

COMPLIANCE ASSESSMENT



*[KSHITIJ PARTE]
[CBS-0104]*

HOW TO USE THIS TEMPLATE

- We have provided these slides as a guide to ensure you submit all the required components to complete your project successfully.
- When presenting your project, remember that these slides are merely a guide. We strongly encourage you to embrace your creative freedom and make changes that reflect your unique vision as long as the required information is present.
- You can add slides to the template when your answers or screenshots do not fit on the previously provided pages.
- Delete this and all other project instruction slides before submitting your project.
- **Remember to add your name and the date to the cover page.**

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 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 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. [OUTDATED SYSTEM UPDATES]

Outdated systems are a hacker's playground. Go to *Settings* → *Update & Security* → *Windows Update* and enable automatic updates immediately. This will ensure that your computer is always armed with the latest defenses against new viruses, malware, and security flaws. Missing critical updates leaves huge gaps for attackers to sneak in. Regularly check for updates manually too, just to be sure you're not waiting on something vital. Staying updated is your first line of real-world digital armor.

2. [DISABLED ANTIVIRUS]

An unprotected computer is like walking into battle naked. Open *Windows Security* and activate Windows Defender or install a reputable third-party antivirus like Bitdefender or Kaspersky. Antivirus software continuously monitors your system for threats, removing viruses, spyware, and ransomware before they wreak havoc. Also, schedule regular scans and keep virus definitions updated. Even free antivirus is way better than nothing. No antivirus = an open invitation for cybercriminals to invade your system.

3. [weak password]

Passwords are your secret weapon. Weak ones are basically handing over your keys. Open *gpedit.msc*, navigate to *Computer Configuration* → *Windows Settings* → *Security Settings* → *Account Policies* → *Password Policy*. Set strong rules: minimum 12–16 characters, with a mix of uppercase, lowercase, numbers, and special characters. Force password changes every 90 days. Disable password hints too. It's a simple move that makes brute-force attacks insanely harder and keeps your confidential data *yours*.

Windows 10 Hardening

4. [FIREWALL DISABLED]

Without a firewall, you're broadcasting "open house" to hackers. Go to *Control Panel → System and Security → Windows Defender Firewall* and ensure it's enabled for Domain, Private, and Public networks. A firewall filters incoming and outgoing traffic, blocking unauthorized access to your computer while allowing safe communications. Set it to block all incoming connections by default, then allow only trusted apps. This silent bodyguard keeps intruders guessing — and out.

5. [AUTO-RUN AUTO -PLAY ENABLE]

AutoRun/AutoPlay is a dream for malware attacks. One infected USB stick can instantly take over your machine. Go to *Control Panel → Hardware and Sound → AutoPlay* and disable AutoPlay for all devices and media. This prevents any external device from automatically executing files without your permission. It puts you back in control — nothing runs without your say-so. Simple, effective, and kills 90% of drive-by attacks that depend on user laziness.

6. [INACTIVE ADMIN ACCOUNT]

That default "Administrator" account is a big red target. Even if you don't use it, attackers know it exists. Open Command Prompt (Admin) and run `net user Administrator /active:no` to deactivate it. Instead, create a new admin account with a strong, unique username and password. This hides your admin privileges behind a fresh wall. Never leave doors open, even if you think no one's looking. In cybersecurity, invisible is invincible.

MacOS Hardening

As Fed First 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. [FileVault encryption]

FileVault encrypts your entire hard drive, turning sensitive data into an unreadable vault unless the correct login credentials are provided. Even if the MacBook is stolen or accessed without permission, your data stays locked down tight. It's the digital chastity belt your confidential files deserve.

2. [Firewall activation]

Activating the Mac firewall prevents unauthorized incoming network connections, keeping cyber intruders out of your system. It acts like a seductive bouncer at the club—only letting in the trusted and booting out the shady. This is essential to block unverified and possibly malicious traffic.

3. [Disable Automatic Login]

Automatic login is basically a welcome mat for hackers. Disabling it ensures that anyone powering on the Mac must authenticate manually, preventing unauthorized access during boot-up. Without this layer, physical access equals open season—so lock that door, baby, every single time.

MacOS Hardening

4. [enable Gatekeeper]

Gatekeeper restricts the execution of apps to those downloaded from the App Store or verified developers. It's like your sexy bodyguard, ensuring no shady, unsigned software slips past your defenses. This protects against malicious code injections and untrusted applications exploiting system permissions.

5. [Turn OFF location for service system]

Gatekeeper restricts the execution of apps to those downloaded from the App Store or verified developers. It's like your sexy bodyguard, ensuring no shady, unsigned software slips past your defenses. This protects against malicious code injections and untrusted applications exploiting system permissions.

6. [Set strong password and enable the touch ID]

A strong password combined with biometric authentication (like Touch ID) creates a robust dual-lock mechanism. The password keeps digital access secure, while Touch ID adds a frictionless yet tight physical layer. Together, they make sure only the chosen one—aka *you*—can unlock your Mac's secrets.

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.

- **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. Prohibit Auto-Forwarding to Personal Email Accounts : Employees are strictly forbidden from enabling auto-forwarding of work emails to personal inboxes. This closes off a dangerous leak point where sensitive data could end up on unsecured or compromised personal devices, far outside the company's security perimeter.

2. Mandatory Use of Multi-Factor Authentication (MFA) : All users must log into their corporate email with MFA enabled. Whether it's a token, biometric, or OTP app, this adds a second layer that makes stealing credentials alone completely useless to an attacker.

3. Ban on Opening Unknown Attachments or Clicking Suspicious Links : Employees must avoid opening attachments or clicking links from unknown or unexpected sources. These are the main payload delivery vectors for malware, ransomware, or phishing attacks—basically the digital equivalent of opening the door to a masked creep.

4. . Encrypt Sensitive Emails and Use Secure Channels : All emails containing confidential company data, client details, or internal secrets must be encrypted. No raw secrets sent in plain text, darling. Use tools like S/MIME or PGP, and always double-check recipient addresses before sending.

5. Mandatory Reporting of Phishing Attempts : Any email suspected to be phishing must be reported immediately to the IT/security team. Employees should be trained to use the "Report Phishing" button or forward suspicious emails to the designated security inbox. Fast reporting means faster neutralization.

BYOD Policy

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

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

BYOD Policy

1. Mandatory Device Encryption

All BYOD devices must have full-disk encryption enabled.

- *Windows/macOS*: Use BitLocker or FileVault
- *Android/iOS*: Native encryption must be activated

This ensures that if a device is lost or stolen, corporate data stays unreadable and out of malicious hands. No exceptions. No unencrypted drama.

2. Enforced Screen Lock and Strong Authentication

All devices must have a secure lock method (password, biometric, PIN) activated. Idle timeout must be configured to lock the screen after no more than 5 minutes of inactivity. Fingerprint, Face ID, or complex passwords are required—slide-to-unlock ain't enough anymore, sweetheart.

3. Mobile Device Management (MDM) Enrollment

All devices must be registered with the organization's MDM solution before being allowed access.

This enables remote management features like policy enforcement, remote wipe, app control, and compliance tracking. If you want access to the kingdom, you play by the kingdom's rules.

4. No Rooted or Jailbroken Devices Allowed

Rooted or jailbroken devices are strictly prohibited.

They're a hacker's playground, with weakened defenses and untrusted app access. Devices must maintain original OS integrity; if you're tampering with your system, you're tampering with our security.

5. Secure Container for Work Data

Work-related apps and data must reside within a secure container.

Data segregation prevents corporate information from mixing with personal files. If your phone gets malware while you're watching cat videos, it shouldn't endanger the confidential Q3 revenue sheet.

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

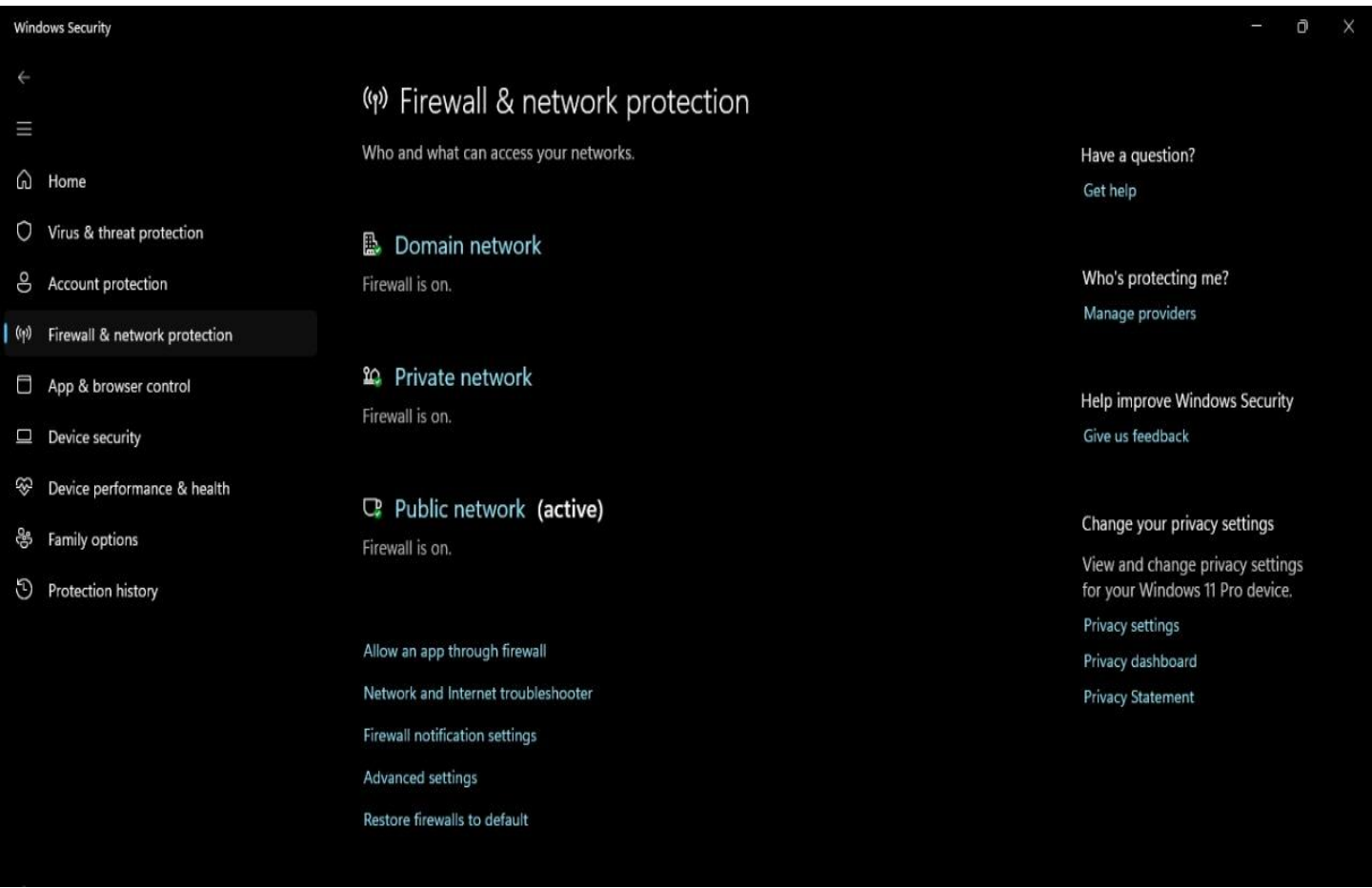
Windows 10 Regulatory Requirement	Met/Not Met
Built-In Administrator account is disabled	
Windows Firewall is enabled	
Automatic updates are enabled	
User Account Control (UAC) is enabled	
Strong password policies are enforced	
Guest account is disabled	
System logging and auditing are enabled	
Windows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

