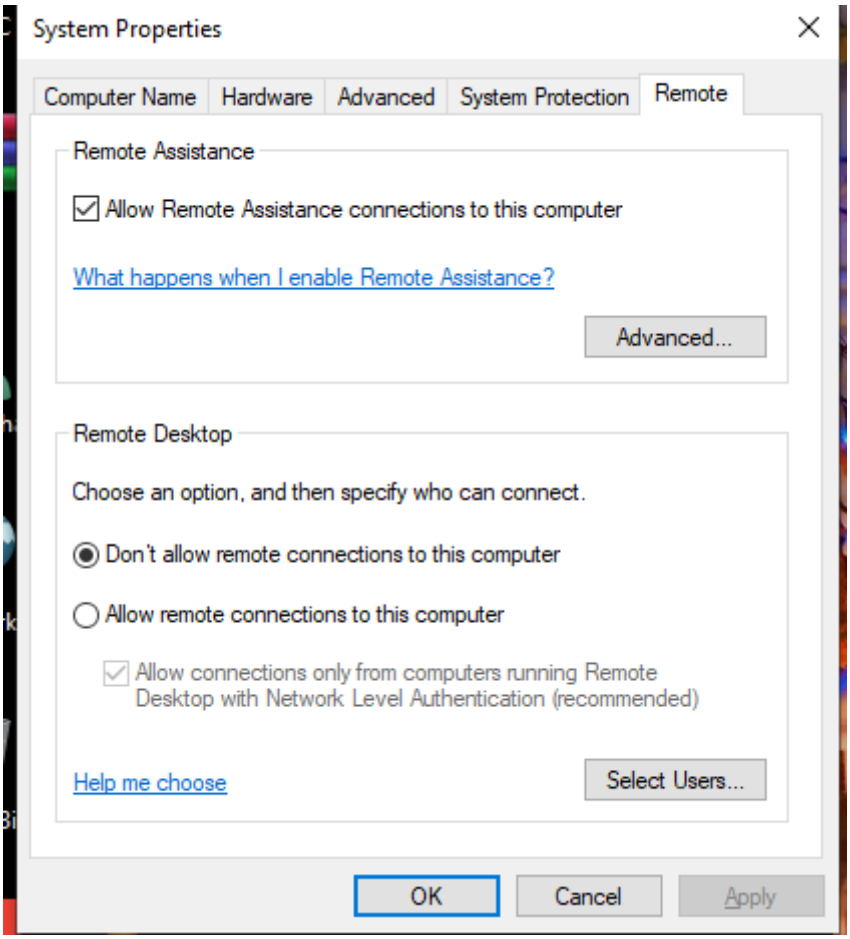
Windows Desktop Compliance

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



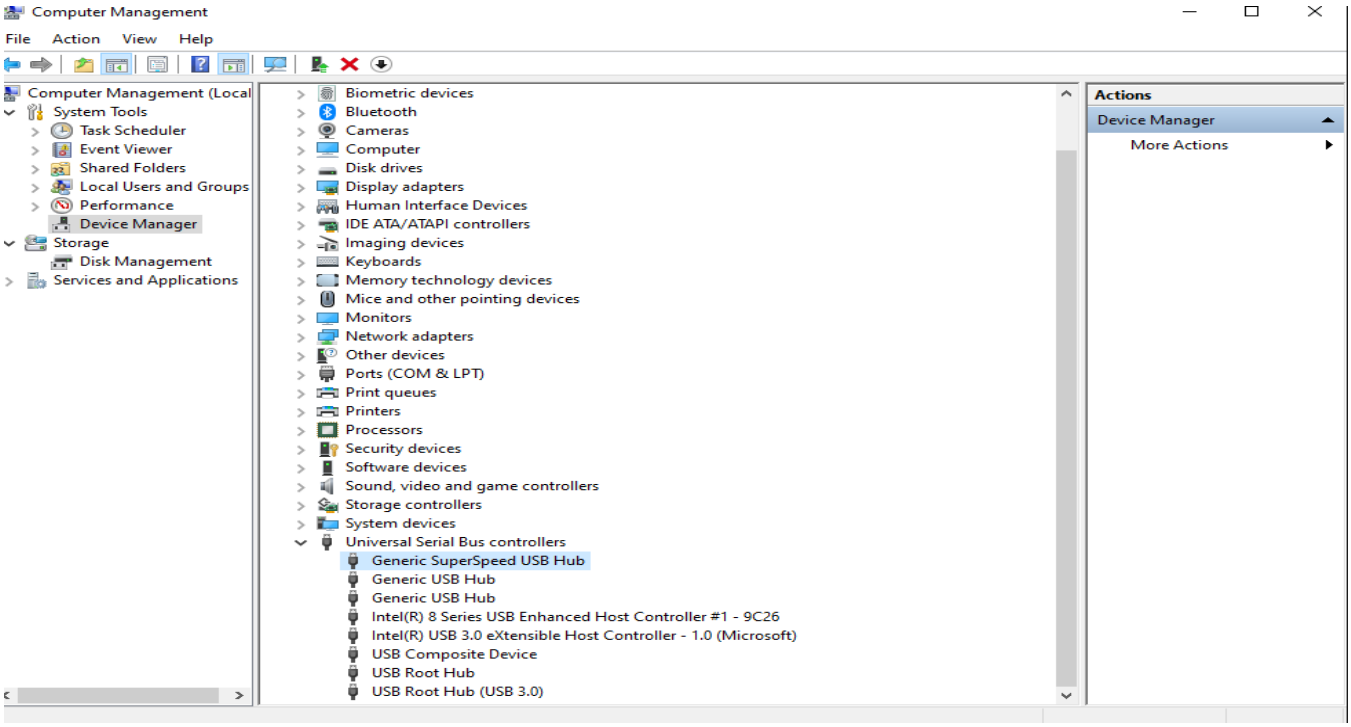
Windows Desktop Compliance

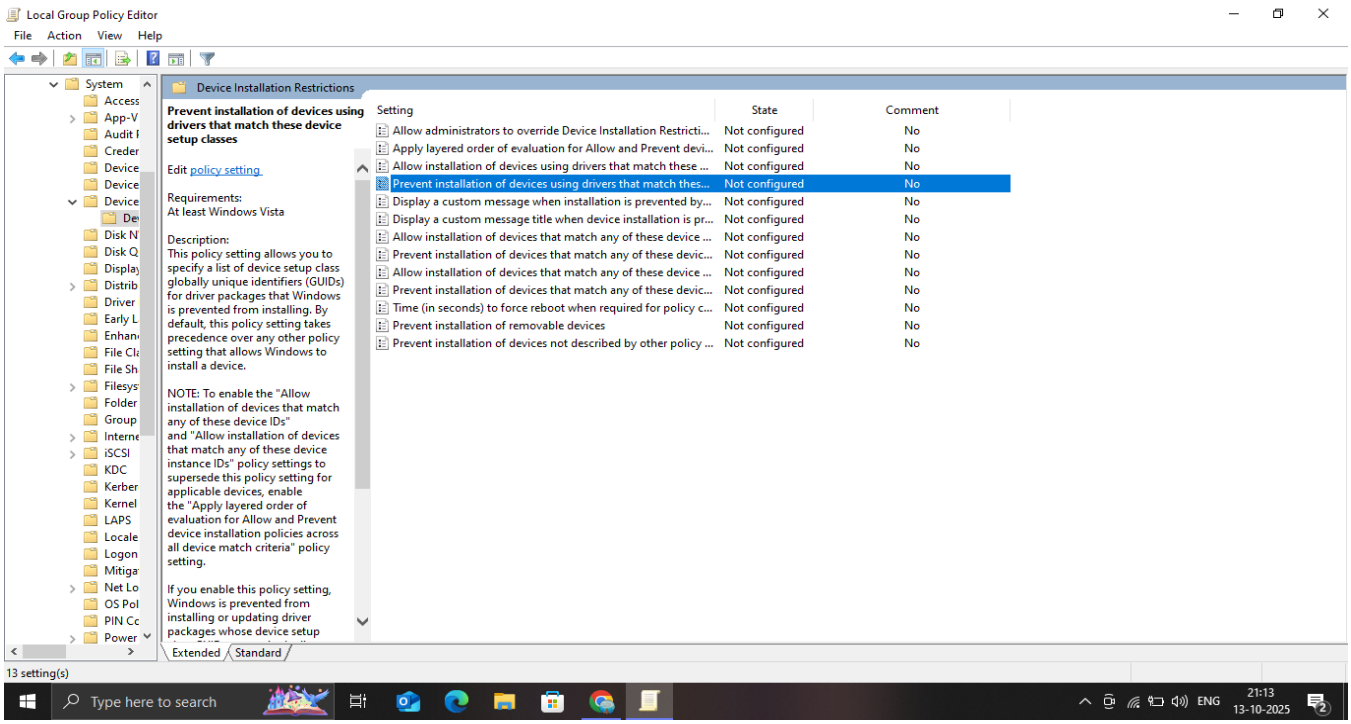
Windows 10 Regulatory Requirement	Met/Not Met
Internet Explorer Enhanced Security Configuration (IE ESC) is enabled	NA

