

COMPLIANCE ASSESSMENT



ARSHADTK
CBS-0004

05-02-2025

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 11 Hardening

In the dynamic environment of Fed First 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 11 desktop. This task involves identifying vulnerabilities that could potentially compromise system security and proposing actionable remediation steps to mitigate these risks.

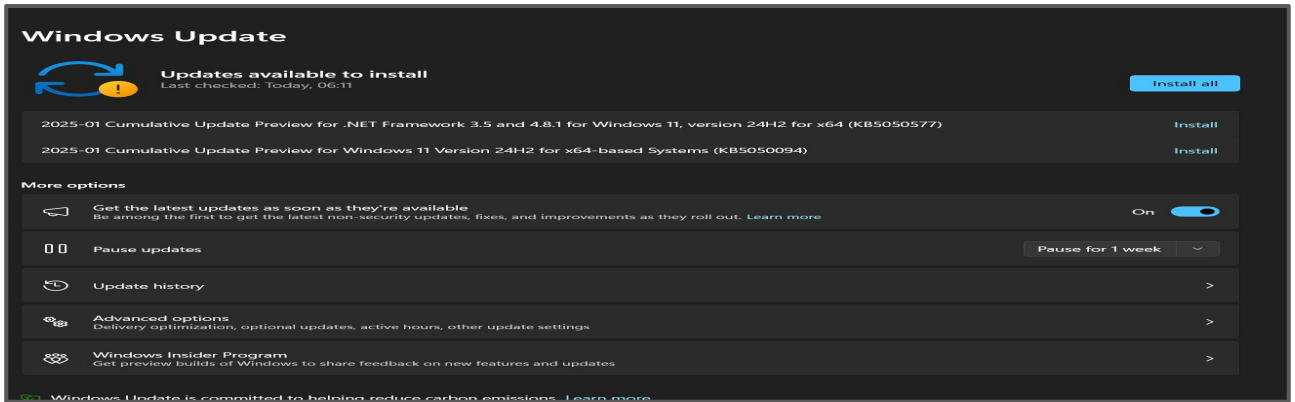
Windows 11 Hardening

Many parts can be hardened in Windows 11, 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

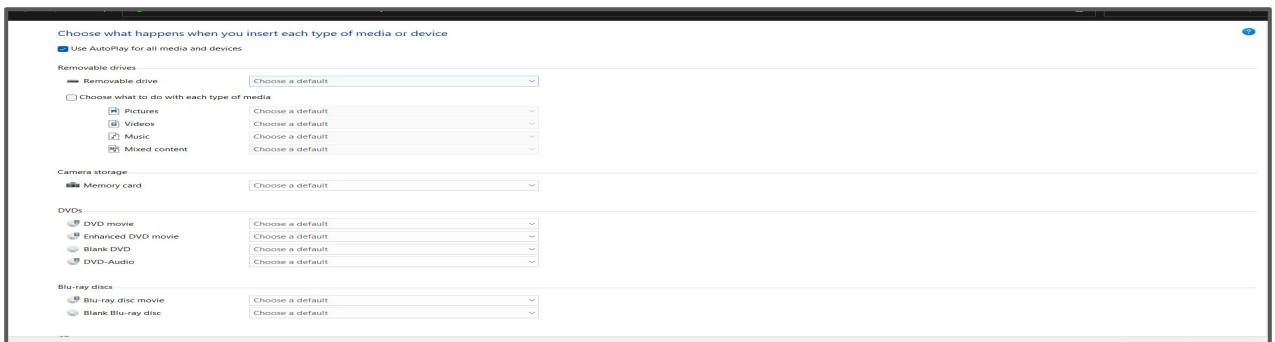
Windows 11 Hardening

1. System Updates



- Enable automatic updates.
- Regularly check for and install updates

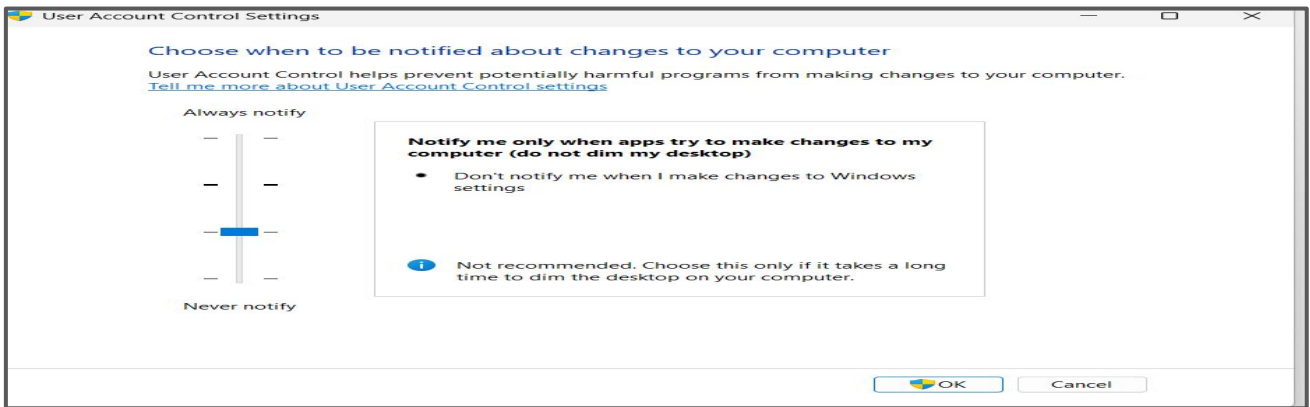
2. AutoRun/AutoPlay



- Disable AutoRun to prevent USB-based malware attacks.

Windows 11 Hardening

3. User Account Control settings



- Set UAC to "Always Notify" to alert you when apps try to make system changes.
- Ensure that only authorized users have admin access to prevent privilege escalation.

4. Guest Account settings

```
C:\Windows\System32>net user guest
User name          Guest
Full Name          Guest
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    29-01-2025 14:19:58
Password expires     Never
Password changeable  29-01-2025 14:19:58
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.
```

- Disable the Guest account
- Ensure no shared or unprotected directories exist that could expose sensitive data.

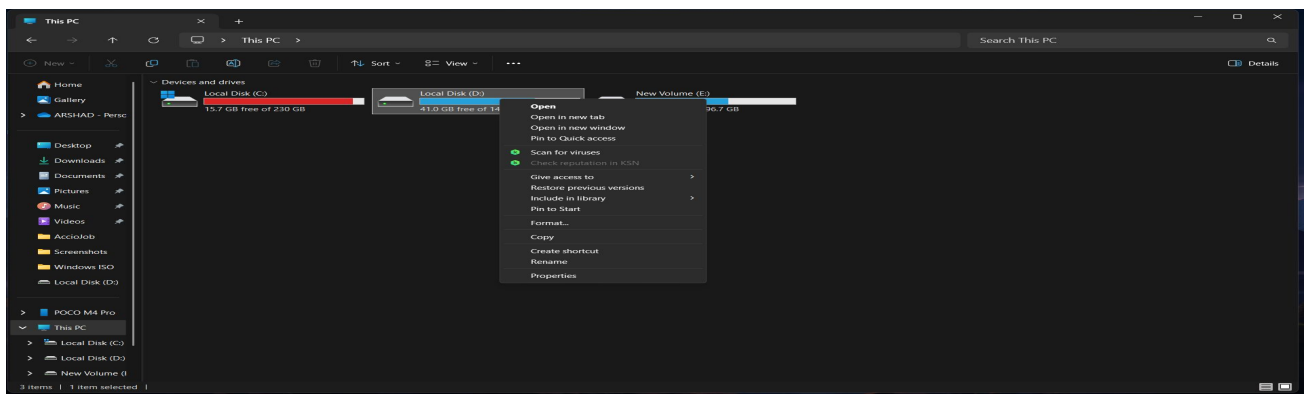
Windows 11 Hardening

5. Administrator Account settings

```
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 Yes
Account expires Never
Password last set 29-01-2025 14:12:13
Password expires Never
Password changeable 29-01-2025 14:12:13
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.
```

- Rename the default Administrator account to a unique name for added security.
- Disable the Administrator account or set a strong, unique password if it's necessary.

6. BitLocker Drive Encryption



- Enable BitLocker for system drive protection.

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.

MacOS Hardening

1. System Updates

- Keeps macOS and applications updated with the latest security patches.
- Protects against vulnerabilities that hackers might exploit.
- Ensures compliance with corporate security policies.

2. Firewall Settings

- Blocks unauthorized incoming network connections.
- Reduces exposure to potential cyber threats and remote attacks.

3. FileVault (Full Disk Encryption)

- Encrypts all data on the disk to prevent unauthorized access.
- Protects sensitive files if the MacBook is lost or stolen.

MacOS Hardening

4. Set Up Strong Password Policies

- Requires complex passwords to strengthen user authentication.
- Prevents brute-force attacks and unauthorized access.

5. Guest User Account

- Prevents unauthorized users from accessing the system.
- Eliminates the risk of an unsecured guest account being exploited.

6. AutoRun & External Media Execution

- Prevents automatic execution of untrusted applications from USB drives.
- Reduces the risk of malware infections from external storage devices.

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 First 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.

Email Policy

1. Enable Multi-Factor Authentication (MFA)

MFA is the additional layer of security that requires a second form of identification, such as a text message or an authentication app, in addition to the password. MFA greatly reduces the risk of unauthorized access, even if an employee's password is compromised.

2.Prohibit the Use of Personal Email for Business Communications

Personal email accounts must not be used for any work-related communications. This policy helps ensure that sensitive company information remains within the company's secure infrastructure, preventing data leaks and protecting corporate confidentiality.

3.Mandatory Phishing Awareness and Reporting

All employees must verify email sources before clicking links or downloading attachments from unknown or suspicious senders. Employees should also report any phishing attempts to the IT security team immediately. By promoting awareness and quick reporting, this policy significantly reduces the risk of falling victim to phishing attacks.

4.Encrypt Sensitive Emails

Emails containing confidential or sensitive information must be encrypted before being sent. Email encryption ensures that only the intended recipient can read the content, even if the email is intercepted. This policy is critical for maintaining the privacy and security of sensitive communications.

5. Strict Password Policy for Email Accounts

Employees must set complex passwords for their email accounts, with specific requirements. Strong passwords reduce the likelihood of unauthorized access, minimizing the risk of breaches that could lead to compromised corporate data.

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.

BYOD Policy

1. Device Enrollment in Mobile Device Management (MDM)

Device Enrollment in MDM ensures that all employee-owned devices comply with company security policies. MDM provides centralized control, enforcing requirements like encryption and password complexity, while also enabling remote management in case of lost or stolen devices, reducing the risk of data breaches.

2. Strong Passwords and Multi-Factor Authentication

Use strong passwords (at least 8 characters with a mix of letters, numbers, and symbols) or biometric authentication like Face ID or fingerprint scanning. Multi-factor authentication (MFA) is required for accessing corporate accounts to add an extra layer of security.

3. Data Encryption and Secure Connections

Enable encryption on your device—FileVault for macOS, BitLocker for Windows, and built-in encryption for iOS and Android. Always use a VPN on public Wi-Fi to protect data in transit, and keep work and personal data separate using tools like Android Work Profiles or Apple Managed Apps.

BYOD Policy

4. Keep Your Device Updated

Install the latest operating system updates and security patches regularly. Enable automatic updates on Apple, Android, Windows, and macOS devices to stay protected against new threats. Outdated or unsupported OS versions will not be allowed to access corporate resources.

5. Report Issues Immediately

If your device is lost, stolen, or compromised, report it to the IT Security team immediately. We can remotely wipe corporate data to prevent unauthorized access. Also, report any malware, phishing attempts, or suspicious activity right away.

6. Prohibited Activities and Monitoring

Jailbreaking or rooting devices is prohibited as it weakens security. Employees must not install unauthorized apps on work devices. The company reserves the right to monitor devices for policy compliance and threat detection, with employees notified of any monitoring.

