UDACITY

FedF1rst Security Assessment

Hazrat Umer

9 Aug 2024

Project Scenario

Project Scenario

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.

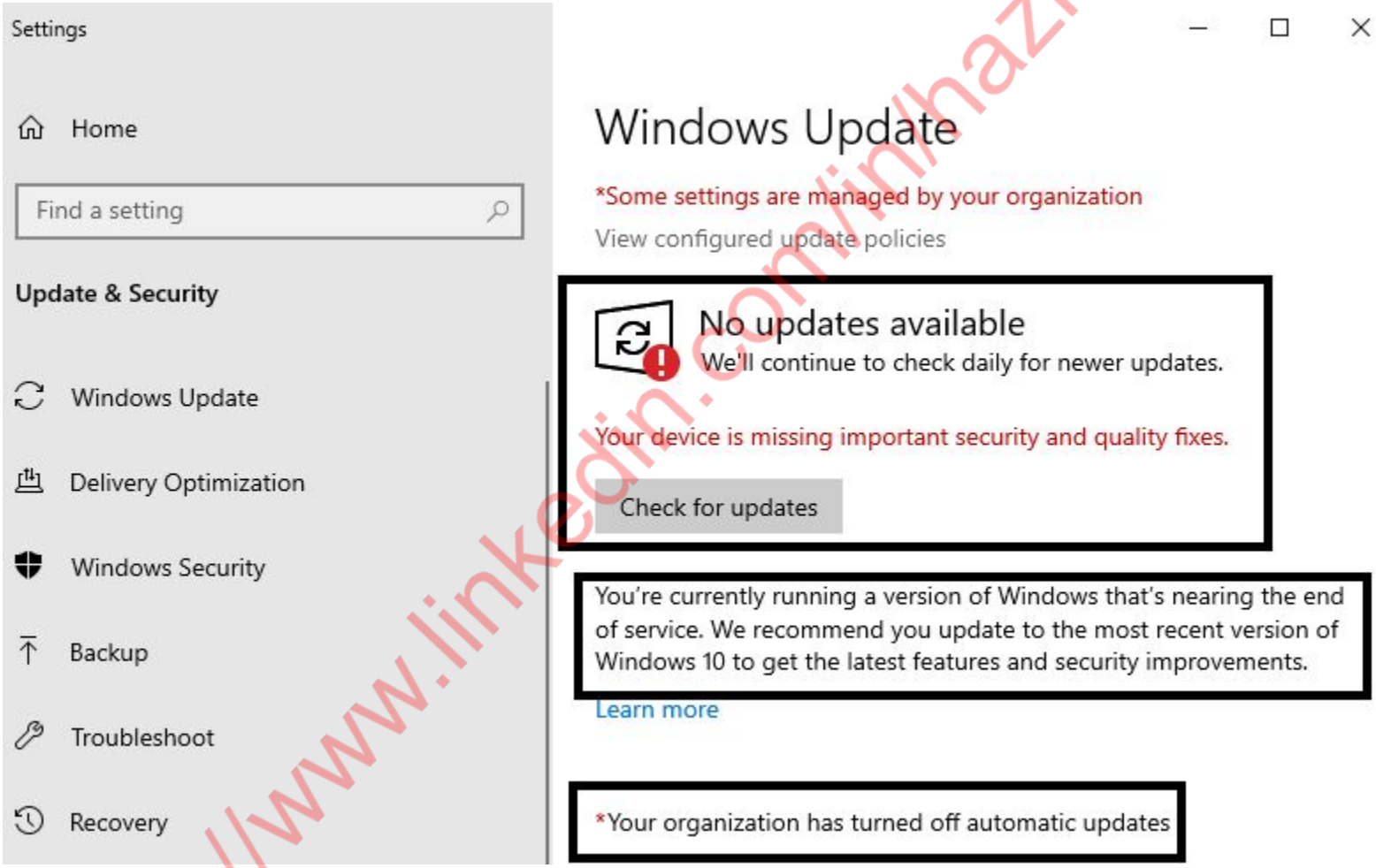
Your mission: to navigate the complexities of digital security, ensuring that every technological advancement—be it through securing desktop environments, fortifying email communications, or aligning with stringent cybersecurity standards—translates into a fortified defense against the cyber threats 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 One: Develop a hardening strategy