[Screenshot]

Windows Desktop Compliance

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





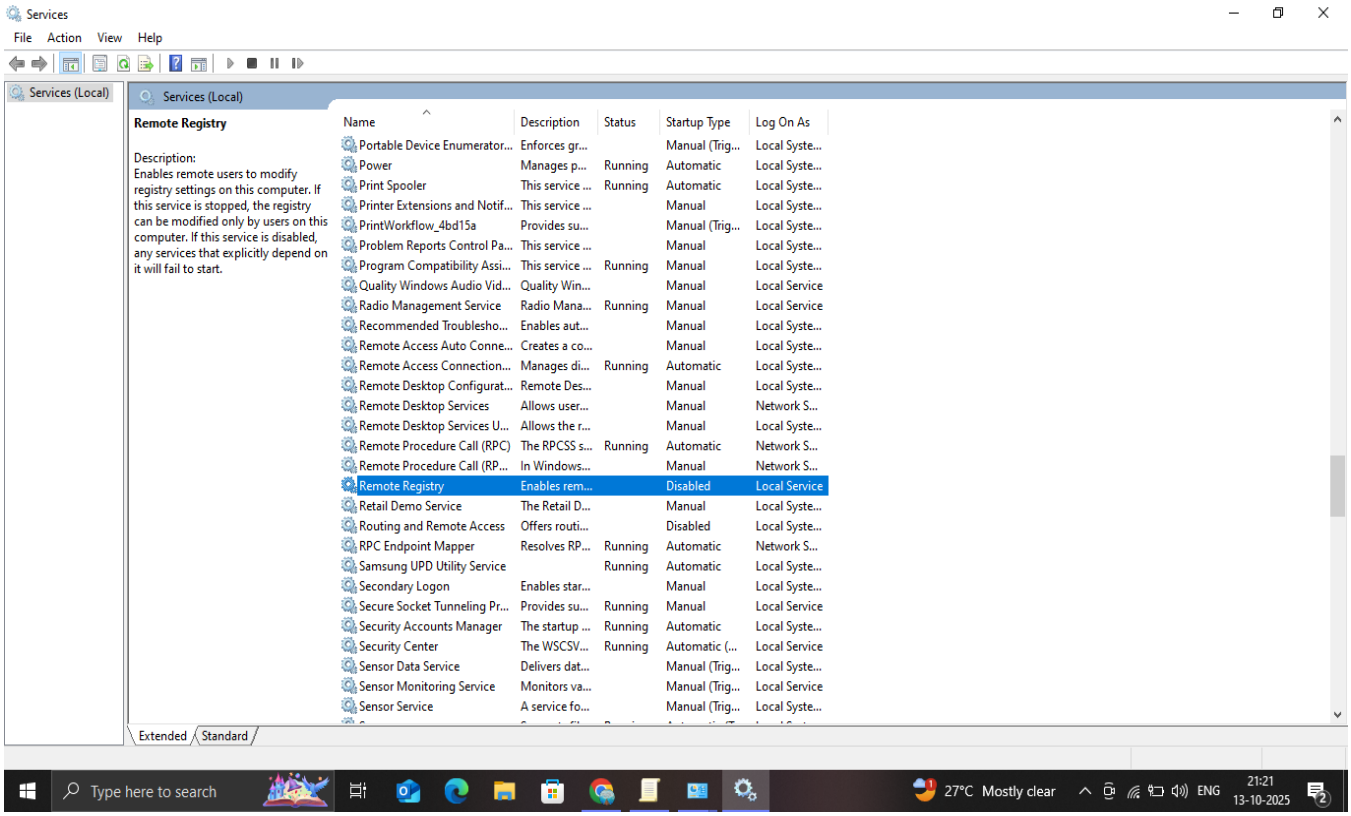
Windows Desktop Compliance

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

[Screenshot]

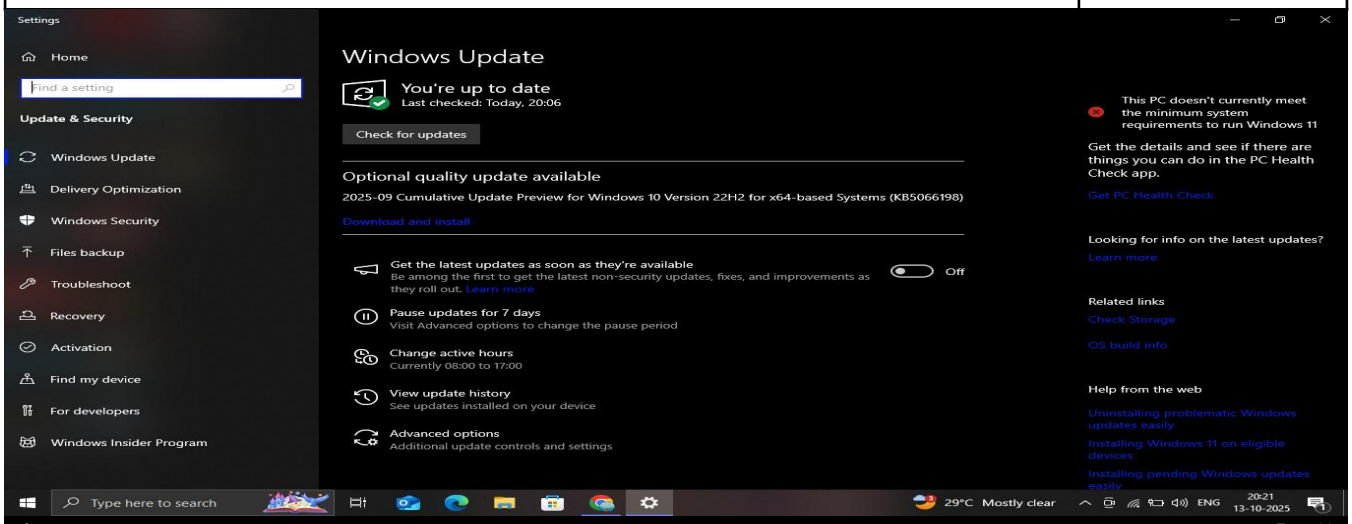
Windows Desktop Compliance

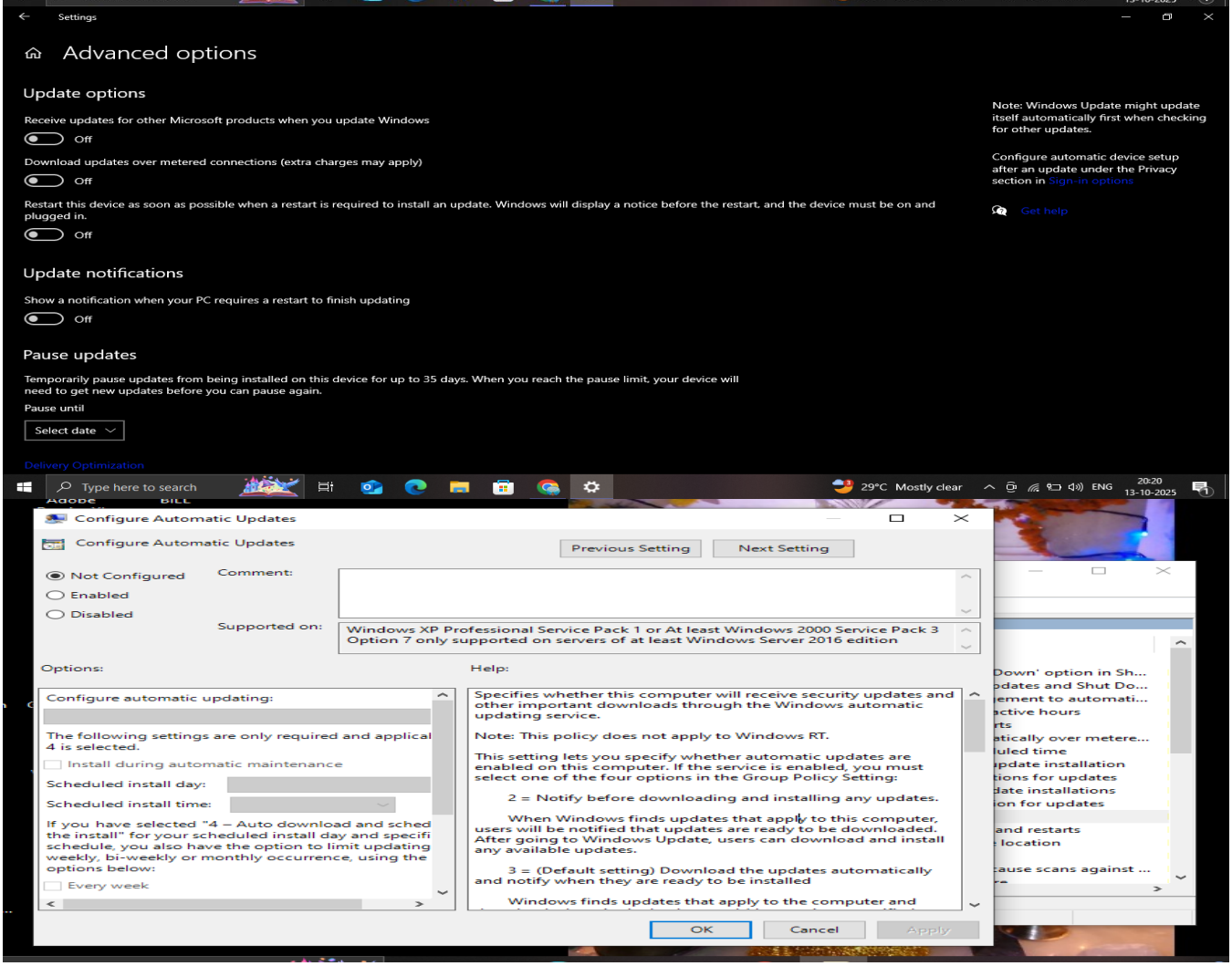
Windows 10 Regulatory Requirement	Met/Not Met
Remote Registry service is disabled	Met



Windows Desktop Compliance

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





Windows Desktop Compliance

Ensuring the Windows 10 desktop at Fed F1rst 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 > Alwoyse 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 Maximun 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 managenment, 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.