Section 3:

Self Assessment

Windows Desktop Compliance

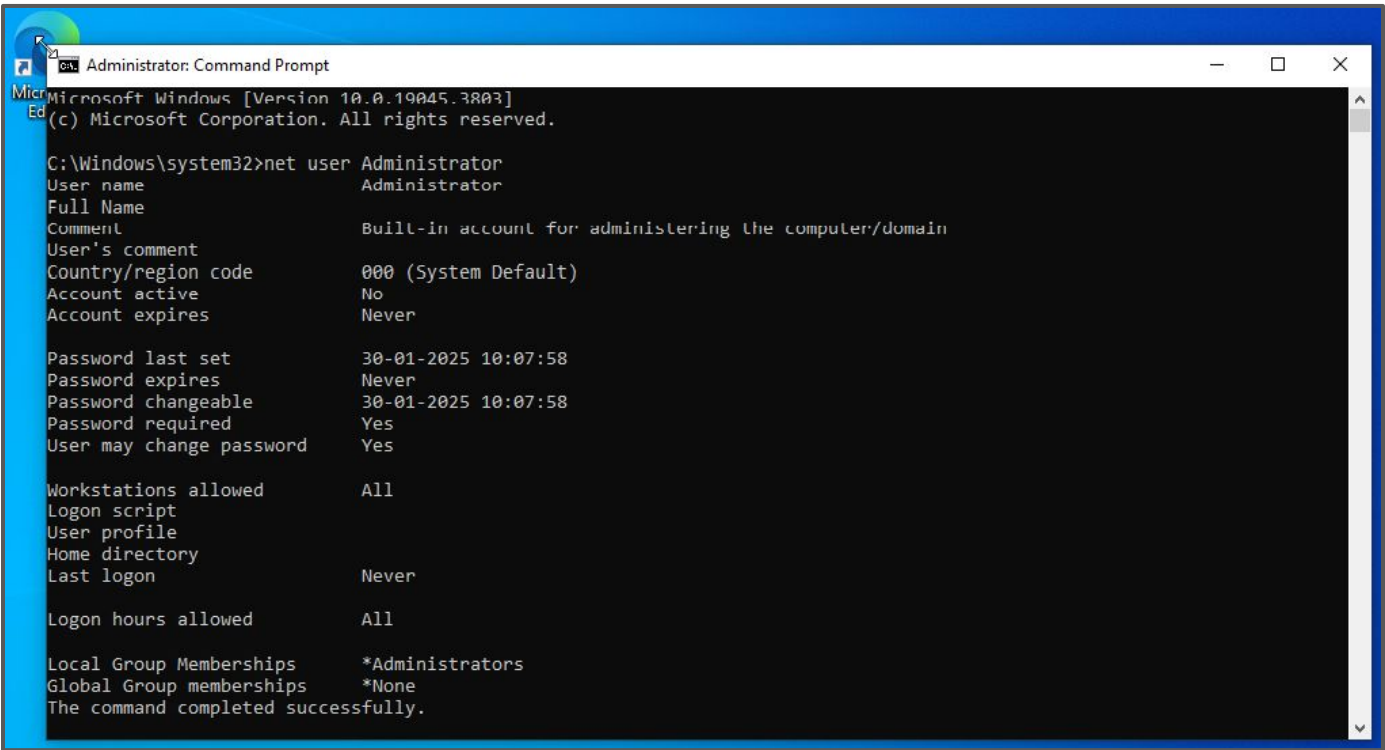
Maintaining robust security measures across all devices is crucial. As part of the organization's commitment to cybersecurity, adhering to the National Institute of Standards and Technology (NIST) guidelines is a top priority. Your task involves evaluating a Windows 10 desktop against specific *NIST 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.

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	Not Met
Guest account is disabled	Met
System logging and auditing are enabled	Not Net
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	NA
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
Built-In Administrator account is disabled	Met

A screenshot of a Windows 10 desktop with a blue taskbar. An 'Administrator: Command Prompt' window is open, displaying the output of the 'net user Administrator' command. The output shows that the Administrator account is active, has a password set to expire on 30-01-2025, and is a member of the Administrators group. The command prompt window has a title bar with standard Windows window controls (minimize, maximize, close) and a scroll bar on the right side.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

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        30-01-2025 10:07:58
Password expires         Never
Password changeable      30-01-2025 10:07:58
Password required         Yes
User may change password Yes

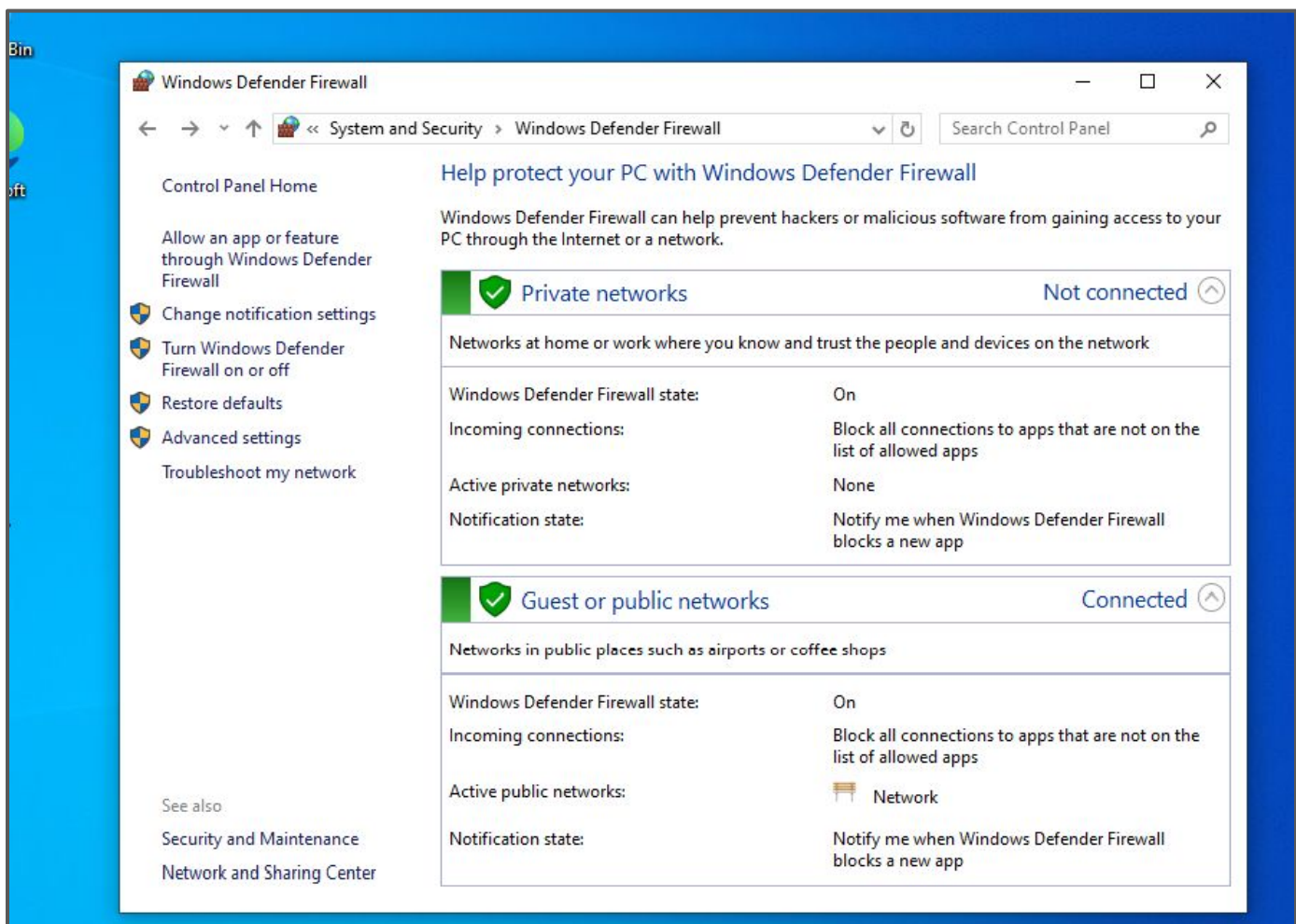
Workstations allowed     All
Logon script
User profile
Home directory
Last logon               Never

Logon hours allowed      All

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

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

← 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

No updates available

We'll continue to check daily for newer updates.

Check for updates

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](#)

☒ On

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

Get ready for Windows 11

To see if this PC can run Windows 11, check the hardware requirements on the [manufacturer's website](#).

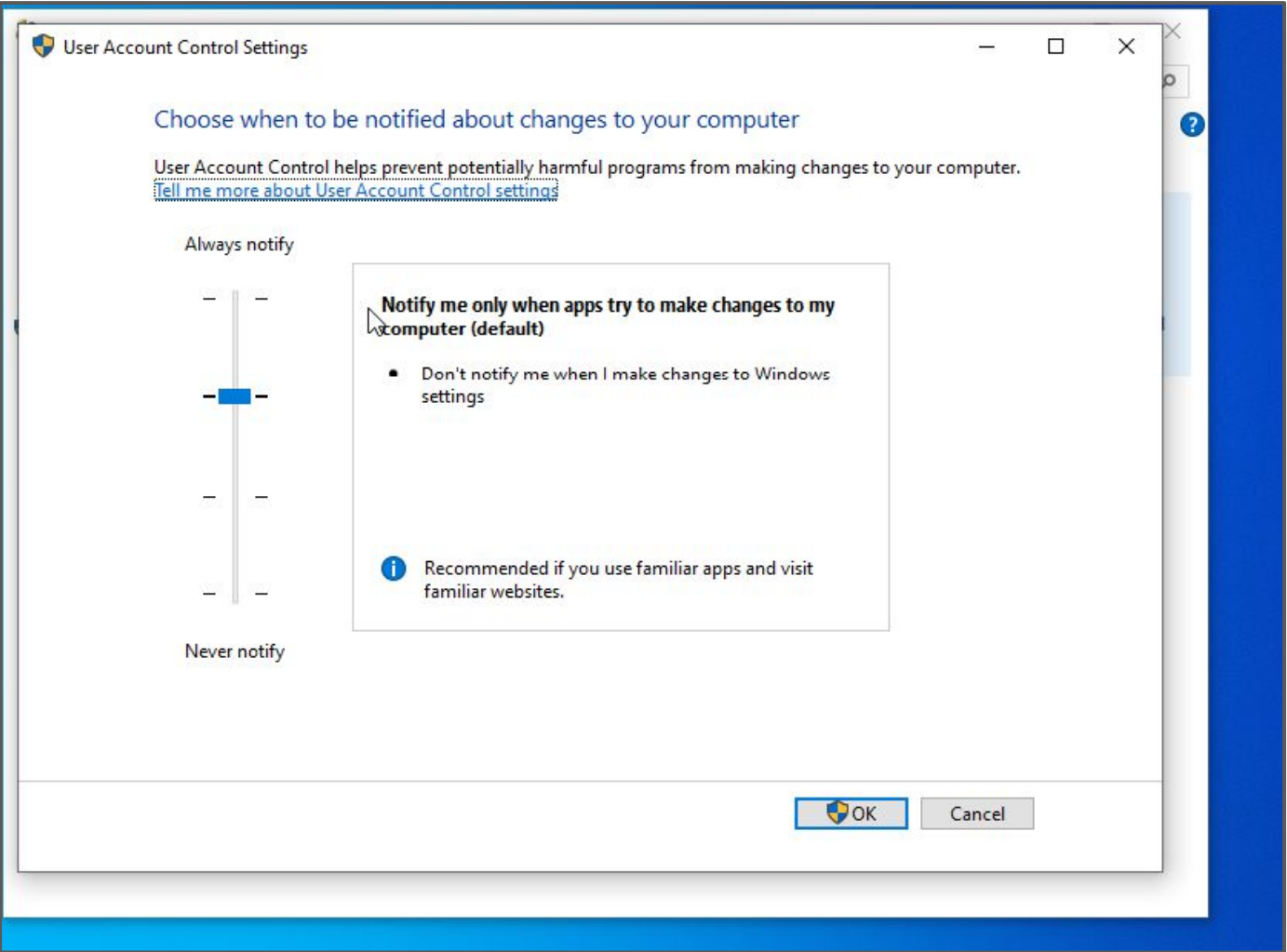
[Check hardware requirements](#)

English (United States)
US keyboard

To switch input methods, press
Windows key+Space.