Windows Desktop Compliance

Windows 10 Regulatory Requirement

Met/Not Met

Windows Firewall is enabled

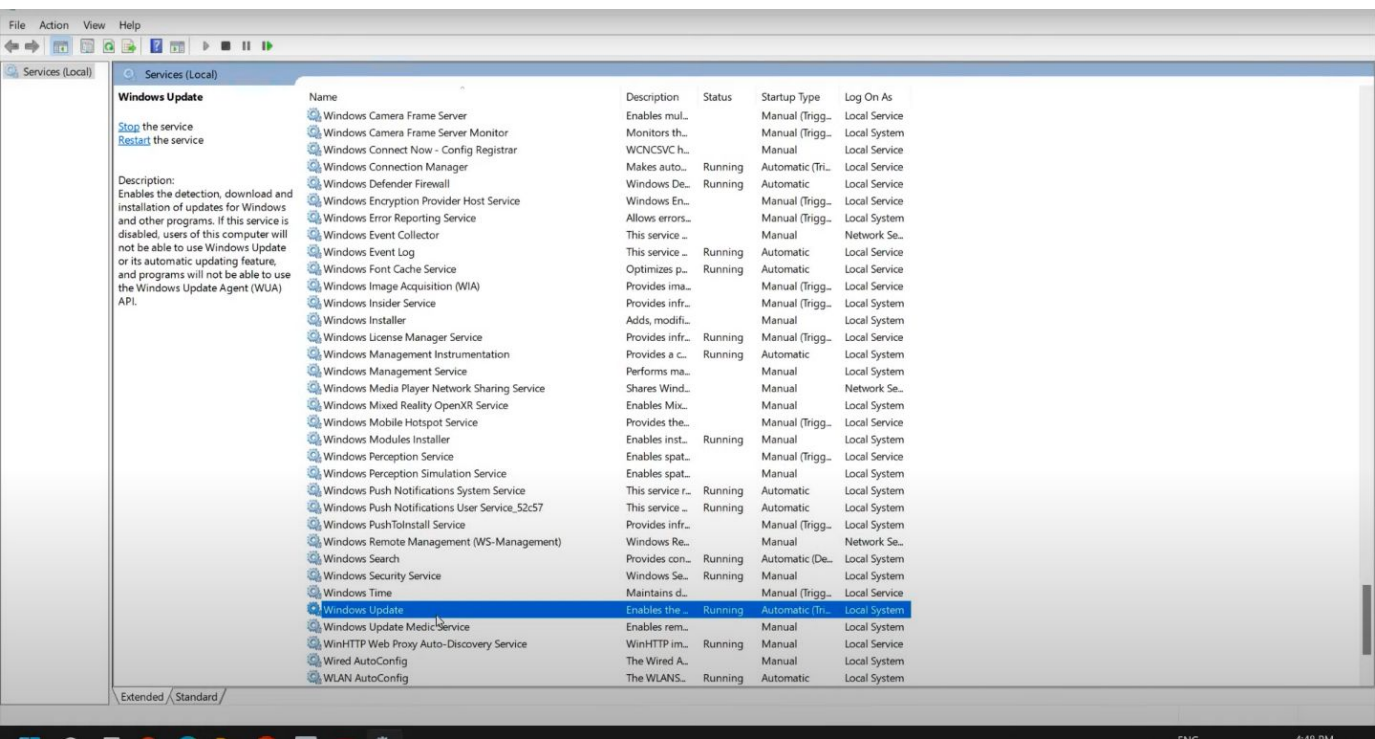


Windows Desktop Compliance

Windows 10 Regulatory Requirement

Met/Not Met

Automatic updates are enabled

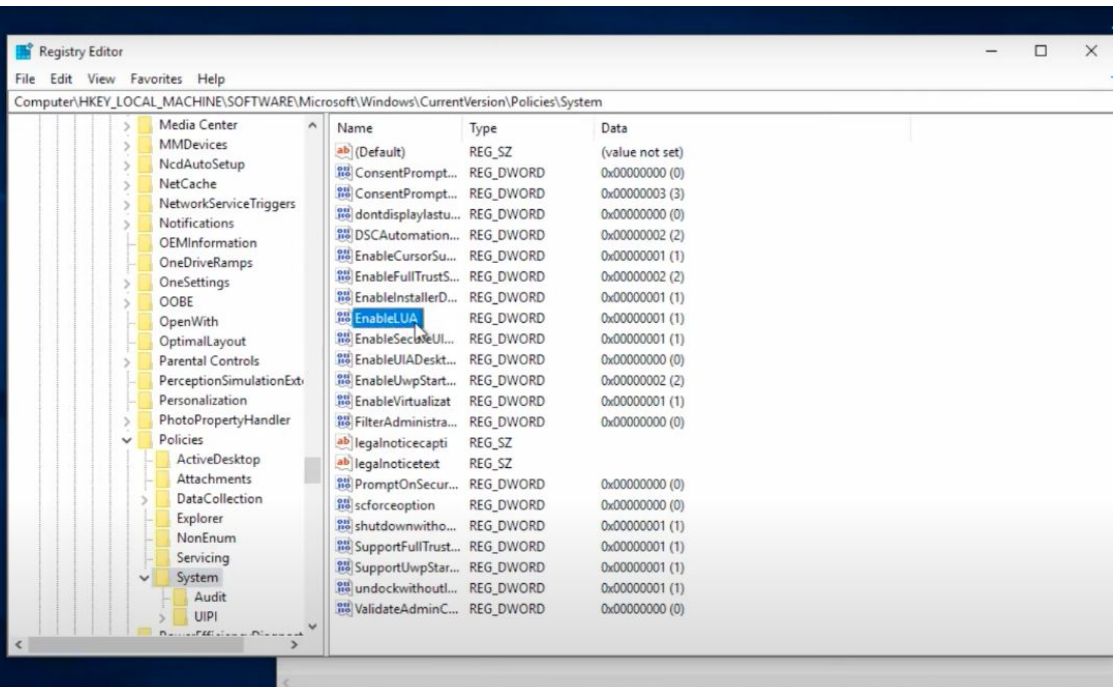


Windows Desktop Compliance

Windows 10 Regulatory Requirement

Met/Not Met

User Account Control (UAC) is enabled

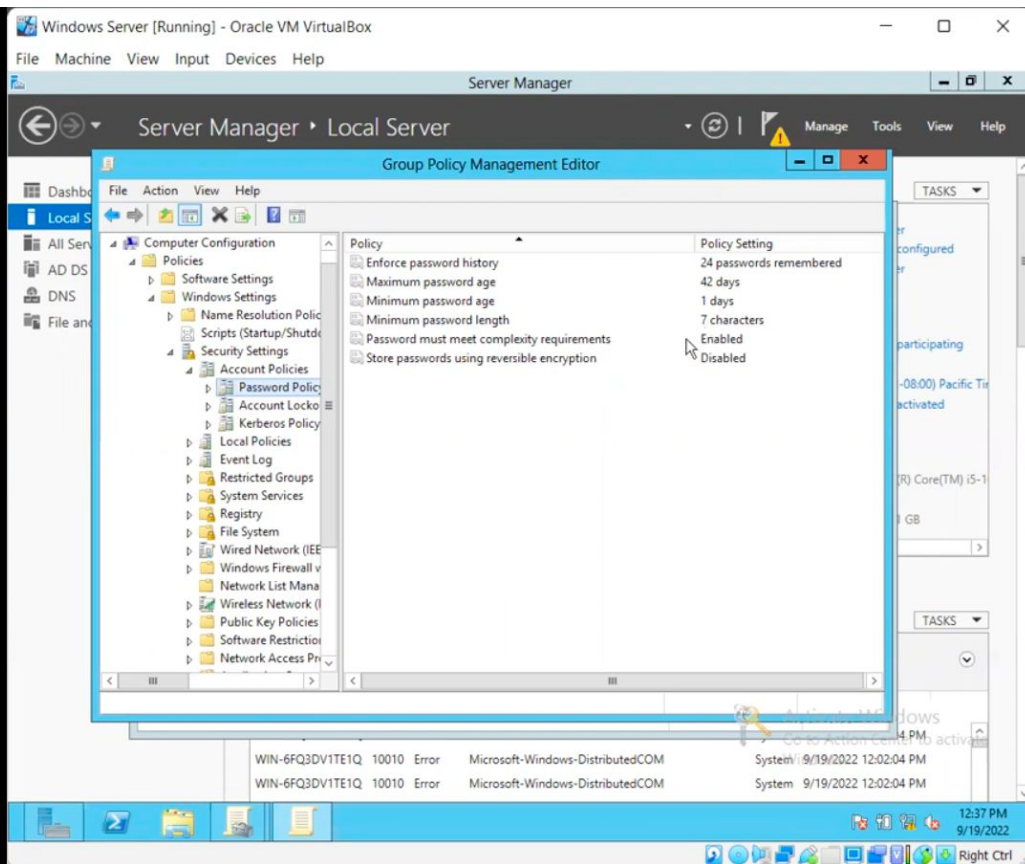


Windows Desktop Compliance

Windows 10 Regulatory Requirement

Met/Not Met

Strong password policies are enforced

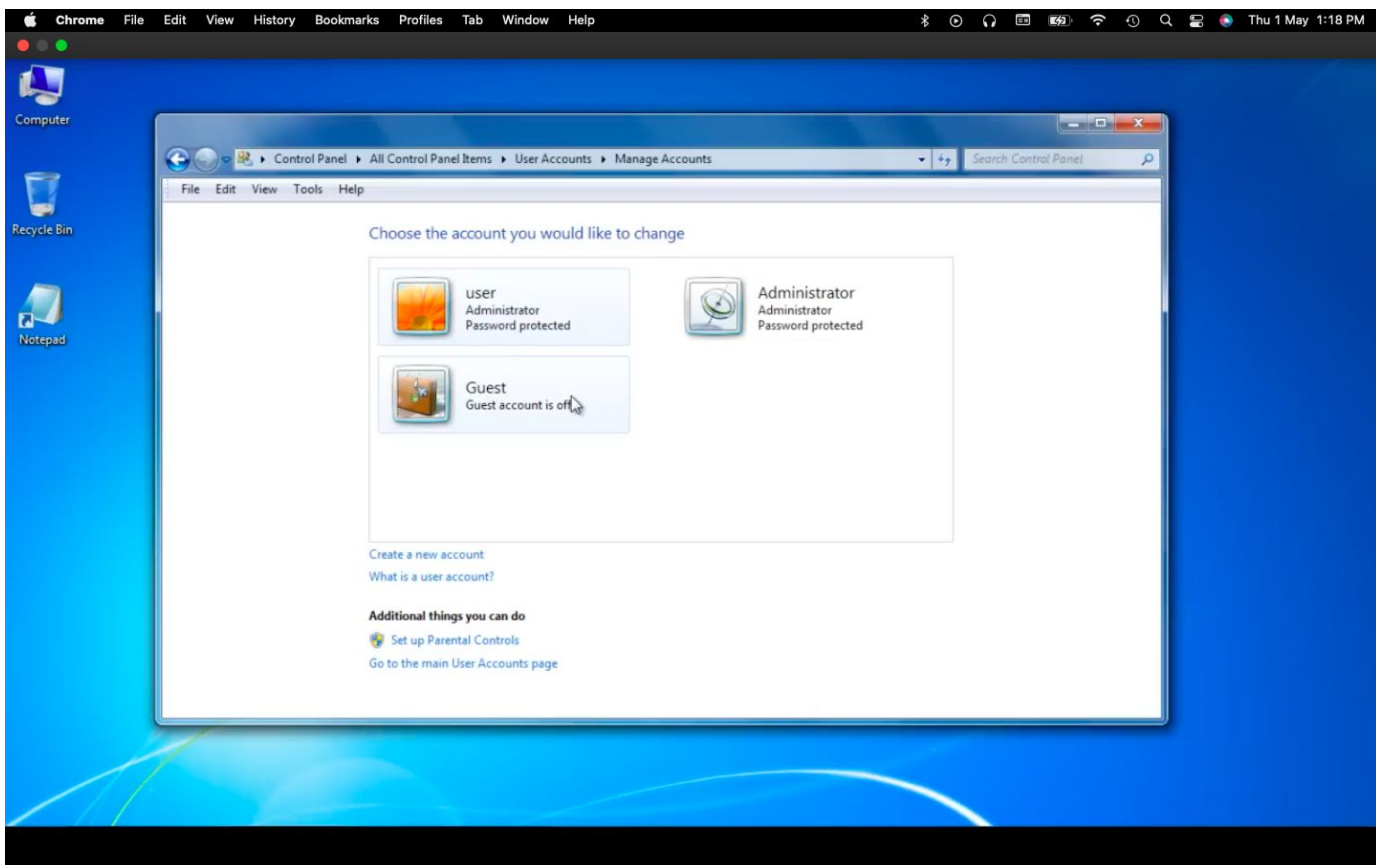


Windows Desktop Compliance

Windows 10 Regulatory Requirement

Met/Not Met

Guest account is disabled

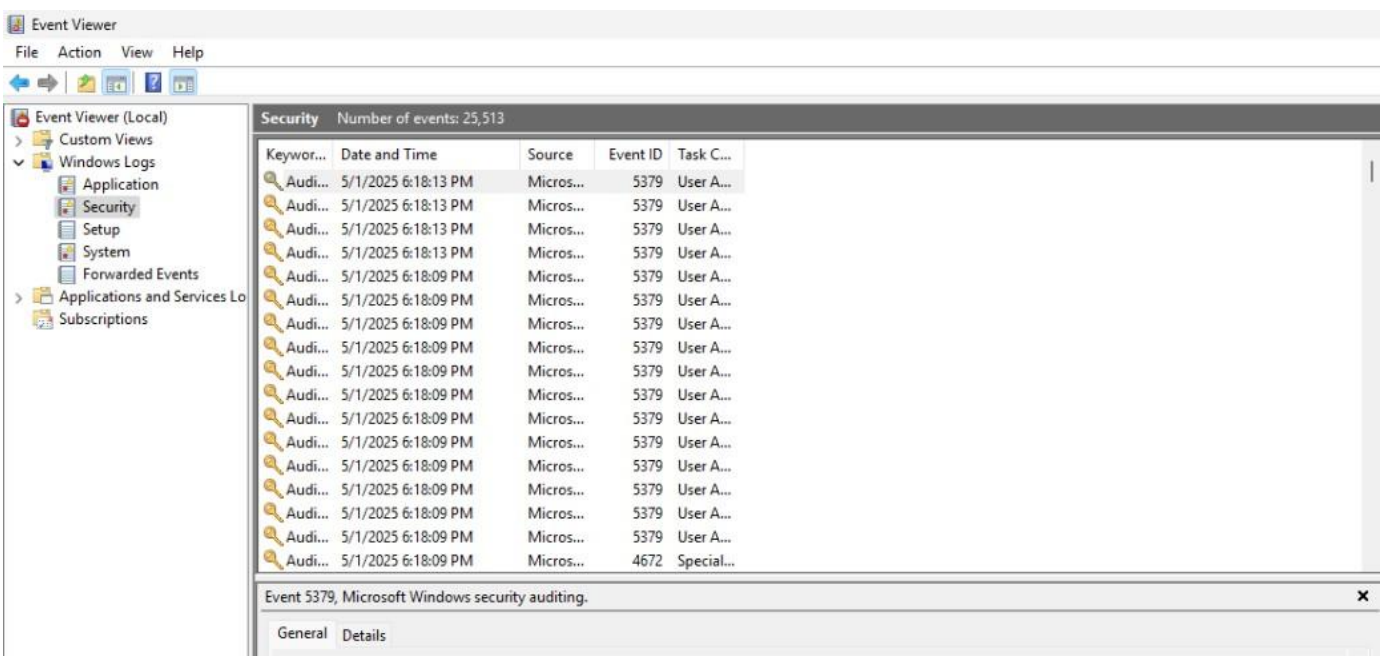


Windows Desktop Compliance

Windows 10 Regulatory Requirement

Met/Not Met

System logging and auditing are enabled

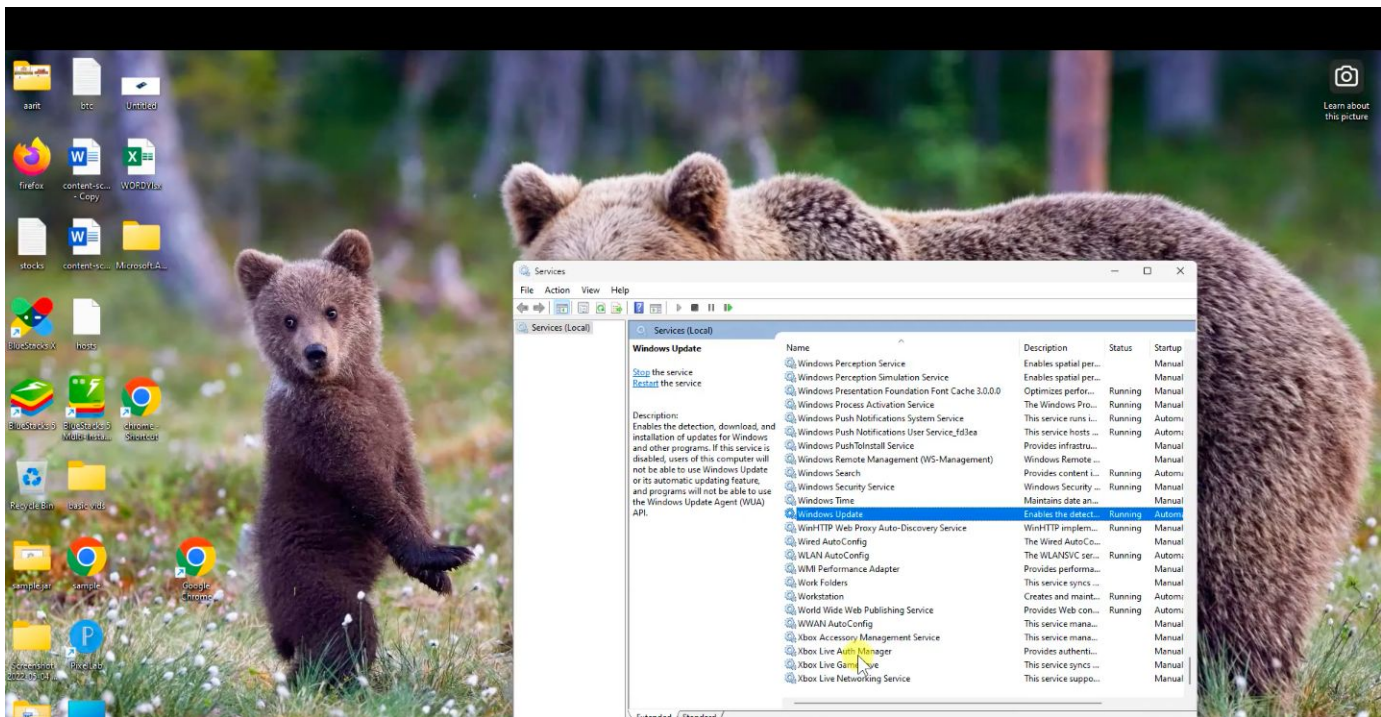


Windows Desktop Compliance

Windows 10 Regulatory Requirement

Met/Not Met

Windows Defender Antivirus is enabled and up to date



Windows Desktop Compliance

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

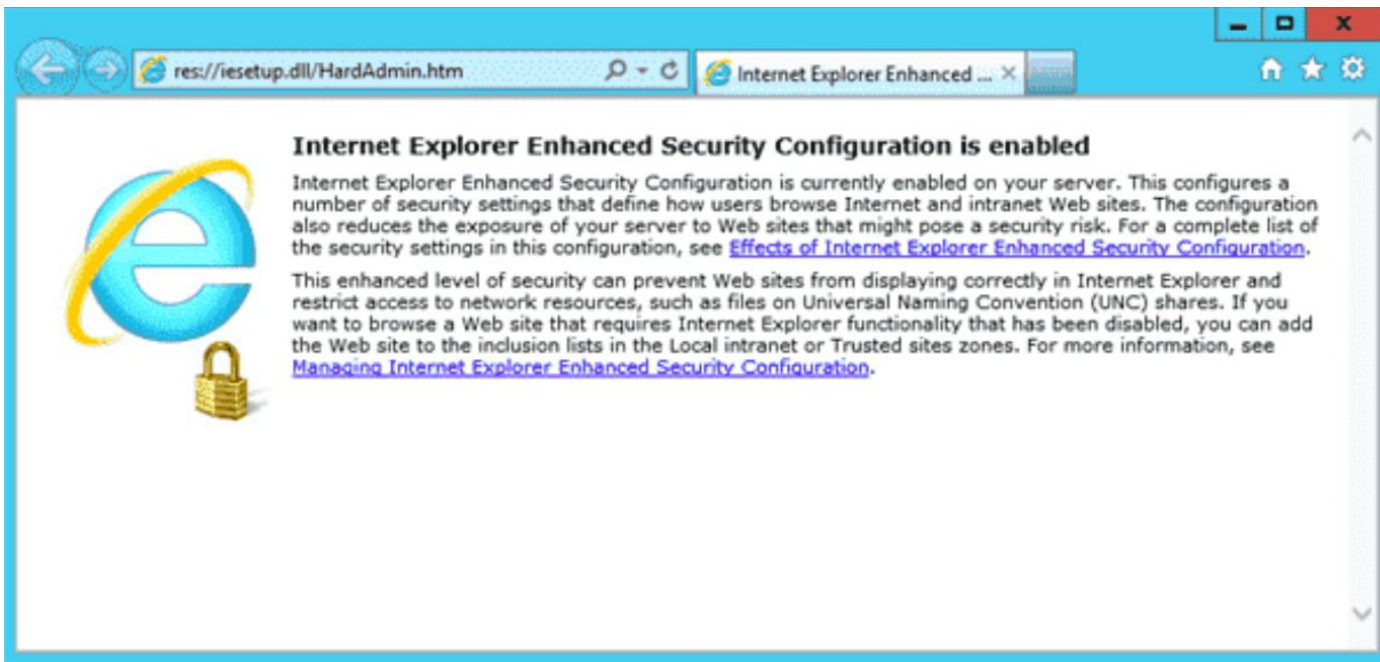
[Screenshot]

Windows Desktop Compliance

Windows 10 Regulatory Requirement

Met/Not Met

Internet Explorer Enhanced Security Configuration (IE ESC) is enabled



Windows Desktop Compliance

Windows 10 Regulatory Requirement

Met/Not Met

USB ports are disabled or restricted to authorized devices only

The screenshot displays the Local Group Policy Editor window. The left-hand navigation pane shows the hierarchy: Computer Configuration > Administrative Templates > Windows Components > Storage > Removable Storage Access. The main pane shows the 'Removable Disks: Deny execute access' policy, which is currently set to 'Not configured'. Below this, a list of other related policies is shown, all of which are also 'Not configured'.

Setting	State	Comment
Set time (in seconds) to force reboot	Not configured	No
CD and DVD: Deny execute access	Not configured	No
CD and DVD: Deny read access	Not configured	No