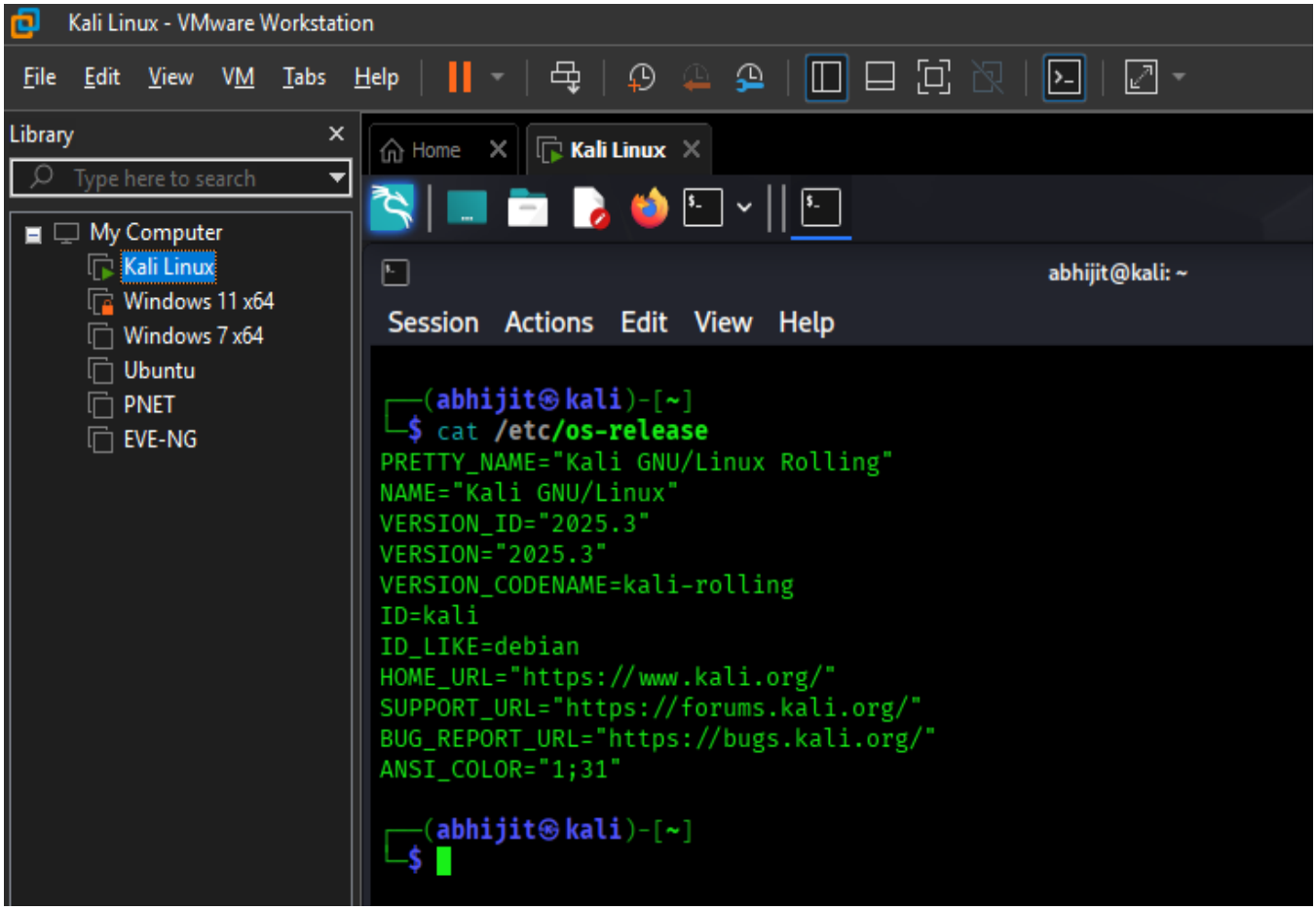
- Review the provided 15-item list of CMMC controls
- Assess a Linux VM for compliance with each listed control
- For each control, determine if it is:
  - **Met:** The Kali Linux VM complies with the CMMC control
  - **Not Met:** The Kali Linux VM does not comply with the CMMC control
  - **NA (Not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