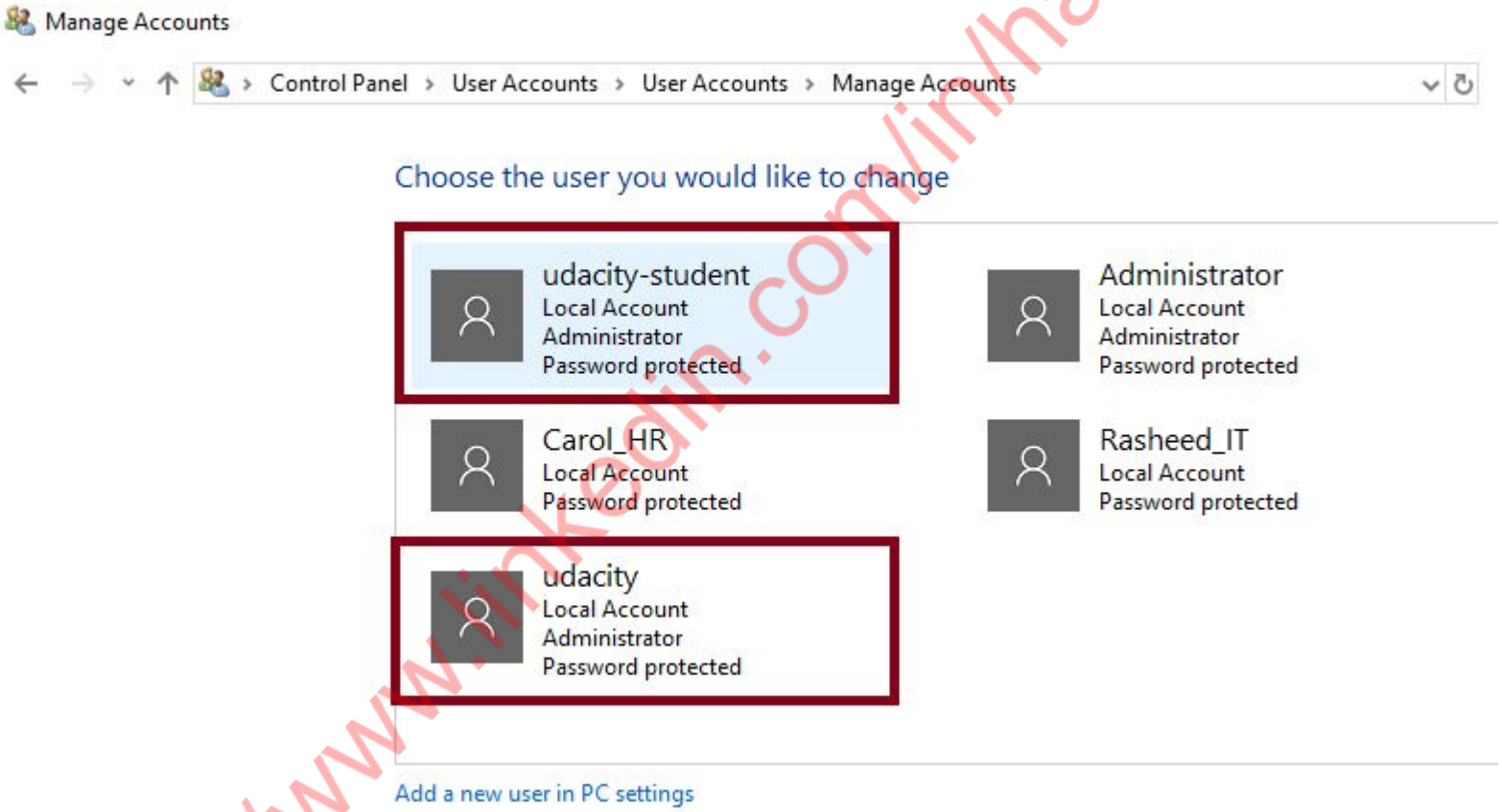
Windows 10 Hardening

1. System Updates



Windows 10 Hardening

2. User Permissions



Windows 10 Hardening

3. Antivirus Status

Windows 10 Hardening

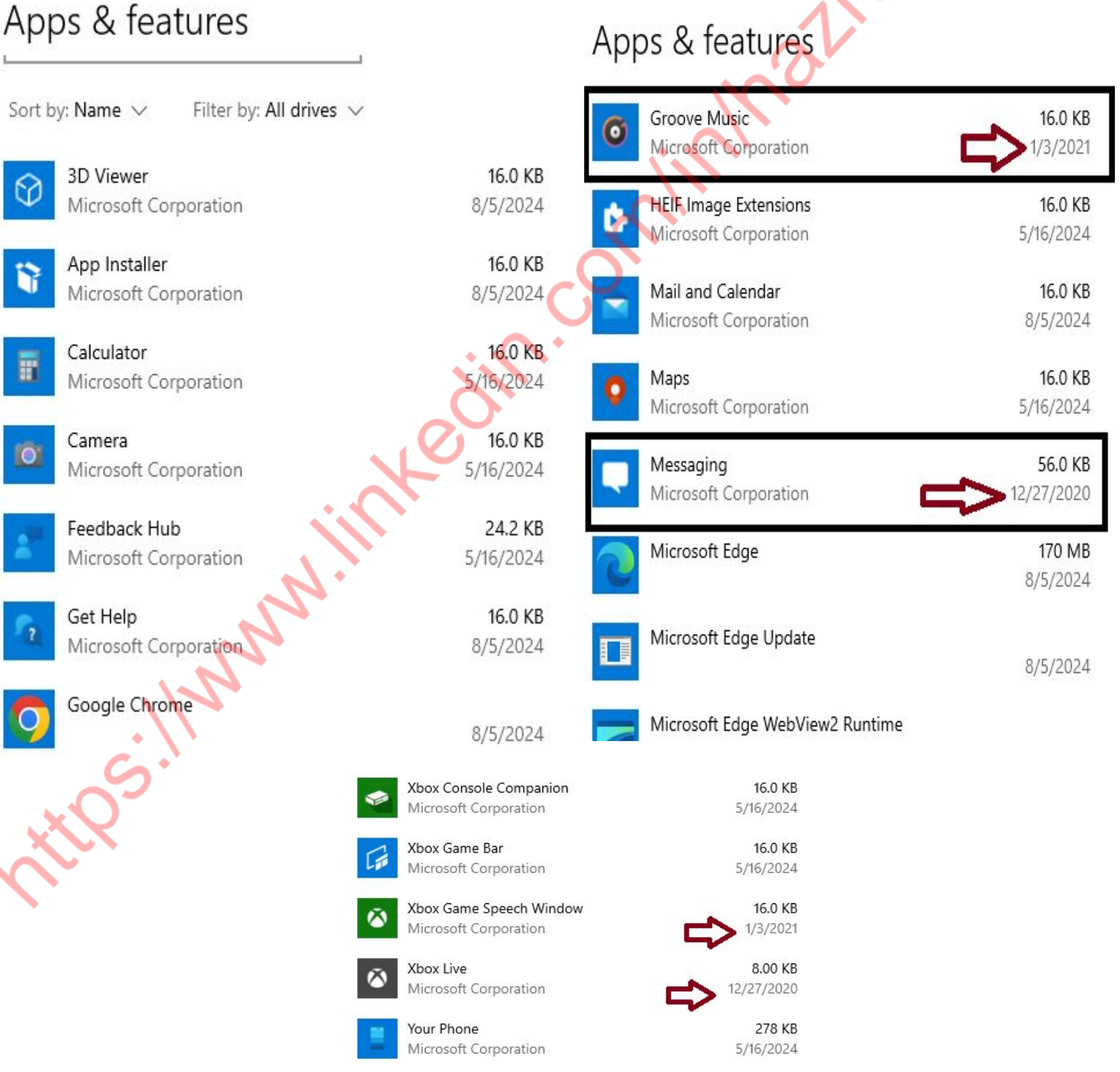
4. Firewall Settings

Windows 10 Hardening

5. Third Party Applications

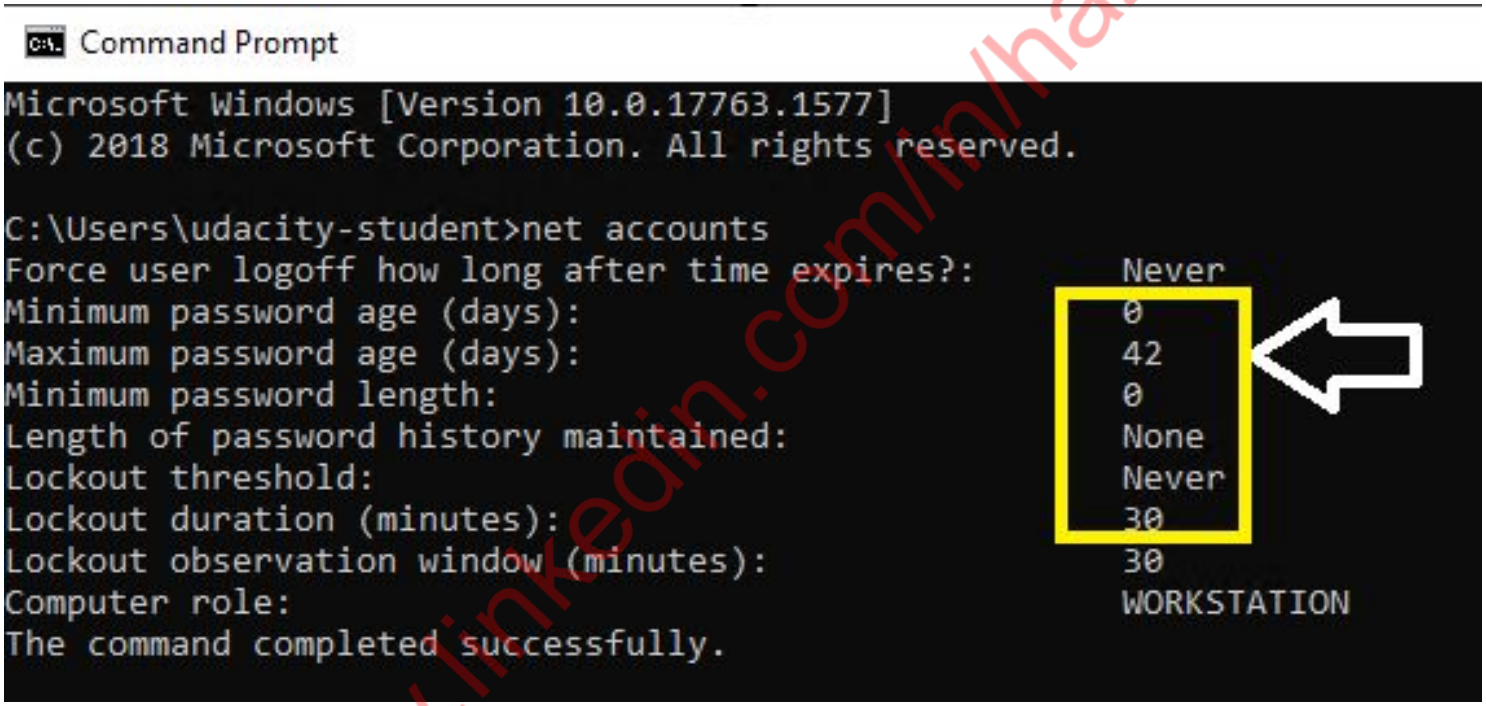
Windows 10 Hardening

Outdated Windows Apps



Windows 10 Hardening

6. Password Policies



Windows 10 Hardening

1. System Updates

A version of Windows was running that's nearing the end of service. Windows updates was available but not updated and automatic updates were turn off.

Remediation:

In order to fix this issue, Windows should be updated and upgraded to the latest version available. Automatic updates should be enabled.

2. User Permissions

I found 5 accounts, Udacity-Student, Administrator, Carol_HR, Udacity, Administrator and Rasheed_IT.

Remediation:

2 accounts which are Udacity-Student and udacity have administrative rights. These administrative rights should be removed and these account types should be changed to normal user.