CD and DVD: Deny write access	Not configured	No
Custom Classes: Deny read access	Not configured	No
Custom Classes: Deny write access	Not configured	No
Floppy Drives: Deny execute access	Not configured	No
Floppy Drives: Deny read access	Not configured	No
Floppy Drives: Deny write access	Not configured	No
Removable Disks: Deny execute access	Not configured	No
Removable Disks: Deny read access	Not configured	No
Removable Disks: Deny write access	Not configured	No
All Removable Storage classes: Deny all access	Not configured	No
All Removable Storage: Allow direct access in remote sessions	Not configured	No
Tape Drives: Deny execute access	Not configured	No
Tape Drives: Deny read access	Not configured	No
Tape Drives: Deny write access	Not configured	No
WPD Devices: Deny read access	Not configured	No
WPD Devices: Deny write access	Not configured	No

Windows Desktop Compliance

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

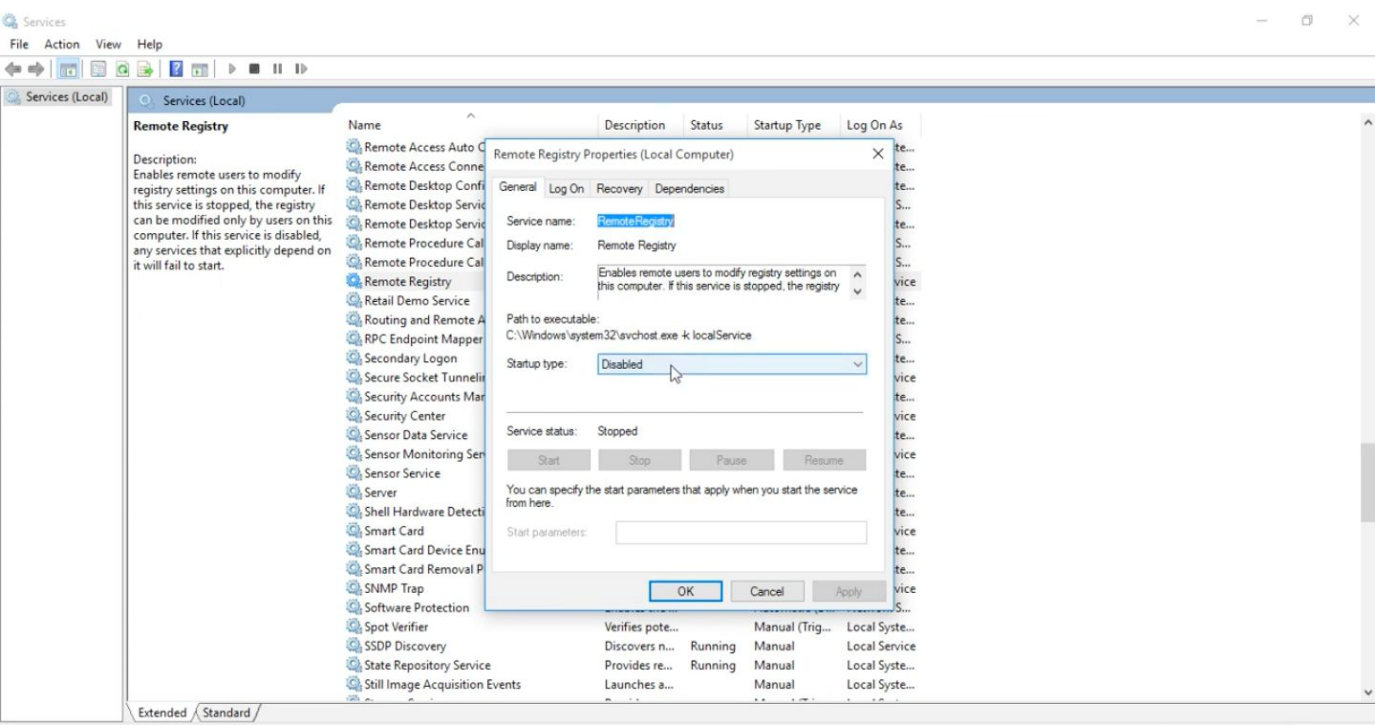
[Screenshot]

Windows Desktop Compliance

Windows 10 Regulatory Requirement

Met/Not Met

Remote Registry service is disabled

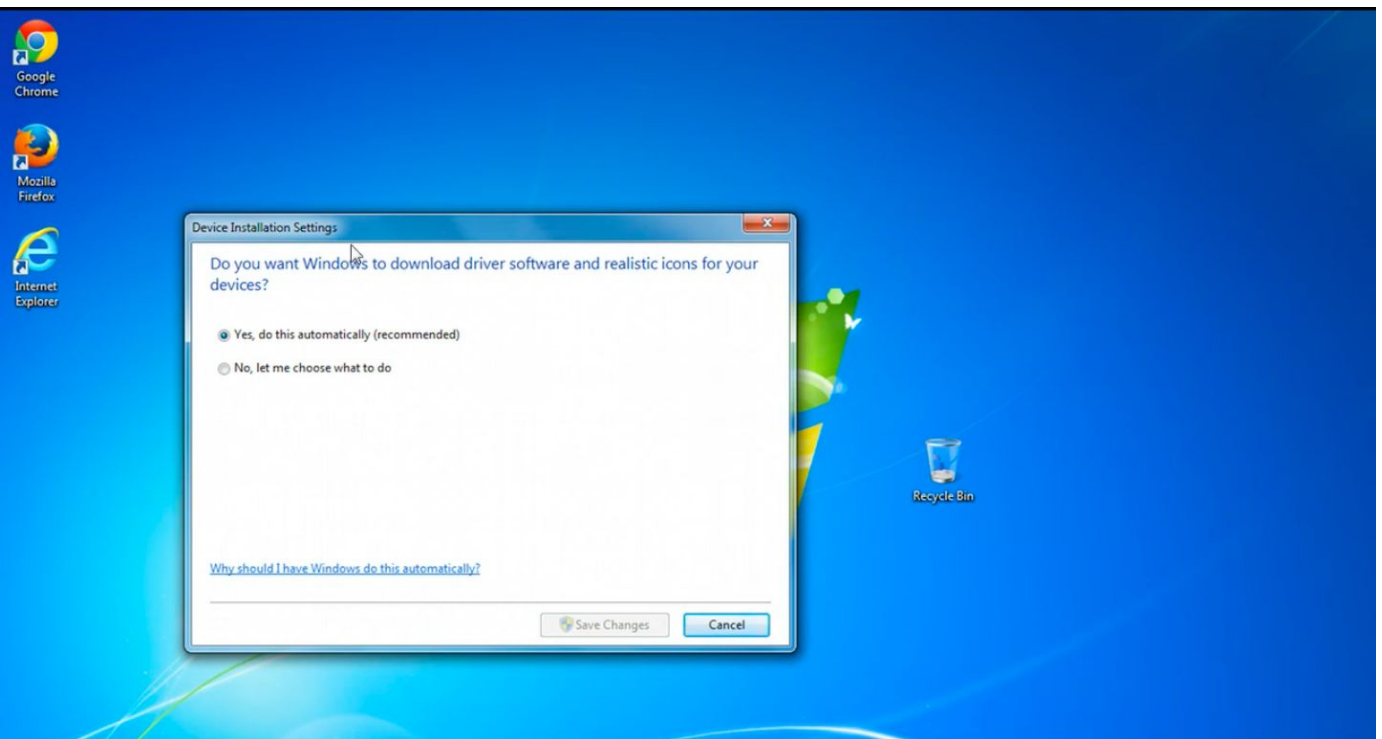


Windows Desktop Compliance

Windows 10 Regulatory Requirement

Met/Not Met

Windows Updates are configured to download and install updates automatically



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.**

Control -ID	Control-name	Remediation ;(One-Line Fix)
AC-2	Account-management	Disable unused user accounts and enable account expiration policies.
AC-6	Least Privilege	Remove admin rights from standard users and enforce role-based access.
AU-2	Audit Events	Enable event logging via Group Policy and configure Security Log settings.
AU-6	Audit Review	Set up scheduled log reviews using Windows Event Viewer or a SIEM tool.
IA-2	Identification and Authentication	Enable password complexity and minimum length via local group policy.
IA-5	Authenticator Management	Enforce password expiration and reuse prevention through Group Policy Editor.
SC-7	Boundary Protection	Enable Windows Defender Firewall for all profiles and restrict inbound ports.