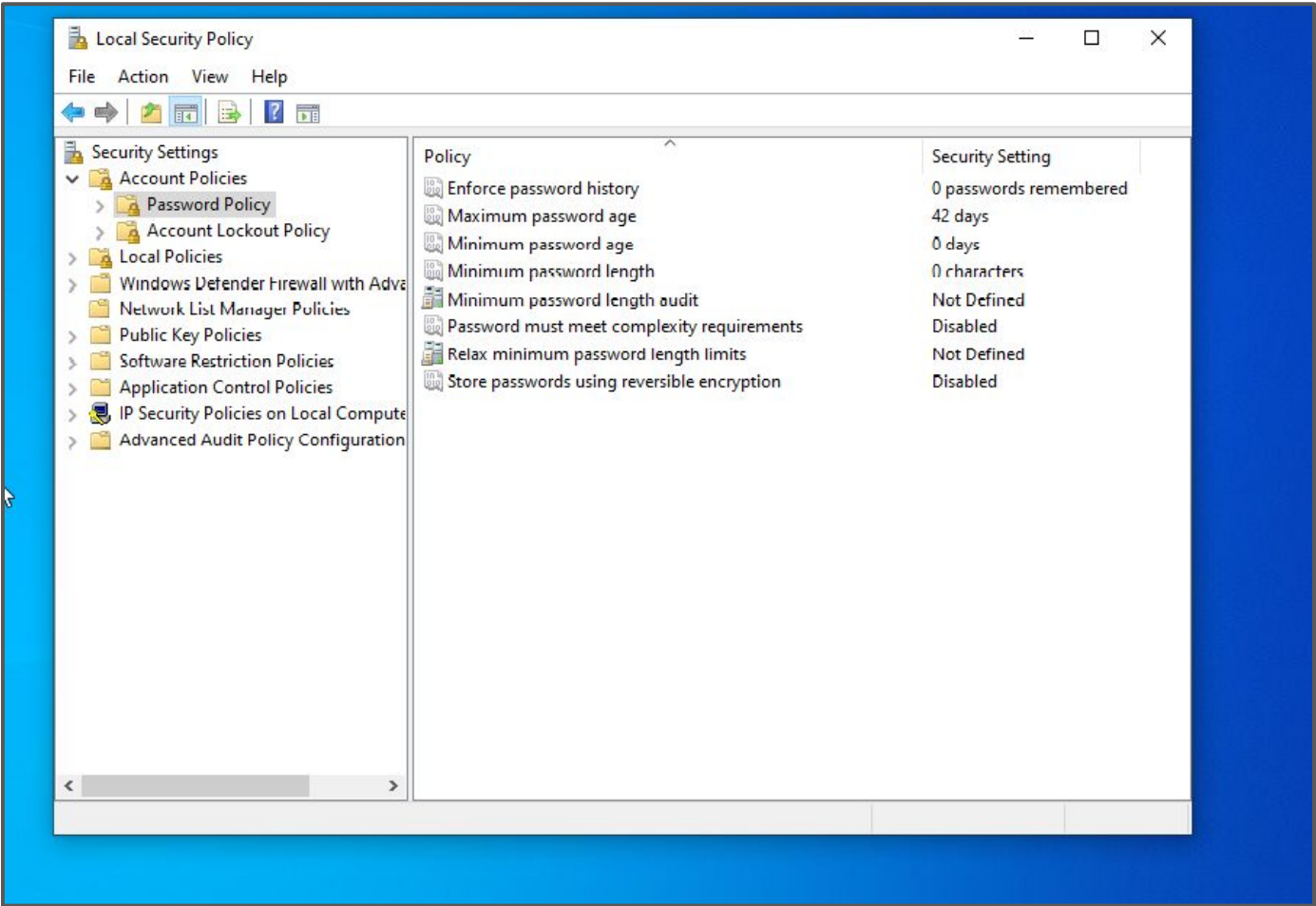
Windows Desktop Compliance

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



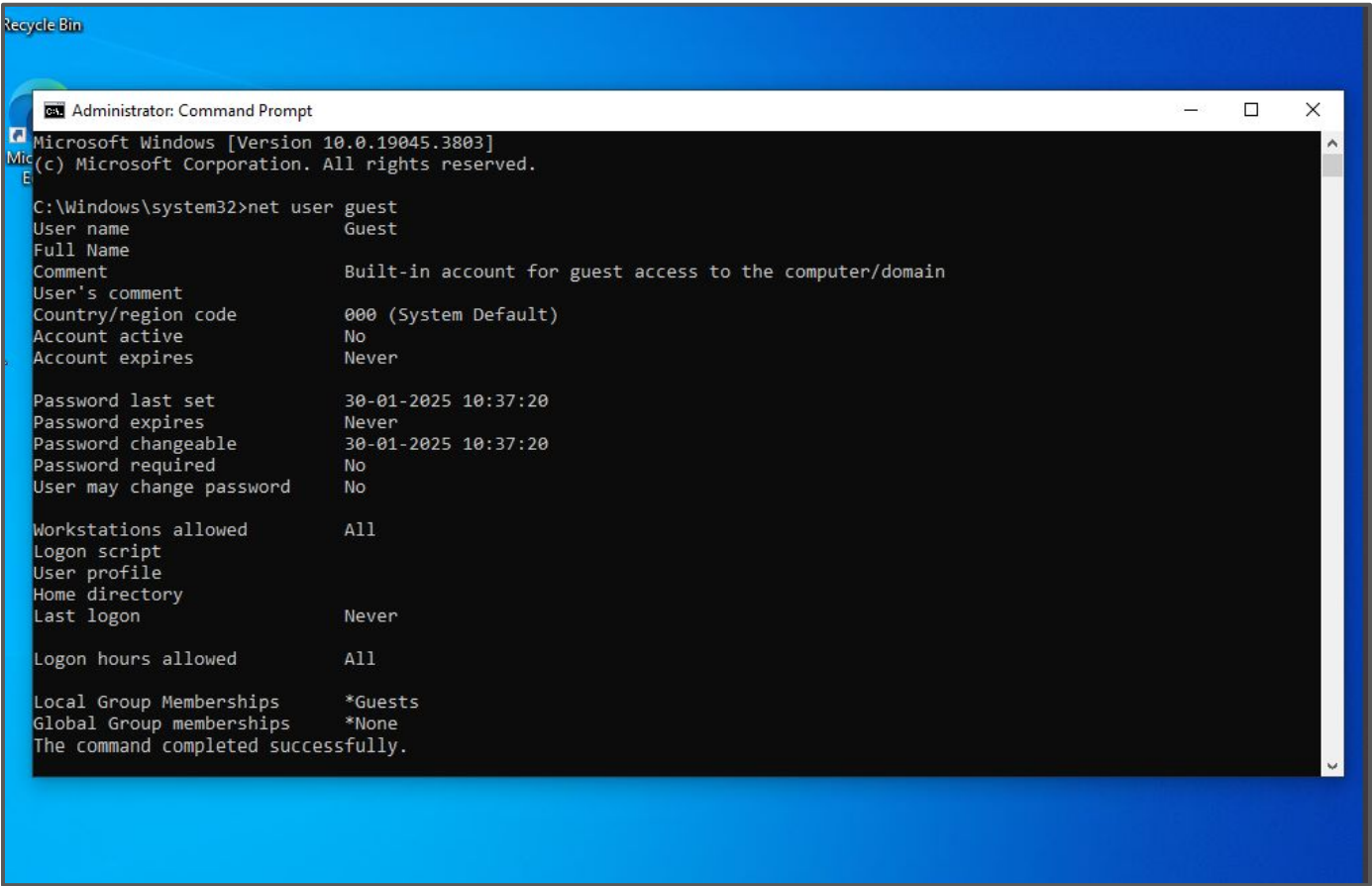
Windows Desktop Compliance

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



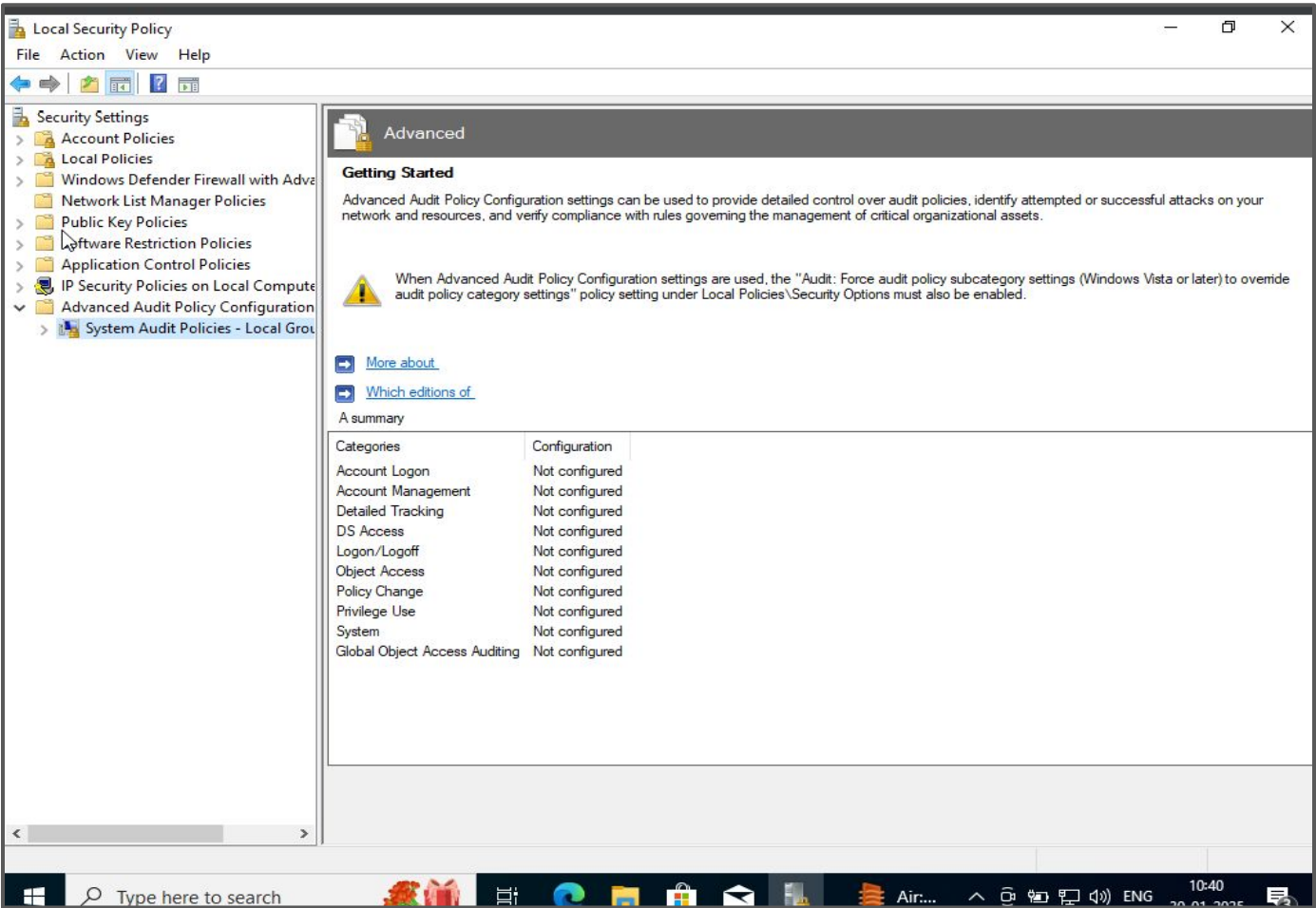
Windows Desktop Compliance

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



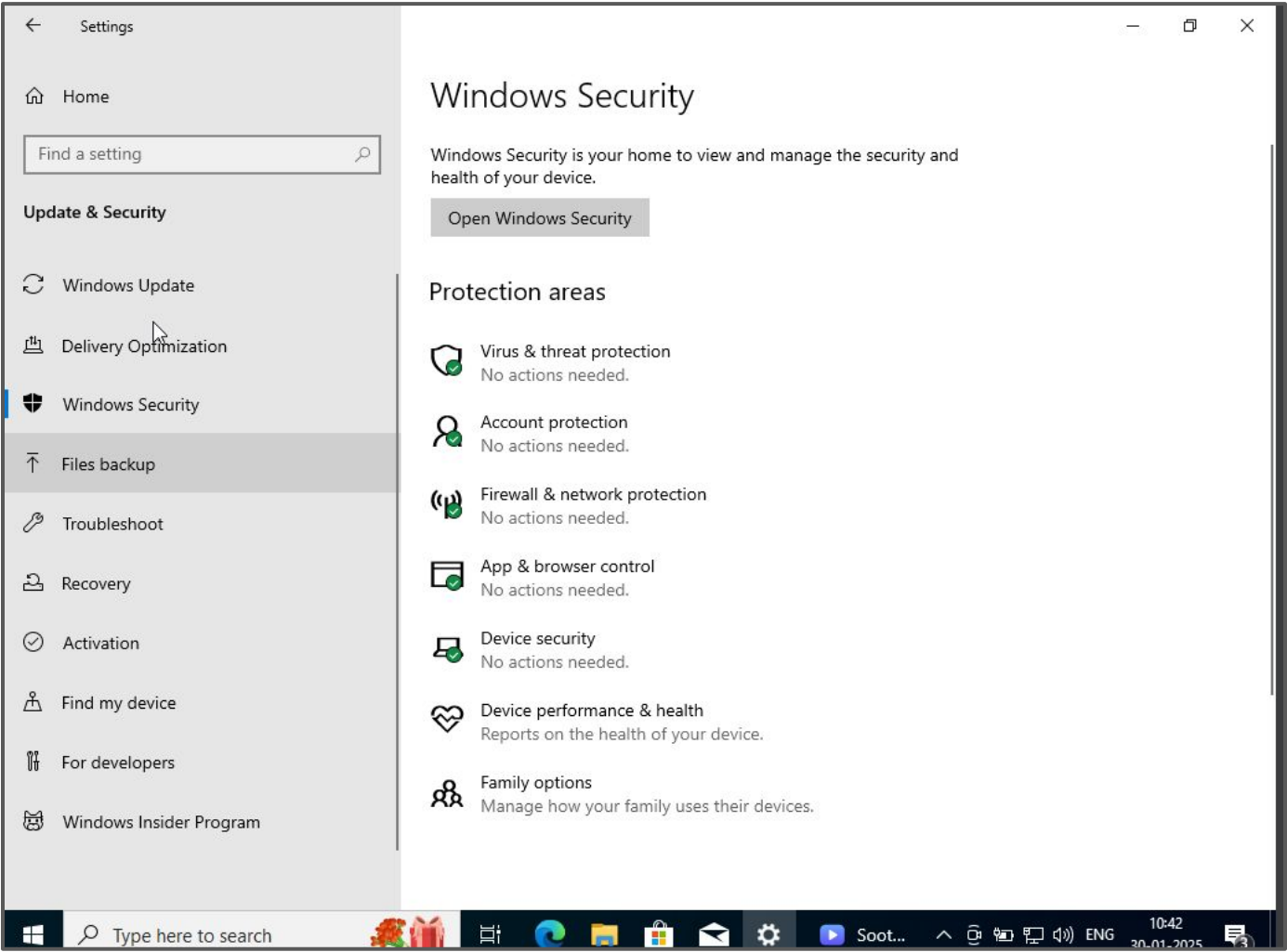
Windows Desktop Compliance

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



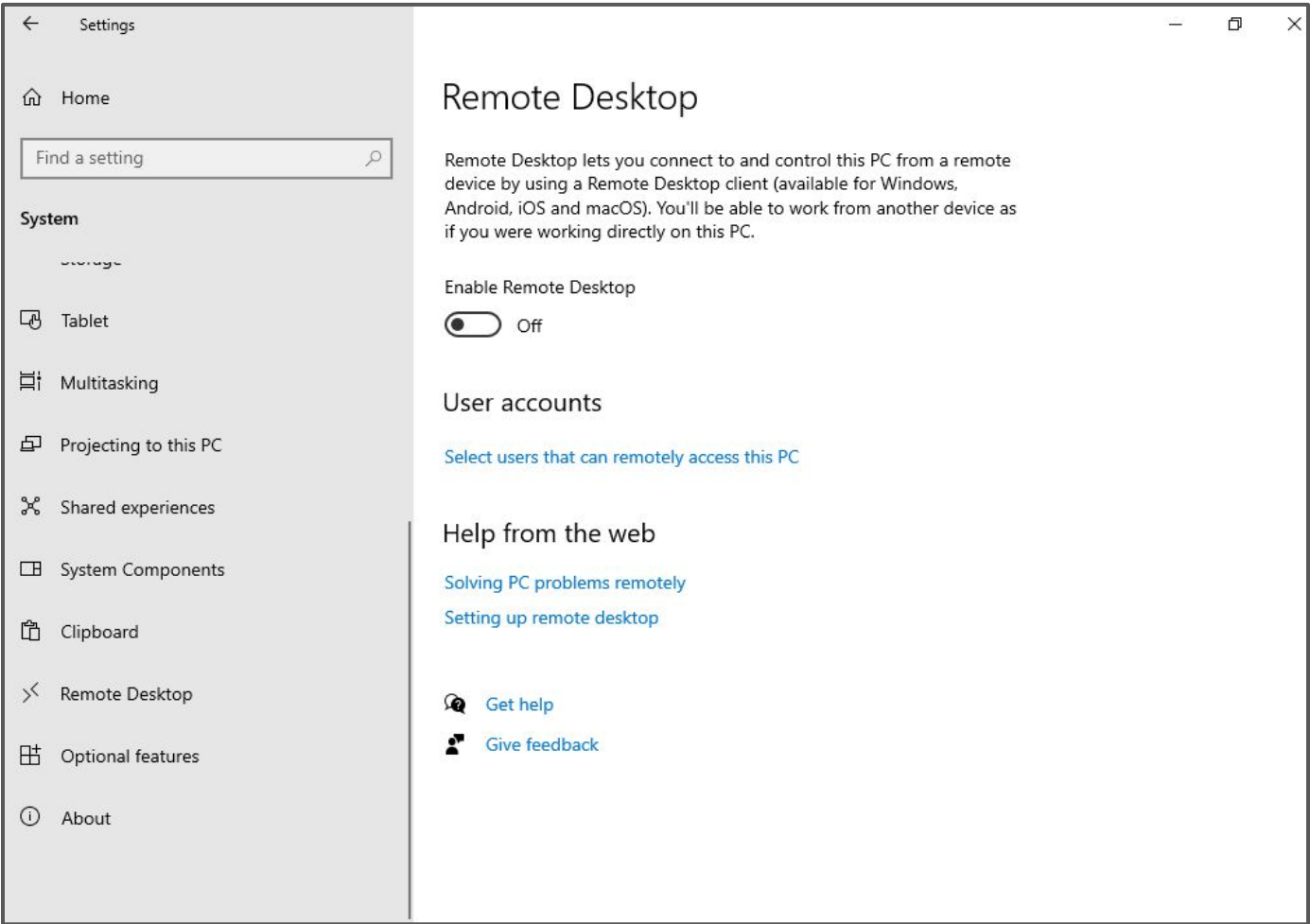
Windows Desktop Compliance

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

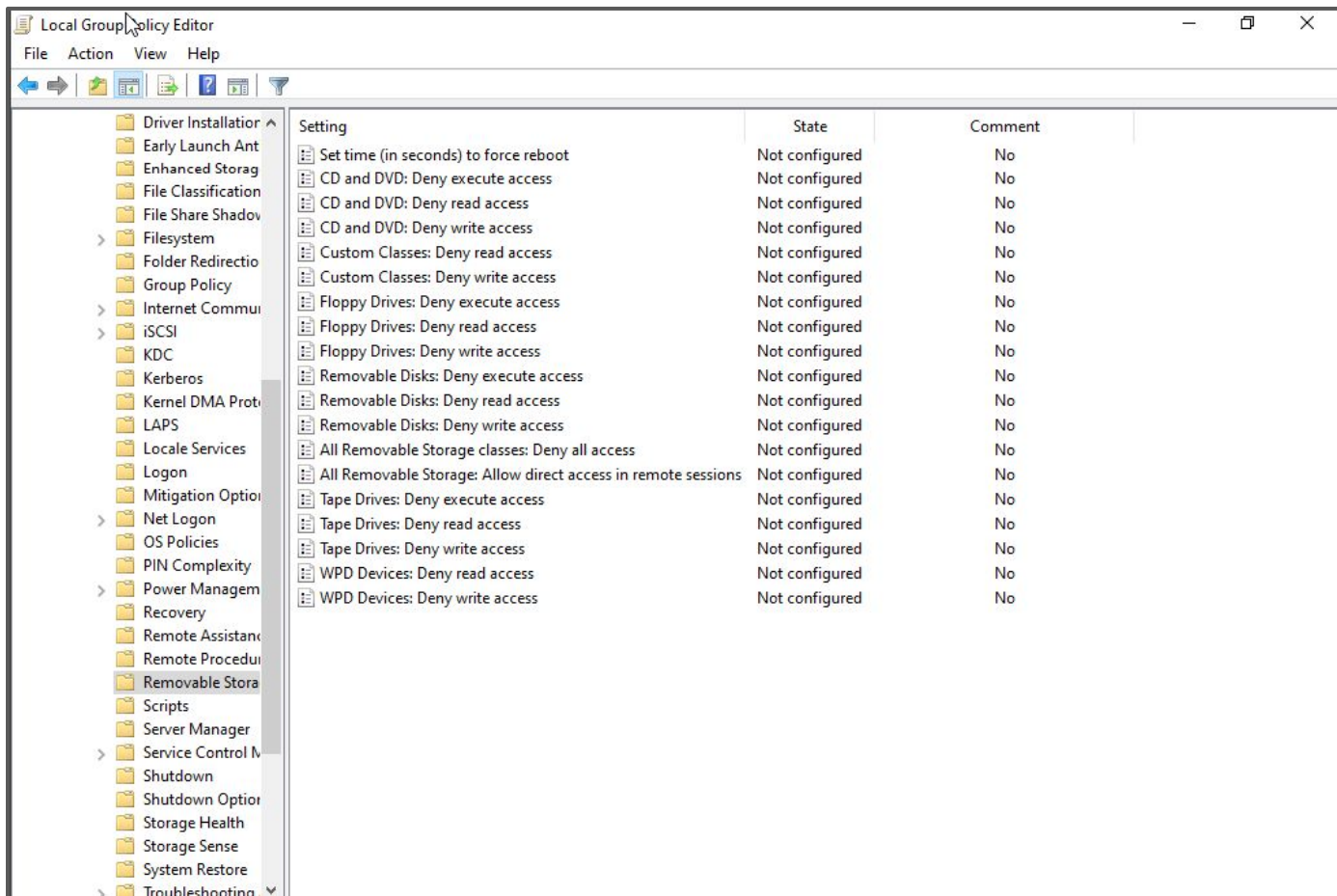


Windows Desktop Compliance

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

Windows Desktop Compliance

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

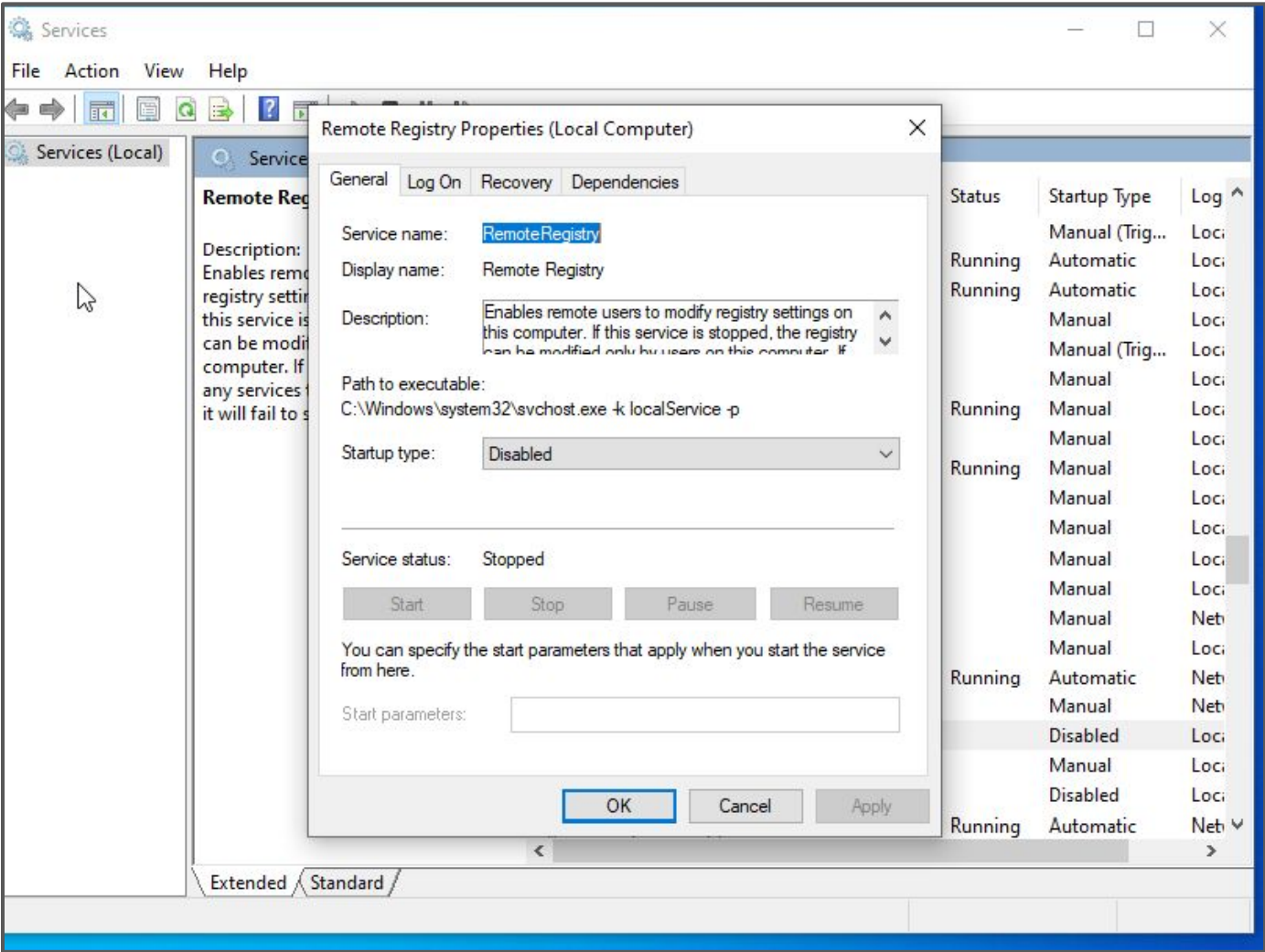


Windows Desktop Compliance

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

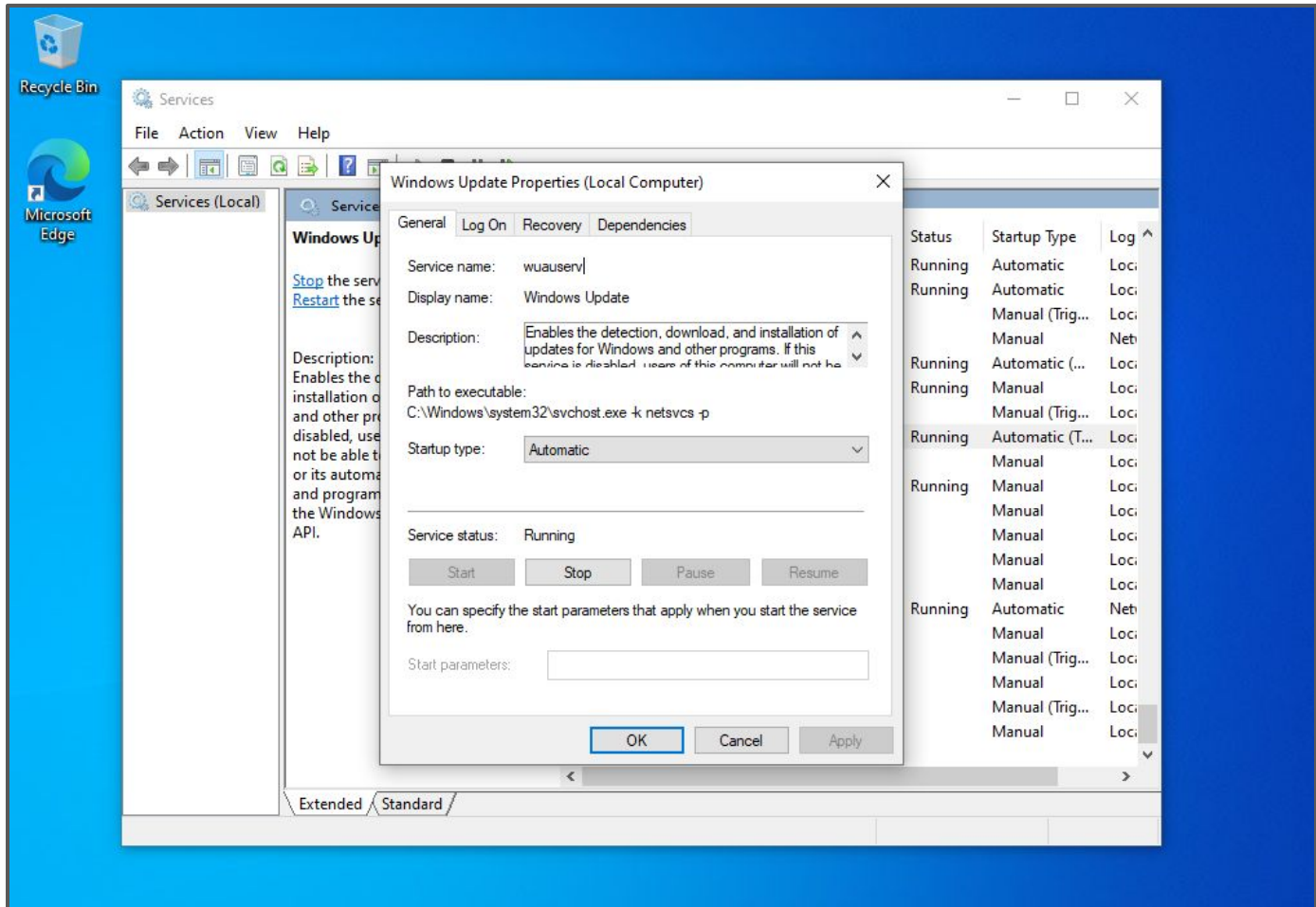
Windows Desktop Compliance

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

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.

Windows Desktop Compliance

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

Requirement	Remediation
Strong password policies are enforced	Open gpedit.msc > Navigate to Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy > Set password complexity, length, and expiration requirements.
System logging and auditing are enabled	Open secpol.msc > Local Policies > Audit Policy > Enable auditing for account logon, object access, and system events.
Remote Desktop Services are configured securely	Enable Network Level Authentication (gpedit.msc > RDP Security) and restrict access to authorized users (sysdm.cpl). Disable RDP if not needed and limit access via firewall rules.
USB ports are disabled or restricted to authorized devices only	Open gpedit.msc > Computer Configuration > Administrative Templates > System > Removable Storage Access > Deny write/read access to unauthorized USB devices.

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.

Linux Compliance

Linux CMMC Requirements	Met/Not Met
