

COMPLIANCE ASSESSMENT



STEVEN REJI GEORGE
03-05-2025

Section 1:

Developing a Hardening Strategy

Windows 10 Hardening

1. Windows update not installed

Issue: The system is missing critical security updates.

Fixation :Go to Settings

> Update & Security

>Windows Update

>Click Check for updates and install all pending updates.



2. Antivirus is Disabled

- Issue: Active antivirus is missing, raising the risk of malware.

- Fixation: Navigate to Settings > Update & Security > Windows Security > Virus & threat protection

- Enable Windows Defender Antivirus or install a reputable third-party antivirus.



3. Windows Firewall is Off

Fixation: Navigate to Control Panel

> System and Security > Windows Defender

Firewall and enable it for

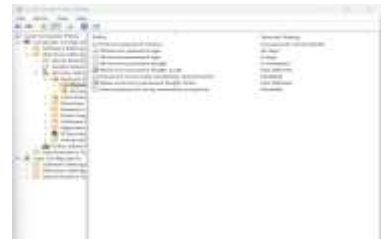
both private and public networks.



Windows 10 Hardening

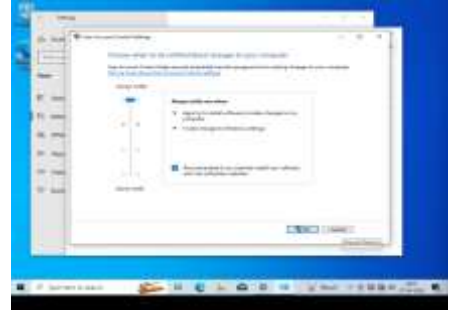
4. Weak Password policy

Fixation: Open gpedit.msc, navigate to Computer Configuration > Windows Settings > Security Settings Account Policies > Password Policy, and apply strong settings such as minimum length 12 and password complexity.



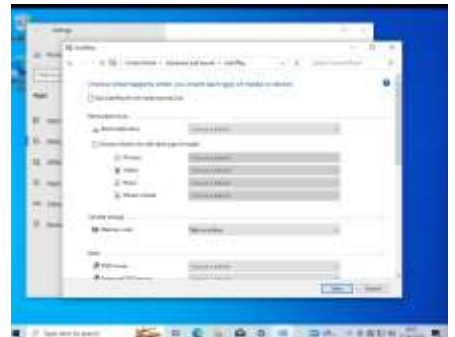
5. User Account Control Settings

Fixation: Go to Control Panel > User Accounts > User Accounts > Change User Account Control settings and move the slider to the top to set it to Always notify.



6. AutoPlay is Enabled

Fixation: Go to Control Panel > Hardware and Sound > AutoPlay, uncheck "Use AutoPlay for all media and devices," and set all media types to Take no action.



MacOS Hardening

1. Set up FileVault full-disk encryption.

FileVault encrypts the Mac's startup disk's full-disk content, keeping sensitive information safe in the event of loss or theft. This is essential to avoid unauthorized access to corporate information.

2. Strong Password Policy

Mandate strong password settings (e.g., minimum length, complexity) and review passwords tools.

Rationale: Secure passwords are the initial line of defense against unauthorized access. Requiring complexity and length makes passwords more difficult to break. Password management software can assist users in generating and storing strong, unique passwords.

3. Firewall

Turn on the built-in macOS firewall.

The firewall prevents unauthorized incoming network connections, keeping malicious individuals from accessing the system remotely.

MacOS Hardening

4. Gatekeeper

Set Gatekeeper to install apps only from the App Store and recognized developers.

Gatekeeper prevents malware by limiting the sources applications can be installed from. This minimizes the possibility of users installing malicious software.

5. System updates

#. Allow automatic system updates

#. It is critical to keep macOS and applications updated in order to patch security vulnerabilities. Automatic updates guarantee that the most recent security patches are applied in a timely manner.

6. Remote Management

#. Disable or limit remote management capabilities (e.g., screen sharing, remote login) unless absolutely necessary and lock them down with strong authentication.

#Remote management capabilities can be used by attackers to achieve unauthorized access to a system. Disabling them or properly locking them down reduces this risk.

Section 2:

Create Security Policies

Email Policy

1. Use strong and distinct passwords for email accounts and turn on two-factor authentication to secure against unauthorized access.

2. Do not open email attachments or click links from untrusted or unknown sources to protect against phishing and malware attacks.

3. Report suspicious emails or phishing attempts to the IT or security team on a regular basis.

4. Log out of corporate email accounts when using public or shared computers to avoid unauthorized use.

5. The organization must implement and maintain email authentication protocols such as SPF, DKIM, and DMARC to prevent email spoofing and ensure sender verification.

BYOD Policy

1. Device Encryption: All BYOD devices need to have full-disk encryption activated (e.g., FileVault for macOS, BitLocker for Windows, and native encryption on iOS/Android) to safeguard sensitive data in the event of device loss or theft.

2. Mandatory Security Software

Devices should have currently installed and active antivirus or endpoint protection software. This is a requirement on laptops and optional on mobile devices where it applies.

3. Regular System Updates

Devices should have the most supported versions of their operating systems and applications installed, with automatic updates turned on to close known security loopholes.

4. Secure Access Controls

VPN and Multi-Factor Authentication (MFA) must be used to enforce access to company systems. Root or jailbroken phones are barred from accessing corporate resources.

5. Remote Wipe and Incident Reporting

IT must be notified by employees at once in case of lost, stolen, or compromised devices. Devices should support and enable remote wipe of corporate data via the organization's mobile device management (MDM) solution.

6. Strong Authentication and Screen Lock

Employees need to set up a secure lock screen via PIN, password, fingerprint, or facial recognition. Devices should automatically lock after a short duration of inactivity.

Section 3:

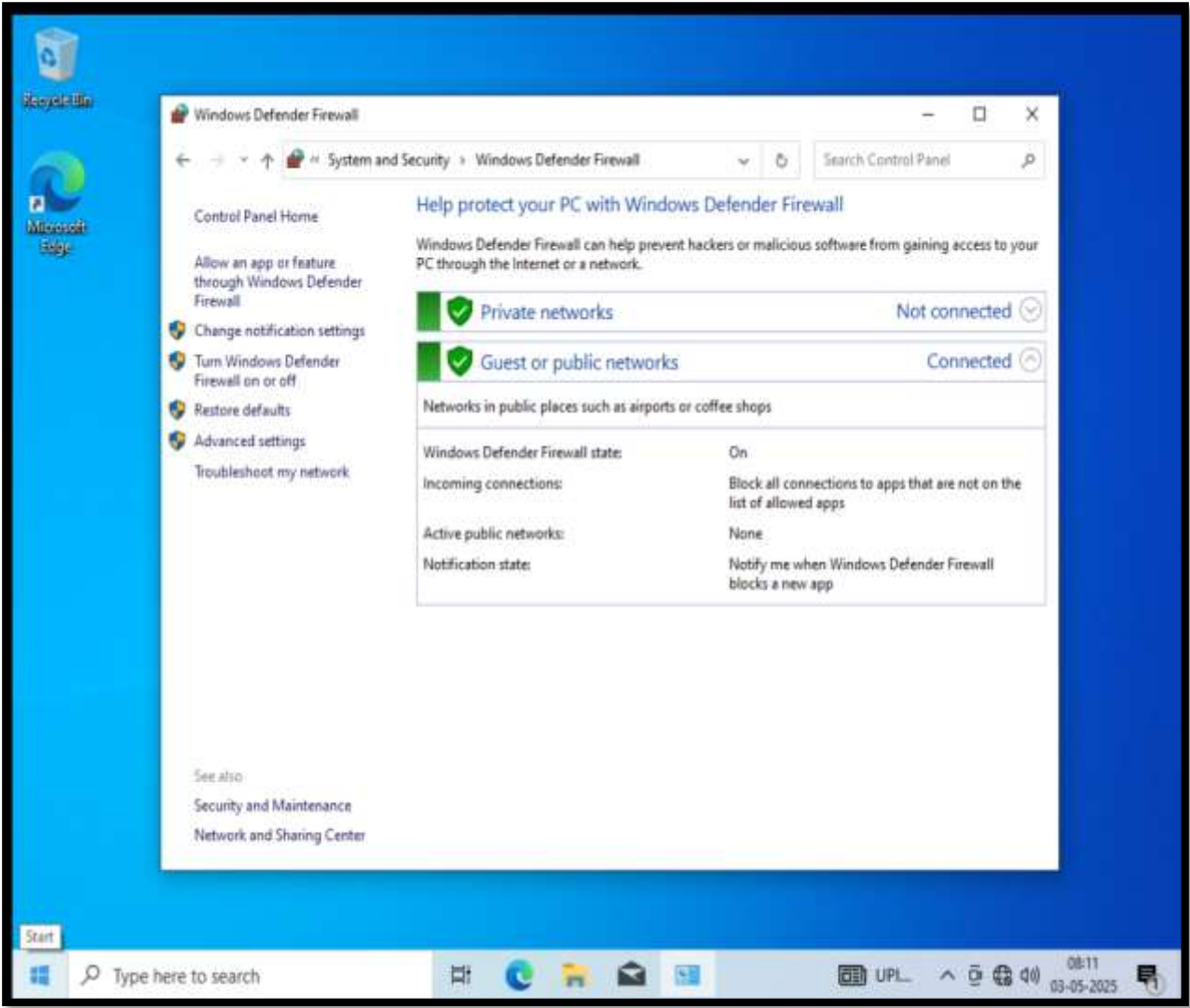
Self Assessment

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	Met
User Account Control (UAC) is enabled	Met
Strong password policies are enforced	Met
Guest account is disabled	Met
System logging and auditing are enabled	Met
Windows Defender Antivirus is enabled and up to date	Met
Remote Desktop Services are configured securely	Met
Internet Explorer Enhanced Security Configuration (IE ESC) is enabled	Met
USB ports are disabled or restricted to authorized devices only	Met
Network access controls are implemented, including VLAN segmentation and port security	Met
Remote Registry service is disabled	Met
Windows Updates are configured to download and install updates automatically	Met