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 CentOS VM complies with the CMMC control
 - **Not Met:** The CentOS 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

Ensure separate partition exists for /var

Disable Automounting of drives

Ensure AIDE is installed

Ensure daytime services are not enabled

Ensure echo services are not enabled

Ensure tftp server is not enabled

Ensure CUPS is not enabled

Ensure DHCP Server is not enabled

Ensure FTP Server is not enabled

Ensure Samba is not enabled

Ensure TCP Wrappers is installed

Ensure DCCP is disabled

Ensure iptables is installed

Ensure audit log storage size is configured

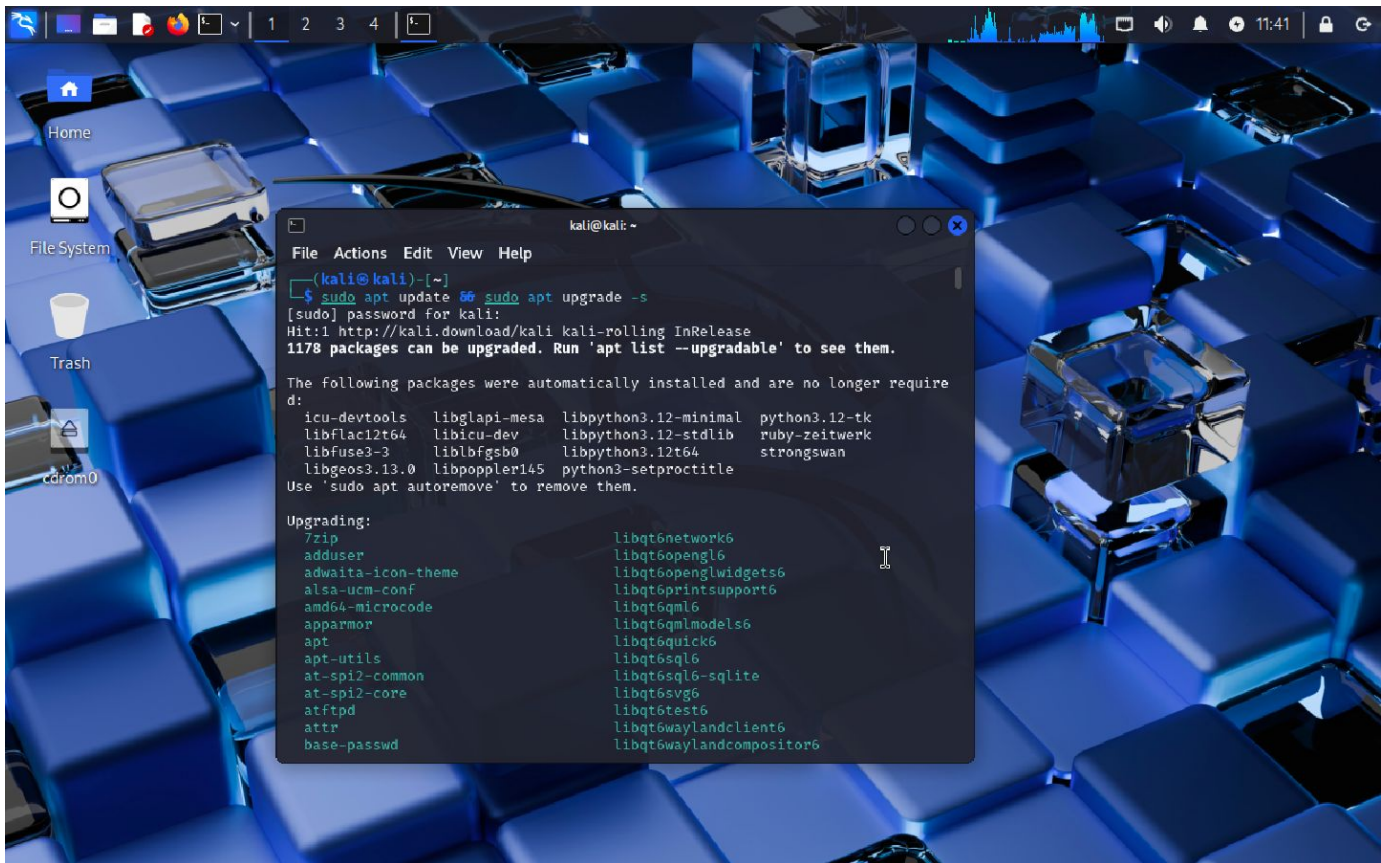
Ensure audit logs are not automatically deleted

Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Current on security updates



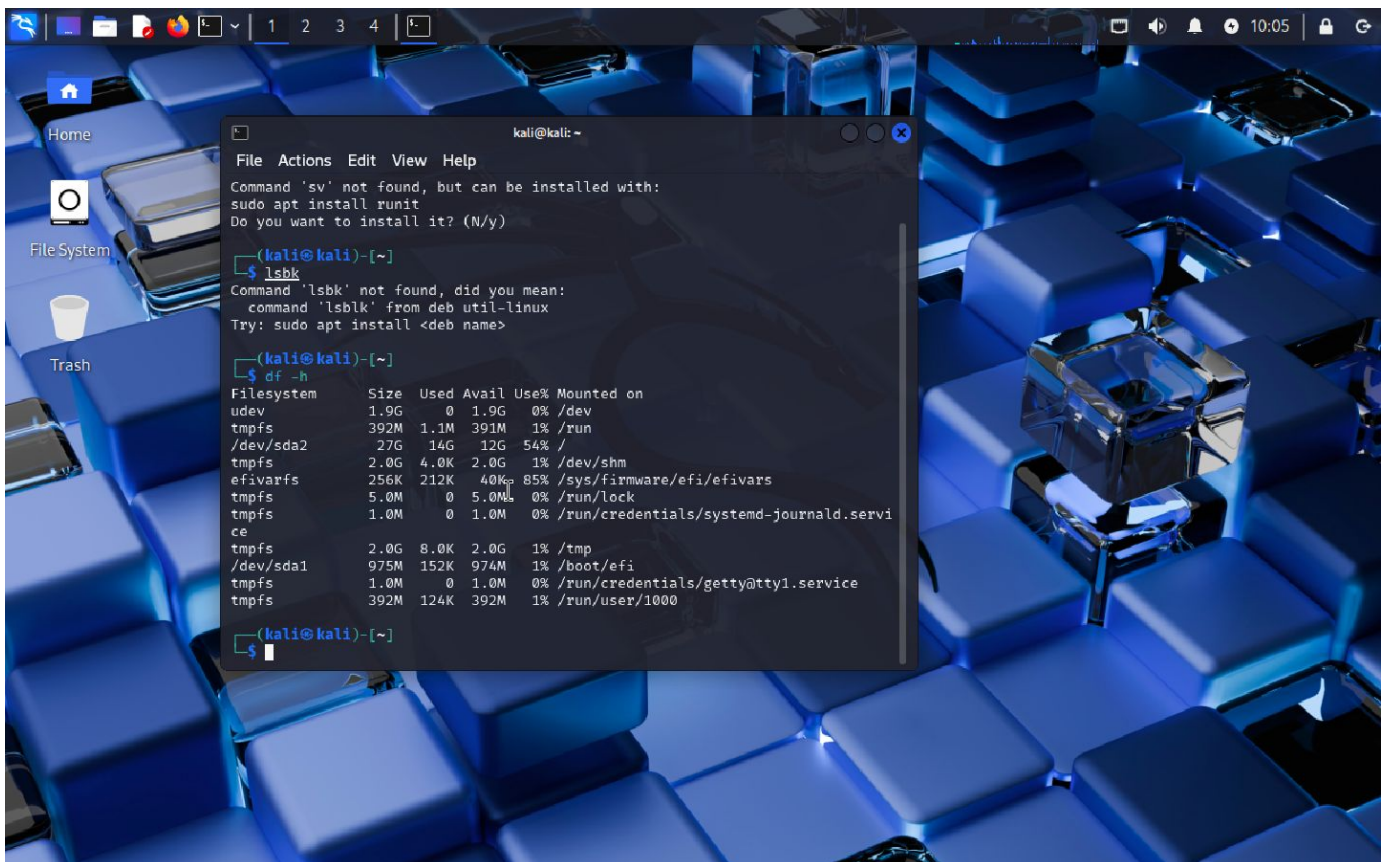
Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure separate partition exists for /var

[Screenshot]

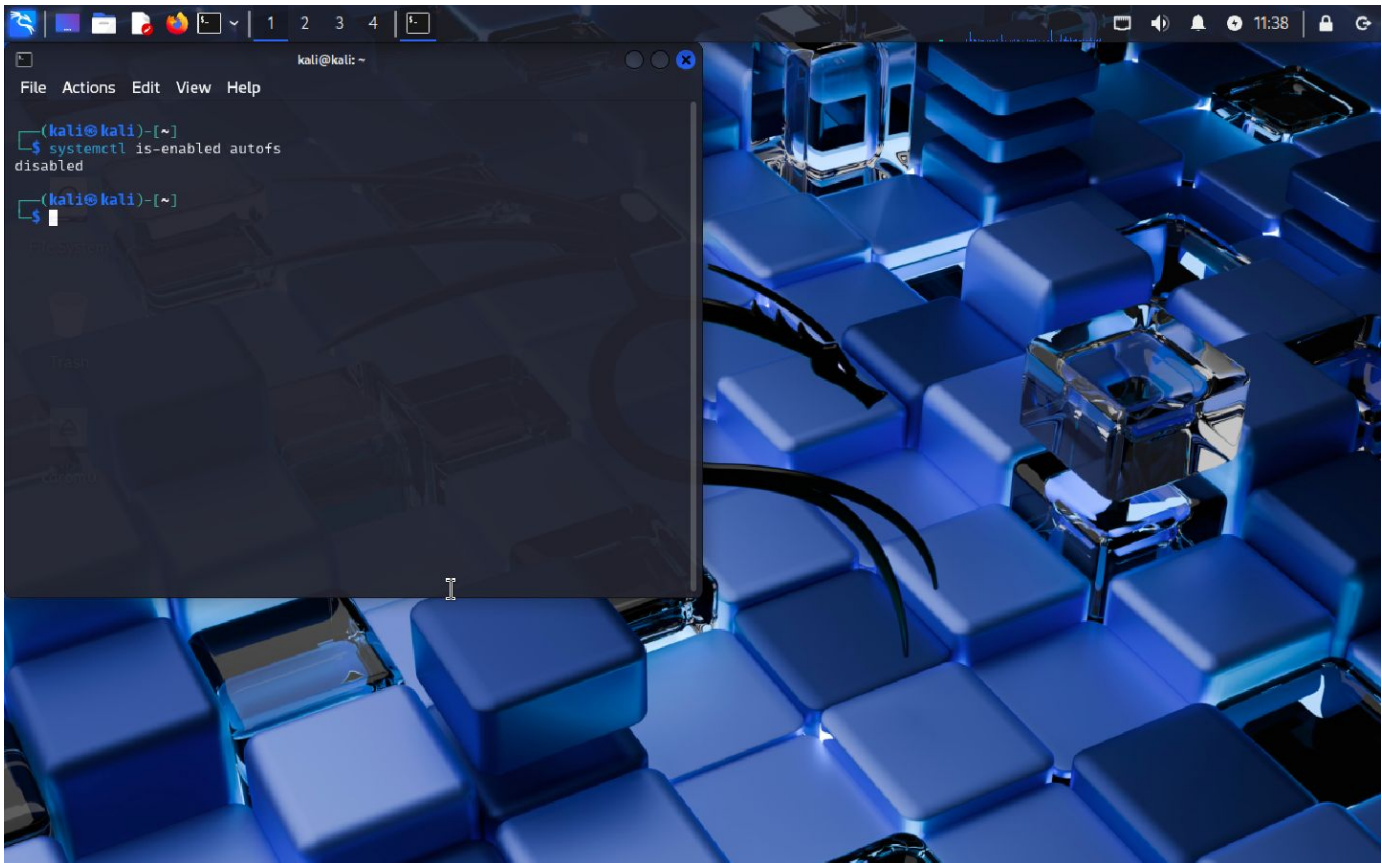


Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Disable Automounting of drives