Current on security updates	No Met
Ensure separate partition exists for /var	No Met
Disable Automounting of drives	Met
Ensure AIDE is installed	No 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	No Met
Ensure DCCP is disabled	No Met
Ensure iptables is installed	Met
Ensure audit log storage size is configured	No Met
Ensure audit logs are not automatically deleted	No Met

Linux Compliance

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

kali@kali: ~/Desktop

File Actions Edit View Help

(kali@kali)-[~/Desktop]

\$ sudo apt list --upgradable

[sudo] password for kali:

7zip/kali-rolling 24.09+dfsg-3 amd64 [upgradable from: 24.08+dfsg-1]

alsa-ucm-conf/kali-rolling 1.2.13-1 all [upgradable from: 1.2.12-1]

aspell/kali-rolling 0.60.8.1-2 amd64 [upgradable from: 0.60.8.1-1+b2]

avahi-daemon/kali-rolling 0.8-15 amd64 [upgradable from: 0.8-13+b3]

avahi-utils/kali-rolling 0.8-15 amd64 [upgradable from: 0.8-13+b3]

base-passwd/kali-rolling 3.6.6 amd64 [upgradable from: 3.6.5]

bash/kali-rolling 5.2.37-1 amd64 [upgradable from: 5.2.32-1+b2]

bind9-dnsutils/kali-rolling 1:9.20.4-3 amd64 [upgradable from: 1:9.20.2-1]

bind9-host/kali-rolling 1:9.20.4-3 amd64 [upgradable from: 1:9.20.2-1]

bind9-libs/kali-rolling 1:9.20.4-3 amd64 [upgradable from: 1:9.20.2-1]

binutils-common/kali-rolling 2.43.50.20241230-1 amd64 [upgradable from: 2.43.1-5]

binutils-x86-64-linux-gnu/kali-rolling 2.43.50.20241230-1 amd64 [upgradable from: 2.43.1-5]

binutils/kali-rolling 2.43.50.20241230-1 amd64 [upgradable from: 2.43.1-5]

bloodhound.py/kali-rolling 1.8.0-0kali1 all [upgradable from: 1.7.2-0kali3]

bluez-hcidump/kali-rolling 5.79-1 amd64 [upgradable from: 5.77-1+kali1]

bluez-obexd/kali-rolling 5.79-1 amd64 [upgradable from: 5.77-1+kali1]

bluez/kali-rolling 5.79-1 amd64 [upgradable from: 5.77-1+kali1]

bsdxextrautils/kali-rolling 2.40.2-13 amd64 [upgradable from: 2.40.2-11]

bsdutils/kali-rolling 1:2.40.2-13 amd64 [upgradable from: 1:2.40.2-11]

bubblewrap/kali-rolling 0.11.0-2 amd64 [upgradable from: 0.11.0-1]

burpsuite/kali-rolling 2024.10.3-0kali2 amd64 [upgradable from: 2024.9.4-0kali1]

