UDACITY

FedF1rst Security Assessment

Uriyah Adriel Sam

19-05-2024

Windows Server Build Sheet

6. Application Frameworks and Dependencies
Install necessary application frameworks (e.g., .NET Framework) and dependencies required to support web applications running on the server.
7. Logging and Monitoring Configuration
Configure logging settings to record server activities and set up monitoring solutions to detect and respond to security incidents in real-time.
8. Backup and Disaster Recovery Plan
Develop and document a backup strategy to regularly back up critical server data and implement a disaster recovery plan to restore operations in case of unexpected outages or data loss.
9. User Access and Authentication
Define user access controls and authentication methods (e.g., Active Directory integration) to ensure secure access to the web server and restrict unauthorized entry.
10. Hardening and Security Policies
Implement security hardening measures, such as disabling unnecessary services, configuring least privilege access, and enforcing password policies, to reduce the server's attack surface and enhance overall security posture.

Digital Project Management

Project Scenario

Digital Project Management Section One:

Develop a hardening strategy

Windows 10 Hardening

1. Operating System Not Updated
Issue: The Windows 10 operating system has not been updated with the latest security patches and feature updates. This can leave the system vulnerable to known exploits and malware that target unpatched vulnerabilities. **Remediation:** Enable automatic updates to ensure the system regularly receives and installs the latest security patches and feature updates.
2. Firewall Disabled
Issue: The Windows Firewall is turned off, exposing the system to unauthorized network access and potential attacks from external sources. **Remediation:** Activate the Windows Firewall for all network profiles (Domain, Private, Public) and configure appropriate rules to restrict unnecessary traffic, ensuring that only authorized applications and services can communicate.
3. Antivirus and Threat Protection Disabled
Issue: Virus and Threat Protection is turned off, leaving the system unprotected against malware, viruses, and other malicious software. **Remediation:** Reactivate real-time protection in the Windows Security settings and schedule regular antivirus scans to detect and remove threats promptly.

Windows 10 Hardening

1. Local Account Type for Users
Issue: User accounts are configured as local accounts instead of domain accounts, which can limit centralized management and policy enforcement. **Remediation:** Migrate user accounts to domain accounts to leverage centralized management, policy enforcement, and enhanced security features provided by the organization's domain infrastructure.
2. Account Protection Not Configured
Issue: Account protection is not signed in, which can prevent the use of features like Windows Hello, Dynamic Lock, and two-factor authentication. **Remediation:** Sign in to the account protection features using the organization's Microsoft or Azure Active Directory account, and enable Windows Hello and two-factor authentication to enhance account security.
3. Ransomware Protection Not Enabled
Issue: Ransomware protection is not enabled, and OneDrive is not set up for data backup, leaving the system vulnerable to data loss from ransomware attacks. **Remediation:** Enable Controlled Folder Access in Windows Security to protect critical folders from unauthorized changes, and set up OneDrive for automatic data backup to ensure data can be recovered in case of a ransomware attack.

MacOS Hardening

1. Enable FileVault
Configuration: FileVault full-disk encryption. **Rationale:** Encrypting the entire disk ensures that all data stored on the MacBook is protected against unauthorized access. This is crucial if the device is lost or stolen, as it prevents sensitive corporate information from being retrieved by unauthorized parties.
2. Enforce Strong Password Policies
Configuration: Require strong passwords for all user accounts. **Rationale:** Strong passwords help protect against brute-force attacks and unauthorized access. By enforcing complexity requirements (such as a mix of uppercase and lowercase letters, numbers, and special characters) and regular password changes, the risk of compromised credentials is significantly reduced.
3. Enable Firewall
Configuration: Activate the macOS built-in firewall. **Rationale:** The firewall helps prevent unauthorized applications, programs, and services from accepting incoming connections. By controlling network traffic, the firewall adds an additional layer of security, protecting the system from potential network-based threats.