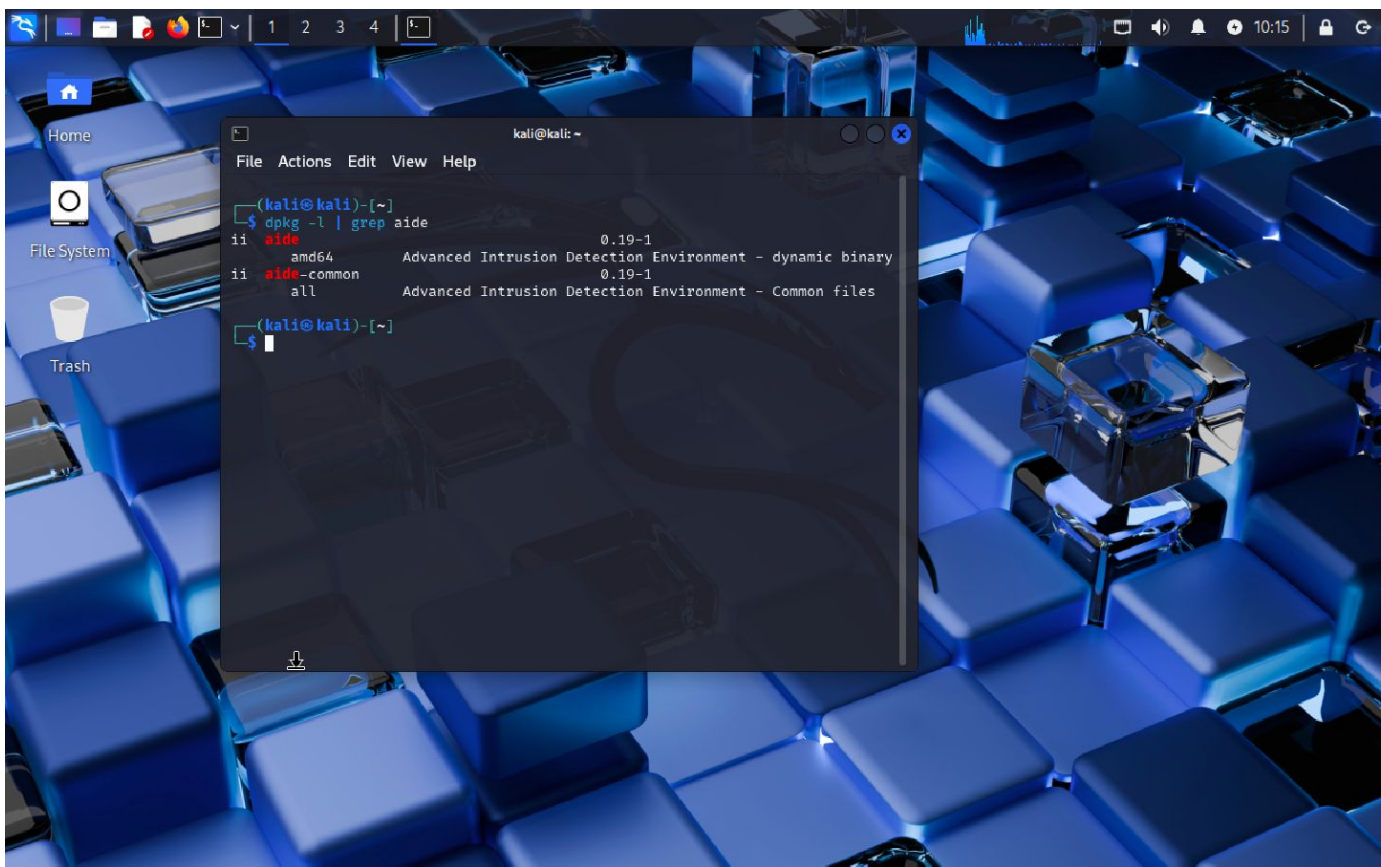


Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure AIDE is installed



The screenshot shows a Kali Linux desktop environment with a blue-themed background featuring a keyboard. A terminal window is open in the center, displaying the command `dpkg -l | grep aide` and its output. The terminal window has a title bar that reads "kali@kali: ~". The desktop includes icons for Home, File System, and Trash. The top panel shows various system icons and the time 10:15.