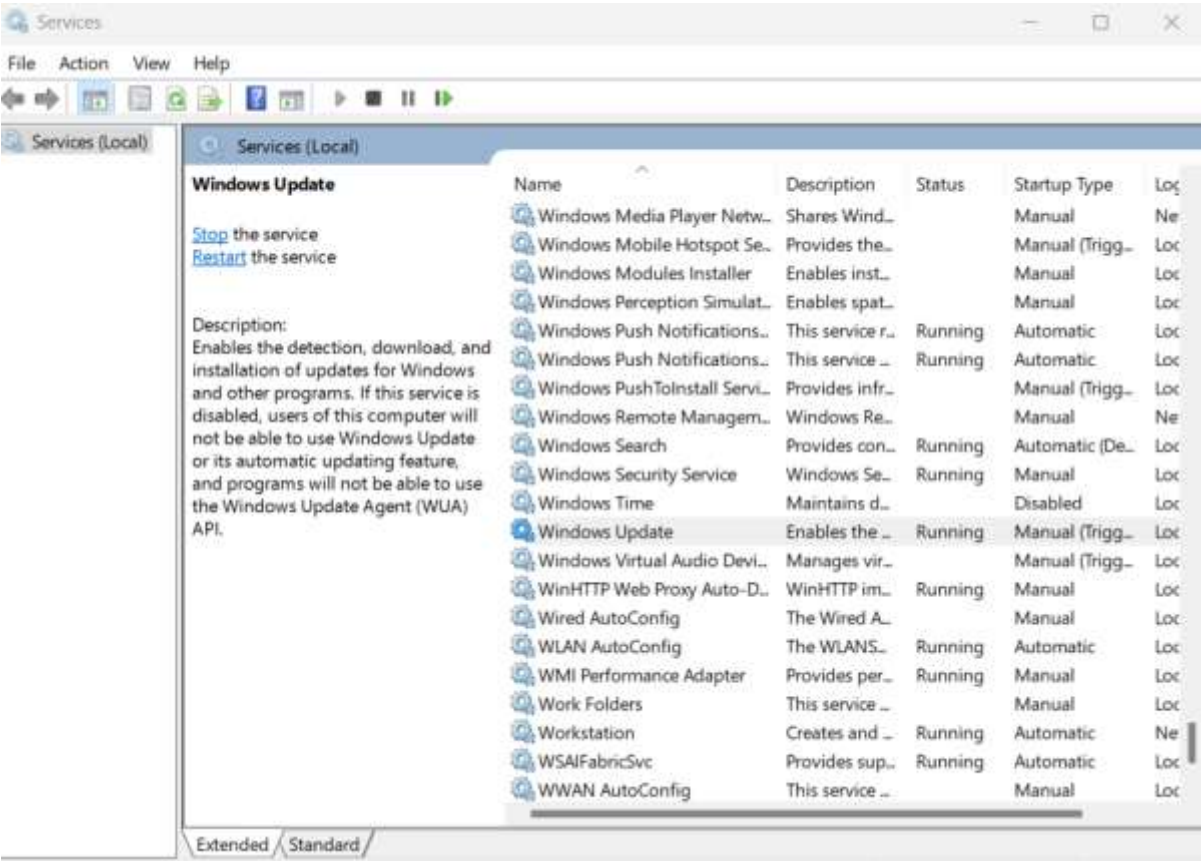
Windows Desktop Compliance

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



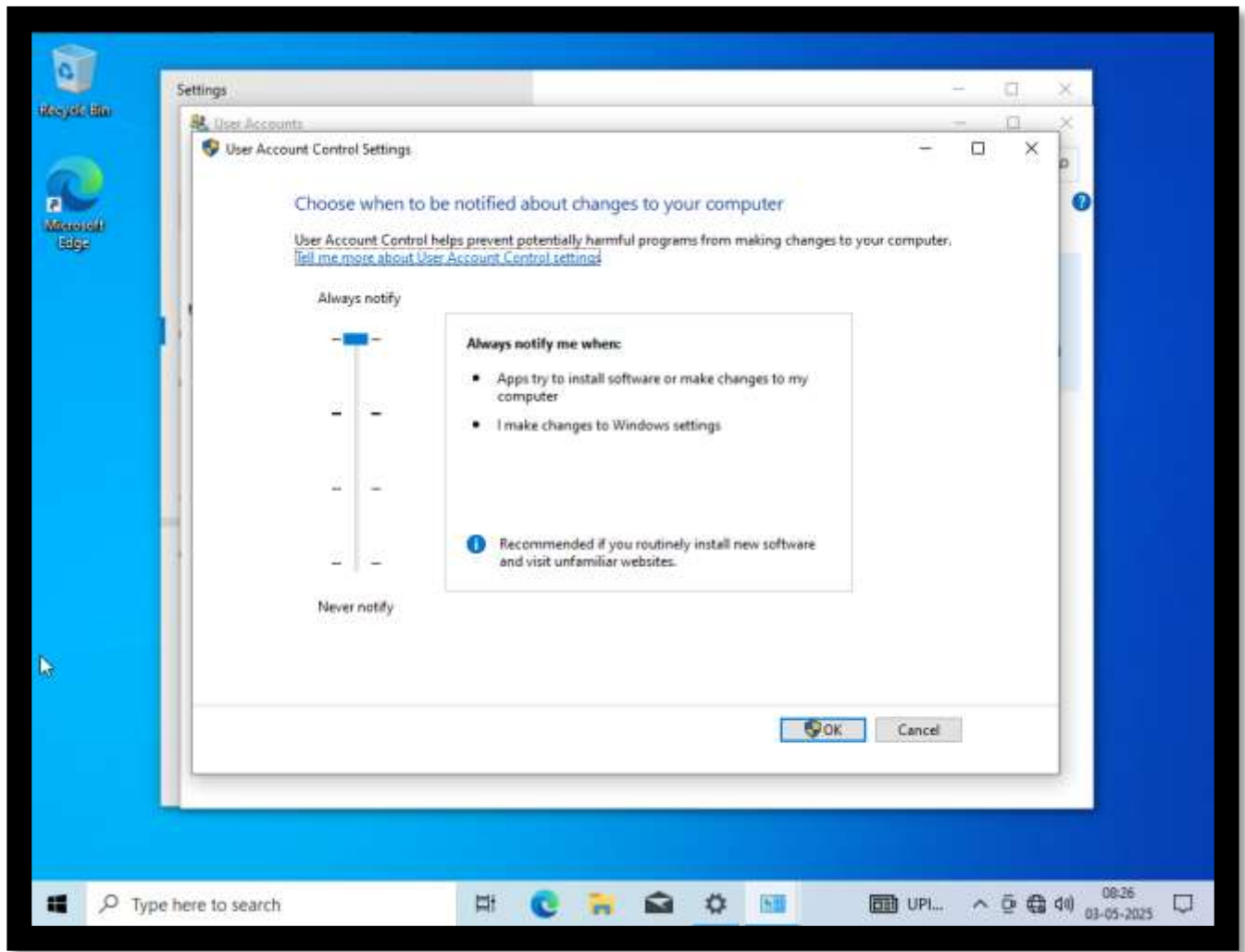
Windows Desktop Compliance

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



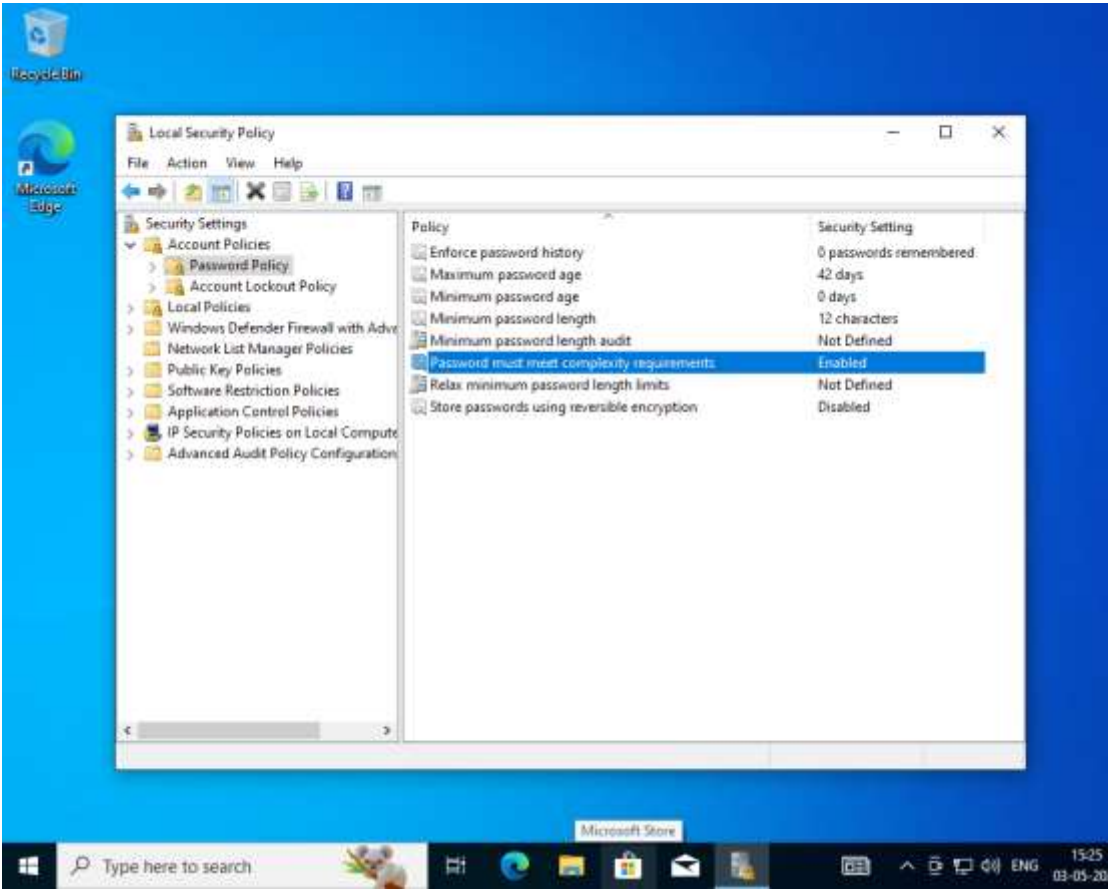
Windows Desktop Compliance

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



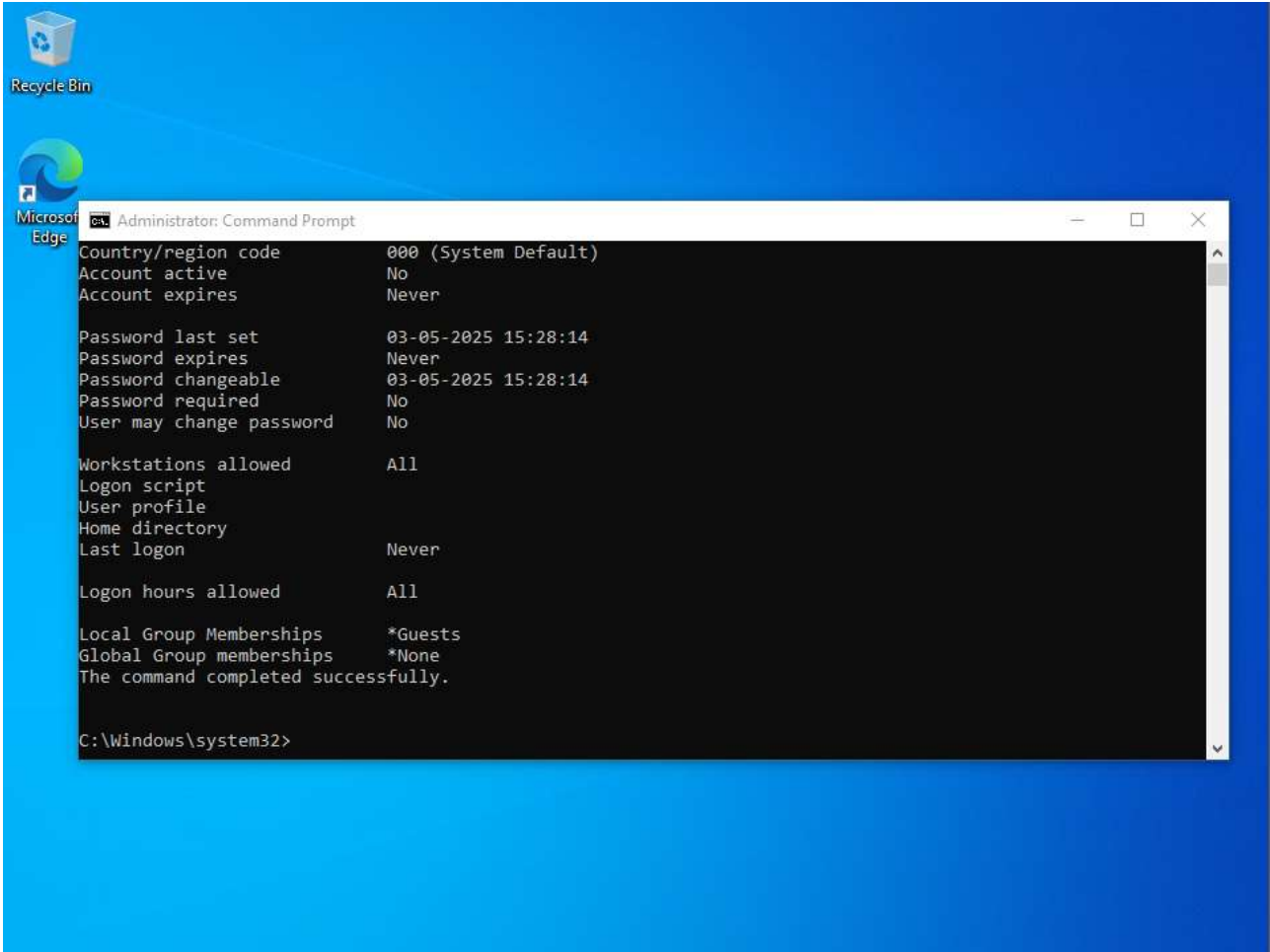
Windows Desktop Compliance

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



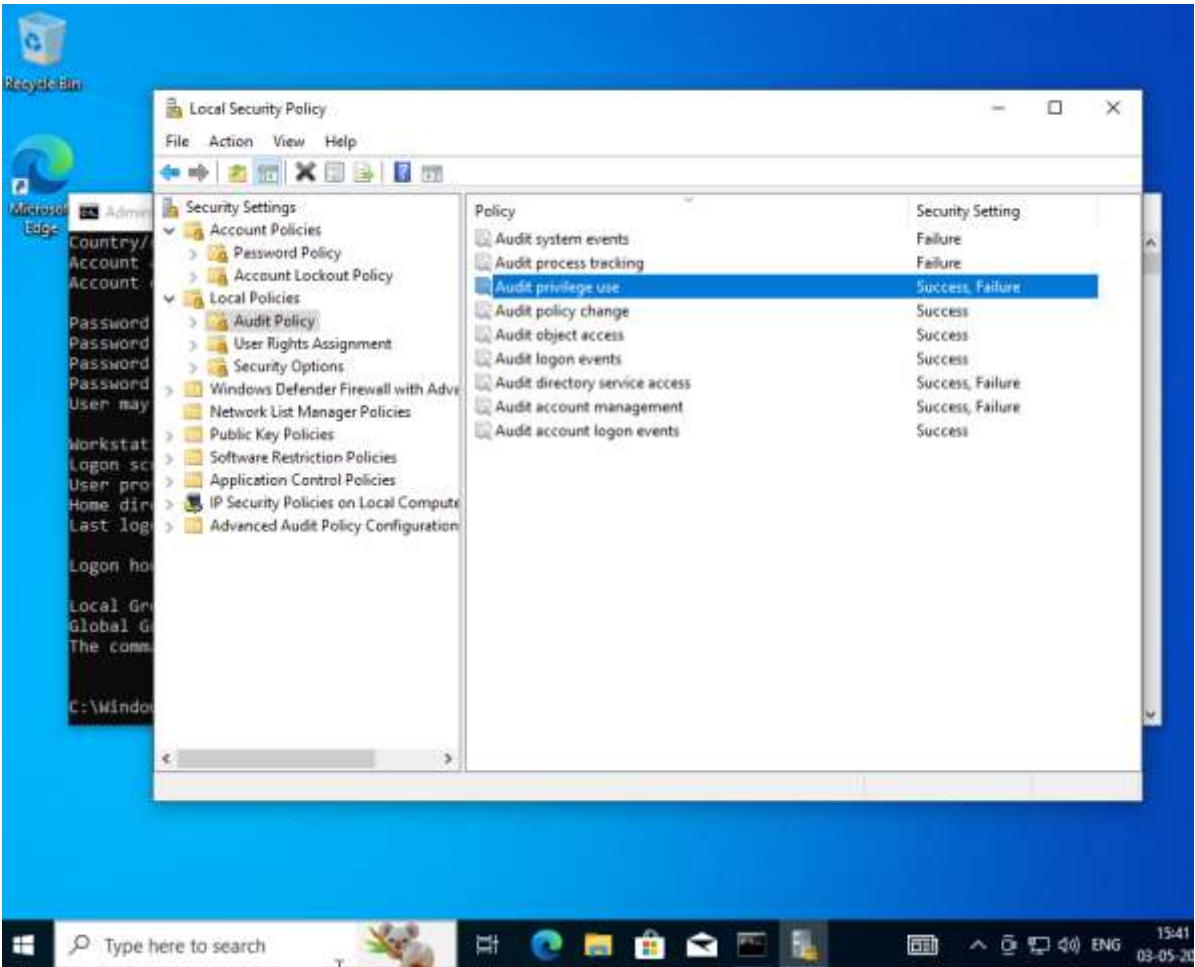
Windows Desktop Compliance

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



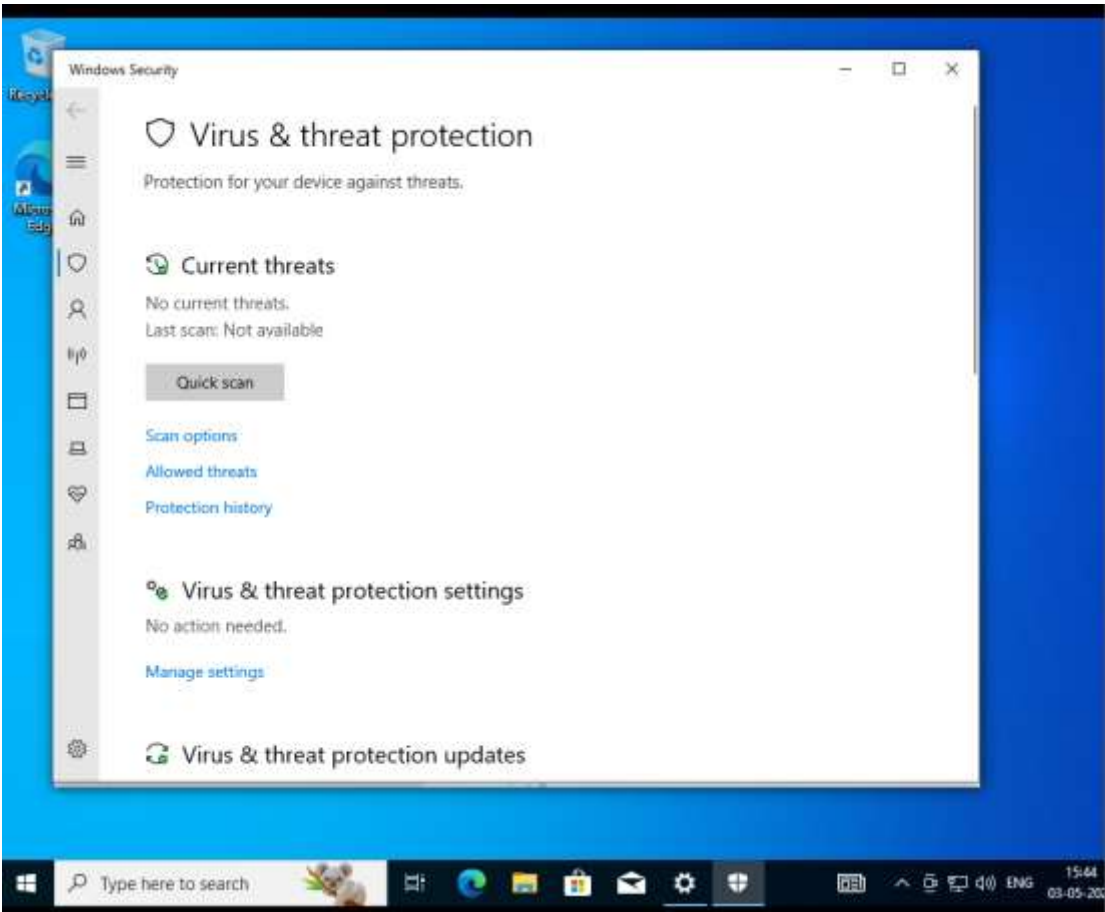
Windows Desktop Compliance

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



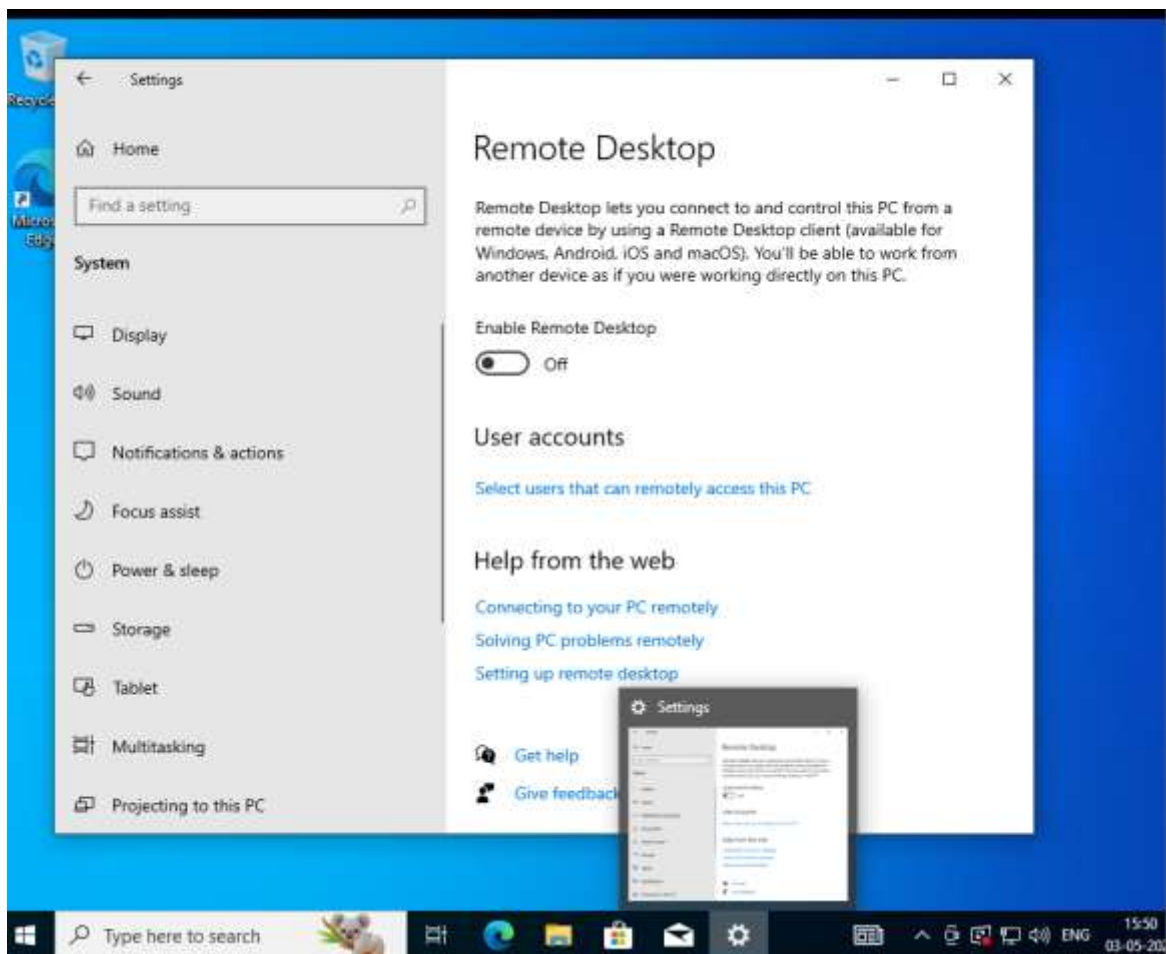
Windows Desktop Compliance

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	Met



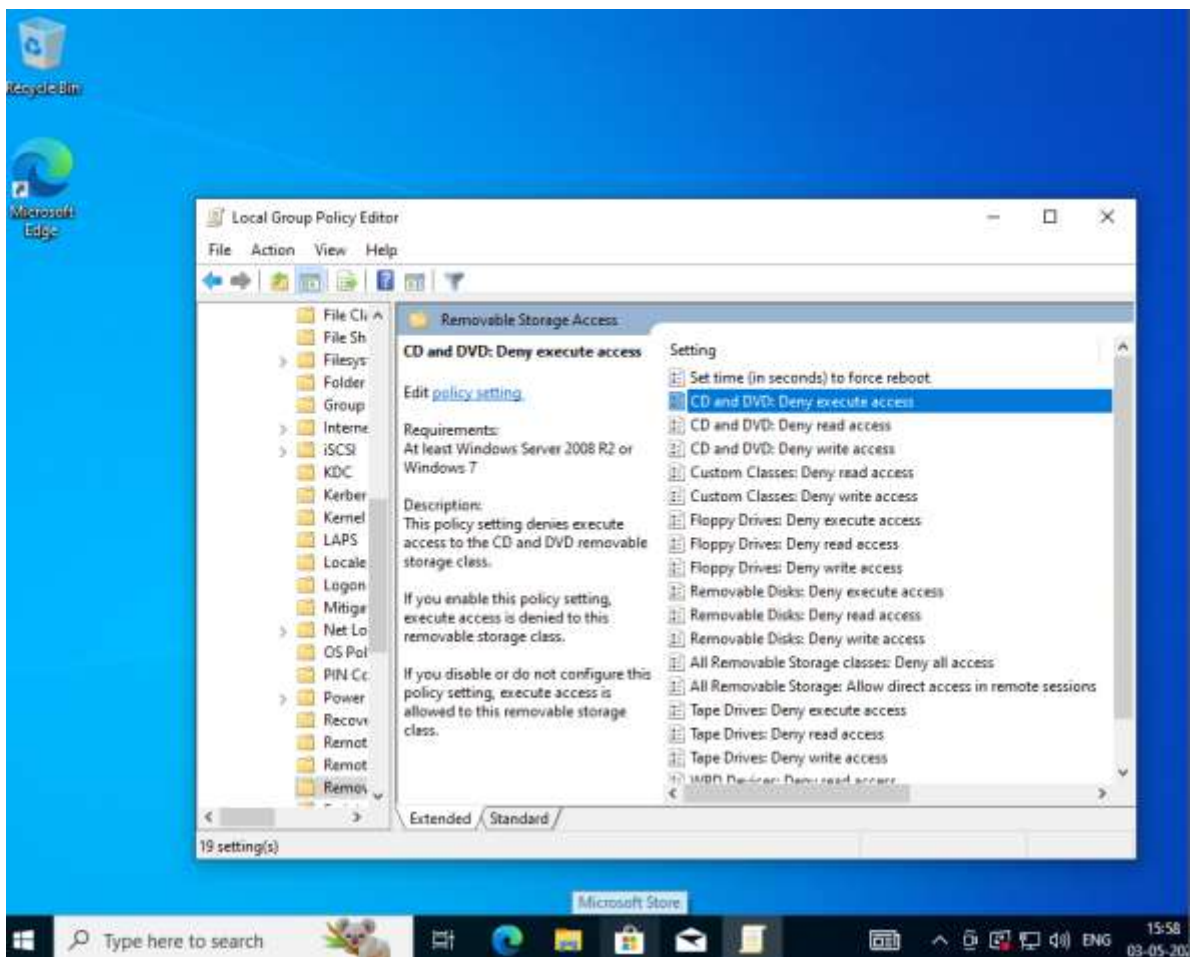
Windows Desktop Compliance

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

Nil IE ESC is not in windows 10

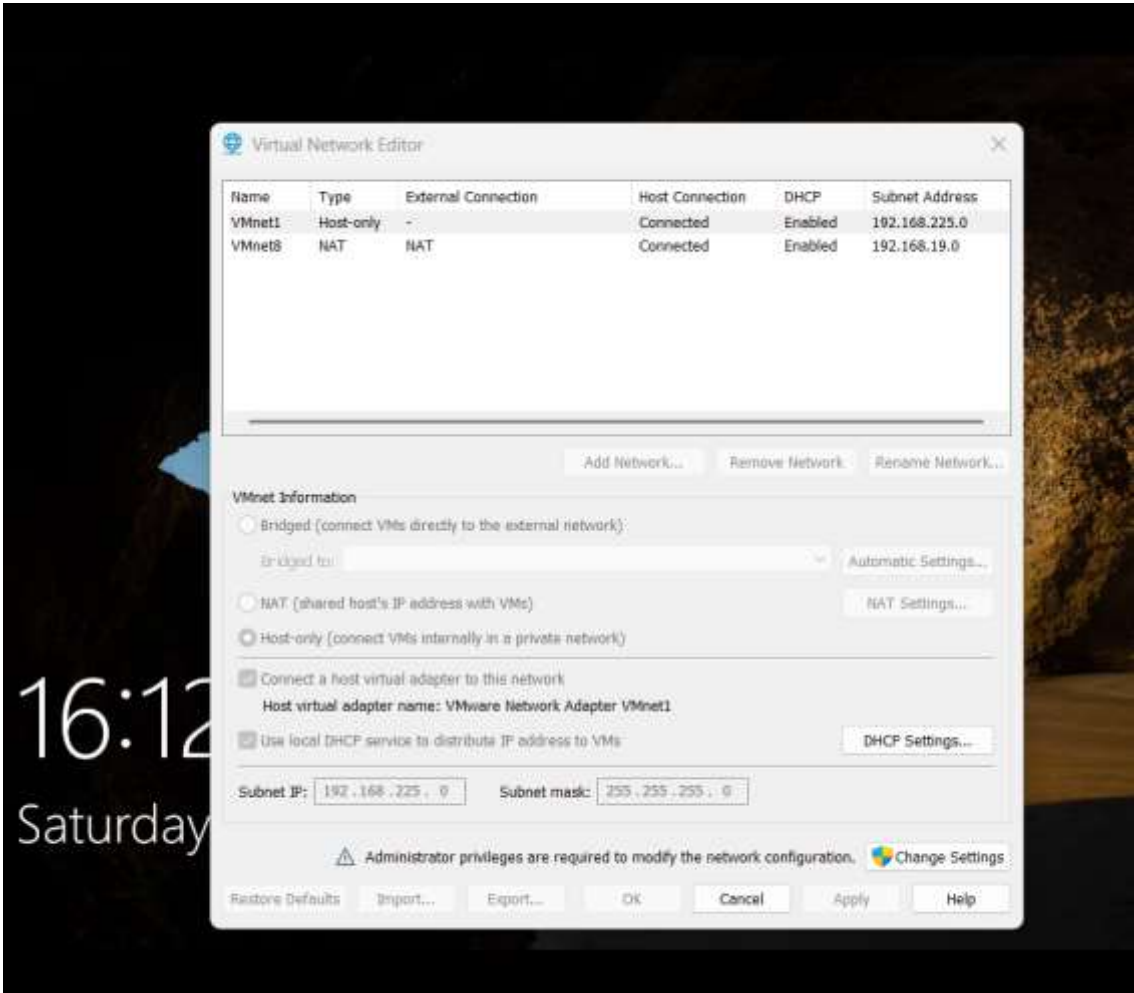
Windows Desktop Compliance

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



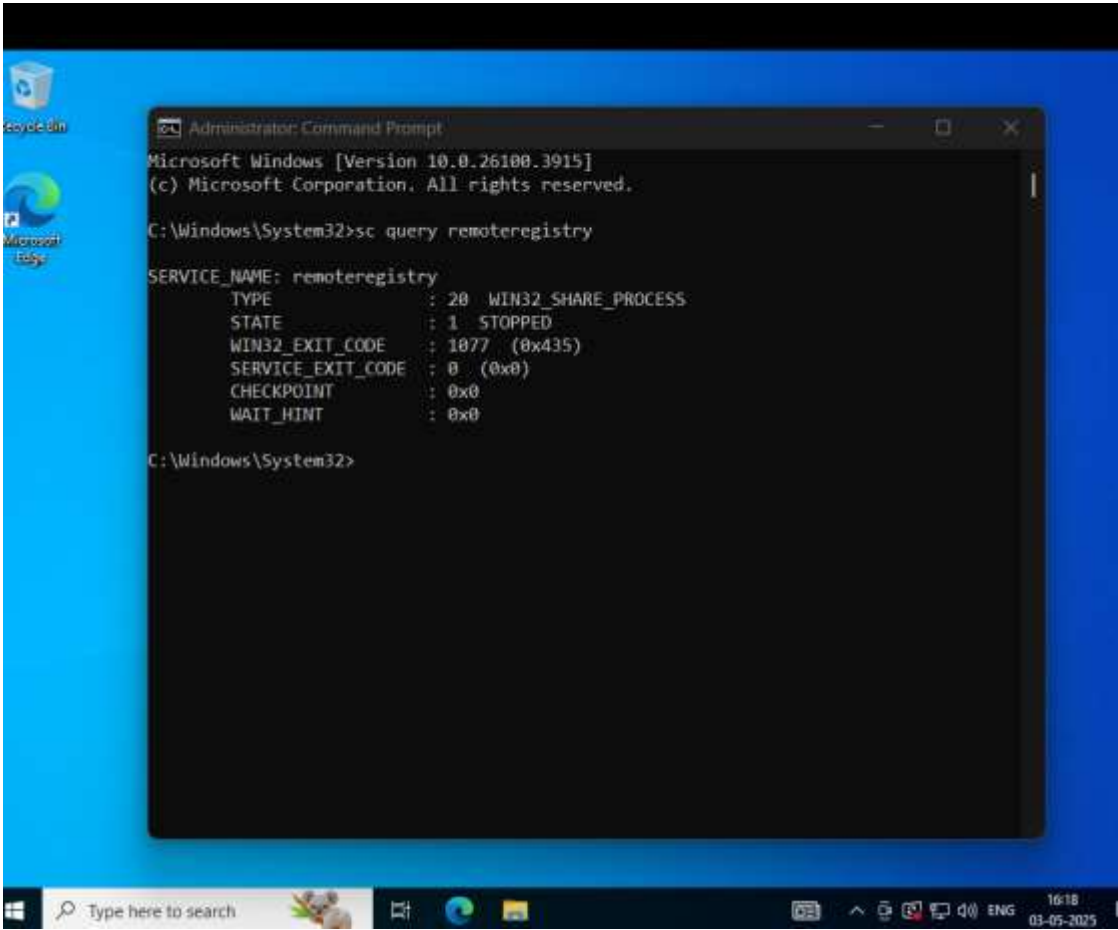
Windows Desktop Compliance