ca-certificates/kali-rolling 20241223 all [upgradable from: 20240203]

cadaver/kali-rolling 0.26+dfsg-2 amd64 [upgradable from: 0.24+dfsg-4]

cgpt/kali-rolling 0~R106-15054.B+dfsg-0.1 amd64 [upgradable from: 0~R106-15054.B-2+b1]

cherrytree/kali-rolling 1.1.2+dfsg-1+b2 amd64 [upgradable from: 1.1.2+dfsg-1+b1]

chromium-common/kali-rolling 131.0.6778.139-1 amd64 [upgradable from: 130.0.6723.116-1]

chromium-sandbox/kali-rolling 131.0.6778.139-1 amd64 [upgradable from: 130.0.6723.116-1]

chromium/kali-rolling 131.0.6778.139-1 amd64 [upgradable from: 130.0.6723.116-1]

cifs-utils/kali-rolling 2:7.1-1 amd64 [upgradable from: 2:7.0-2.1]

clang-17/kali-rolling 1:17.0.6-19 amd64 [upgradable from: 1:17.0.6-18]

clang/kali-rolling 1:19.0-63 amd64 [upgradable from: 1:16.0-58.1]

comerr-dev/kali-rolling 2.1-1.47.2-1 amd64 [upgradable from: 2.1-1.47.1-1+b1]

commix/kali-rolling 4.0-0kali1 all [upgradable from: 3.9+git20241118.92cf5d0-0kali1]

console-setup-linux/kali-rolling 1.233 all [upgradable from: 1.232]

console-setup/kali-rolling 1.233 all [upgradable from: 1.232]

coreboot-utils-doc/kali-rolling 24.08+dfsg-2 all [upgradable from: 4.15-dfsg2-2]

coreboot-utils/kali-rolling 24.08+dfsg-2 amd64 [upgradable from: 4.15-dfsg2-2]

cpp-14-x86-64-linux-gnu/kali-rolling 14.2.0-12 amd64 [upgradable from: 14.2.0-8]

cpp-14/kali-rolling 14.2.0-12 amd64 [upgradable from: 14.2.0-8]

cracklib-runtime/kali-rolling 2.9.6-5.2 amd64 [upgradable from: 2.9.6-5.1+b3]

curl/kali-rolling 8.11.1-1 amd64 [upgradable from: 8.11.0-1]

cutycapt/kali-rolling 0.0+20130714-1 amd64 [upgradable from: 0.0-svn10-0.1+b3]

dbus-bin/kali-rolling 1.16.0-1 amd64 [upgradable from: 1.14.10-6]

dbus-daemon/kali-rolling 1.16.0-1 amd64 [upgradable from: 1.14.10-6]

dbus-session-bus-common/kali-rolling 1.16.0-1 all [upgradable from: 1.14.10-6]

dbus-system-bus-common/kali-rolling 1.16.0-1 all [upgradable from: 1.14.10-6]

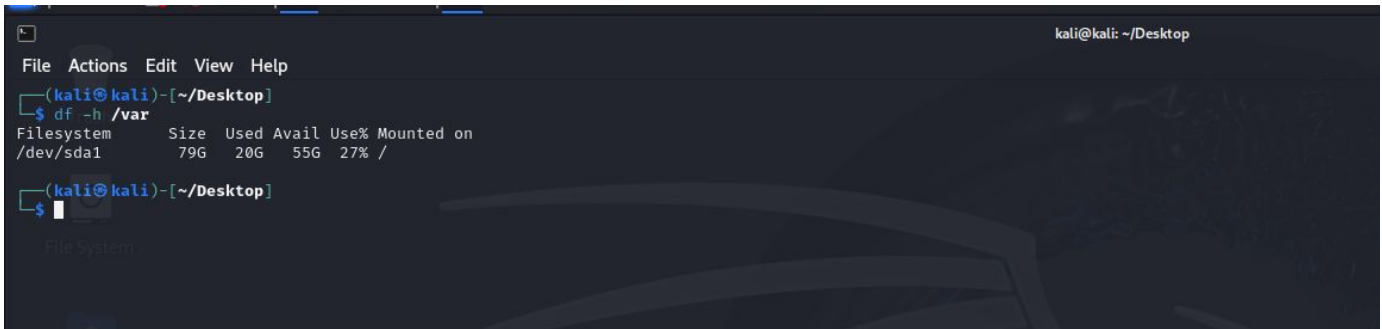
dbus-user-session/kali-rolling 1.16.0-1 amd64 [upgradable from: 1.14.10-6]

dbus-x11/kali-rolling 1.16.0-1 amd64 [upgradable from: 1.14.10-6]

dbus/kali-rolling 1.16.0-1 amd64 [upgradable from: 1.14.10-6]