3. Antivirus Status

Antivirus was turned off but the signatures were updated.

Remediation:

Antivirus should be enabled.

Windows 10 Hardening

4. Firewall Settings

Windows Defender Firewall was turned off .

Remediation:

In order to fix this the Windows Defender firewall should be turned on and updated.

5. Third Party Applications

Found WinScp 5.1.3 third party applicatio which is outdated version.

Remediation:

WinSCP 5.1.3 should be updated to WinSCP 6.3. It is the current version of this application.

6. Password Policies

Password Age was set to 42 days, Length of password history not maintained. Lockout threshold was not set. Maximum password lengh was set to 0.

Remediations:

Password Age should be set to 180 days. Password history should be maintained. There should be a lockout threshold. And the Maximum password lentth should be set to 15 characters.

MacOS Hardening

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

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

MacOS Hardening

1. FileValut for Full Disk Encryption

Configuration:

Go to System Preferences
Then Security & Privacy
and click on FileVault.

Rationale:

If the device containing sensitive data is lost or stolen, full disk encryption helps protect the data on the MacBook by encrypting the entire drive. An unauthorized person cannot read the data and data remain confidential.

2. Strong Password Policy

Configuration:

Go to System Preferences
Then Go to Users and Groups
You will find the password policy there.

Rationale:

Implementing a strong password policy will help an organization prevent unauthorized access to their MacBooks. Complex passwords are difficult to guess by an attacker and it also help to reduce the risks of brute force attacks and helps to safeguard an organization's sensitive data.

MacOS Hardening

3. Enable Firewall

Configuration:

Go to System Preferences
then go to Security and Privacy
and click on Firewall

Rationale:

Firewall acts as an additional layer of defense against various network-based attacks. It helps to protect the MacBook from unauthorized access.

4. Automatic Software Updates

Configuration:

Go to System Preferences
and click on Software Update

Rationale:

By enabling automatic updates your Mac OS will get the latest updates and security patches. This will help protect your MacBook from different vulnerabilities and exploits that target outdated software.

MacOS Hardening

5. Gatekeeper Configuration

Configuration:

Go to Preferences
Security and Privacy
Click on general and you will find an option "Allow apps downloaded from App Store"
Allow this option.

Rationale:

Gatekeeper is a built-in feature in MacBook, It helps to allow only trusted applications from the App Store. This feature helps MacBook users in reducing the risk of installing untrusted or malicious software that can compromise their MacBook's security.

6. Enabling and configuring file sharing controls

Configuration:

Go to System Preferences
Click on Sharing
Here you can enable and configure file-sharing controls

Rationale:

Shared files and folders on a MacBook can be prevented from unauthorized access by properly implementing file-sharing controls. It reduces the risk of data leakage and through these controls only authorized people will access to sensitive data.