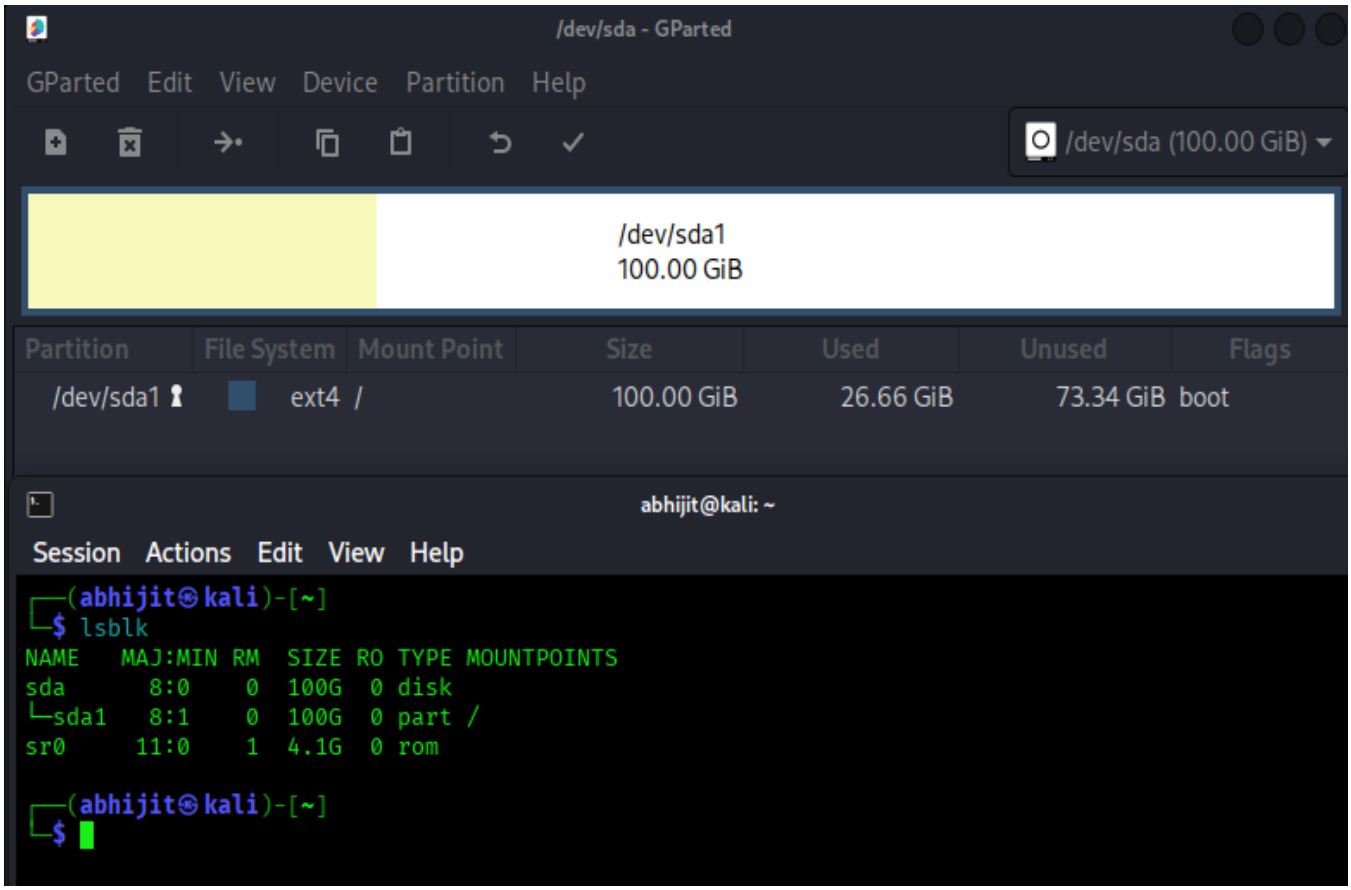
Linux Compliance

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



Linux Compliance

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



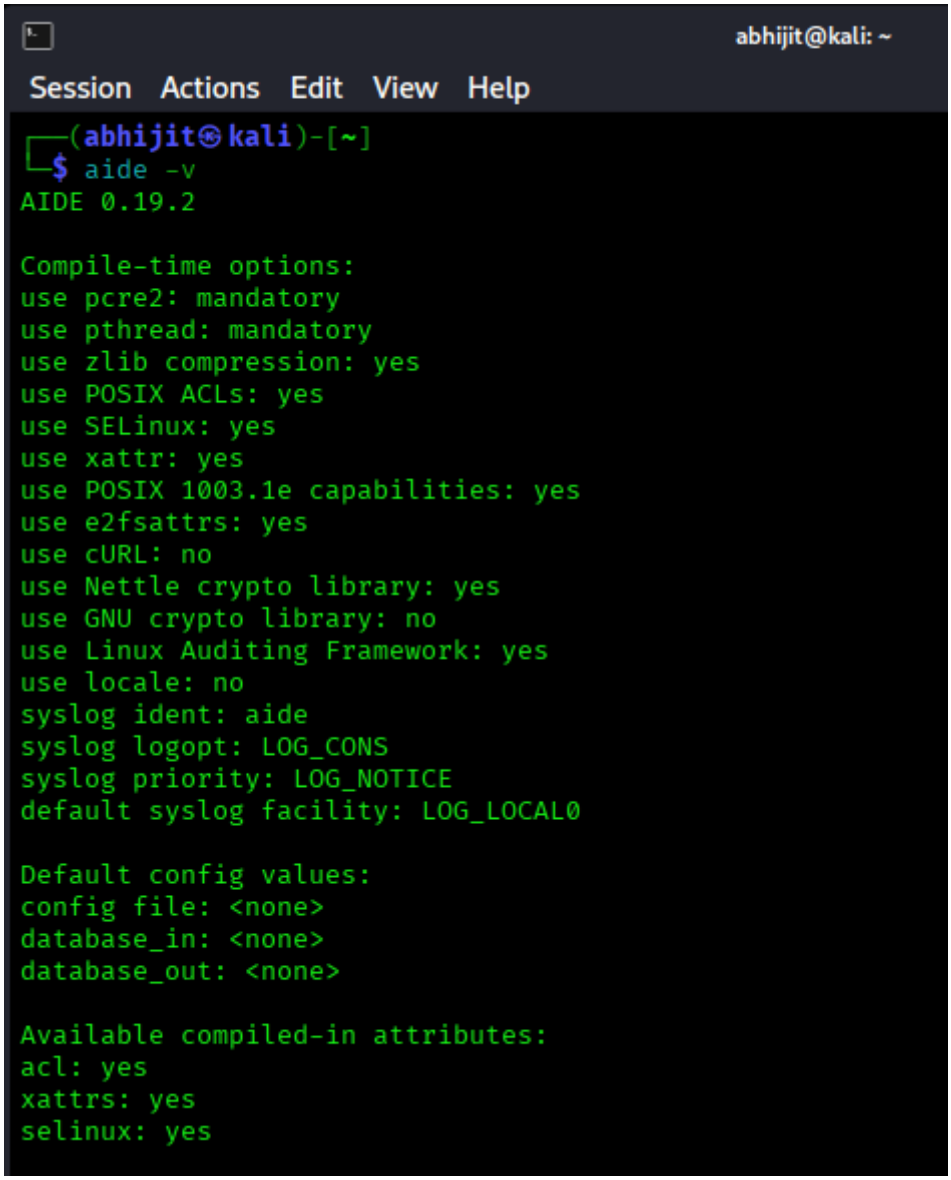
Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Disable Automounting of drives	

[Screenshot]