Linux Compliance

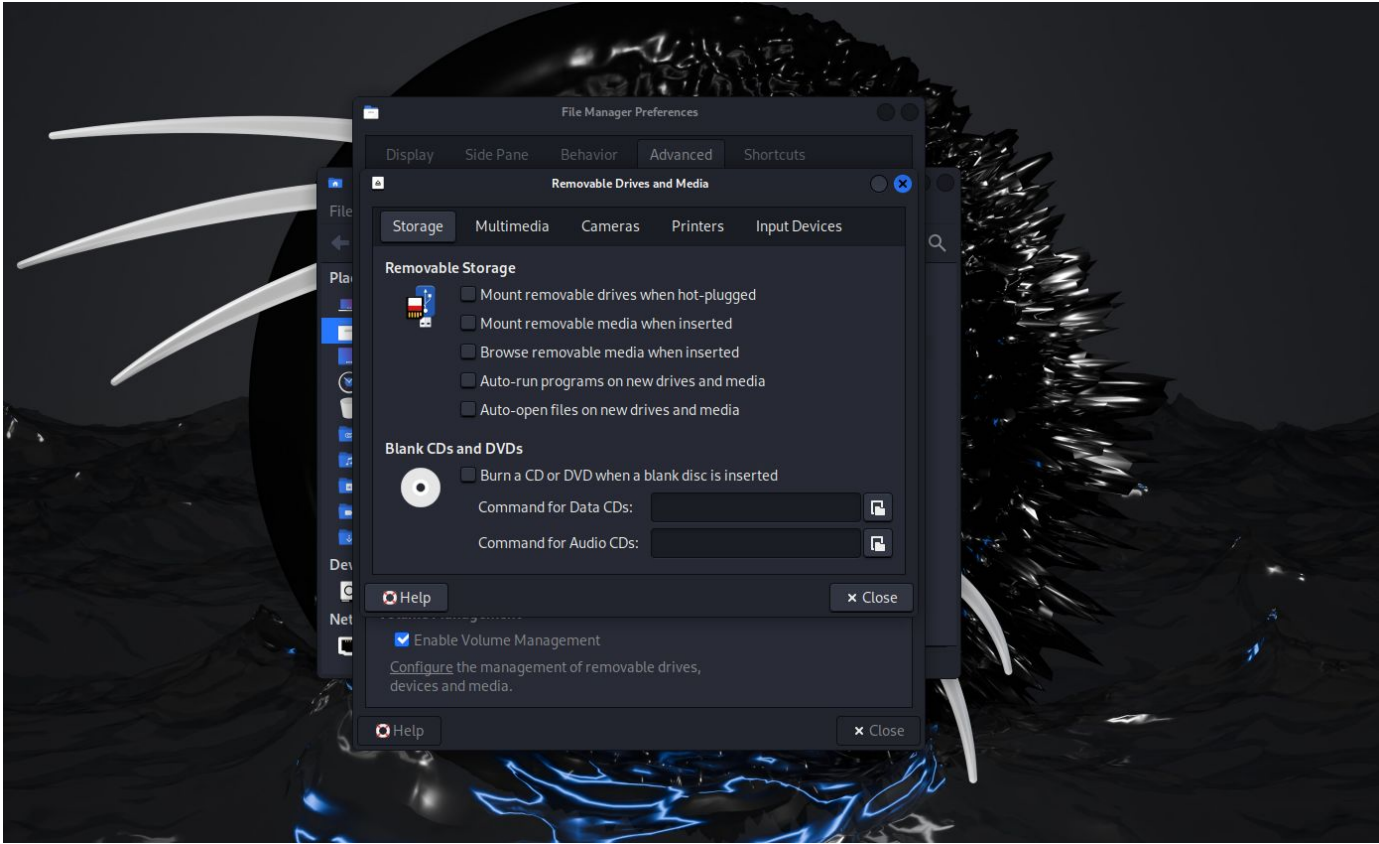
Linux Regulatory Requirement	Met/Not Met
Ensure separate partition exists for /var	Not Met

A terminal window screenshot from a Kali Linux system. The window title is 'kali@kali: ~/Desktop'. The terminal shows a command prompt '(kali@kali)-[~/Desktop]' followed by the command '\$ df -h /var'. The output is a table with columns: Filesystem, Size, Used, Avail, Use%, and Mounted on. The data row shows '/dev/sda1' with a size of 79G, 20G used, 55G available, 27% usage, and mounted on '/'.

```
kali@kali: ~/Desktop
(kali@kali)-[~/Desktop]
$ df -h /var
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1       79G   20G   55G  27% /
```

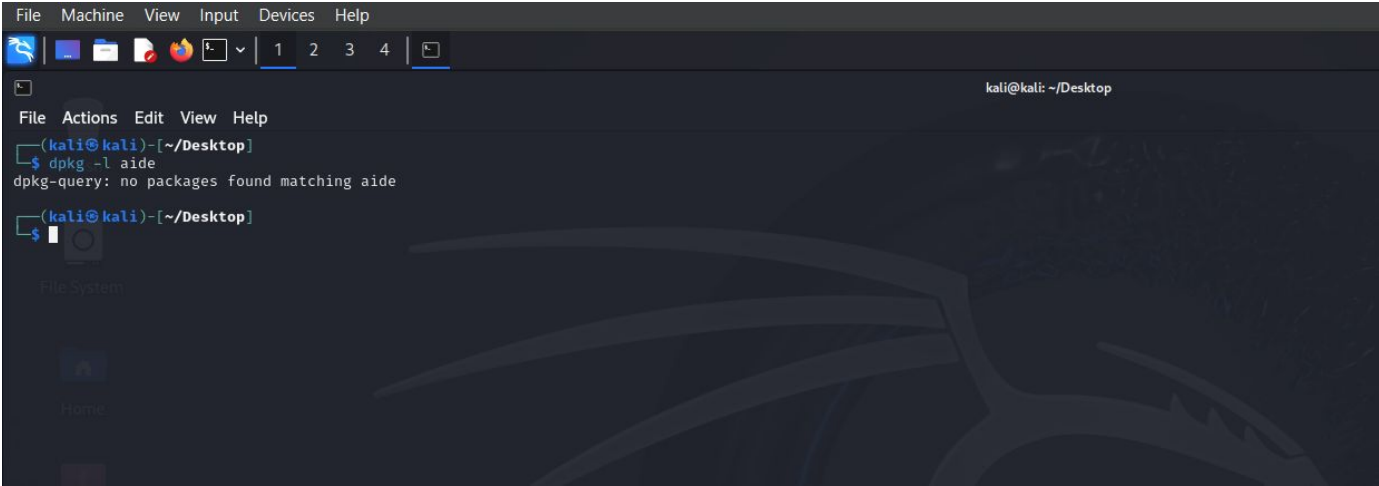
Linux Compliance

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



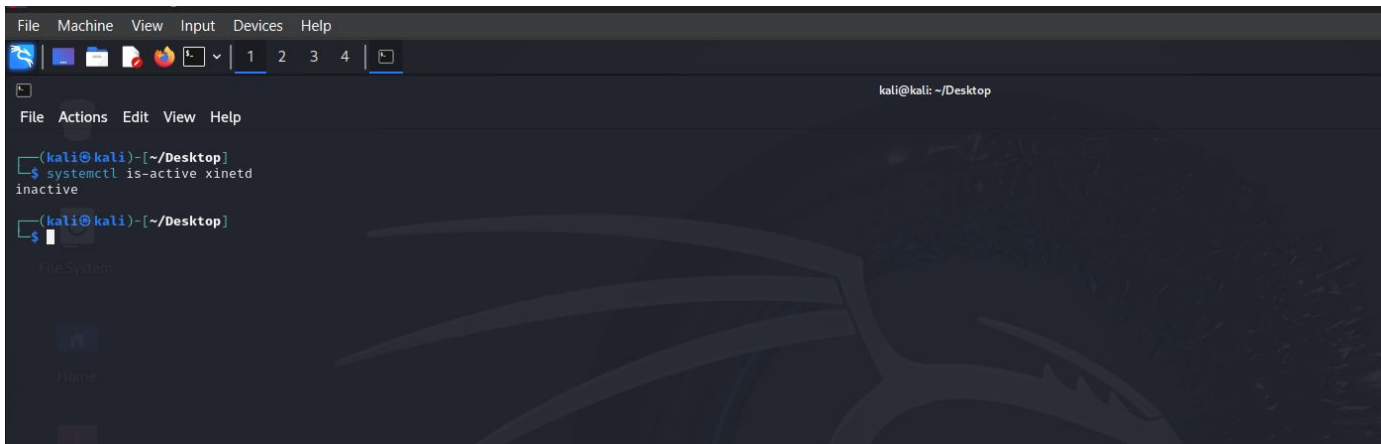
Linux Compliance

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



Linux Compliance

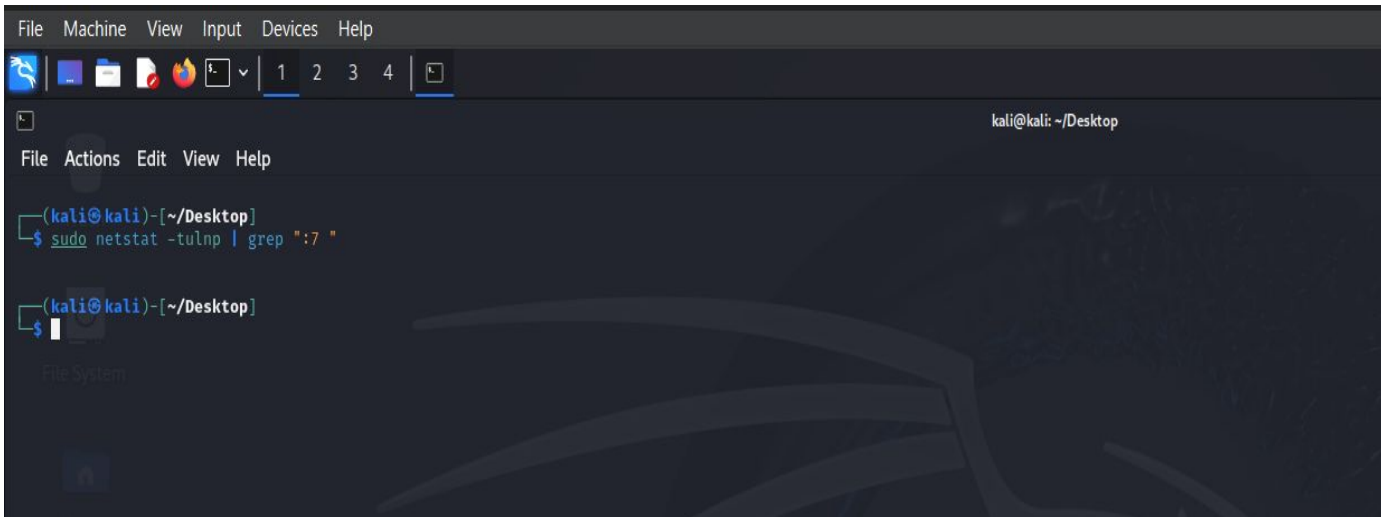
Linux Regulatory Requirement	Met/Not Met
Ensure daytime services are not enabled	Met



The screenshot displays a Kali Linux desktop environment. At the top, there is a menu bar with options: File, Machine, View, Input, Devices, and Help. Below this is a taskbar with various application icons and a window manager showing tabs 1, 2, 3, and 4. The main desktop area has a dark background with a faint Kali Linux logo. A terminal window is open, showing the command prompt '(kali@kali)-[~/Desktop]' and the command 'systemctl is-active xinetd'. The output of the command is 'inactive'. The terminal window also shows a 'File System' panel on the left side.