Section Two:
Create Security Policies

Email Policy

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

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

Email Policy

1. While sending Confidential and sensitive information via email should be encrypted using approved encryption mechanisms.

2. Each employee of the organization should attend phishing awareness training yearly conducted by the security team, so that they can immediately report any suspected phishing email to the security team.

3. Each employee should use complex passwords containing Upper Case Letters, Lower case letters, numbers and special characters, use unique passwords for their email accounts and should enable multi factor authentication (MFA) for all of the accounts including email.

4. Never open email attachments or click on any links from untrusted or unknown sources. Before opening any attachment, it should be scanned with antivirus software.

5. Email's data should be classified according to company's data classification policy. Confidential information should not be sent via email, if necessary then it should be sent in encrypted format.

BYOD Policy

As Fed F1rst Control Systems embraces a Bring Your Own Device (BYOD) policy to enhance flexibility and productivity, the security of corporate data on employee-owned devices becomes a critical concern. These devices, ranging from smartphones to laptops, introduce various security challenges that must be addressed to protect both the company's and employees' information. Your role is to contribute to the development of a robust BYOD policy by writing the Security section. This will ensure that employees can use their own devices without compromising the organization's digital security.

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

BYOD Policy

1. All those personnel devices that are used for organizational work purposes must be enrolled in Company's MDM System. The Mobile device management will enforce different types of policies such as security policies, manage software updates and monitoring compliance. Those devices that are not enrolled with MDM will not be able to access organizational resources.
2. All those devices that are used to access corporate resources must be secured using complex passwords or biometric authentication.
3. Multi-factor authentication should be enabled for accessing corporate data, networks and applications.
4. Full disk encryption should be enabled on all devices. Sensitive or confidential data should be encrypted using VPN or various protocols such as TLS/SSL.
5. To monitor and control the transfer of sensitive or confidential data DLP Software should be installed on all devices.
6. The lost or stolen devices should immediately reported to the IT department and the IT department will remotely wipe data of stolen or lost device.

Section Three: 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 the 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

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Built-In Administrator account is disabled	Not Met
Windows Firewall is enabled	Not Met
Automatic updates are enabled	Not Met
User Account Control (UAC) is enabled	Not Met
Strong password policies are enforced	Not Met
Guest account is disabled	Not MET
System logging and auditing are enabled	Not Met
Windows Defender Antivirus is enabled and up to date	Not Met
Remote Desktop Services are configured securely	Met
Internet Explorer Enhanced Security Configuration (IE ESC) is enabled	Not Met
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	Not Met

Windows Desktop Compliance

Ensuring the Windows 10 desktop at Fed F1rst Control Systems meets all *NIST SP 800-53 Rev. 5* controls is vital for maintaining a strong security posture. After identifying controls that are not met, the next step is to outline straightforward remediation actions. Simplifying the remediation process by focusing on concise, one-line solutions will facilitate a more efficient path to compliance. This approach enables you to quickly address vulnerabilities and enhance the system's security with minimal complexity.

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

Windows Desktop Compliance

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

Built-In Administrator account is disabled:Disable the Built-In Administrator account using Group Policy or Local Security Policy (secpol.msc).
Windows Firewall is enabled:Enable Windows Firewall through the Control Panel or by running the command netsh advfirewall set allprofiles state on in an elevated command prompt.
Automatic updates are enabled: Configure Windows Update settings to automatically download and install updates through Group Policy (gpedit.msc) or by setting Configure Automatic Updates to Auto download and notify for install.
User Account Control (UAC) is enabled: Enable UAC through the Control Panel or by modifying the registry key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System and setting EnableLUA to 1.
Strong password policies are enforced: Set strong password policies through Group Policy (gpedit.msc) by enforcing password complexity, minimum length, and maximum password age.
Guest account is disabled: Disable the Guest account through Local Users and Groups (lusrmgr.msc) or using the command net user guest /active:no in an elevated command prompt.
System logging and auditing are enabled: Enable and configure logging and auditing settings through Group Policy (gpedit.msc) by turning on audit policies under Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration.
Windows Defender Antivirus is enabled and up to date: Enable Windows Defender Antivirus and ensure it is up to date through the Windows Security app or by running Set-MpPreference -DisableRealtimeMonitoring 0 in PowerShell.