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



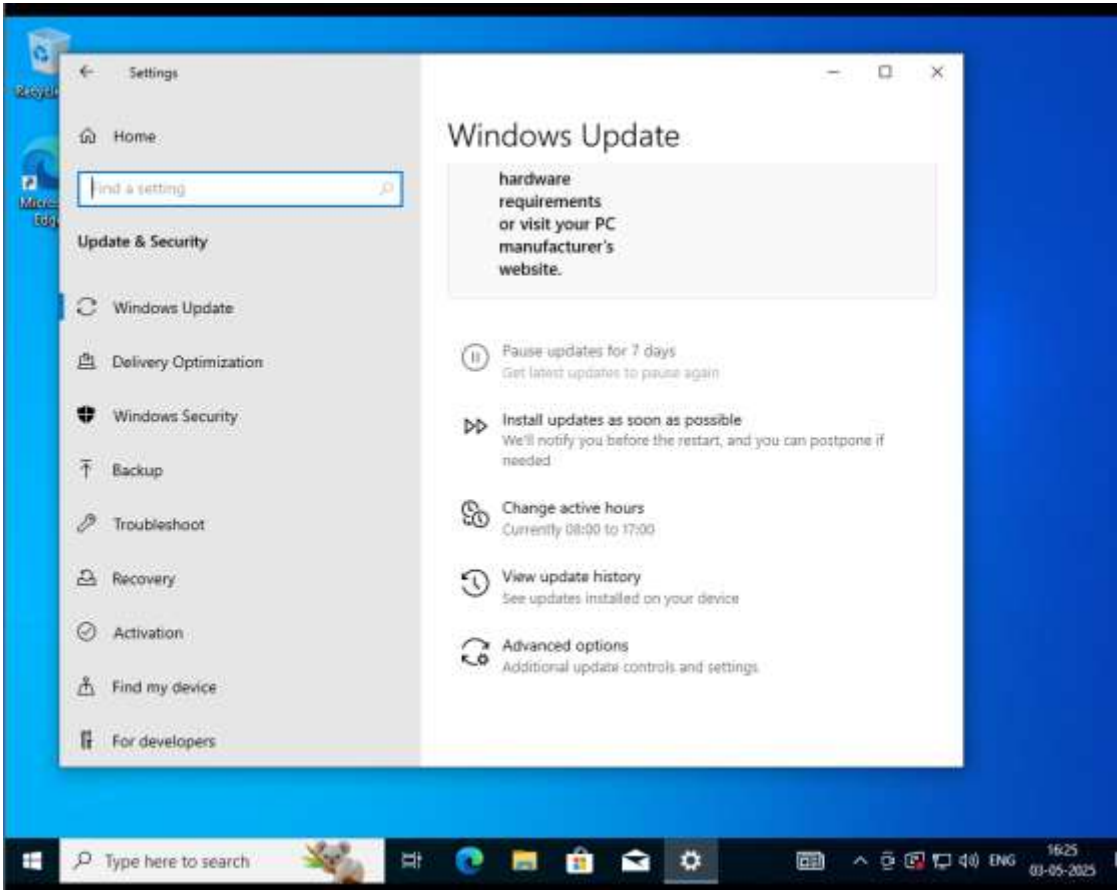
Windows Desktop Compliance

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	Met



Windows Desktop Compliance

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

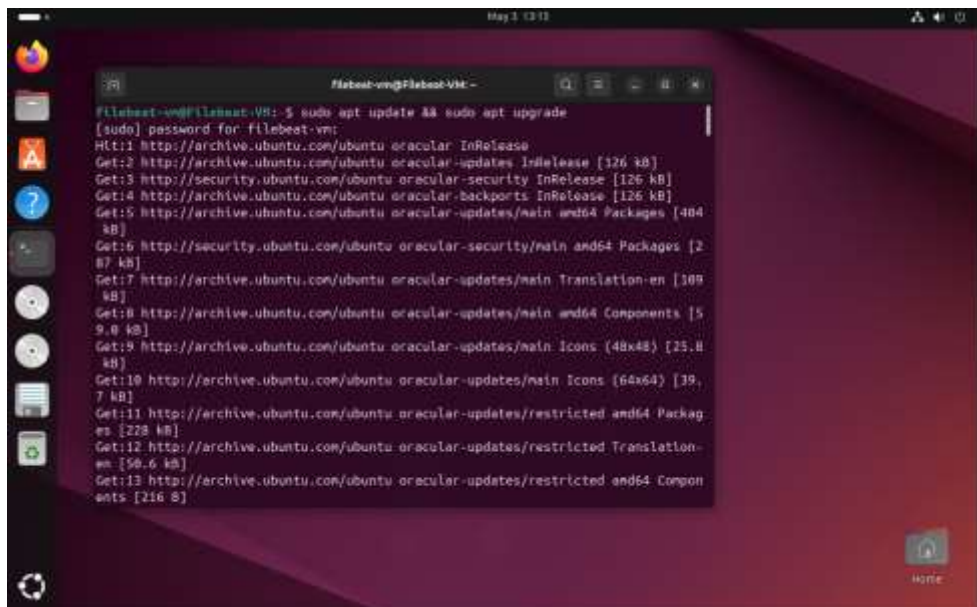
[Account Management]: [Disable or remove unused local user accounts through lusrmgr.msc.]
[Authenticator Management]: [Enforce strong password policy through gpedit.msc > Windows Settings > Account Policies > Password Policy.]
[Protection of Information at Rest]: [Allow BitLocker encryption on all drives by Control Panel > BitLocker Drive Encryption.]
[Malicious Code Protection]: [Make sure Microsoft Defender is turned on and set to real-time protection in Windows Security settings.]

Linux Compliance

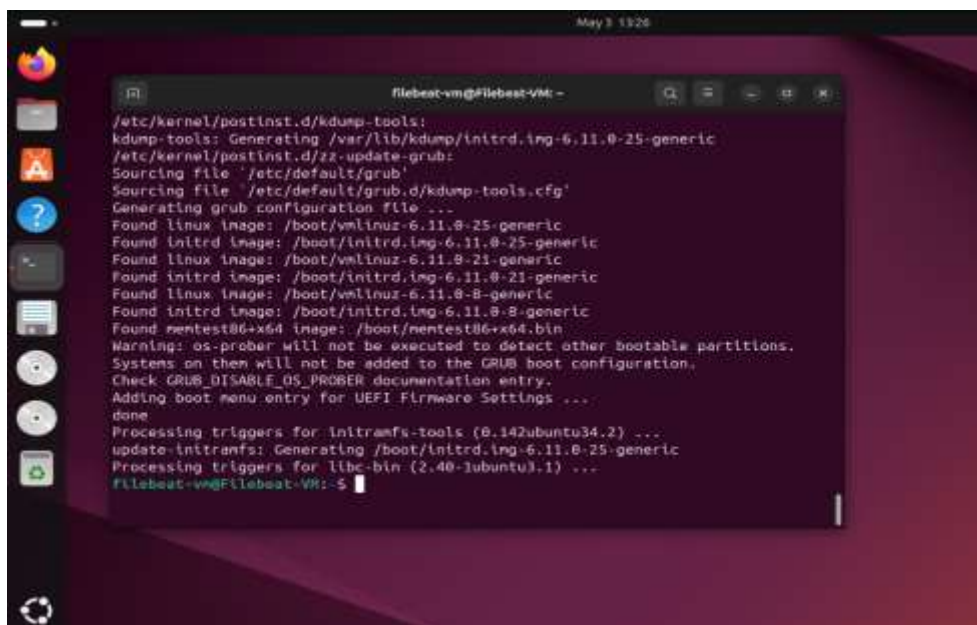
Linux CMMC Requirements	Met/Not Met
Current on security updates	Met
Ensure separate partition exists for /var	Not Met
Disable Automounting of drives	Met
Ensure AIDE is installed	Met
Ensure daytime services are not enabled	Met
Ensure echo services are not enabled	Met
Ensure tftp server is not enabled	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	Met