MacOS Hardening

4. Set Up Automatic Updates
Configuration: Configure macOS to automatically download and install updates for the operating system and applications. **Rationale:** Keeping the operating system and software up to date is critical for protecting against known vulnerabilities and exploits. Automatic updates ensure that the MacBooks receive the latest security patches and feature enhancements without relying on manual intervention.
5. Configure System Integrity Protection (SIP)
Configuration: Ensure that System Integrity Protection is enabled. **Rationale:** SIP helps protect the macOS from malware and malicious software by restricting the root user account and preventing potentially harmful software from modifying protected files and folders. This security measure helps maintain the integrity of the operating system.
6. Deploy Endpoint Security Solutions
Configuration: Install and configure endpoint security software, such as antivirus and anti-malware programs. **Rationale:** Endpoint security solutions provide real-time protection against a wide range of threats, including viruses, malware, and ransomware. By actively monitoring the system, these solutions can detect and neutralize threats before they cause significant harm.

Digital Project Management

Section Two: Create Security Policies

Email Policy

1. Use of Strong and Unique Passwords

Policy Item: Employees must use strong, unique passwords for their corporate email accounts, consisting of at least 12 characters, including a mix of uppercase and lowercase letters, numbers, and special characters.

Rationale: Strong passwords help prevent unauthorized access to email accounts, protecting sensitive communications from being compromised by brute-force attacks or password breaches.

2. Regular Phishing Awareness Training

Policy Item: Employees must participate in mandatory phishing awareness training sessions biannually, which include identifying phishing attempts, safe email practices, and reporting suspicious emails.

Rationale: Phishing attacks are a common method for cybercriminals to gain access to sensitive information. Regular training ensures employees are vigilant and equipped to recognize and respond appropriately to phishing attempts.

3. Use of Email Encryption

Policy Item: All sensitive and confidential information transmitted via email must be encrypted using the company's approved encryption methods and tools.

Rationale: Encrypting sensitive information helps protect it from being intercepted and read by unauthorized individuals during transmission, ensuring the confidentiality and integrity of corporate communications.

Email Policy

4. Restriction on Personal Email Use for Business Purposes

Policy Item: Employees are prohibited from using personal email accounts for conducting any business-related activities or sharing company information.

Rationale: Using personal email accounts for business purposes increases the risk of data breaches and makes it difficult to enforce security policies. Ensuring all business communications occur through corporate email accounts helps maintain security and accountability.

5. Automatic Email Archiving and Monitoring

Policy Item: All corporate email communications will be automatically archived and monitored for compliance with company policies and regulatory requirements. Employees must not delete or alter any email records without proper authorization.

Rationale: Archiving and monitoring emails ensure that there is a complete record of all communications, which is essential for compliance, legal discovery, and internal investigations. It also helps detect and respond to potential security incidents in a timely manner.

BYOD Policy

1. Device Enrollment and Management

Requirement: All employee-owned devices must be enrolled in the company's Mobile Device Management (MDM) system.

Rationale: MDM allows the IT department to enforce security policies, deploy necessary updates, and manage device settings remotely, ensuring all devices meet the company's security standards.

2. Strong Authentication Mechanisms

Requirement: Devices must be secured with strong authentication methods such as biometrics (fingerprint or facial recognition) or a complex password/PIN.

Rationale: Strong authentication helps prevent unauthorized access to devices and corporate data, enhancing overall security.

3. Data Encryption

Requirement: Full-disk encryption must be enabled on all devices used to access corporate data. This includes using FileVault on macOS, BitLocker on Windows 11, and native encryption on iOS and Android.

Rationale: Encryption protects data stored on devices from being accessed by unauthorized parties, especially in case of loss or theft.

BYOD Policy

4. Secure Access Controls

Requirement: Access to corporate applications and data must be secured through VPNs (Virtual Private Networks) and multifactor authentication (MFA).

Rationale: VPNs and MFA provide an additional layer of security by ensuring that only authorized users can access sensitive corporate resources from their personal devices.

5. Regular Software Updates and Patch Management

Requirement: Employees must ensure that their devices' operating systems and applications are kept up to date with the latest security patches and updates.

Rationale: Regular updates and patches fix vulnerabilities and protect devices from known security threats, reducing the risk of exploitation.

6. Incident Reporting and Response

Requirement: Employees must immediately report any lost or stolen devices, as well as any suspected security incidents, to the IT department.

Rationale: Prompt reporting allows the IT team to take swift action to mitigate risks, such as remotely wiping data from lost or stolen devices and investigating potential breaches.