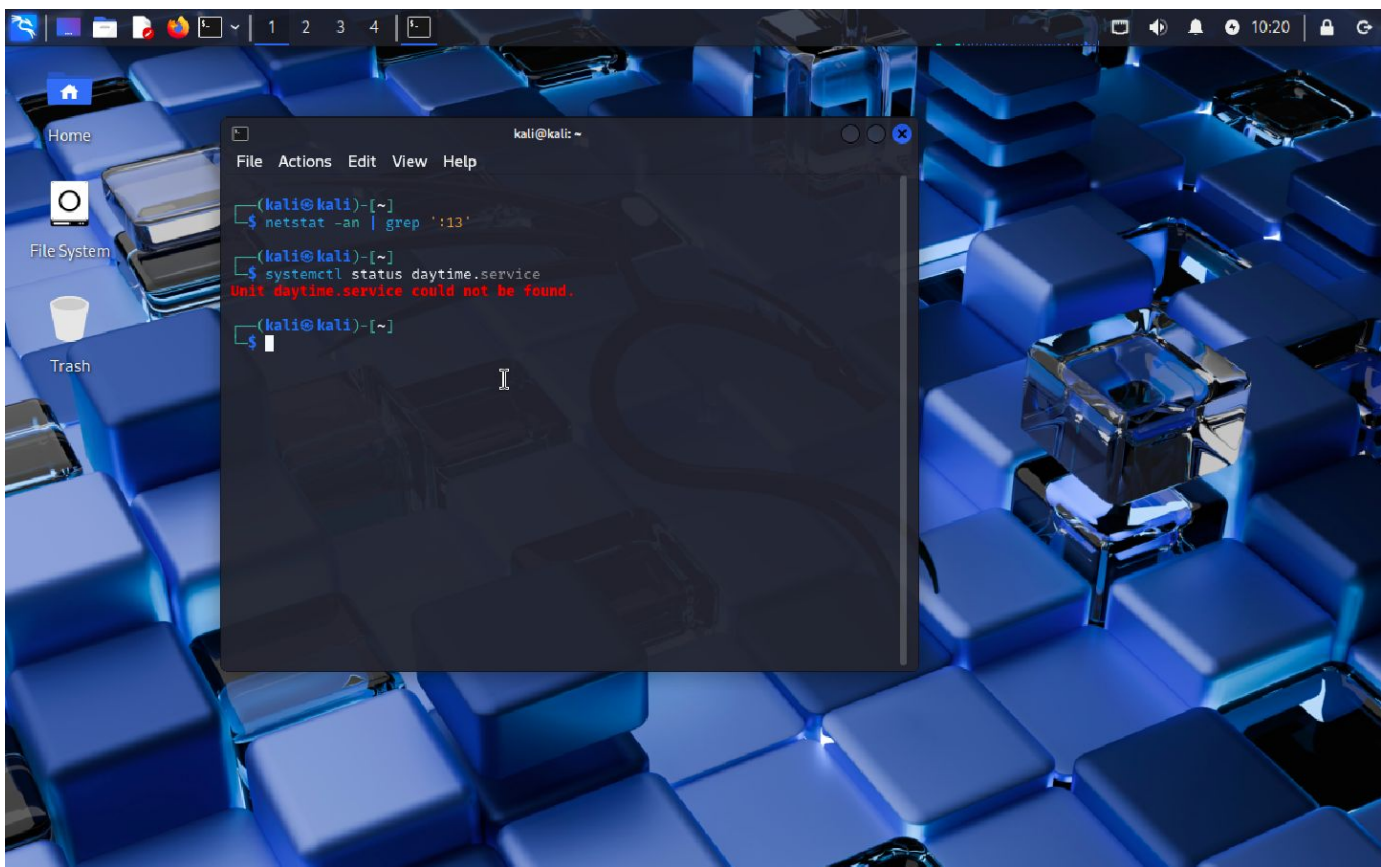
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ dpkg -l | grep aide  
ii aide 0.19-1  
    amd64 Advanced Intrusion Detection Environment - dynamic binary  
ii aide-common 0.19-1  
    all Advanced Intrusion Detection Environment - Common files  
(kali@kali)-[~]  
$
```

Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure daytime services are not enabled

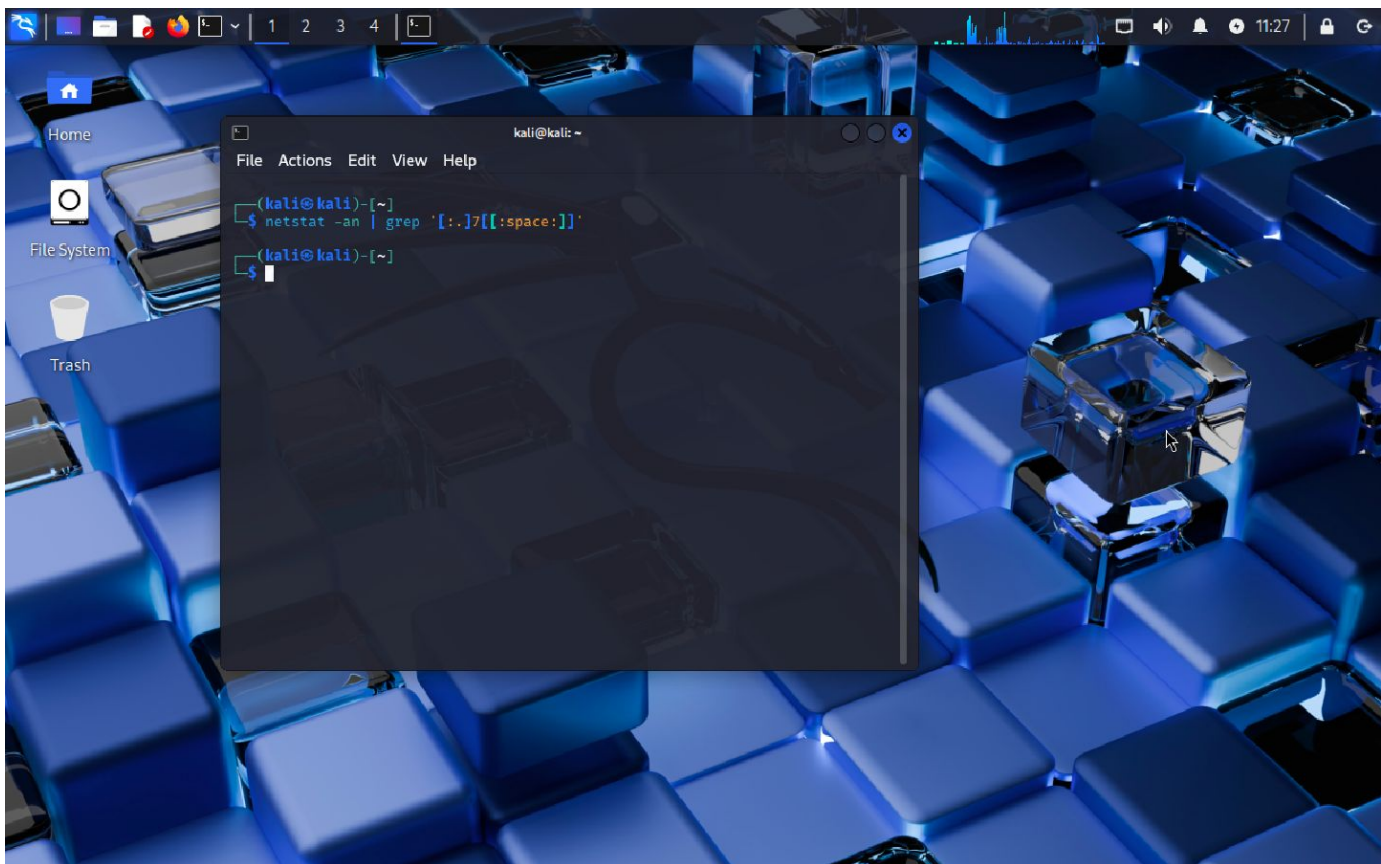


Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure echo services are not enabled

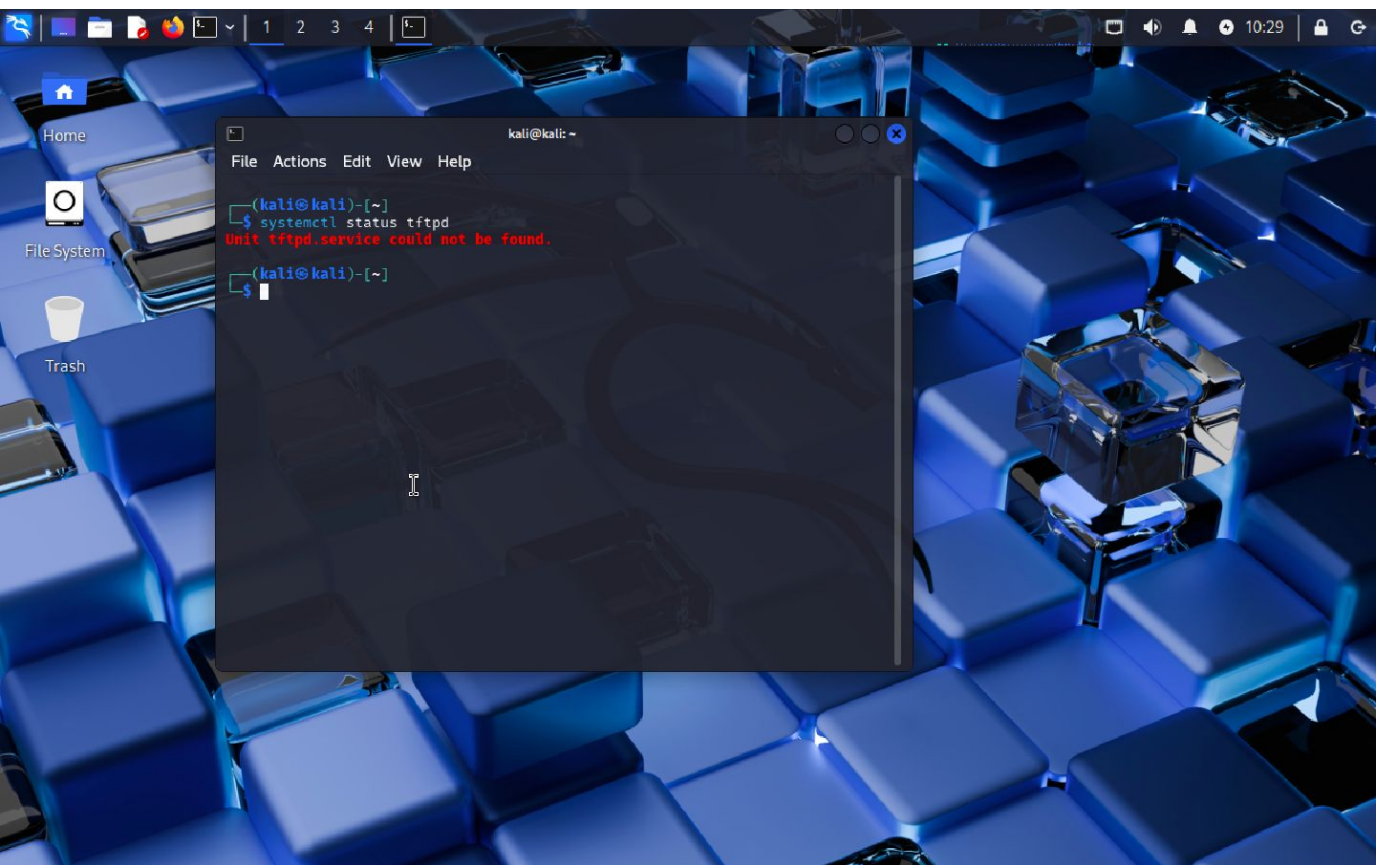


Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure tftp server is not enabled

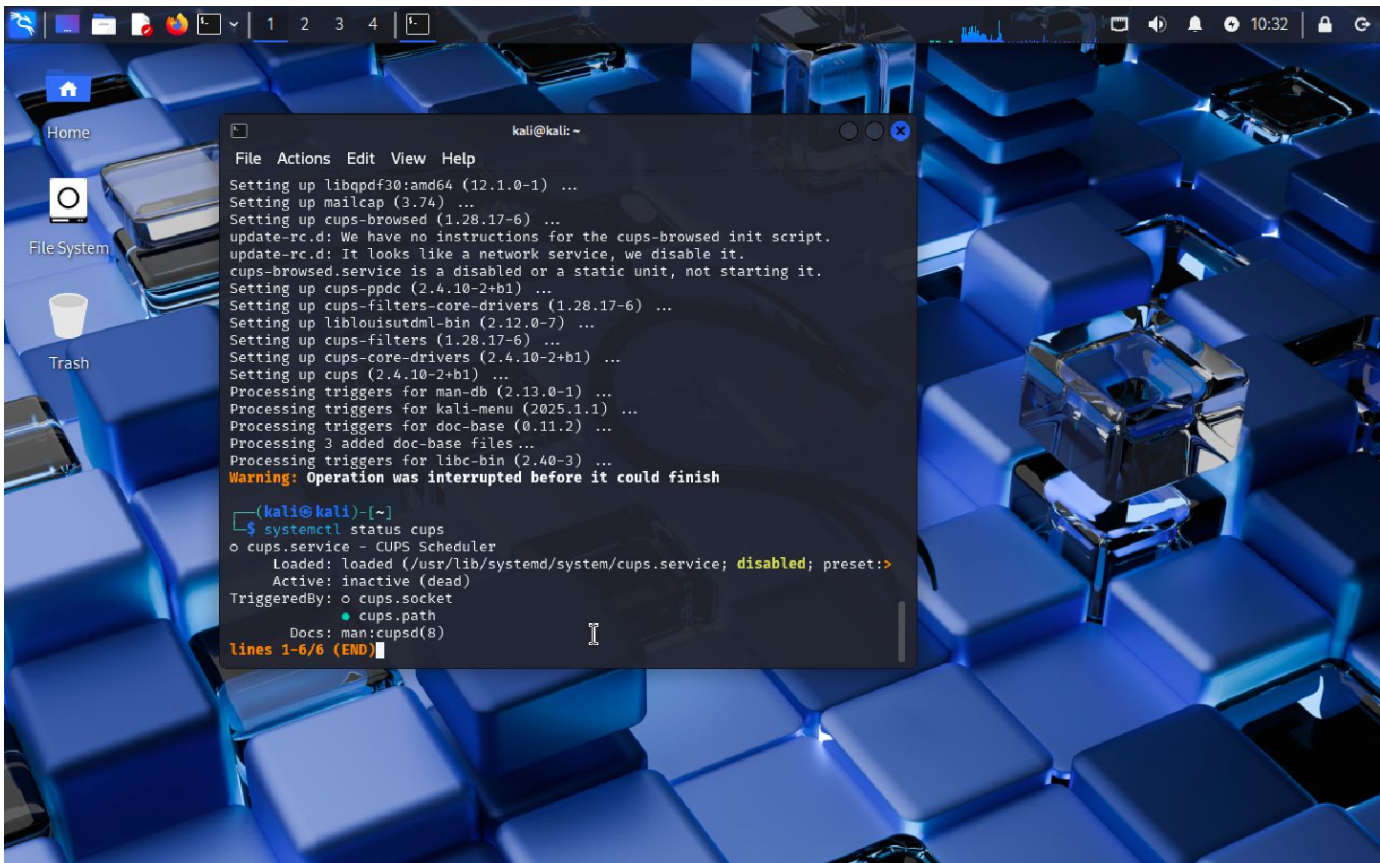


Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure CUPS is not enabled

A terminal window is open on a Kali Linux desktop. The desktop background is a blue-lit keyboard. The terminal window has a title bar that says 'kali@kali: ~'. The terminal output shows the installation of various CUPS-related packages: libqpdf30:amd64, mailcap, cups-browsed, cups-ppdc, cups-filters-core-drivers, liblouisutdml-bin, cups-filters, cups-core-drivers, and cups. A warning message states: 'Warning: Operation was interrupted before it could finish'. Below this, the user runs the command 'systemctl status cups'. The output shows that the cups.service is loaded but disabled, and its active state is inactive (dead). The terminal also shows the triggered by services (cups.socket and cups.path) and the documentation file (man:cupsd(8)). The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The desktop has icons for 'Home', 'File System', and 'Trash'. The top panel shows the time as 10:32 and the date as 10:32. The terminal window is titled 'kali@kali: ~' and shows the command 'systemctl status cups' and its output. The output indicates that the cups.service is loaded but disabled, and its active state is inactive (dead). The terminal also shows the triggered by services (cups.socket and cups.path) and the documentation file (man:cupsd(8)). The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The desktop has icons for 'Home', 'File System', and 'Trash'. The top panel shows the time as 10:32 and the date as 10:32.

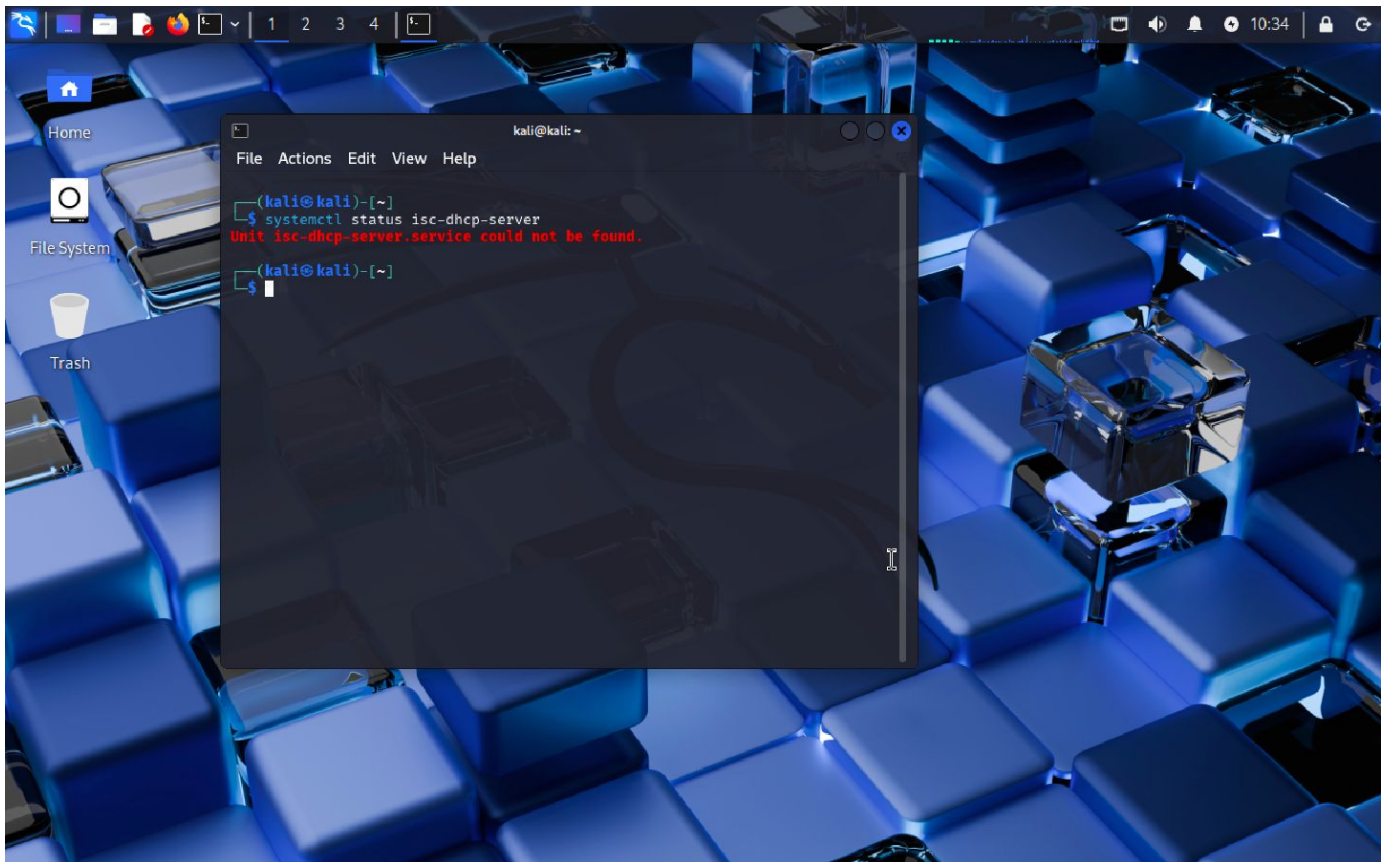
Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure DHCP Server is not enabled

[Screenshot]

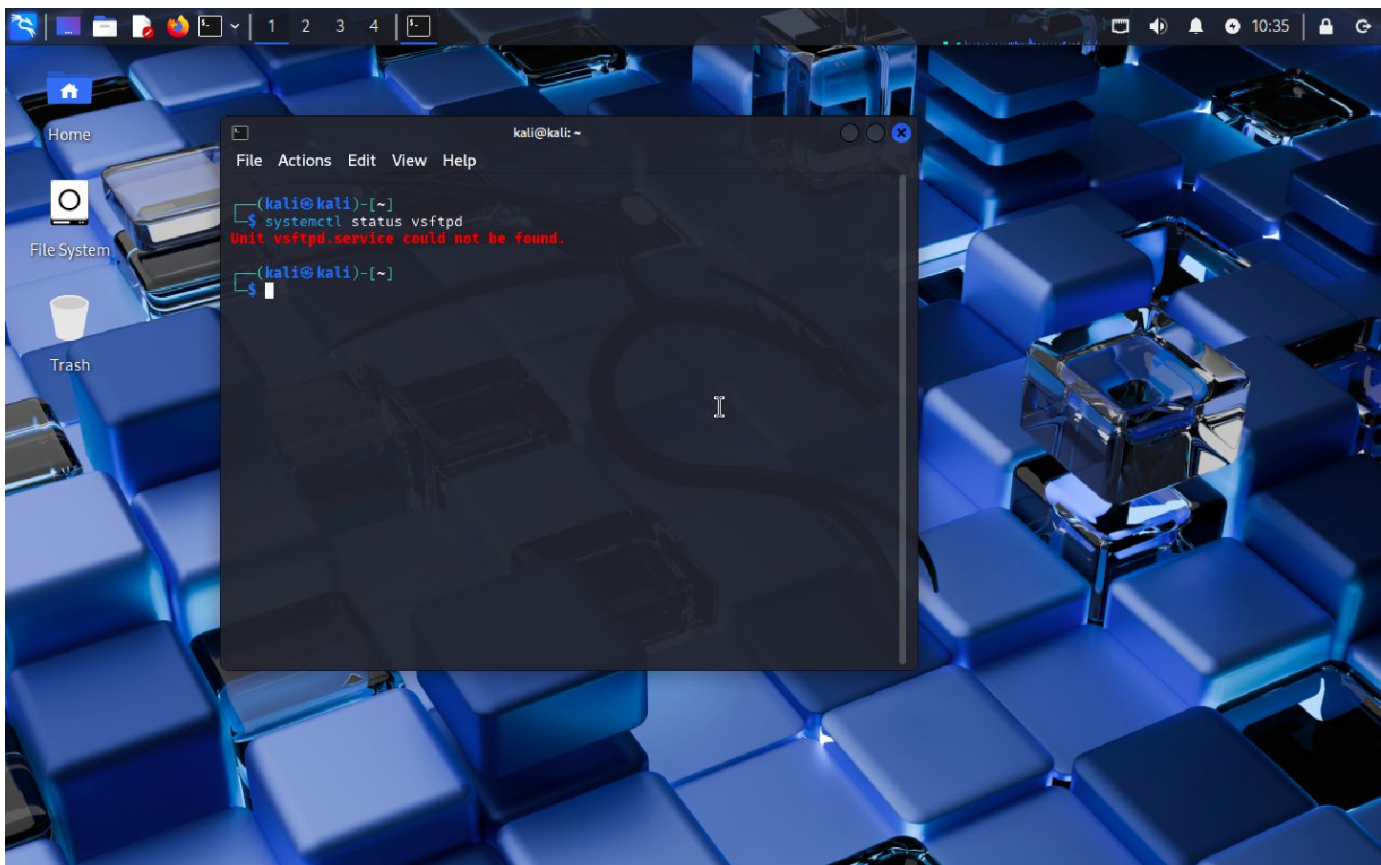


Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure FTP Server is not enabled

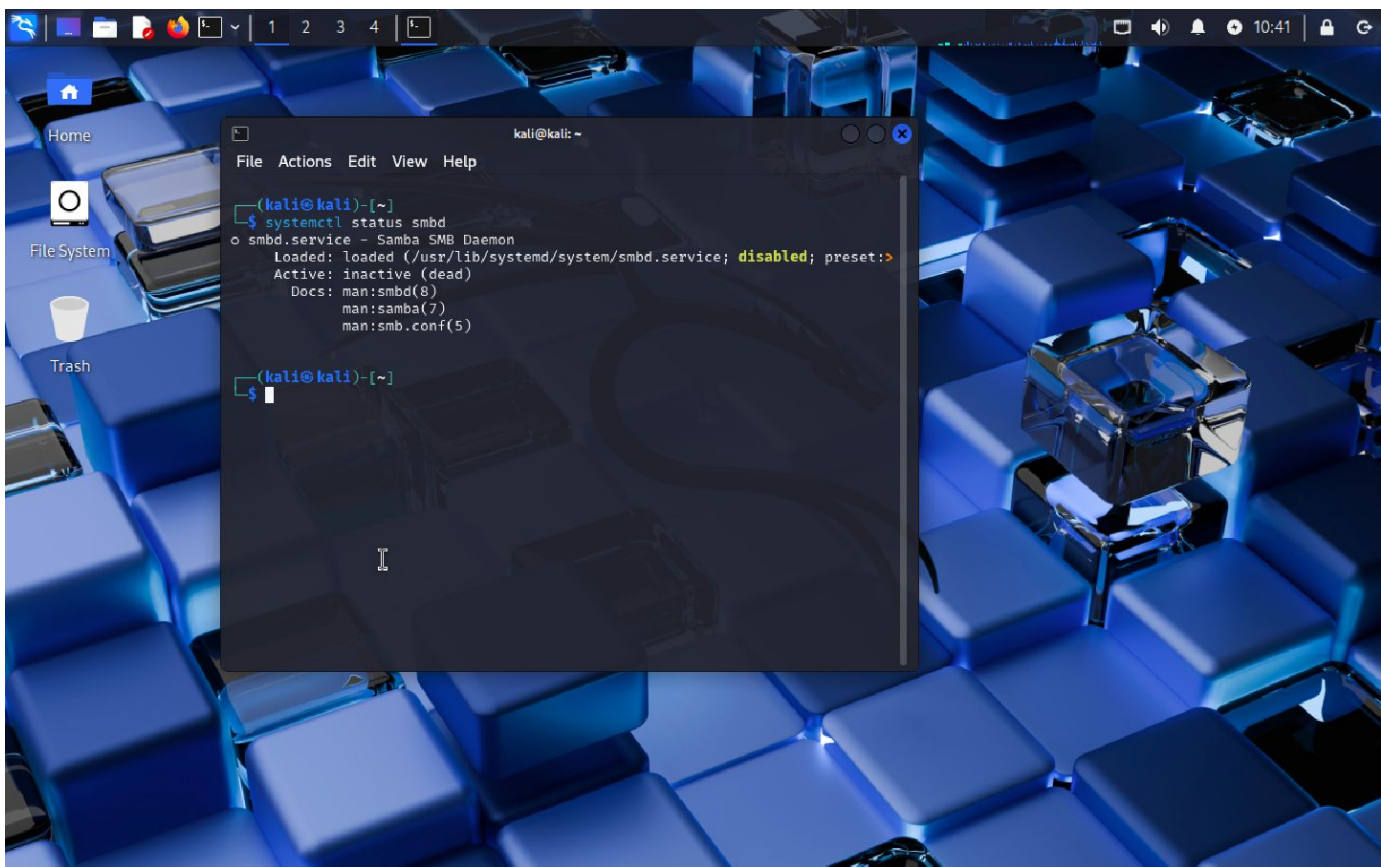


Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure Samba is not enabled

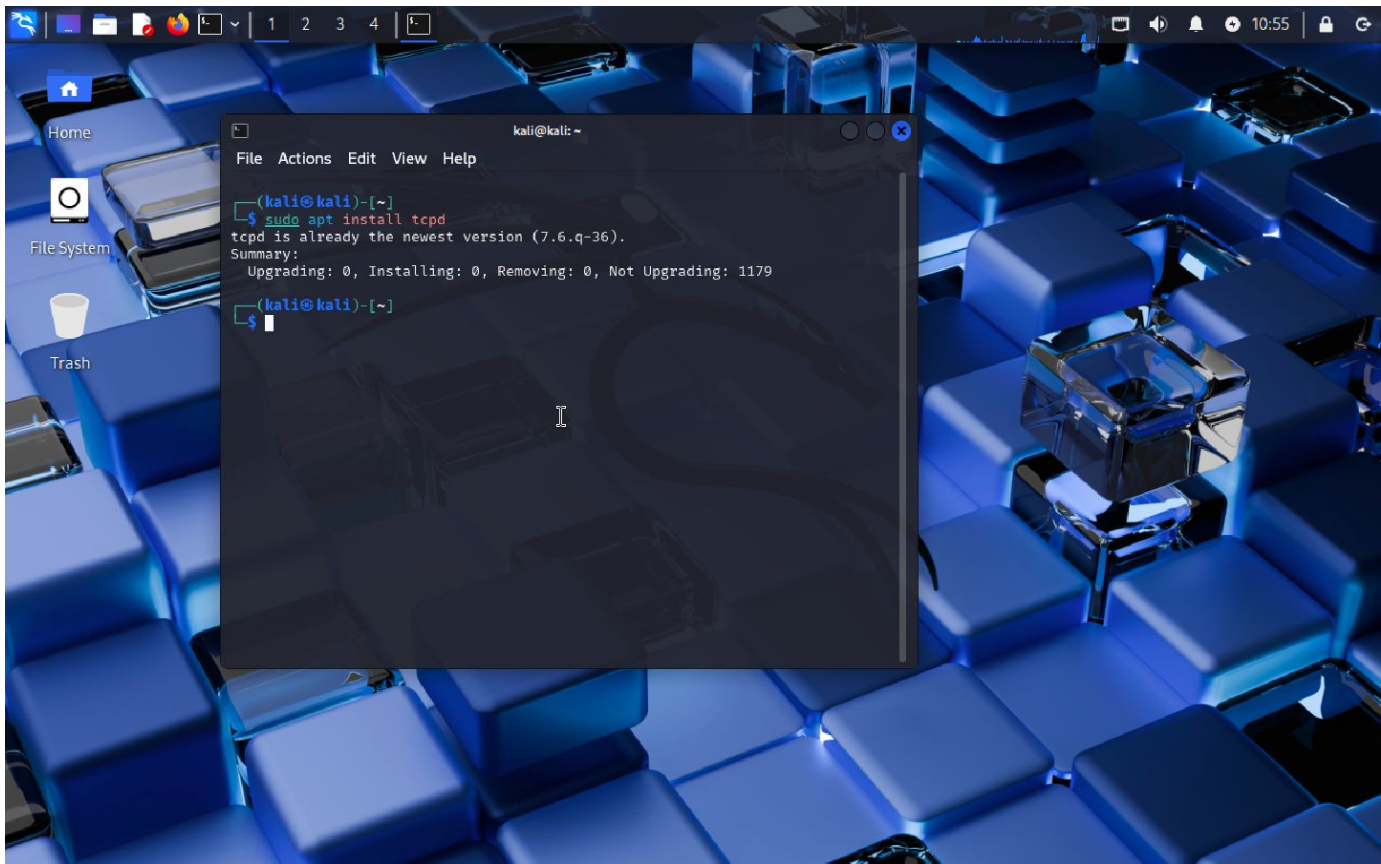


Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure TCP Wrappers is installed

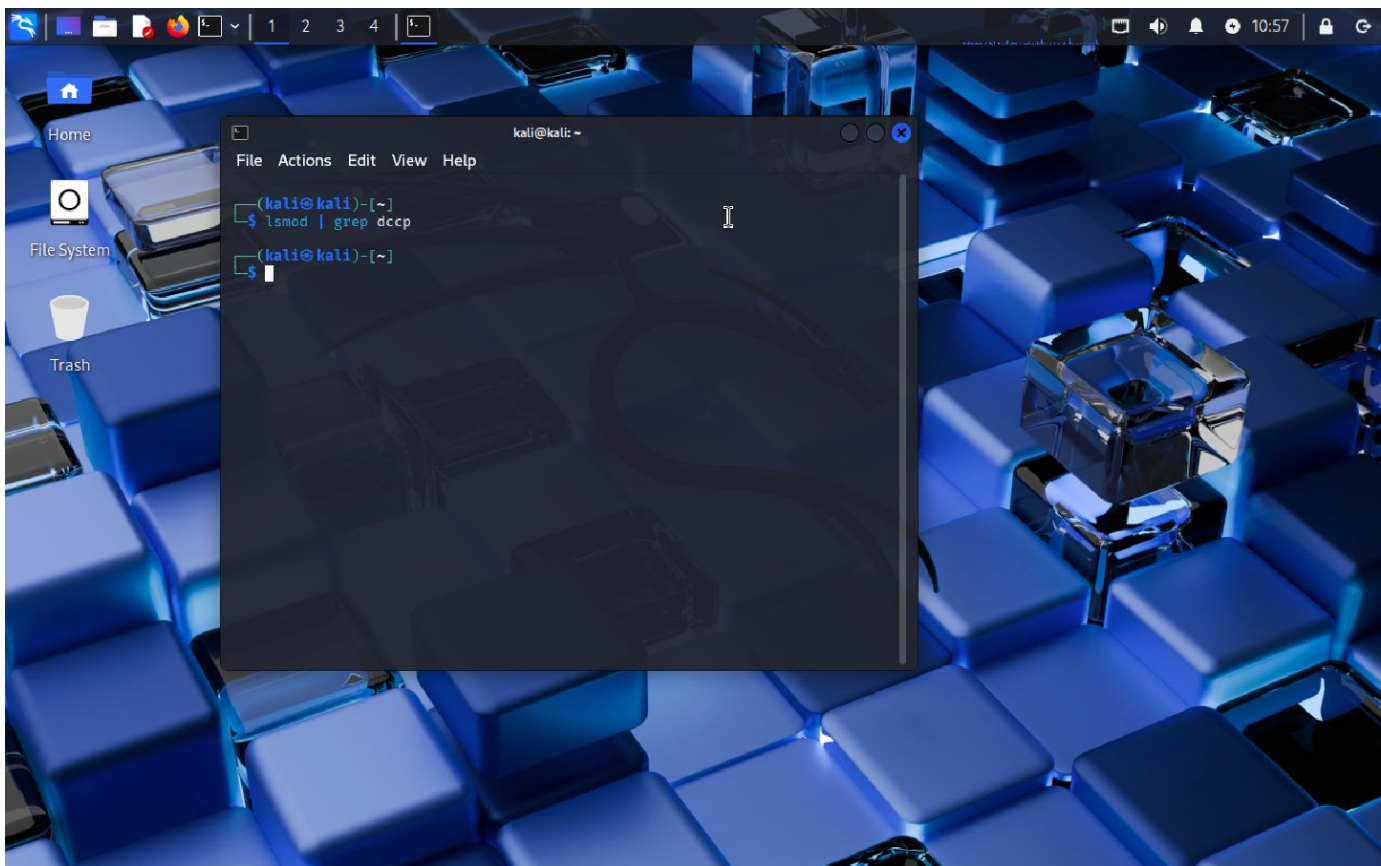


Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure DCCP is disabled

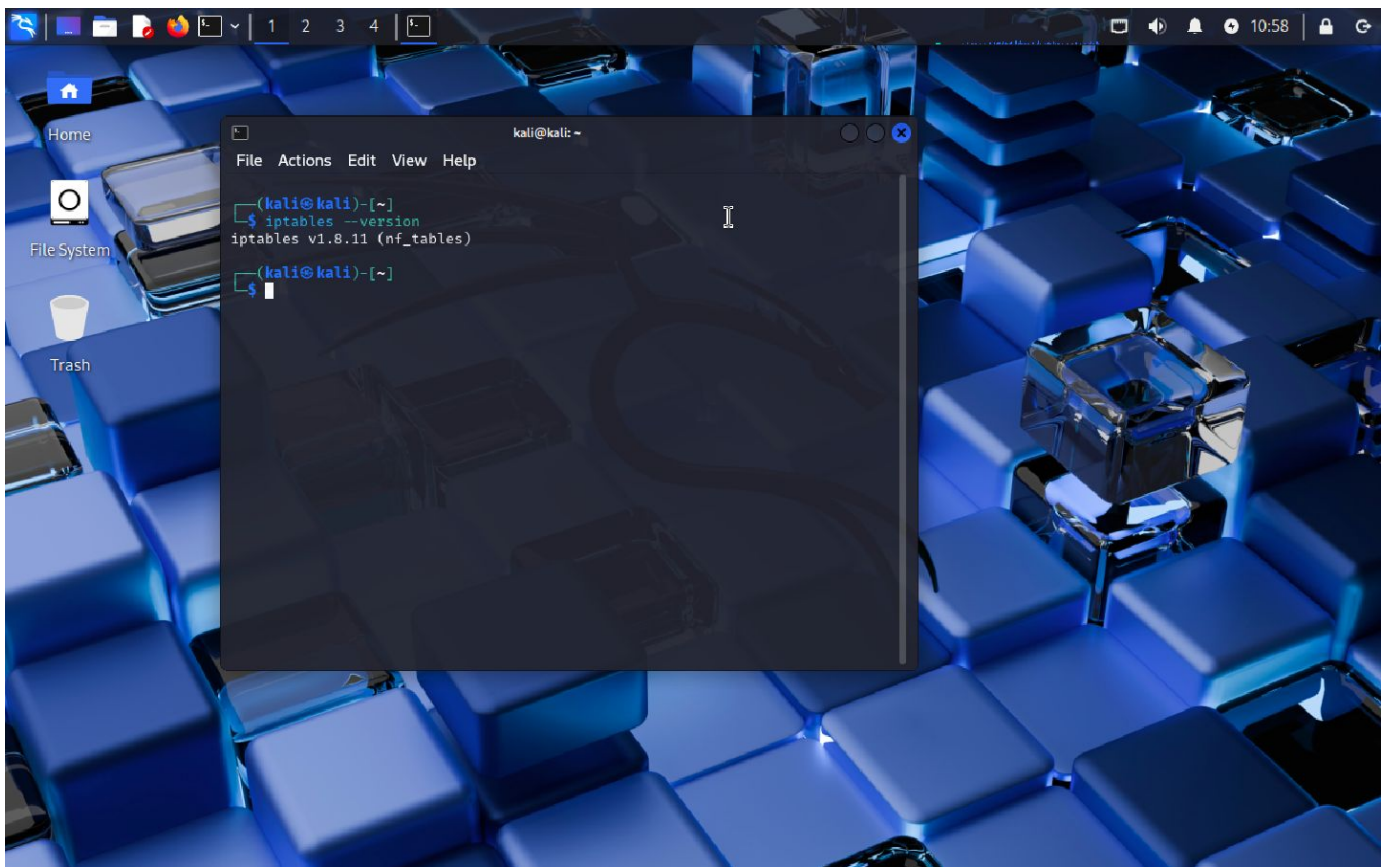


Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure iptables is installed

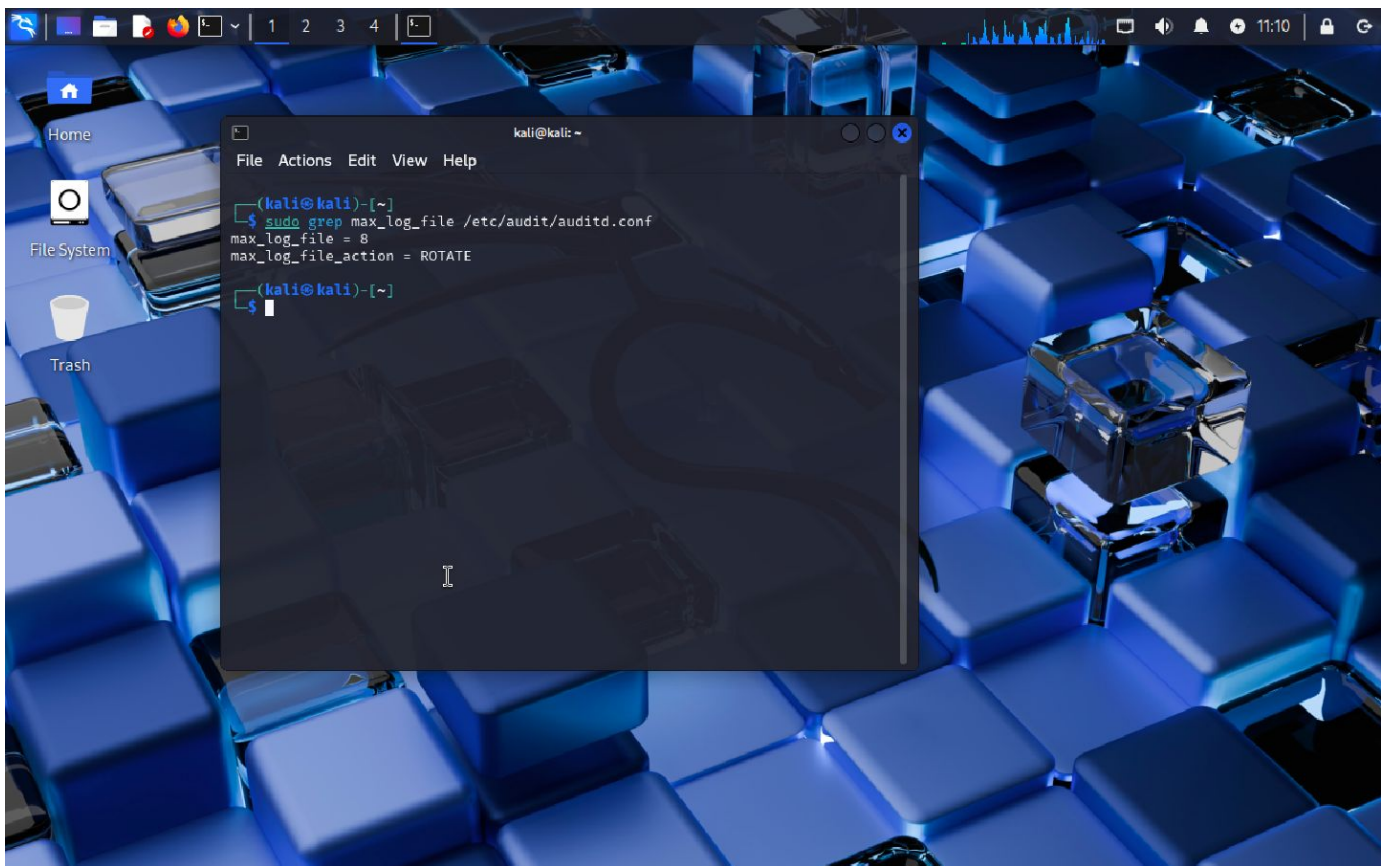


Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure audit log storage size is configured

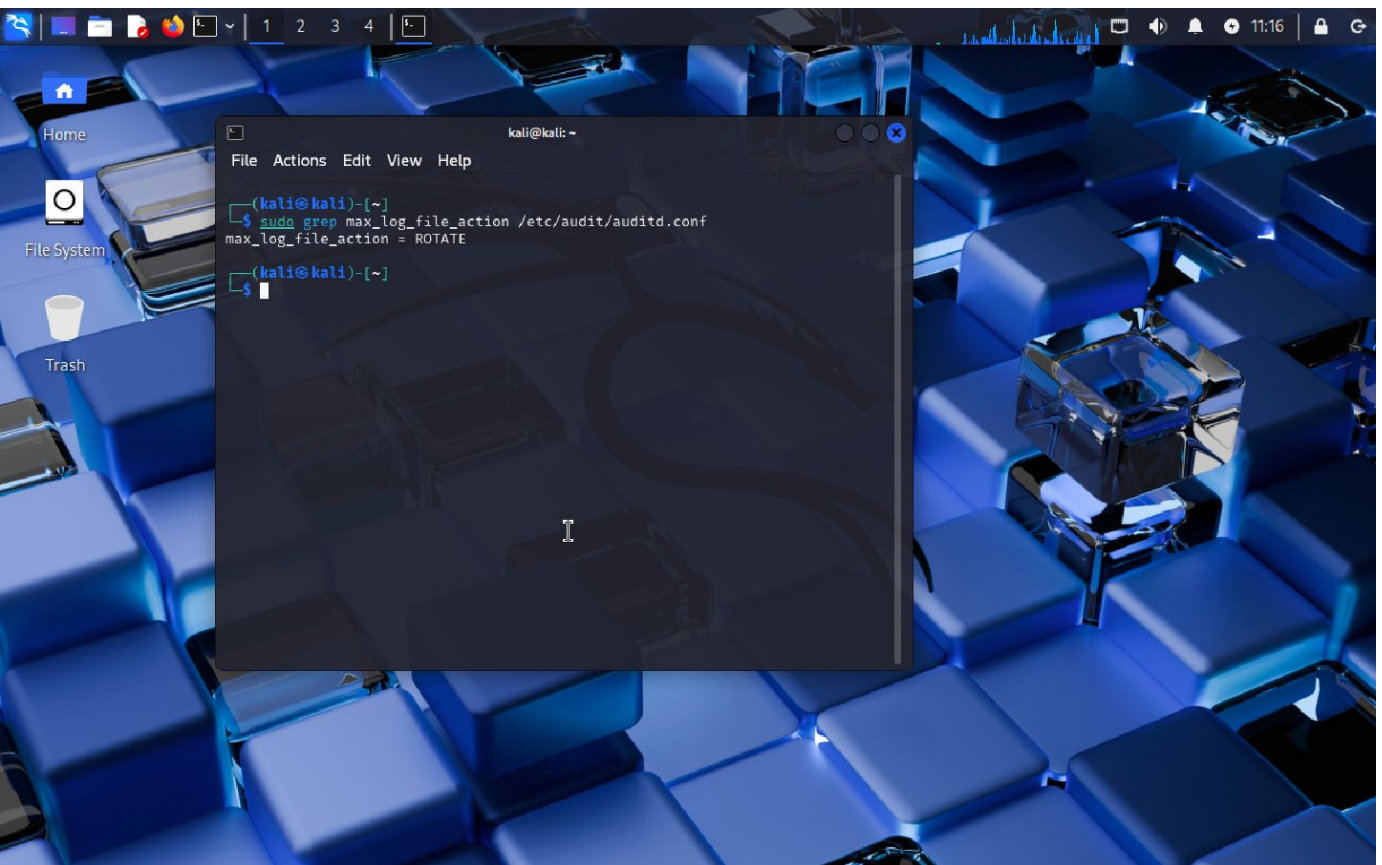


Linux Compliance

Linux Regulatory Requirement

Met/Not Met

Ensure audit logs are not automatically deleted



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]

Using the latest supported version of Windows Server is crucial for ensuring long-term stability, performance, and security. For a production-grade cloud-hosted web server, Windows Server 2022 (preferably the Datacenter edition) should be used. Microsoft frequently releases updates to address vulnerabilities and introduce security features. Running older versions like Server 2012 or 2016 puts you at risk of unpatched exploits and software compatibility issues. Standardizing on one OS version also helps with automation and consistent patching. Always deploy from a known-good base image (or golden image) that's regularly updated with the latest patches before spinning up new instances.

2. [Server Role Configuration]