Linux Compliance

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

A screenshot of a Kali Linux desktop environment. The desktop has a dark theme with a Kali Linux logo watermark. The top panel shows a menu bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. Below the menu bar is a taskbar with icons for a web browser, file manager, terminal, and other applications. A terminal window is open, showing the command prompt '(kali@kali)-[~/Desktop]' and the command 'sudo netstat -tulnp | grep ":7 "'. The output of the command is not visible. The terminal window has its own menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'.

```
(kali@kali)-[~/Desktop]
$ sudo netstat -tulnp | grep ":7 "
```

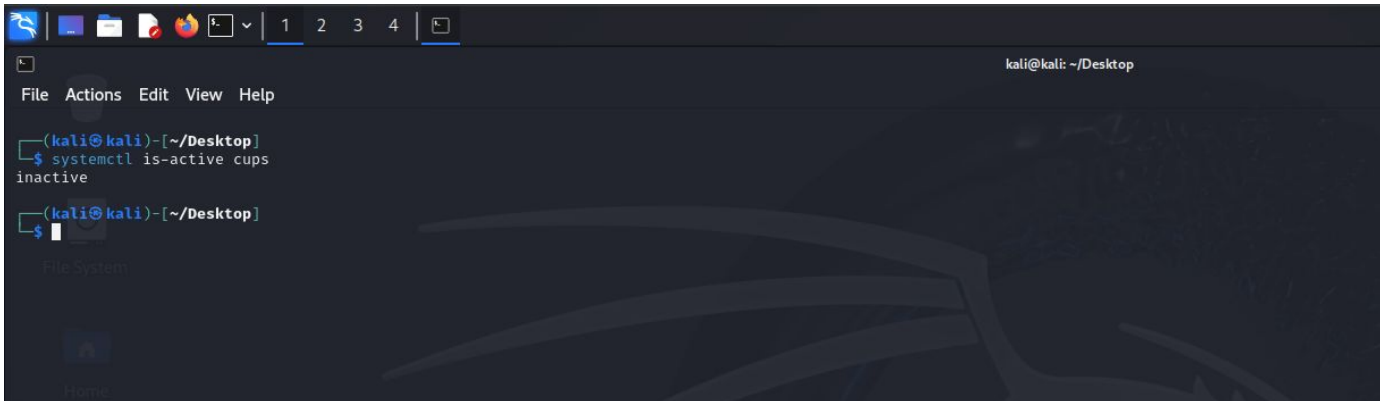
Linux Compliance

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



Linux Compliance

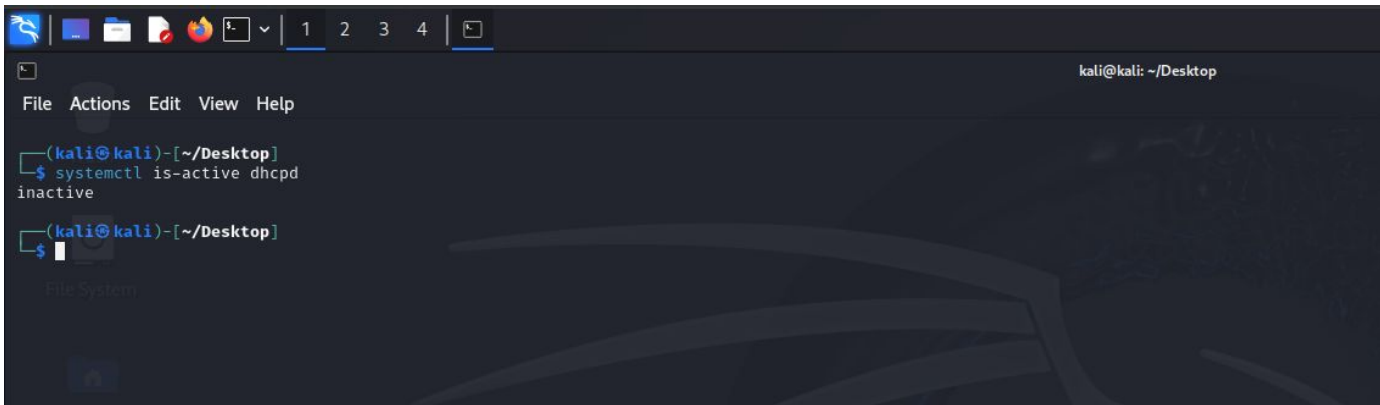
Linux Regulatory Requirement	Met/Not Met
Ensure CUPS is not enabled	Met

A terminal window on a Kali Linux desktop environment. The window title is 'kali@kali: ~/Desktop'. The terminal shows the command 'systemctl is-active cups' being executed, with the output 'inactive'. The desktop background is dark with a faint Kali Linux logo. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'.

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ systemctl is-active cups
inactive
(kali@kali)-[~/Desktop]
$
```

Linux Compliance

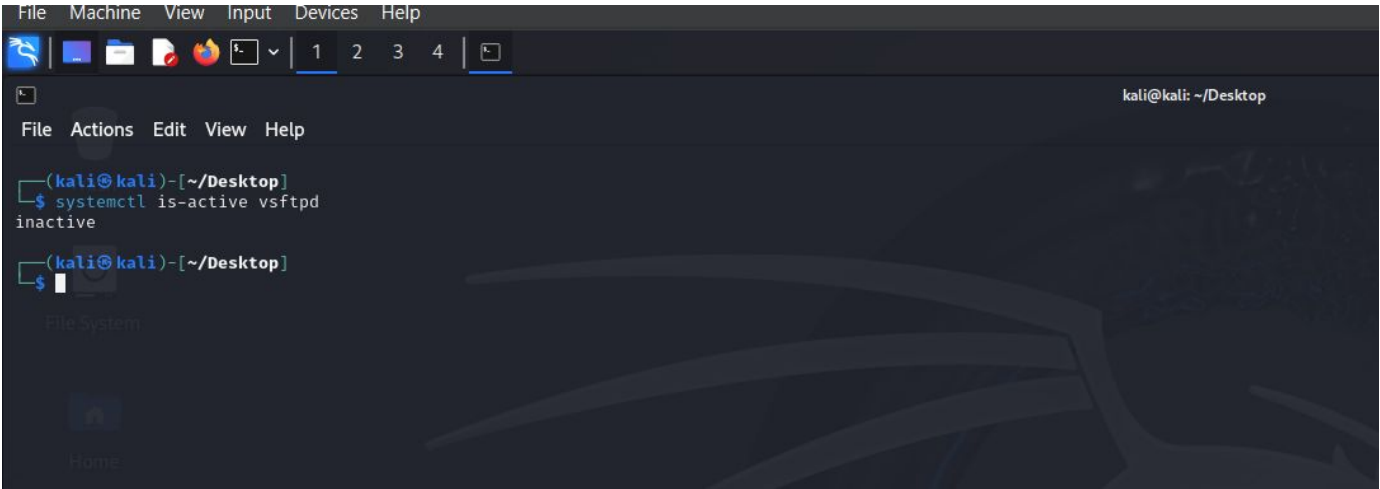
Linux Regulatory Requirement	Met/Not Met
Ensure DHCP Server is not enabled	Met

A screenshot of a Kali Linux terminal window. The window has a dark theme and a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the user is at the prompt '(kali@kali)~[~/Desktop]'. The command 'systemctl is-active dhcpcd' has been entered, and the output is 'inactive'. The terminal also shows a file manager icon in the bottom left corner.

```
(kali@kali)~[~/Desktop]
$ systemctl is-active dhcpcd
inactive
(kali@kali)~[~/Desktop]
$
```

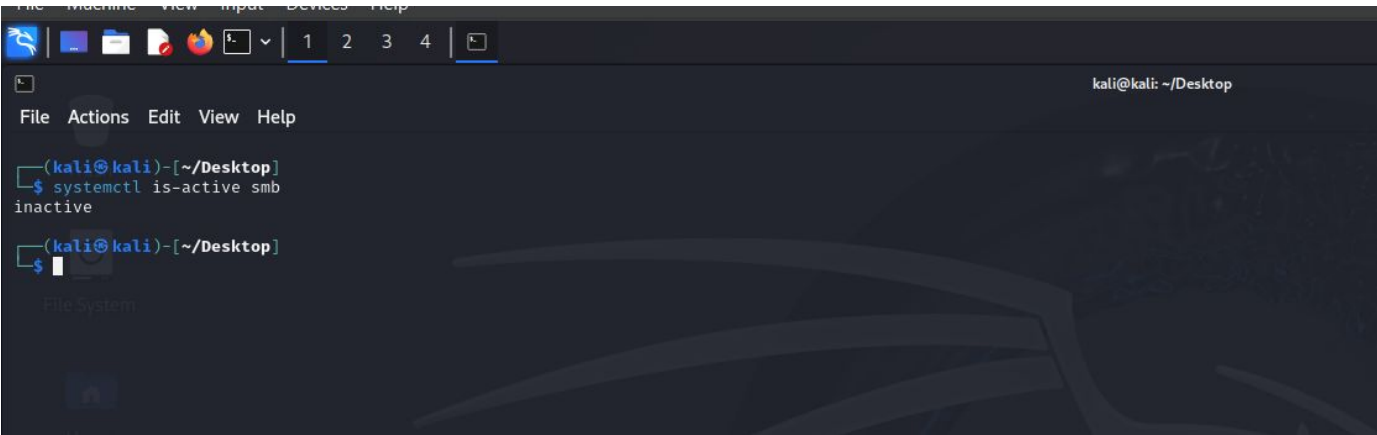

Linux Compliance

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



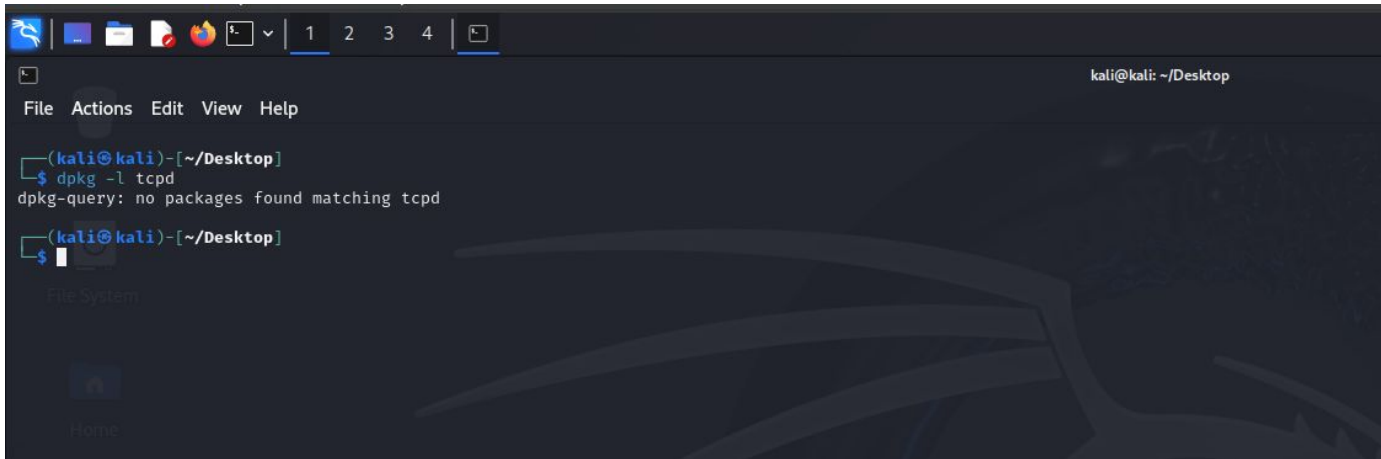
Linux Compliance

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	Not Met

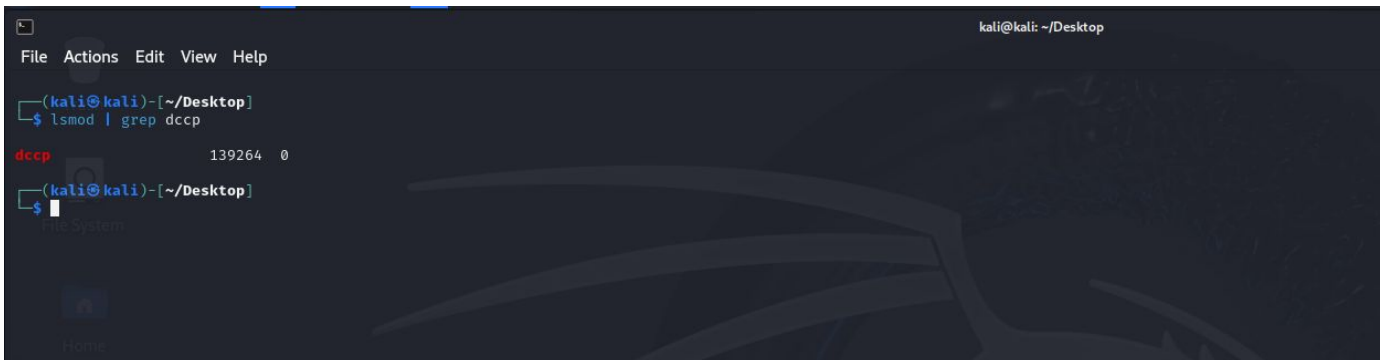
A screenshot of a Kali Linux desktop environment. The top panel shows various application icons and a window manager with tabs numbered 1 to 4. The terminal window is open, displaying the command prompt (kali@kali) and the directory (~/Desktop). The user has entered the command 'dpkg -l tcpd', and the output is 'dpkg-query: no packages found matching tcpd'. The desktop background is dark with a faint, abstract graphic. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'.