Ensure audit logs are not automatically deleted	Met

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Current on security updates	



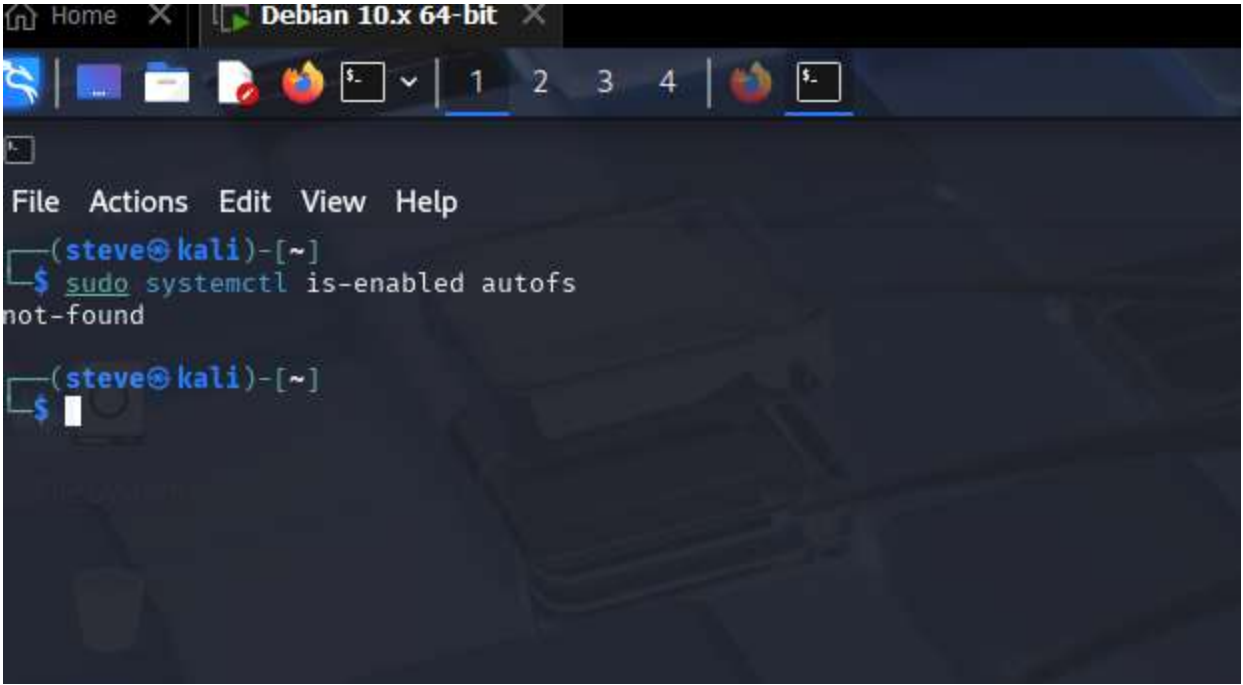
```
filebeat-vm@filebeat-VM: ~  
filebeat-vm@filebeat-VM:~$ sudo apt update && sudo apt upgrade  
[sudo] password for filebeat-vm:  
Hit:1 http://archive.ubuntu.com/ubuntu oracular InRelease  
Get:2 http://archive.ubuntu.com/ubuntu oracular-updates InRelease [126 kB]  
Get:3 http://security.ubuntu.com/ubuntu oracular-security InRelease [126 kB]  
Get:4 http://archive.ubuntu.com/ubuntu oracular-backports InRelease [126 kB]  
Get:5 http://archive.ubuntu.com/ubuntu oracular-updates/main amd64 Packages [404 kB]  
Get:6 http://security.ubuntu.com/ubuntu oracular-security/main amd64 Packages [287 kB]  
Get:7 http://archive.ubuntu.com/ubuntu oracular-updates/main Translation-en [109 kB]  
Get:8 http://archive.ubuntu.com/ubuntu oracular-updates/main amd64 Components [59.0 kB]  
Get:9 http://archive.ubuntu.com/ubuntu oracular-updates/main Icons (48x48) [25.8 kB]  
Get:10 http://archive.ubuntu.com/ubuntu oracular-updates/main Icons (64x64) [39.7 kB]  
Get:11 http://archive.ubuntu.com/ubuntu oracular-updates/restricted amd64 Packages [228 kB]  