A best practice in cloud server deployment is to install only the necessary roles and features required for the server's intended purpose. In this case, the server is designed to host web applications, so only the IIS Web Server role should be enabled. Avoid installing unnecessary services like Print Server or File Server, as these increase the attack surface. Use PowerShell or Server Manager to install only the required role and subcomponents (e.g., static content, ASP.NET, WebSockets if needed). Minimal installation not only reduces vulnerabilities but also improves system performance and simplifies maintenance.

3. [Firewall Rules]

Your firewall should follow a default-deny model, meaning all inbound and outbound traffic is blocked unless explicitly allowed. For a public-facing web server, you typically only need to allow port 80 (HTTP) and 443 (HTTPS). All other ports should be blocked unless there is a specific reason (e.g., RDP on 3389, which should be IP-restricted). You can configure the firewall using the built-in Windows Defender Firewall or through your cloud provider's network security groups (NSGs in Azure or Security Groups in AWS). This is your first line of defense against random internet scans and brute-force attacks.

Windows Server Build Sheet

4. [Administrator Account Hardening]

By default, the local administrator account is a prime target for brute-force and credential stuffing attacks. Rename this account to something non-obvious and set a complex password (at least 16 characters with symbols and numbers). Better yet, disable it if not needed and use Role-Based Access Control (RBAC) through Active Directory or Azure AD for access. Use local group policy or PowerShell to enforce password complexity and expiration. Also, consider logging and alerting every login attempt on this account to detect potential breach attempts early.

5. [Windows update configurations]

Outdated systems are a hacker's paradise. Ensure that the server is set to automatically download and install Windows Updates, especially security patches. In enterprise environments, using WSUS (Windows Server Update Services) or Azure Update Management can centralize and automate update deployment. Regular patching not only addresses vulnerabilities but also ensures compatibility with modern applications and compliance with security standards like NIST or CIS. Document your patch cycles and test updates in a staging environment before rolling out to production.

6.[Antivirus and Threat Protection]

Even in the cloud, antivirus is a must-have. Microsoft Defender Antivirus comes built-in with Windows Server and should be enabled with real-time protection, cloud-delivered protection, and automatic sample submission. For advanced threat protection, integrate with Microsoft Defender for Endpoint or use third-party tools like CrowdStrike or SentinelOne. Schedule regular full scans and ensure that virus definitions are updated frequently. Also, create exclusion rules carefully so legitimate apps are not blocked. AV is your last defense against malware, web shells, and ransomware on the system.

Windows Server Build Sheet

7. [Logging and monitoring]

A secure server is a monitored server. Enable Event Logging, especially for login attempts, system errors, and application-specific events. Integrate these logs into a centralized log management system like Azure Monitor, Log Analytics, or a SIEM like Splunk or ELK. This allows for real-time alerts and incident correlation. Log retention policies should be set, and sensitive logs must be protected against tampering. Monitor IIS logs for unusual requests, 500 errors, or slow responses that may indicate probing or attacks.

8. [Backup and recovering]

No system is truly secure unless it's also recoverable. Set up a backup policy to create daily snapshots or file-based backups of the server and its critical data. These backups should be encrypted and stored off-server, ideally in another availability zone or region using tools like Azure Backup, Veeam, or Windows Server Backup. Test your recovery process regularly — a backup you can't restore is useless. Also consider versioning and retention policies for backups to protect against ransomware attacks and accidental deletion.

9. [SSL/TLS configuration]