```
(kali@kali)~[~/Desktop]
$ dpkg -l tcpd
dpkg-query: no packages found matching tcpd

(kali@kali)~[~/Desktop]
$
```

Linux Compliance

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

A terminal window on a Kali Linux desktop environment. The window title is 'kali@kali: ~/Desktop'. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal prompt is '(kali@kali)-[~/Desktop]'. The user has entered the command 'lsmod | grep dccp'. The output shows 'dccp' loaded with a size of 139264 and 0 references. The desktop background is dark with a faint, abstract graphic. A 'The System' window is partially visible in the bottom left corner.

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ lsmod | grep dccp
dccp                  139264  0
(kali@kali)-[~/Desktop]
$
```

Linux Compliance

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

```
File Machine View Input Devices Help
kali@kali: ~/Desktop

File Actions Edit View Help

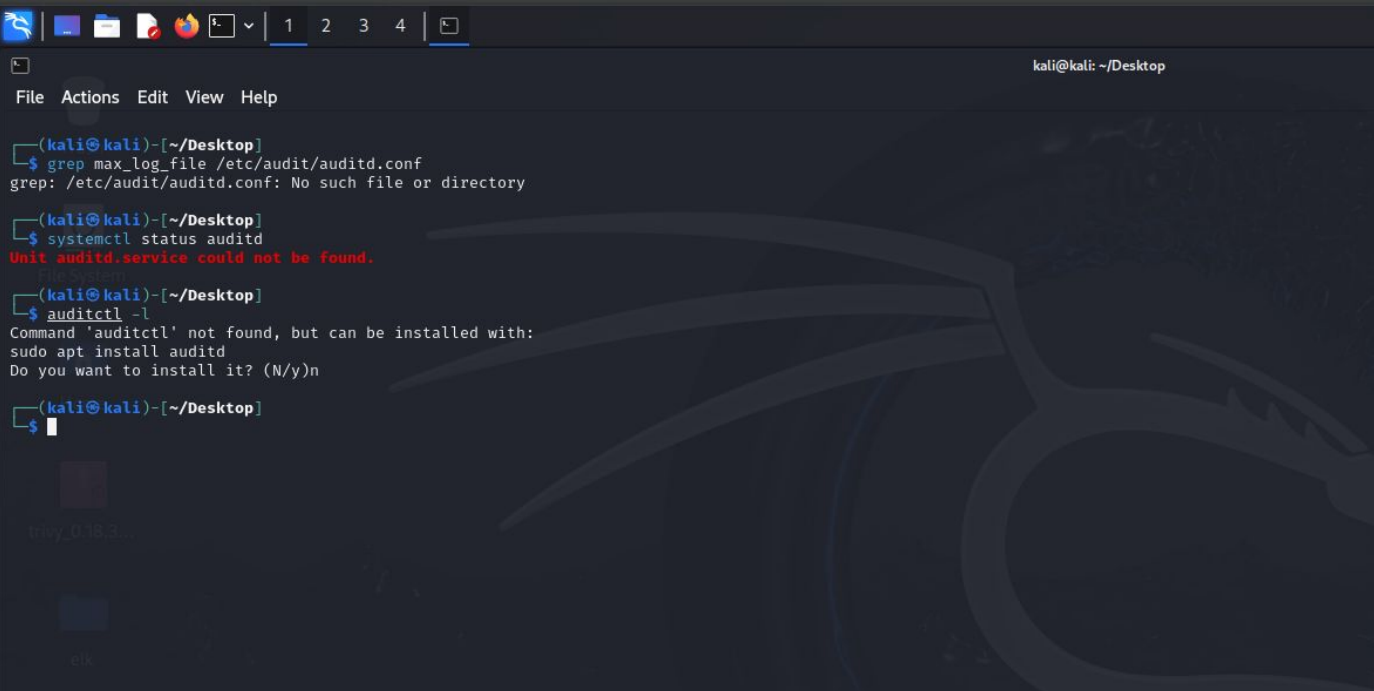
(kali@kali)-[~/Desktop]
$ dpkg -l iptables
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name          Version        Architecture Description
+++-+-----+-----+-----+-----+
ii  iptables        1.8.10-4+b1    amd64        administration tools for packet filtering and NAT

(kali@kali)-[~/Desktop]
$ sudo iptables --version
iptables v1.8.10 (nf_tables)

(kali@kali)-[~/Desktop]
$
```

Linux Compliance

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



```
(kali@kali)-[~/Desktop]
$ grep max_log_file /etc/audit/auditd.conf
grep: /etc/audit/auditd.conf: No such file or directory

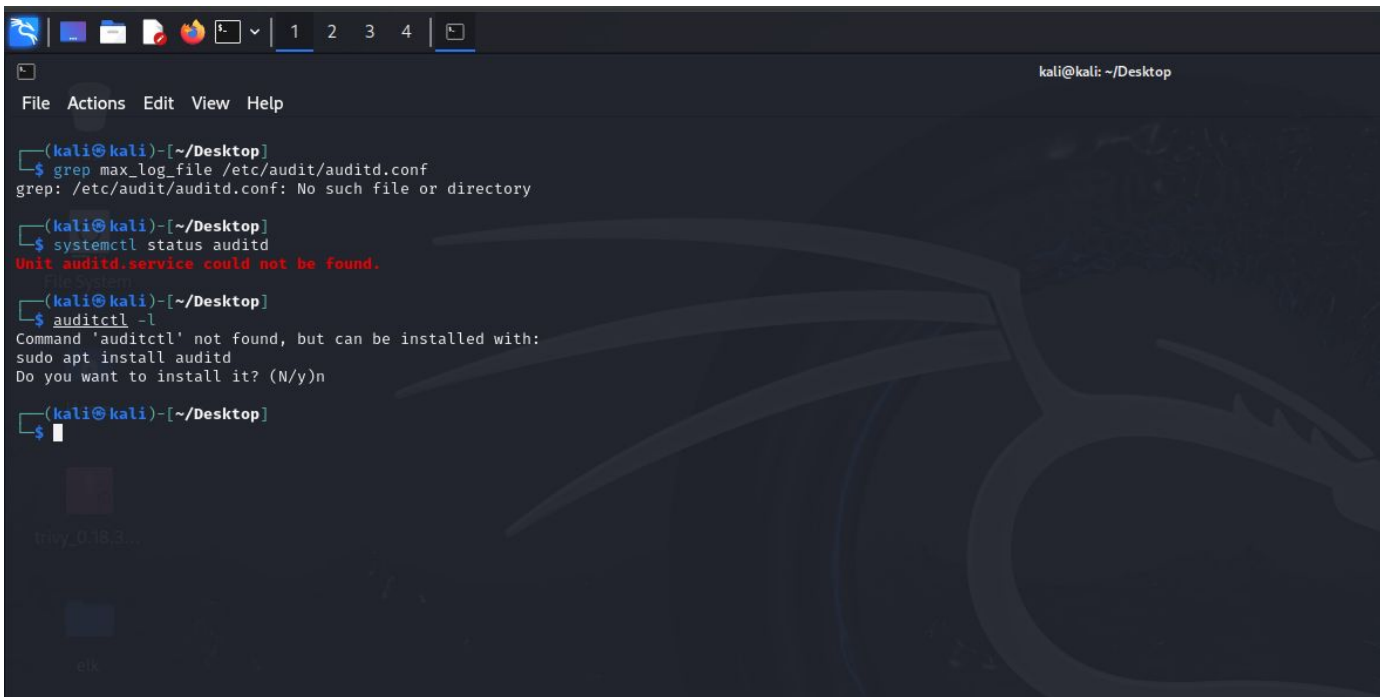
(kali@kali)-[~/Desktop]
$ systemctl status auditd
Unit auditd.service could not be found.

(kali@kali)-[~/Desktop]
$ auditctl -l
Command 'auditctl' not found, but can be installed with:
sudo apt install auditd
Do you want to install it? (N/y)n

(kali@kali)-[~/Desktop]
$
```

Linux Compliance

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

A terminal window on a Kali Linux desktop environment. The window title is 'kali@kali: ~/Desktop'. The terminal shows a series of commands and their outputs. First, 'grep max_log_file /etc/audit/auditd.conf' is run, resulting in 'grep: /etc/audit/auditd.conf: No such file or directory'. Then, 'systemctl status auditd' is run, resulting in 'Unit auditd.service could not be found.'. Next, 'auditctl -l' is run, resulting in 'Command 'auditctl' not found, but can be installed with: sudo apt install auditd'. Finally, a prompt 'Do you want to install it? (N/y)n' is shown, with 'n' entered. The terminal background has a dark theme with a faint dragon logo.

```
(kali@kali)-[~/Desktop]
$ grep max_log_file /etc/audit/auditd.conf
grep: /etc/audit/auditd.conf: No such file or directory

(kali@kali)-[~/Desktop]
$ systemctl status auditd
Unit auditd.service could not be found.

(kali@kali)-[~/Desktop]
$ auditctl -l
Command 'auditctl' not found, but can be installed with:
sudo apt install auditd
Do you want to install it? (N/y)n
```

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.

Windows Server Build Sheet

1. Operating System Version

Specify the exact OS version to ensure compatibility and security updates. Avoid using end-of-life versions.
Eg: Windows Server 2022 Datacenter Edition

2. Server Size and Configuration

Define the VM size based on workload requirements to balance performance and cost.
Eg: Azure VM Size - Standard_D4s_v3 (4 vCPUs, 16 GB RAM)

3. Network Configuration

Ensure proper network settings for secure and efficient communication.
Eg: Assign a static public IP, configure NSG (Network Security Group) rules to allow HTTP (port 80) and HTTPS (port 443) traffic, and block all other ports.

4. Security Hardening

Follow Microsoft's security baseline recommendations to reduce vulnerabilities.
Eg: Disable unused services (e.g., Telnet, FTP)

5. Web Server Software Installation

Set up the web server software with necessary components for hosting applications.
Eg: Install IIS (Internet Information Services)

Windows Server Build Sheet

6. SSL/TLS Configuration

Ensure encrypted communication to protect sensitive data.
Eg: Configure SSL certificates

7. Backup and Recovery

Implement a backup strategy to recover data in case of failures or attacks.
Eg: Set up automated daily backups using Azure Backup

8. Monitoring and Logging

Monitor server performance and security events to detect and respond to issues quickly.
Eg: Enable Azure Monitor and configure alerts

9. Access Control and Authentication

Restrict access to authorized personnel only and implement least privilege principles.
Eg: Use Azure Active Directory (AD) for user authentication and enforce role-based access control (RBAC).

10. Application Deployment and Configuration

Ensure consistent and automated deployment processes to reduce human error.
Eg: Deploy the web application using a CI/CD pipeline

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.

Enhancing Cloud Security with CASB

1. Visibility into Cloud Usage

CASBs provide detailed insights into all cloud services being used across the organization. This visibility helps identify risks and enforce compliance with security policies.

2. Data Loss Prevention (DLP)

CASBs monitor and control the movement of sensitive data in and out of cloud applications. They can detect and prevent unauthorized sharing, downloads, or transfers of confidential information, ensuring data protection.

3. Threat Detection and Prevention

CASBs use advanced analytics and machine learning to detect suspicious activities, such as malware, ransomware, or compromised accounts. They can block threats in real-time, reducing the risk of breaches.

4. Access Control and Authentication

CASBs enforce granular access policies, such as multi-factor authentication (MFA) and role-based access control (RBAC). This ensures that only authorized users can access sensitive cloud resources.

5. Compliance and Governance

CASBs help organizations meet regulatory requirements (e.g., GDPR, HIPAA) by providing audit trails, encryption, and policy enforcement. They ensure that cloud usage aligns with legal and industry standards.