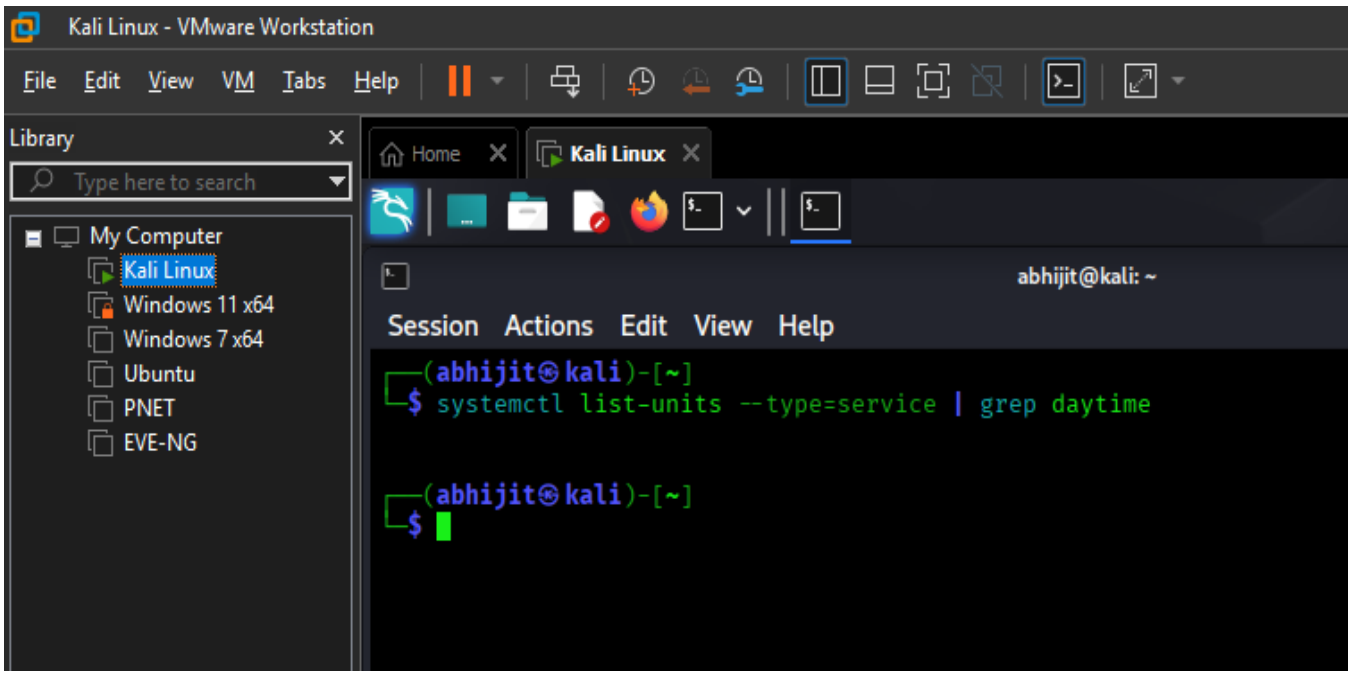
Linux Compliance

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



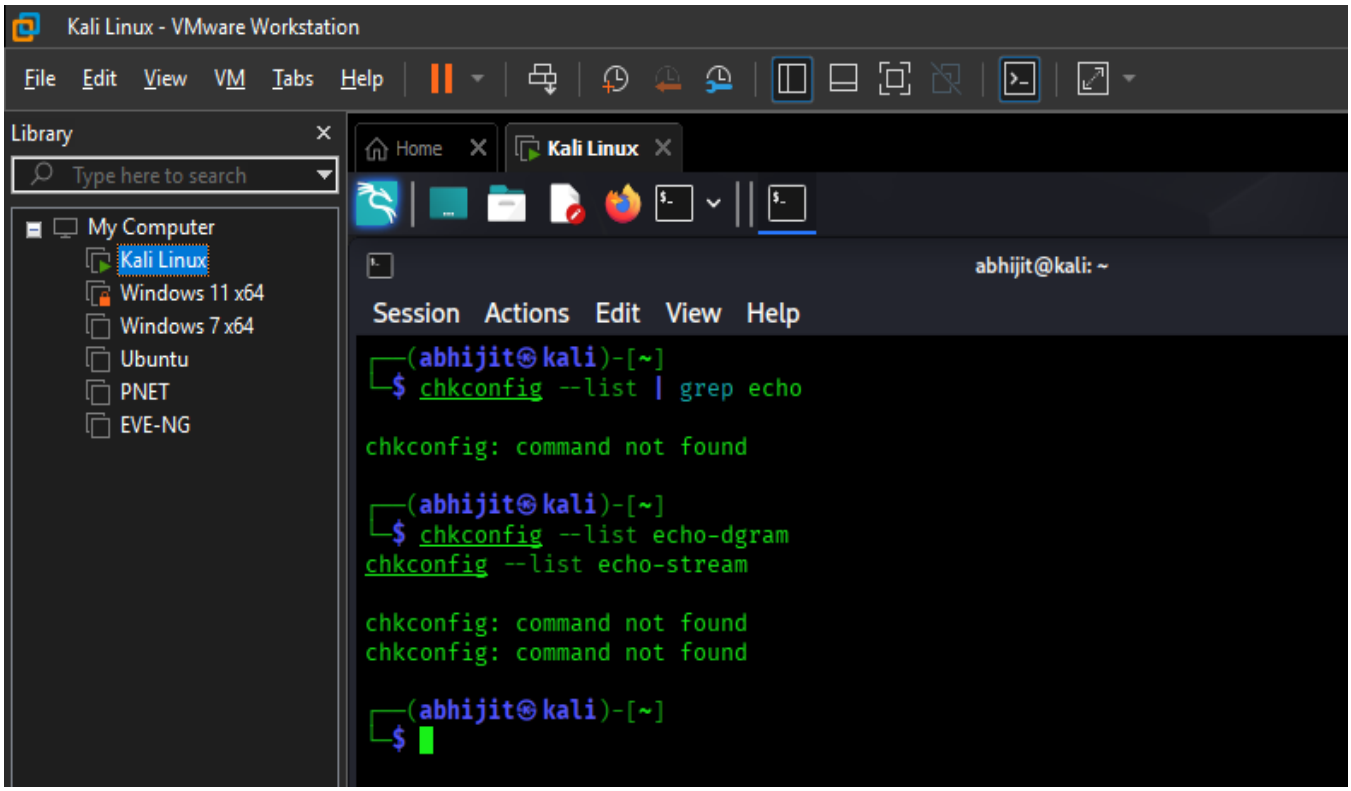
Linux Compliance

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



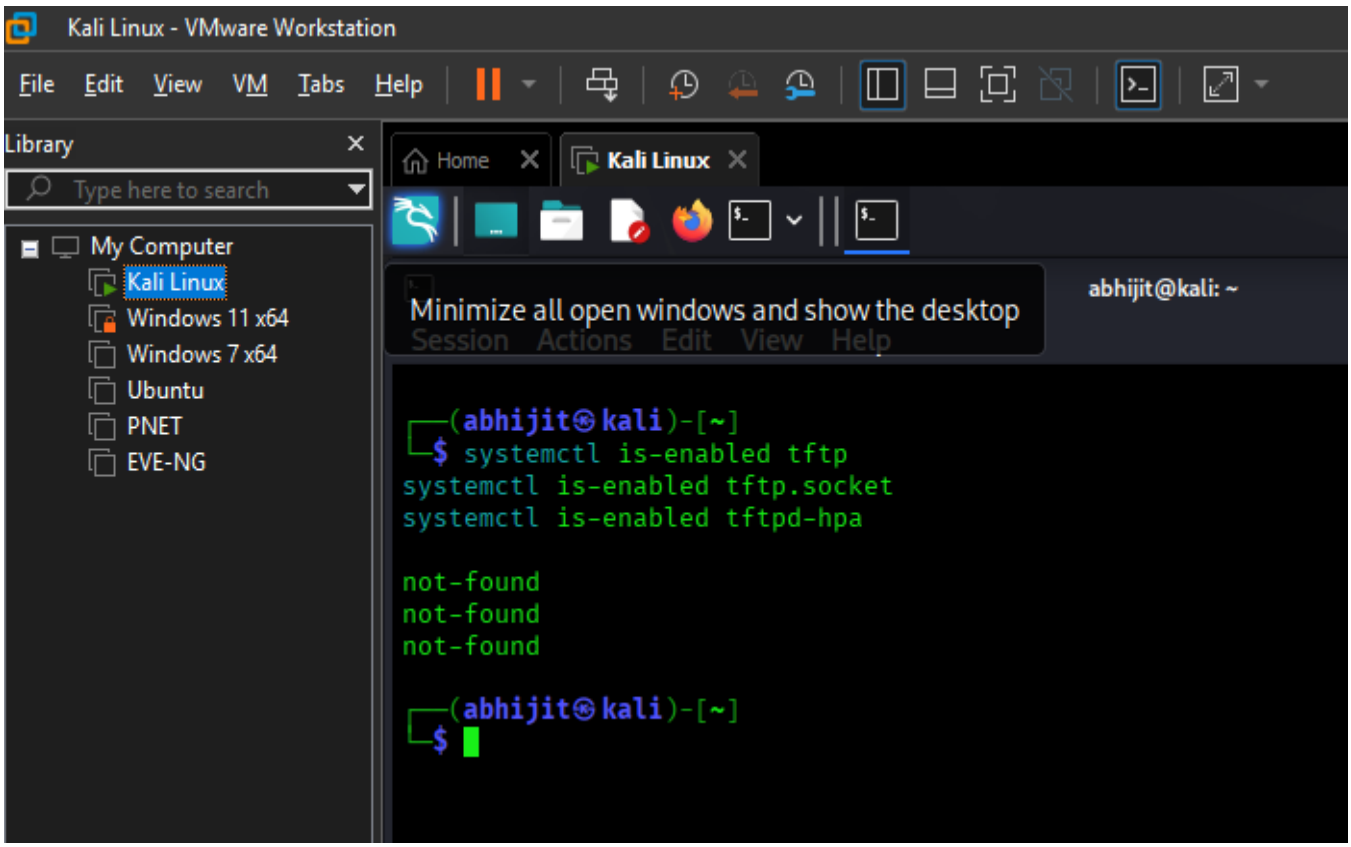
Linux Compliance

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



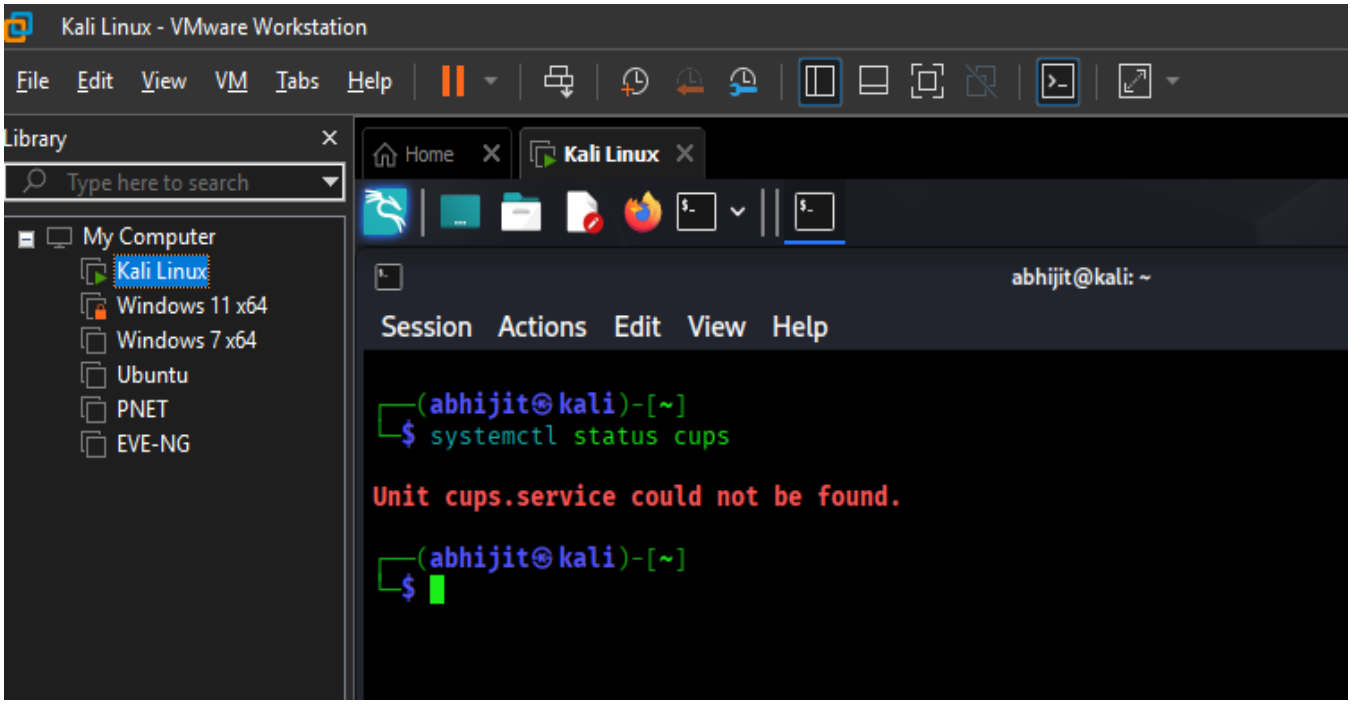
Linux Compliance

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



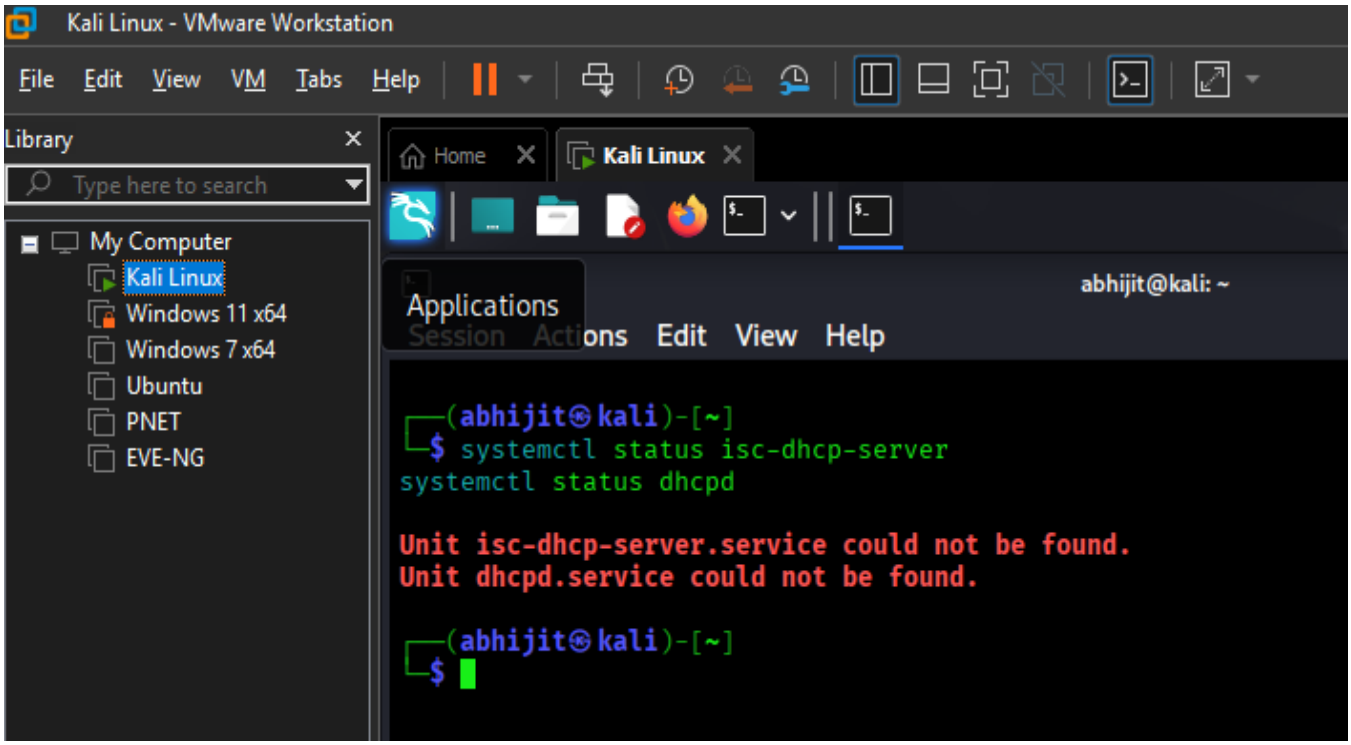
Linux Compliance

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



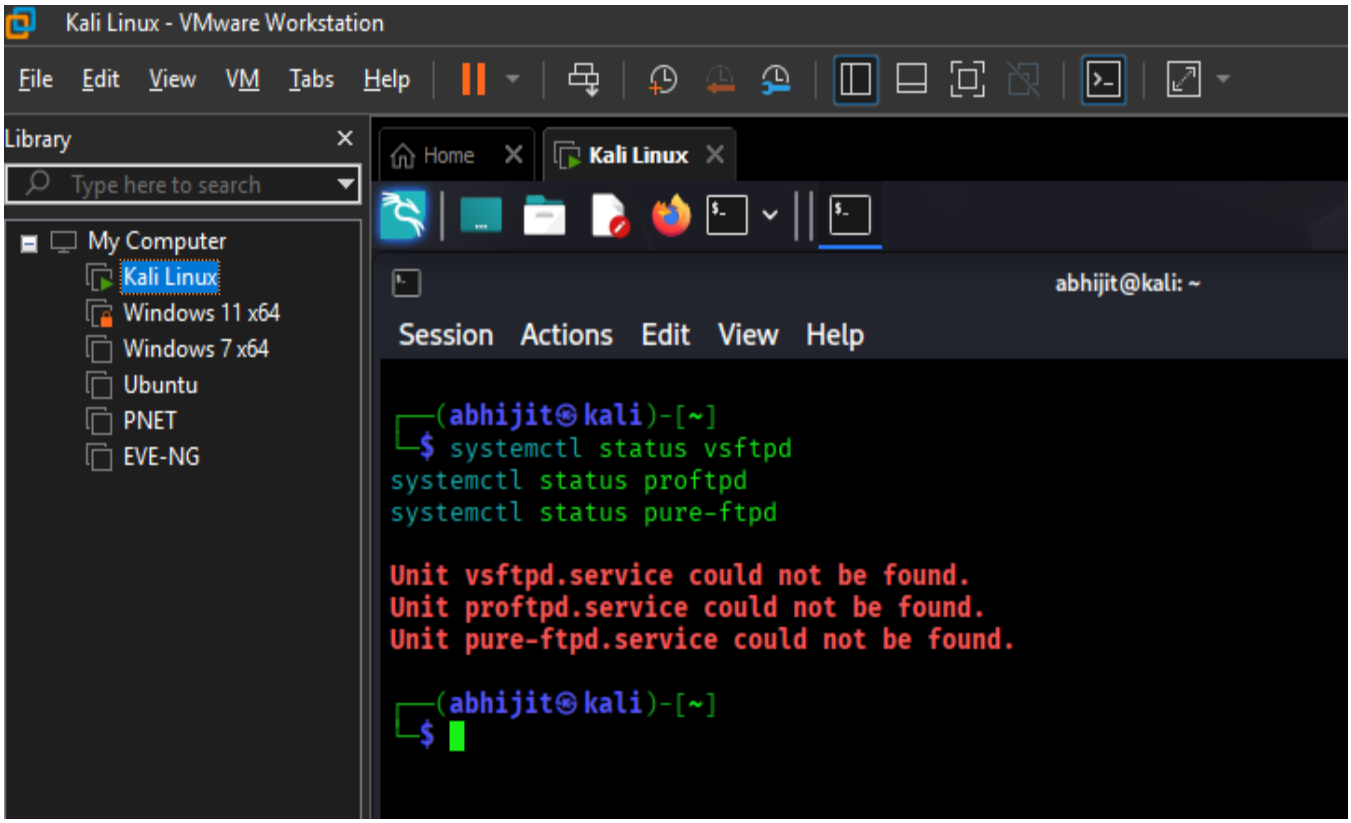
Linux Compliance

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



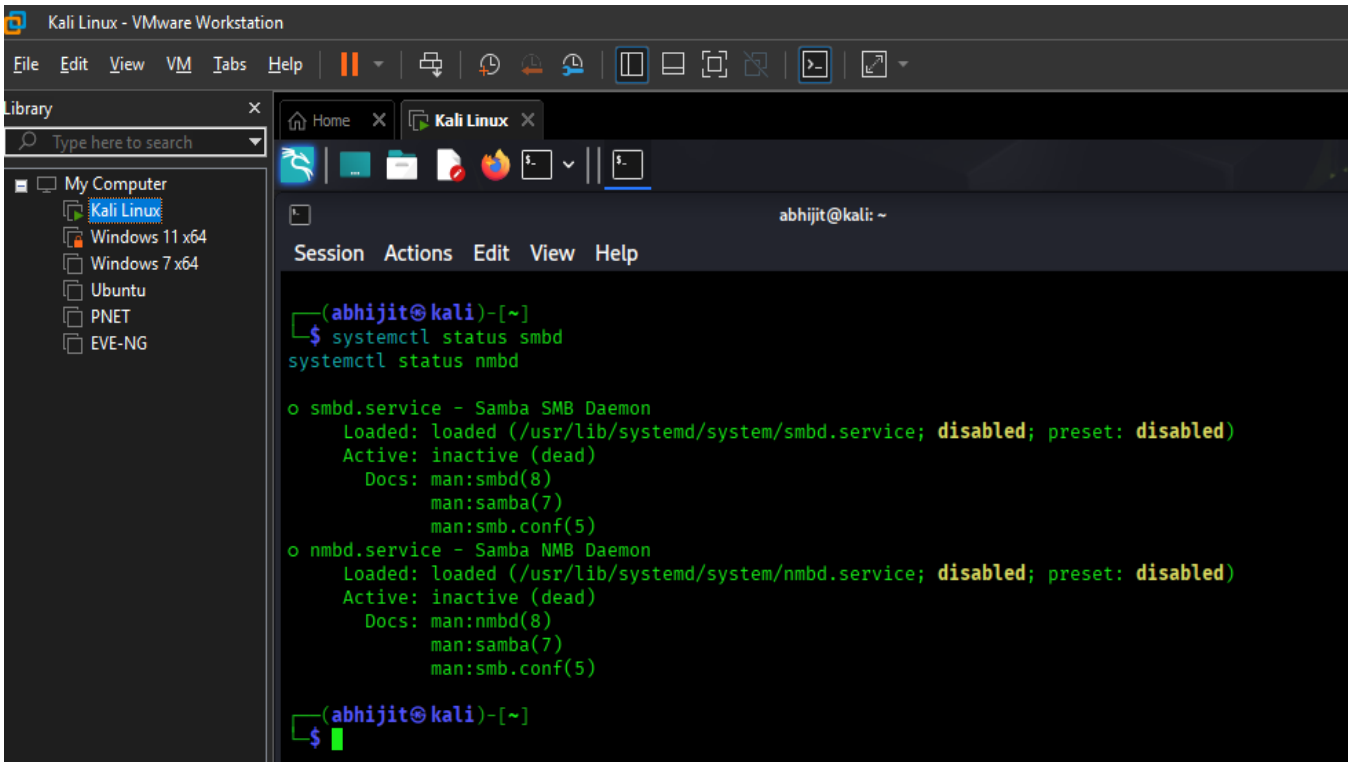
Linux Compliance

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