Digital Project Management

Section Three: Self Assessment

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	NA
USB ports are disabled or restricted to authorized devices only	NA
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

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

Requirement: The Built-In Administrator account should be disabled. Remediation: Run the following command in an elevated PowerShell prompt: Disable-LocalUser -Name Administrator
Requirement: Windows Firewall should be enabled. Remediation: Run the following command in an elevated PowerShell prompt: Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True
Requirement: Automatic updates should be enabled. Remediation: Configure Windows Update settings to automatically download and install updates: Go to Settings > Update & Security > Windows Update > Advanced Options, then ensure "Automatic (recommended)" is selected under "Choose how updates are installed."
Requirement: User Account Control (UAC) should be enabled. Remediation: Ensure UAC settings are set to the default level: Go to Control Panel > User Accounts > Change User Account Control settings, then set the slider to the default level or higher.
Requirement: Strong password policies should be enforced. Remediation: Configure Group Policy to enforce strong password policies: Press Win + R, type gpedit.msc, then navigate to Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy, and set the desired password policy settings.

Windows Desktop Compliance

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

Requirement: The Guest account should be disabled. Remediation: Run the following command in an elevated PowerShell prompt: Disable-LocalUser -Name Guest
Requirement: System logging and auditing should be enabled. Remediation: Configure auditing settings via Group Policy: Press Win + R, type gpedit.msc, then navigate to Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration, and configure the desired audit policies.
Requirement: Windows Defender Antivirus should be enabled and up to date. Remediation: Ensure Windows Defender Antivirus is enabled and set to update automatically: Go to Settings > Update & Security > Windows Security > Virus & threat protection, then ensure "Real-time protection" is turned on and that "Automatic sample submission" is set to the desired option.
Requirement: Windows Updates should be configured to download and install updates automatically. Remediation: Configure Windows Update settings to automatically download and install updates: Go to Settings > Update & Security > Windows Update > Advanced Options, then ensure "Automatic (recommended)" is selected under "Choose how updates are installed."

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

Digital Project Management

Section Four: Cloud Management

Windows Server Build Sheet

1.Operating System Version and Patch Level
Specify the Windows Server version (e.g., Windows Server 2019) and ensure that all available security patches and updates are applied to the system.
2. Security Groups and Firewall Rules
Define the security groups and firewall rules necessary to control incoming and outgoing traffic to the web server, ensuring only authorized connections are allowed.
3. Antivirus and Endpoint Protection
Install and configure antivirus software to protect against malware and other security threats, and ensure regular updates and scans are scheduled.
4. SSL/TLS Certificate Configuration
Configure SSL/TLS certificates to encrypt data transmitted between the web server and clients, ensuring secure communication over HTTPS.
5. Web Server Software and Configuration
Install and configure the web server software (e.g., Internet Information Services - IIS) and customize settings according to best practices and security requirements.

Enhancing Cloud Security with CASB

1. Visibility and Control
CASBs provide comprehensive visibility into cloud usage across various cloud services, allowing Fed F1rst to monitor and control data access and activities. This visibility enables proactive identification of shadow IT, unauthorized cloud usage, and potential security risks, ensuring better governance and compliance.
2. Data Protection and Encryption
CASBs offer robust data protection capabilities, including encryption, tokenization, and data loss prevention (DLP) policies. By encrypting sensitive data at rest and in transit, CASBs help mitigate the risk of unauthorized access and data breaches, ensuring data privacy and regulatory compliance.
3. Access Control and Identity Management
CASBs integrate with identity and access management (IAM) systems to enforce granular access controls and authentication policies for cloud resources. This ensures that only authorized users with proper credentials can access sensitive data and applications, reducing the risk of unauthorized access and insider threats.
4. [CASB Benefit]
[Short description of the benefit]
5. [CASB Benefit]
[Short description of the benefit]

Enhancing Cloud Security with CASB

4. Threat Detection and Incident Response
CASBs employ advanced threat detection techniques, such as anomaly detection, behavior analytics, and machine learning, to identify and respond to security threats in real-time. By detecting suspicious activities, unusual access patterns, and potential data exfiltration attempts, CASBs help Fed F1rst mitigate the risk of data breaches and cyberattacks, enabling swift incident response and remediation.
5. Compliance and Risk Management
CASBs offer robust compliance and risk management capabilities, helping Fed F1rst ensure adherence to regulatory requirements and industry standards (e.g., GDPR, HIPAA, PCI DSS). CASBs provide detailed compliance reports, audit logs, and policy enforcement mechanisms, enabling Fed F1rst to demonstrate compliance, mitigate risks, and protect sensitive data effectively.