Get:12 http://archive.ubuntu.com/ubuntu oracular-updates/restricted Translation-en [50.6 kB]  
Get:13 http://archive.ubuntu.com/ubuntu oracular-updates/restricted amd64 Components [216 B]  
done
```



```
filebeat-vm@filebeat-VM: ~  
filebeat-vm@filebeat-VM:~$ sudo update-grub  
Generating grub configuration file ...  
Found linux image: /boot/vmlinuz-6.11.0-25-generic  
Found initrd image: /boot/initrd.img-6.11.0-25-generic  
Found linux image: /boot/vmlinuz-6.11.0-21-generic  
Found initrd image: /boot/initrd.img-6.11.0-21-generic  
Found linux image: /boot/vmlinuz-6.11.0-8-generic  
Found initrd image: /boot/initrd.img-6.11.0-8-generic  
Found memtest86-x64 image: /boot/memtest86-x64.bin  
Warning: os-prober will not be executed to detect other bootable partitions.  
Systems on them will not be added to the GRUB configuration.  
Check GRUB_DISABLE_OS_PROBER documentation entry.  
Adding boot menu entry for UEFI Firmware Settings ...  
done  
Processing triggers for initramfs-tools (0.142ubuntu34.2) ...  
update-initramfs: Generating /boot/initrd.img-6.11.0-25-generic  
Processing triggers for libc-bin (2.40-1ubuntu3.1) ...  
filebeat-vm@filebeat-VM:~$
```


Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Disable Automounting of drives	Met