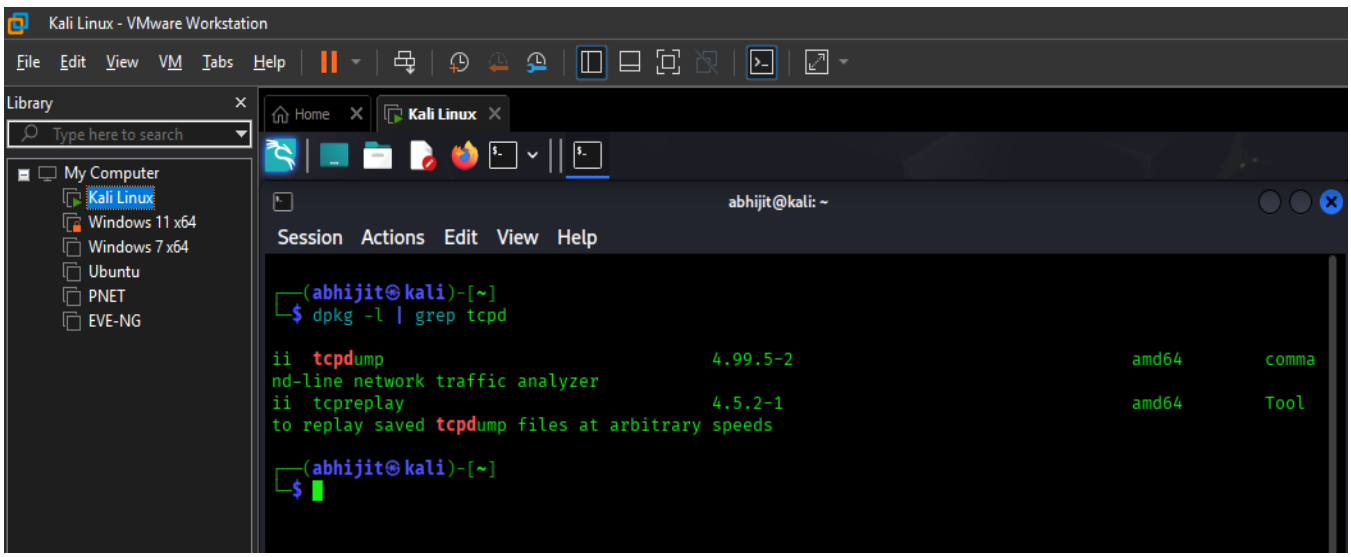
Linux Compliance

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



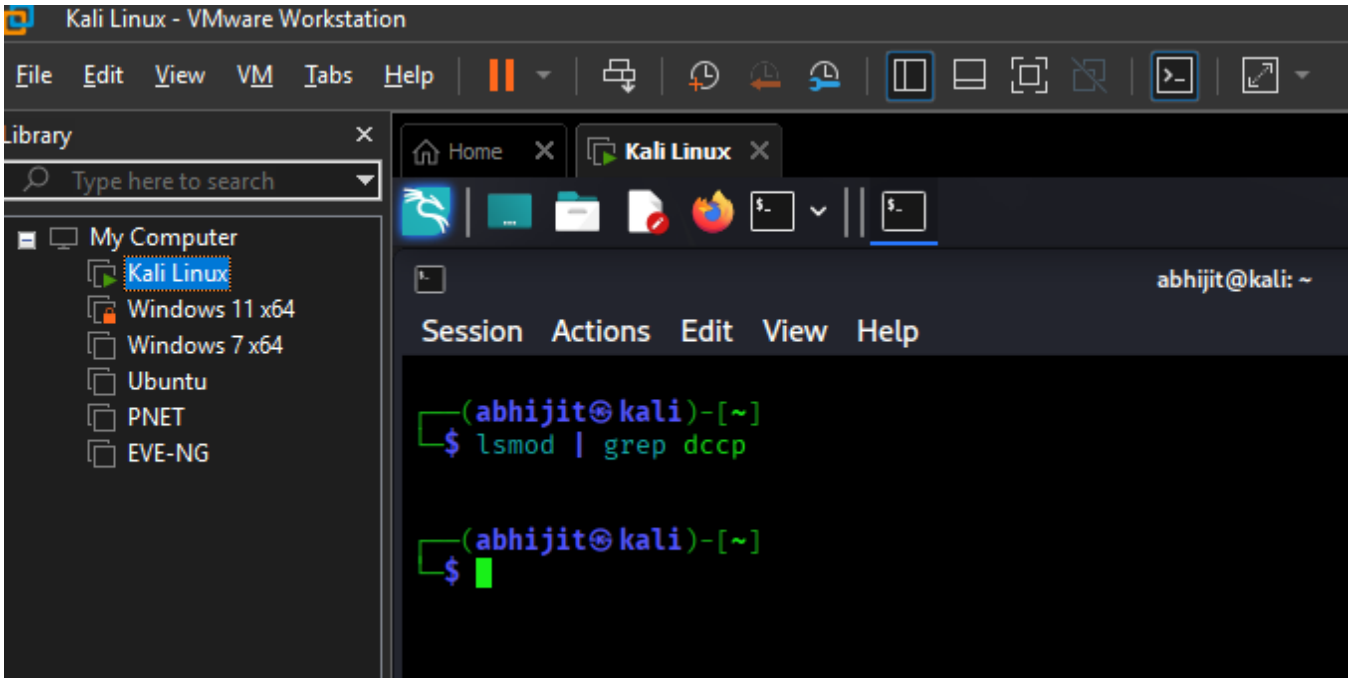
Linux Compliance

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



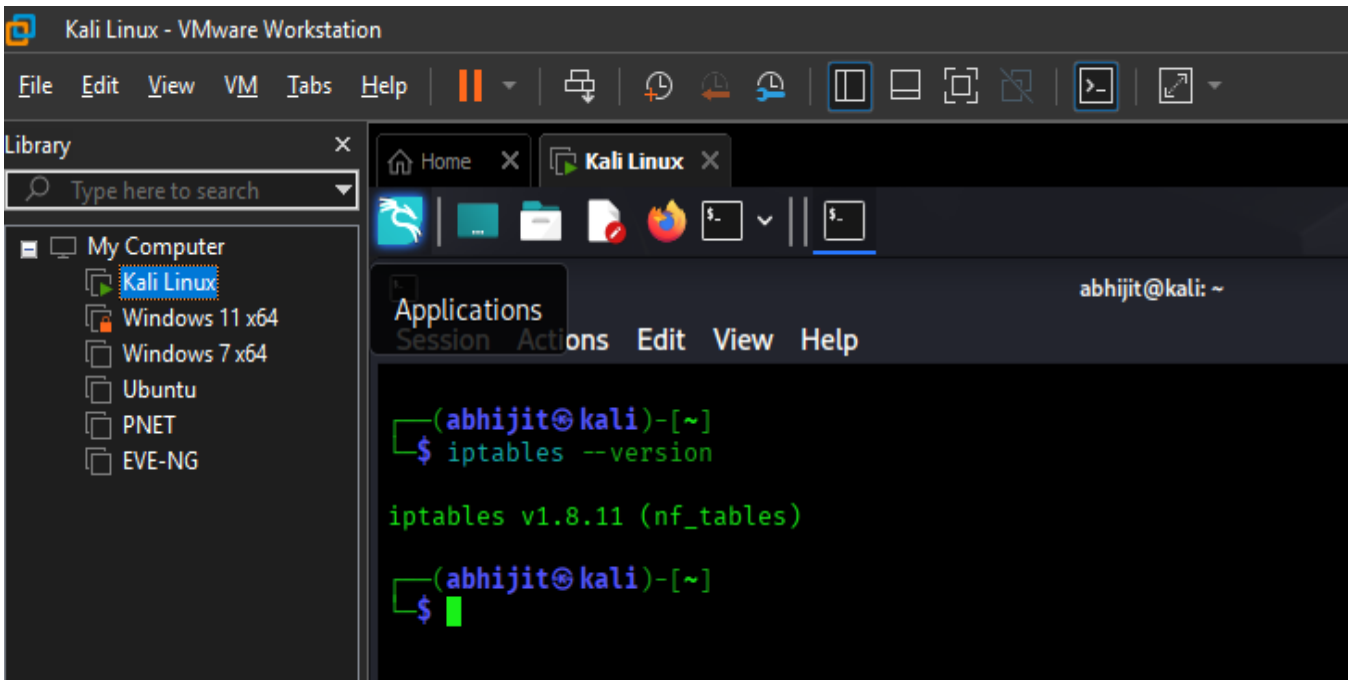
Linux Compliance

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



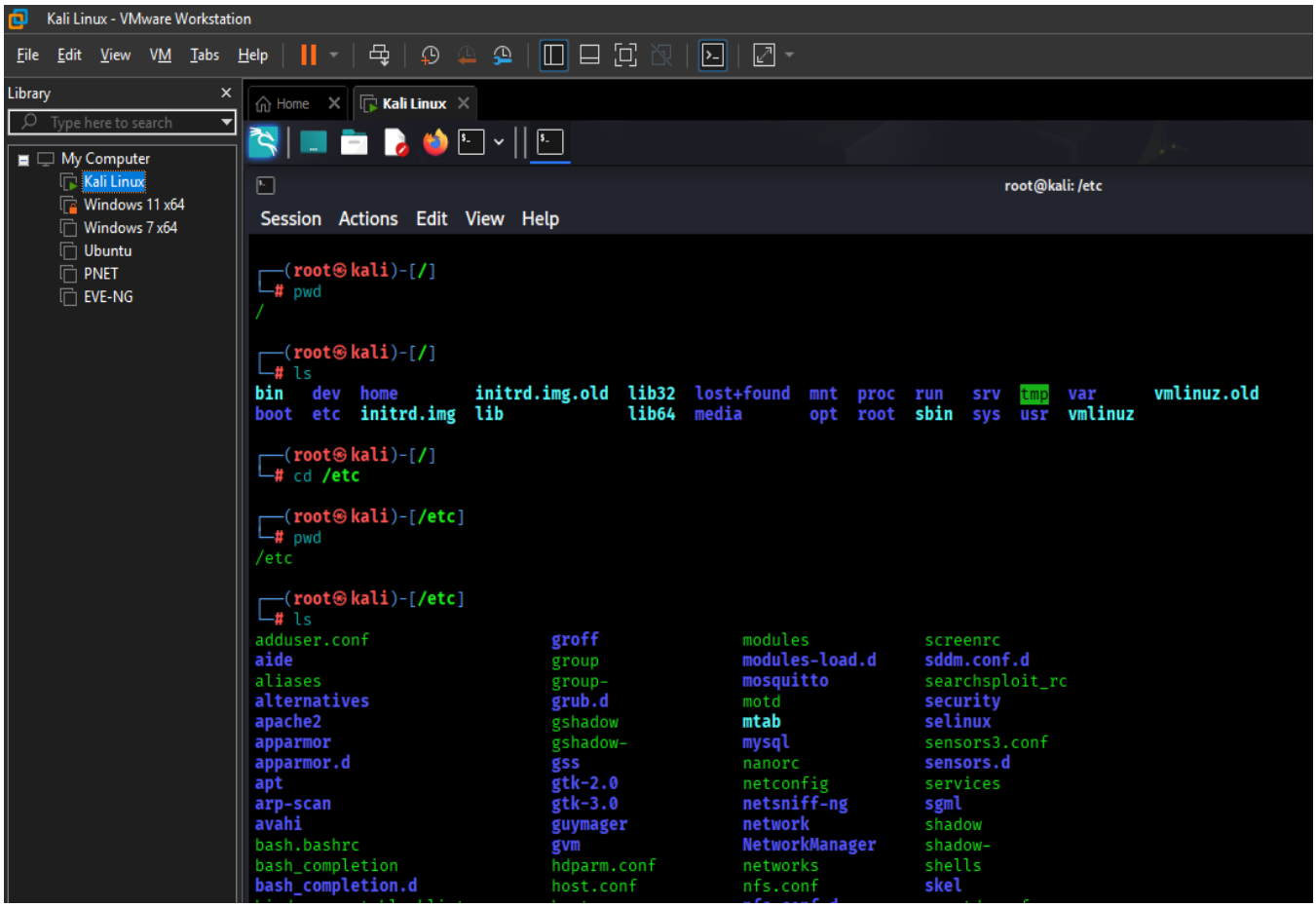
Linux Compliance

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



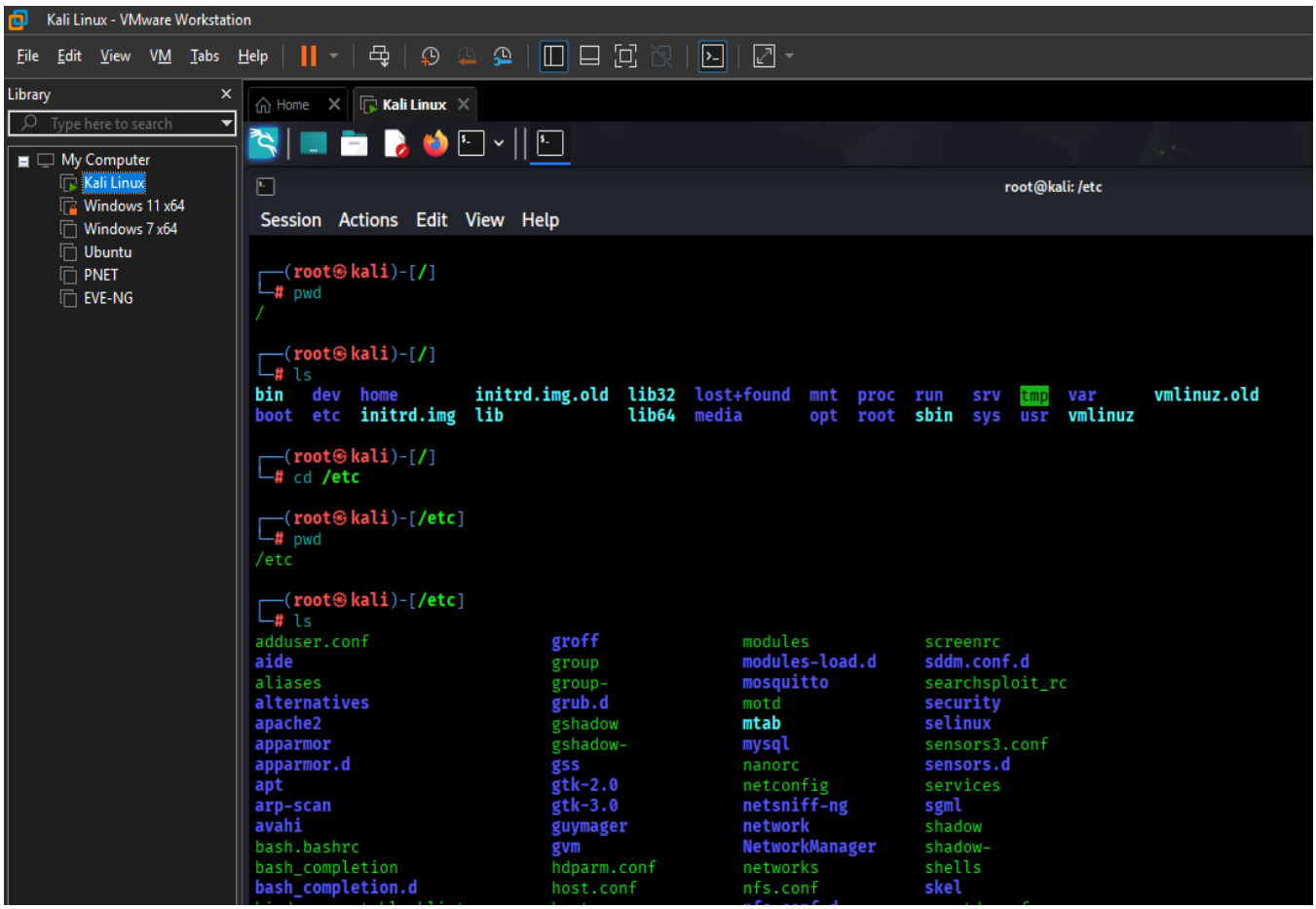
Linux Compliance

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



Linux Compliance

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



Section 4: Cloud Management

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 requirmentsand patch automation setup like using AWS patch manager or Azure update management.]

3. [Cloud instance configaration]

[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 desidnated 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 configaration]
[Document settings for Internet Information Services (IIS), including IIS modules, application pools setup HTTPS enforcement and minimumTLS version configaration.]
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 Monitore.]
8. [Backup and Recovery]
[Configure automated backup procedures for critical OS, data and IIS configuration, including retention policies and regular backup testing like seheduled 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 enforching 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 wed deploy tool used for application deployment. List any required software packages, runtime versions like .NET and configurations, as well as a referance 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 cloude usage]
[CASBs provide comprehensiv 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 allowing to monitore both sanctioned and unsanctioned services and identify shadow IT risks, monitor data flow, ensure only authorised usageof 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 remidiate unauthorised 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 supports 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 requirments 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 helth, location, and realtime risk lavel. Will gain granular and flexible user authentication, minimizing risk from compromised accounts or unsafe devises while supporting remote work.]