Windows Desktop Compliance

Internet Explorer Enhanced Security Configuration (IE ESC) is enabled: Enable IE ESC through the Server Manager or by setting the registry key HKLM\Software\Microsoft\Active Setup\Installed Components\{29e42c6f-2401-4bb2-8ab9-8b7c1655e929} to 1.
USB ports are disabled or restricted to authorized devices only: Restrict USB port usage by configuring Group Policy settings under Removable Storage Access or using device installation restrictions in gpedit.msc.
Windows Updates are configured to download and install updates automatically: Set Windows Update to automatic by configuring the Group Policy setting Configure Automatic Updates under Computer Configuration > Administrative Templates > Windows Components > Windows Update.

CentOS 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 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 the CentOS 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

CentOS Compliance

CentOS CMMC Requirements	Met/Not Met
Current on security updates	Not Met
Ensure separate partition exists for /var	Not Met
Disable Automounting of drives	Met
Ensure AIDE is installed	Not 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	Not 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	Not Met

Section Four: 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. Machine Name
There should be a meaningful machine name. E.g WebServer001
2. Operating System Version
Ensure there is a supported and up-to-date version of the operating system running. e.g Windows Server 2022
3. Firewall Configuration
Configure the Windows server firewall to allow only necessary inbound or outbound traffic. e.g. Only allow HTTP, and HTTPS and block other ports and protocols that are not necessary.
4. Web Server Installation
For Example: Install and configure IIS as a web server. Make sure to use the latest stable version.
5. Secure Remote Access
Implement secure remote access methods for your server. E.g Use RDP over SSL or VPN. Use SSH and enforce multi-factor authentication.

Windows Server Build Sheet

6. Anti-Malware and Endpoint protection
Install and configure anti-malware. Configure an autoscan and auto-updates. e.g Enabling Windows Defender
7. SSL/TLS Configuration
Configure SSL/TLS. Install a valid certificate from a trusted certificate authority (CA).
8. Users and Permission Management
Implement the principle of least privilege (PoLP), remove or disable default any default accounts. Only create a single administrator account and any other accounts should have minimum level of required permissions.
9. Patch Management
Configure an automated patch management. e.g Use a Windows update or a centralized patch management solution such as Windows Server Update Services (WSUS)
10. Logging and Monitoring
Configure logging for IIS or Windows logs. Configure centralized logging and monitoring solutions to track any potential security incidents. e.g. Using Azure Monitor for real-time insights.

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. Data Loss Prevention:

CASBs provide robust Data Lost Prevention (DLP) capabilities through which we can monitor and control the movement of sensitive data across cloud services. This helps in preventing unauthorized leakage and transfer of data. It ensures that sensitive and confidential information remains secure within the organization limit.

2. Compliance Monitoring:

CASBs enables organizations to monitor data flows and user actions in real time. This ensures compliance with some regulatory standards such as HIPPA, GDPR etc and this also helps organizations to identify and mitigate non-compliance behavior quickly.

3. Threat Protection:

CASBs helps in enhancing security by detecting and responding to different types of threats for e.g Malware and Ransomware etc in cloud environment. CASBs advanced threat protection helps in detecting different types of anomalies.

4. Access Control and Identity Management:

Through Identity and access management (IAM), CASBs can enforce different access controls such as user roles, device types and location. It minimize the risk of unauthorized access and data breaches and ensures that only authorized users can access to sensitive resources of the cloud.

5. Shadow IT Discovery and Management:

Using CASBs helps in discovering and managing shadow IT. This will help an organization to ensure that no one should use cloud unauthorizedly.