Linux Compliance

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

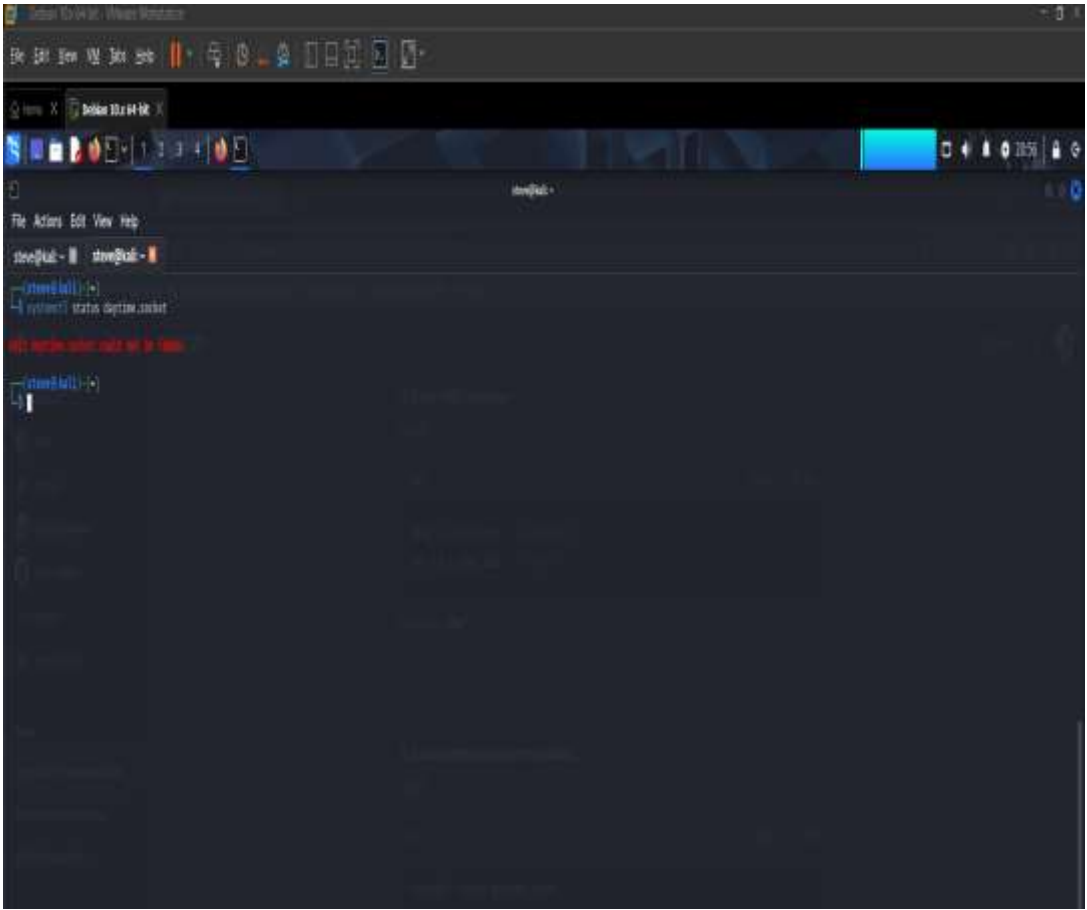
```

root@kali: ~# dpkg-query -f='${Package} ${Version} ${Architecture} ${Description}\n' -W app
Package: app
Version: 0.00-1
Architecture: all
Description: Advanced Persistent Penetration (APP) Framework - English Version
Advanced Persistent Penetration (APP) Framework - Chinese Version