Every web server needs a valid SSL certificate to encrypt data in transit. Use certificates from a trusted CA like Let's Encrypt, DigiCert, or your organization's internal PKI. Configure IIS to force HTTPS, and disable insecure protocols and ciphers (e.g., SSL 3.0, TLS 1.0). Use TLS 1.2 or 1.3 and enable features like HSTS (HTTP Strict Transport Security). Test your server using tools like SSL Labs to ensure it meets modern security standards. This builds trust with users and prevents data interception.

Windows Server Build Sheet

7. [Logging and monitoring]

A secure server is a monitored server. Enable Event Logging, especially for login attempts, system errors, and application-specific events. Integrate these logs into a centralized log management system like Azure Monitor, Log Analytics, or a SIEM like Splunk or ELK. This allows for real-time alerts and incident correlation. Log retention policies should be set, and sensitive logs must be protected against tampering. Monitor IIS logs for unusual requests, 500 errors, or slow responses that may indicate probing or attacks.

8. [Backup and recovering]

No system is truly secure unless it's also recoverable. Set up a backup policy to create daily snapshots or file-based backups of the server and its critical data. These backups should be encrypted and stored off-server, ideally in another availability zone or region using tools like Azure Backup, Veeam, or Windows Server Backup. Test your recovery process regularly — a backup you can't restore is useless. Also consider versioning and retention policies for backups to protect against ransomware attacks and accidental deletion.

8. [SSL/TLS configuration]

Every web server needs a valid SSL certificate to encrypt data in transit. Use certificates from a trusted CA like Let's Encrypt, DigiCert, or your organization's internal PKI. Configure IIS to force HTTPS, and disable insecure protocols and ciphers (e.g., SSL 3.0, TLS 1.0). Use TLS 1.2 or 1.3 and enable features like HSTS (HTTP Strict Transport Security). Test your server using tools like SSL Labs to ensure it meets modern security standards. This builds trust with users and prevents data interception.

10. [RDP]

Remote Desktop Protocol (RDP) is a necessary evil in many setups. If RDP must be used, limit access to specific IP addresses using NSGs or firewalls. Require Network Level Authentication (NLA) and consider enforcing MFA for RDP via Azure AD or third-party solutions. Disable clipboard and drive redirection to prevent data leakage. Log all RDP sessions and set session timeouts. If possible, use a jump box (bastion host) or VPN to add an extra layer between the public

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. [Visibility into cloud storage]

CASBs provide deep visibility into cloud service usage across the organization — both sanctioned and unsanctioned (a.k.a. "shadow IT"). It helps detect risky behavior like users uploading sensitive data to personal cloud accounts or accessing services not approved by IT. You can't secure what you can't see — CASB fixes that.

2. [Data loss prevention(DLP)]

CASBs monitor and control data in motion and at rest in cloud apps. They enforce DLP policies by detecting sensitive content (e.g., PII, PHI, credit card data) and preventing it from being shared, downloaded, or leaked — even in apps like Google Drive, OneDrive, or Slack.

3. [Threat protection]

CASBs detect malware, phishing attempts, account takeovers, and insider threats by analyzing user behavior and cloud activity. They integrate with sandboxing and threat intel to block malicious content before it reaches users — a much-needed shield in today's zero-trust cloud world.

4. [Compliance Enhancement]

With built-in templates for regulations like GDPR, HIPAA, PCI-DSS, and ISO 27001, CASBs help ensure that cloud usage complies with industry standards. They automate audits, generate reports, and enforce security policies — making it easier to pass compliance checks without pulling all-nighters.

5. [Access control and conditional policy]

CASBs enable granular access controls based on device health, location, user role, and activity. For example, they can block downloads from unmanaged devices or require MFA for high-risk logins. This ensures only the right users, from the right places, get access — reducing the attack surface.