```

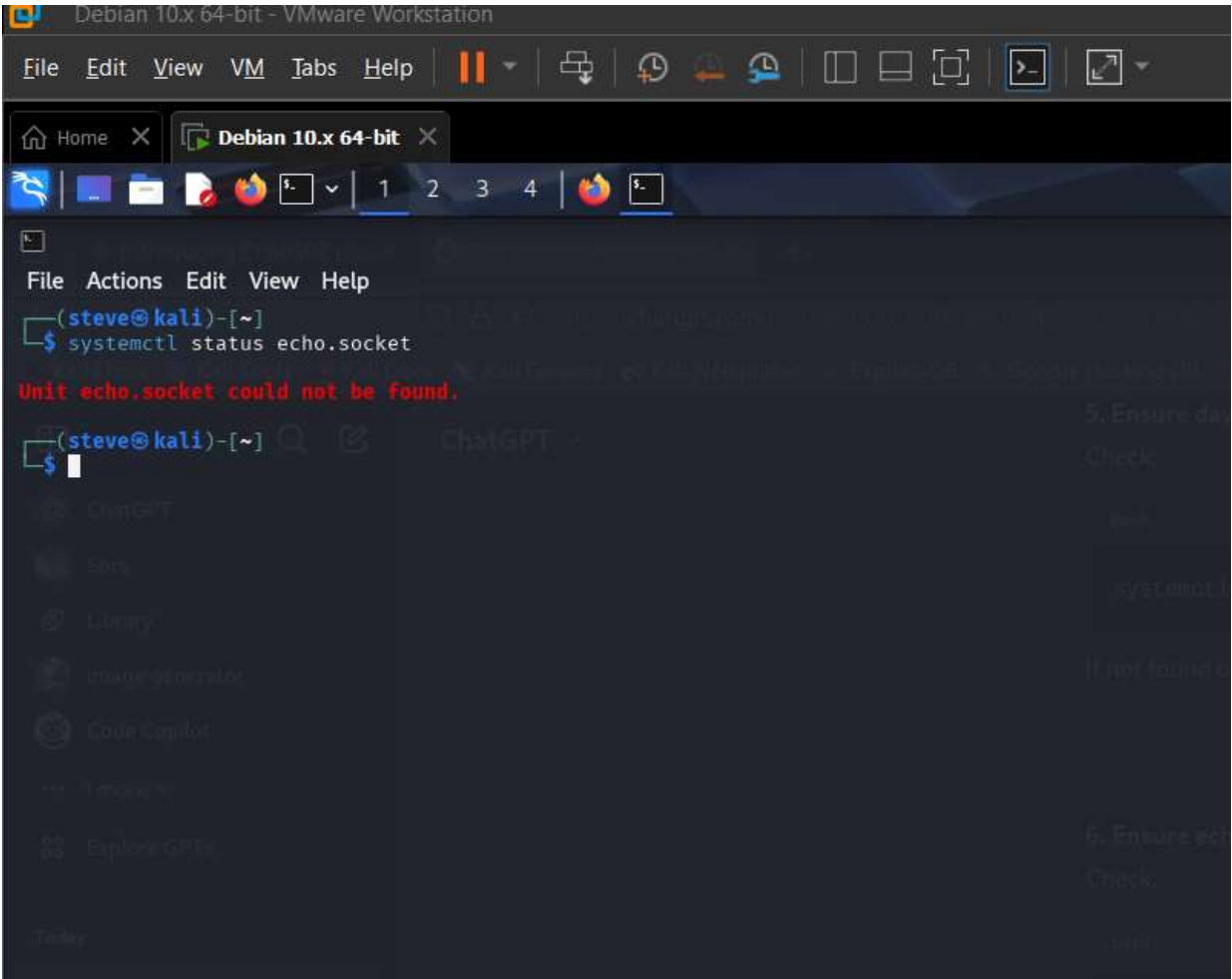
Linux Compliance

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



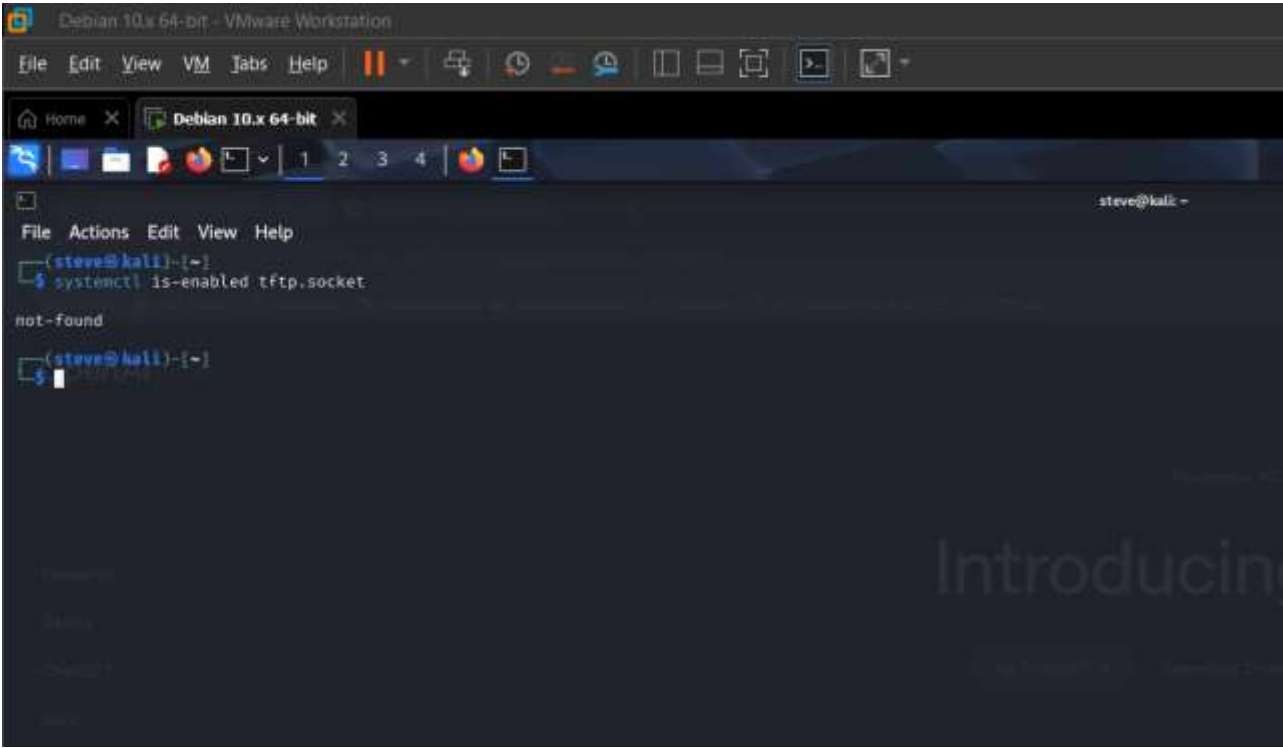
Linux Compliance

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



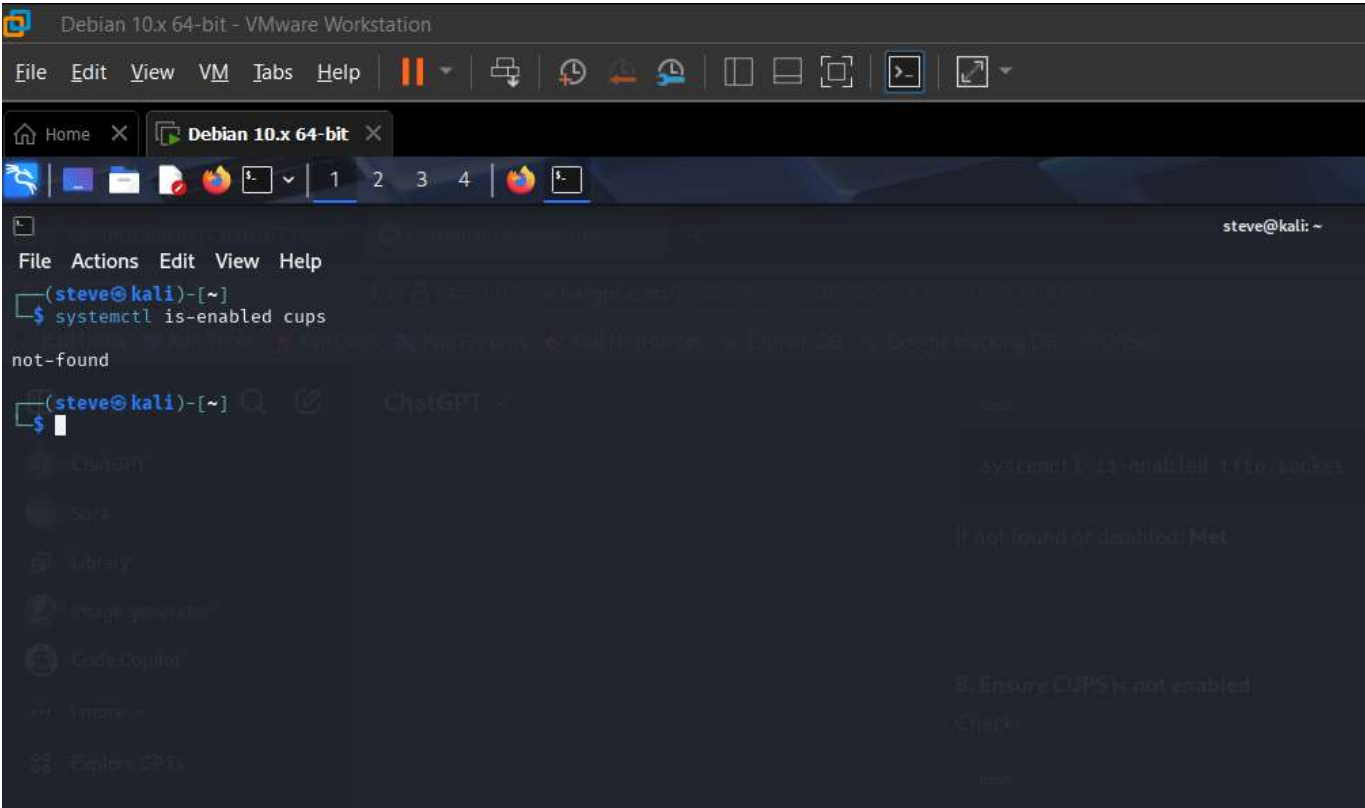
Linux Compliance

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



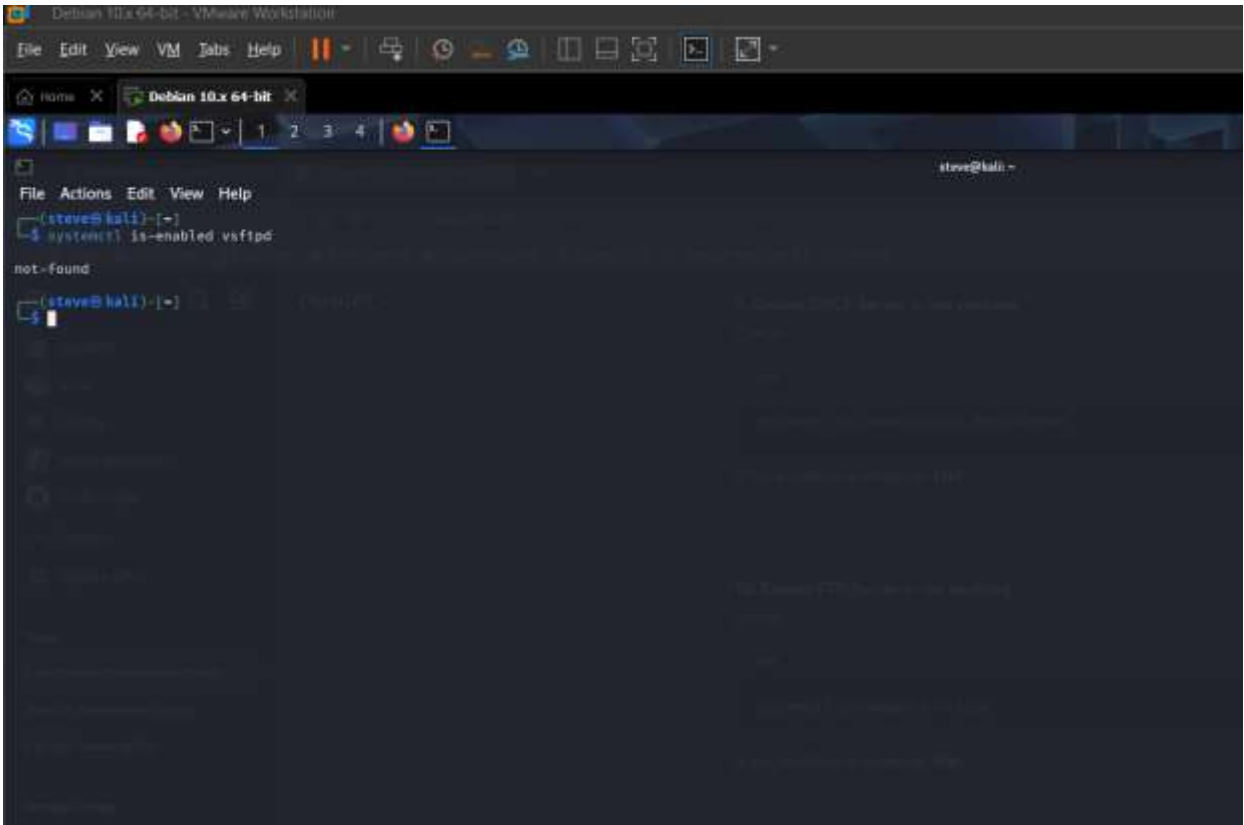
Linux Compliance

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

The screenshot shows a Kali Linux terminal window. The prompt is `(steve@kali):~#`. The user has entered the command `systemctl is-enabled isc-dhcp-server`. The output of the command is `not-found`. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The title bar of the terminal window is 'Debian 10.x 64-bit'.

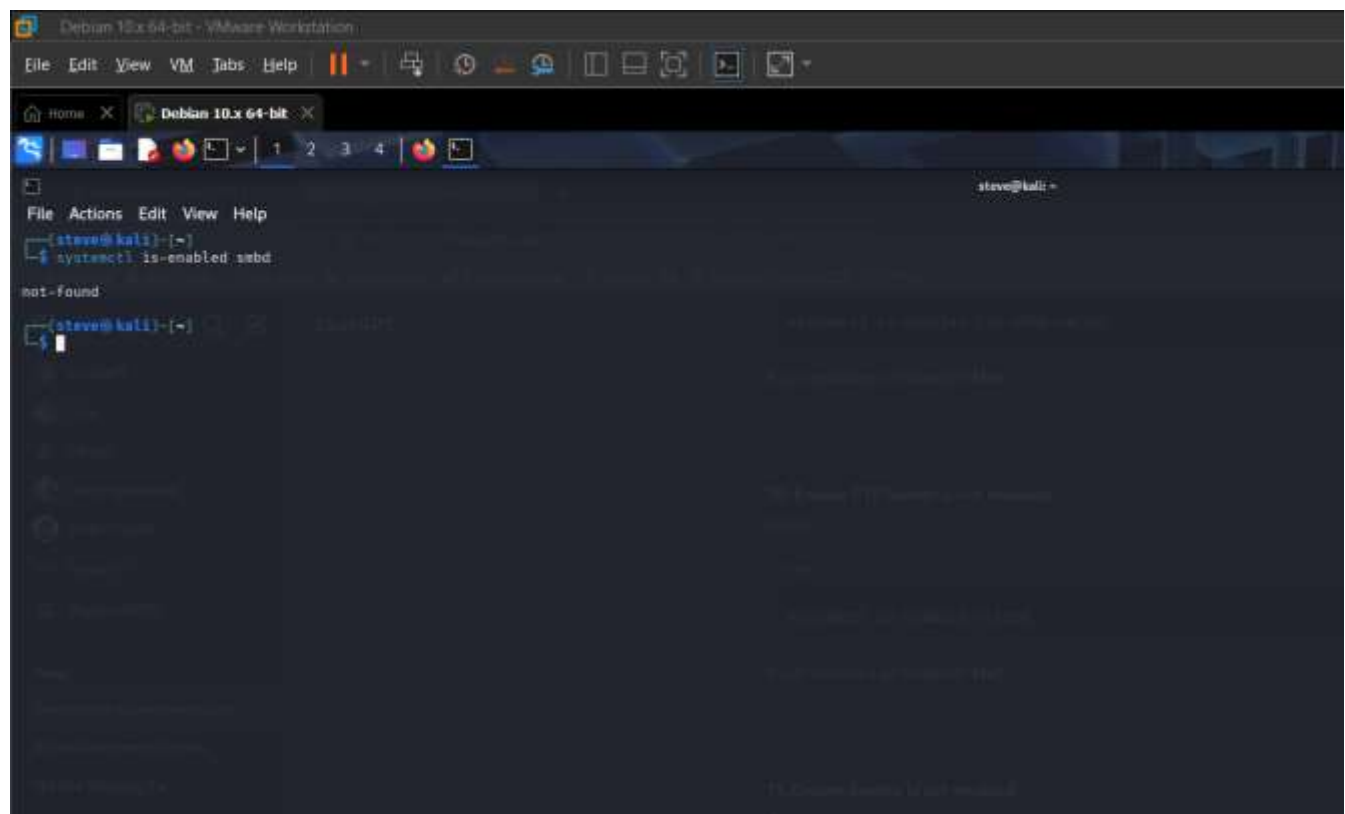
Linux Compliance

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



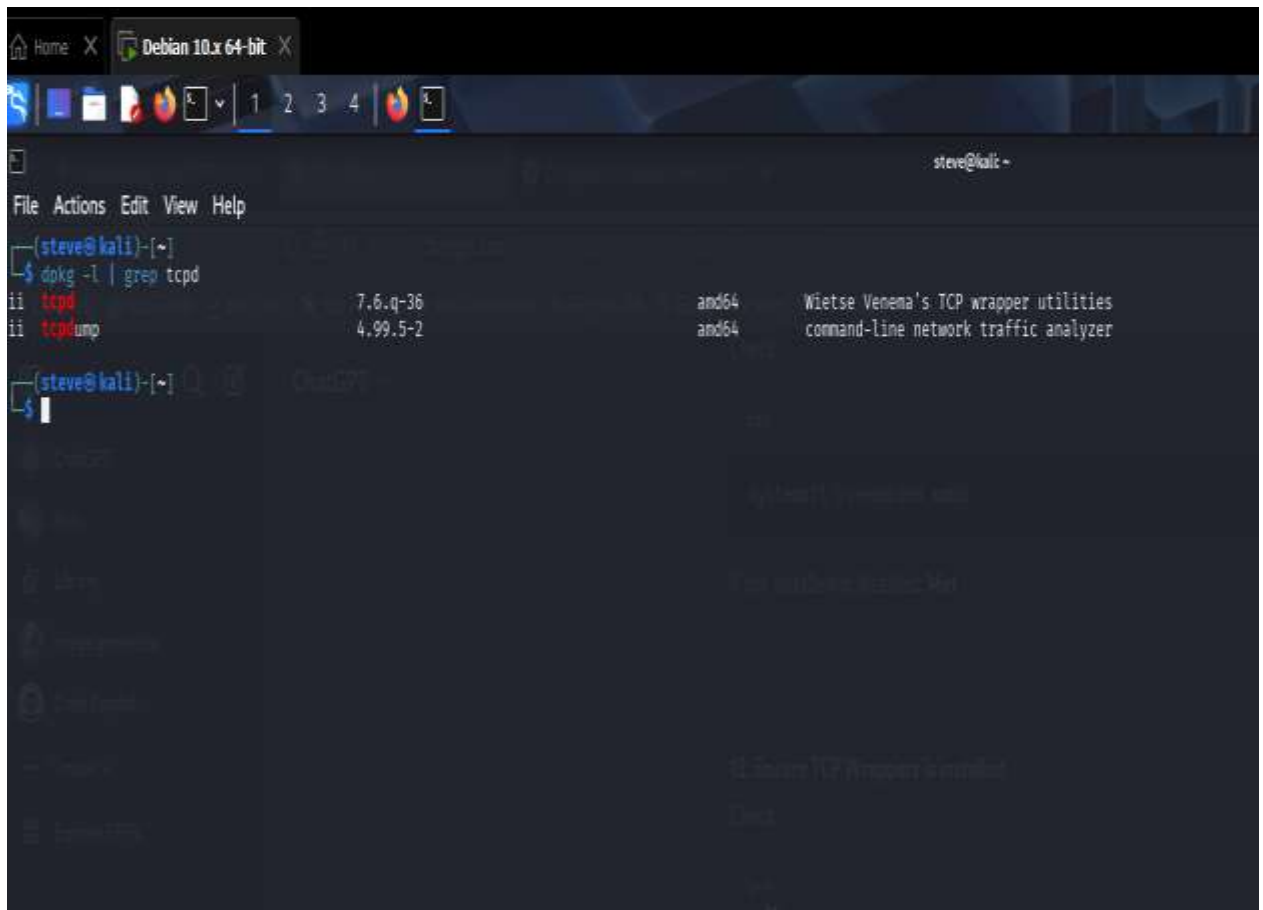
Linux Compliance

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



Linux Compliance

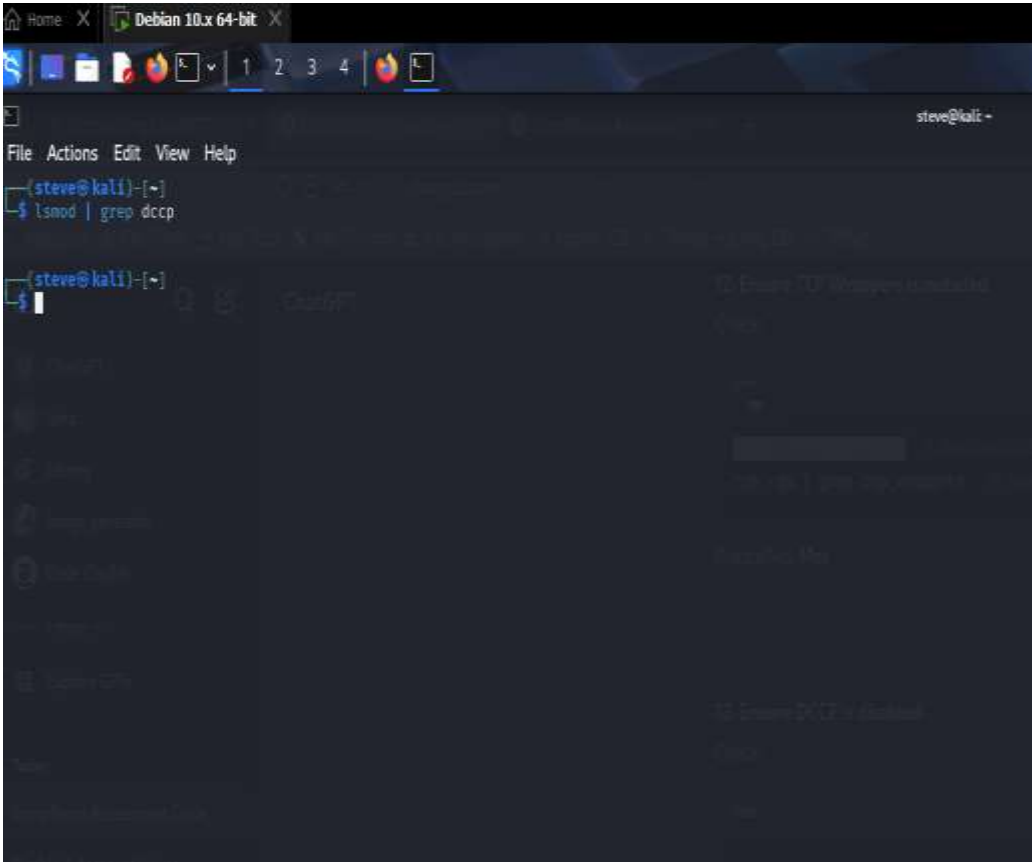
Linux Regulatory Requirement	Met/Not Met
Ensure TCP Wrappers is installed	Met



```
Debian 10.x 64-bit X
1 2 3 4
File Actions Edit View Help
(steve@kali)-[~]
$ dpkg -l | grep tcpd
ii  tcpd                7.6.q-36      amd64      Wietse Venema's TCP wrapper utilities
ii  tcpdump              4.99.5-2      amd64      command-line network traffic analyzer
(steve@kali)-[~]
$
```

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

The screenshot shows a terminal window on a Kali Linux machine. The user is logged in as 'steve' and is in the directory '~'. The terminal output shows the following commands and results:

```
(steve@kali)~$ iptables -L
iptables v1.8.11 (nf_tables): Could not fetch rule set generation id: Permission denied (you must be root)

(steve@kali)~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

(steve@kali)~$
```

The output of the `iptables -L` command shows three chains: INPUT, FORWARD, and OUTPUT, all with a policy of ACCEPT. Each chain has a target, protocol, options, source, and destination field. The output is empty, indicating that no rules are currently defined in the iptables configuration.

Linux Compliance

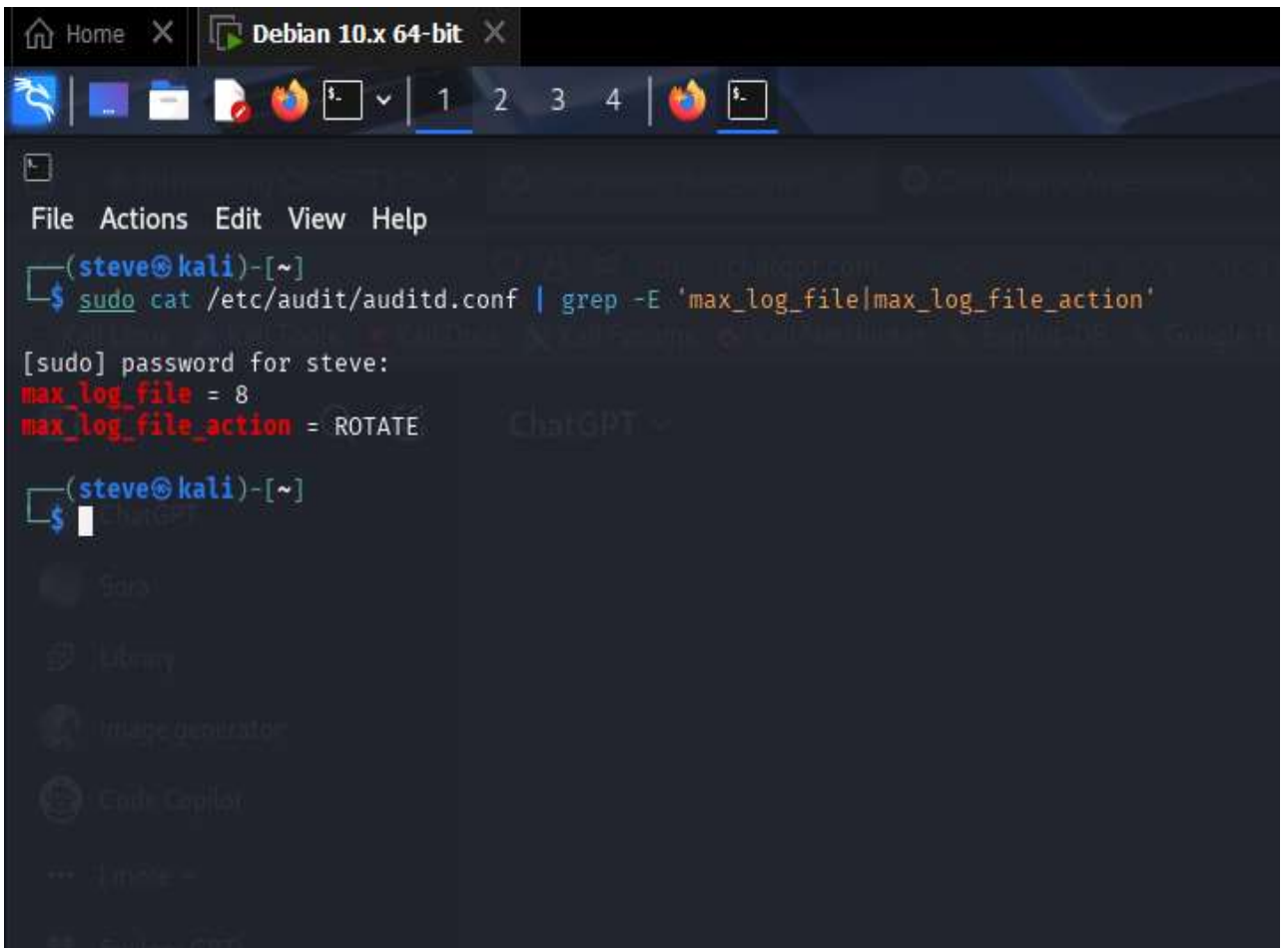
Linux Regulatory Requirement	Met/Not Met
Ensure audit log storage size is configured	Met

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the command `sudo cat /etc/audit/auditd.conf | grep -E 'max_log_file|max_log_file_action'` being executed. The output shows `max_log_file = 8` and `max_log_file_action = ROTATE`. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The desktop background is dark, and there are several application icons in the top bar, including a file manager, a web browser, and a terminal. The terminal window title is 'Debian 10.x 64-bit'.

```
(steve@kali)-[~]  
$ sudo cat /etc/audit/auditd.conf | grep -E 'max_log_file|max_log_file_action'  
[sudo] password for steve:  
max_log_file = 8  
max_log_file_action = ROTATE  
(steve@kali)-[~]  
$
```

Linux Compliance

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



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the following commands and output:

```
(steve@kali)-[~]  
$ sudo cat /etc/audit/auditd.conf | grep -E 'max_log_file|max_log_file_action'  
[sudo] password for steve:  
max_log_file = 8  
max_log_file_action = ROTATE  
  
(steve@kali)-[~]  
$
```

The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The desktop background is dark, and there are several application icons in the top bar, including a file manager, a terminal, and a web browser. The window title bar indicates the system is 'Debian 10.x 64-bit'.

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

Windows Server 2022 Datacenter Ensures compatibility and long-term support. It is compactable to most of the systems in real world application

2. Firewall Configuration

Allow inbound HTTP (80), HTTPS (443); block all other unsolicited inbound traffic – Reduces attack surface and prevent attacks from bad actors

3. Web Server Role Installation

Install IIS (Internet Information Services) with required features ,allow us to host and deploy web applications

4. System Updates are Applied

Apply latest Windows Updates via sconfig or Windows Update GUI – Protects against known vulnerabilities, by patch updates.

5. Secure the Admin Account

Don't use the default "Administrator" name—change it and set a strong password. This helps protect against brute-force attacks.

Windows Server Build Sheet

6. Install Antivirus for end point protection

Use Microsoft Defender or another trusted endpoint protection tool(3rd party). It's our first defense against viruses and malware that may attack our endpoints.

7. Configure Remote Access properly

Limit RDP (Remote Desktop Protocol) access to trusted IPs only, and turn on Network Level Authentication (NLA) for added security.

8. Enable Logging and Monitoring

Set up Windows Event Logging and link it to a monitoring system like Azure Sentinel. It helps catch issues early, to investigate if an attack occurred

9. Plan for Backups

Use a cloud backup solution (like Azure Backup) to make regular snapshots of the system—just in case something goes wrong,Hope for the best and always prepare for the worst.

10. Deploy Apps Securely

Make sure apps run with the least privileges they need, like using the IIS App Pool Identity, so they can't do damage if compromised. Use SDLC for the development and deployment process.

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. Full Visibility into Cloud Apps

You'll instantly see every SaaS, IaaS or PaaS service your team is using—whether it's sanctioned or not. No more surprises when someone spins up a rogue instance or starts sharing data in a tool the security team hasn't approved.

2. Smart Data Protection

A CASB spots when sensitive files—think customer records or trade secrets—are being uploaded, downloaded, or shared in the cloud. It can automatically encrypt, quarantine, or block risky moves, so nothing slips through the cracks.

3. User Behavior Analytics

By keeping an eye on how people actually use cloud services, a CASB can flag oddball patterns: logins from strange locations, massive downloads at 2 AM, or someone suddenly poking around in folders they never touch. That kind of anomaly detection helps you catch insider threats or compromised accounts fast.

4. Unified Access Control

Instead of piecing together policies across different cloud consoles, a CASB lets you enforce one set of rules—who can log in, from where, and on what device—across all your apps. It means logins come with the right MFA, device checks, and network restrictions every single time.

5. Continuous Compliance Monitoring

A CASB can map your cloud footprint against those requirements and generate reports on demand. You'll know exactly where you stand, what's out of line, and what to do next without digging through a hundred consoles.