Mini-Project 11: System Hardening

- **Windows Server 2019**
  - Domain Controllers:

    Domain controllers provide the physical storage for the Active Directory Domain Services (AD DS) database, in addition to providing the services and data that allow enterprises to effectively manage their servers, workstations, users, and applications (Microsoft, 2022). Windows 2019 is configured, by default, for ease of installation and not necessarily security-driven. As a result, we are going to take a few steps to ramp up the server's security.

    Hardening Guidelines:

    1. CIS Control 2 sets the application guidelines for securing the domain system by creating an allowlist that authorizes software, libraries, and scripts. This list ensures that only authorized software can be executed, or accessed. The list also ensures that authorized libraries like .dll are allowed to be loaded into a system process. Finally, using digital signatures and version controls ensures that authorized scripts, such as .py, are allowed to be executed. Windows server has a few tools in the Windows Server Manager that will enable such controls. We can use the file server resource manager system's file screening manager to dictate the types of files that are authorized on the server. We can use the Windows Encryption File System to ensure that the scripts that we are receiving are not corrupted. Digital signatures are based on Microsoft public key infrastructure technology which is an EFS capability.
    2. CIS Controls 5, Account Management, sets the guidelines for securing users on the domain. CIS Control 5 specifically sets guidelines that establish and maintain an inventory of all accounts in the enterprise including administrators and users. We need to continuously validate that all active accounts are authorized. We need to ensure password standards with a minimum of 8 characters with multi-factor authentication or 14 characters passwords for accounts not using multi-factor authentication. We need to disable dormant accounts and direct login to root users. We should also ensure that only one user has root user ID privileges. We restrict administrator privileges to dedicated administrator accounts. Windows provides a group policy management tool that allows us to control user privileges, create audit policies, and implement password policies.
    3. CIS Control 3.10 guides us to encrypt sensitive data in transit. CIS benchmark 2.3.5, level 1, ensure that LDAP server channel binding token requirements are set to "Always", allow vulnerable Netlogon secure channel connections' is set to 'Not Configured',: and LDAP server signing requirements' is set to 'Require signing', domain member: digitally encrypt or sign secure channel data (always)' is set to 'Enabled', and domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled'.

  - Web servers running Microsoft IIS (Intranet mainly):

Web servers running Microsoft IIS role provide a secure, easy-to-manage, modular, and extensible platform for reliably hosting websites, services, and applications. This is a level 1 benchmark.
Hardening Guidelines:

1. CIS Controls 9 improves the protection and detection of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement. We would need to ensure 'Impersonate a client after authentication is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' and (when the Web Server (IIS) Role with Web Services Role Service is installed) 'IIS_IUSRS'
2. CIS Controls 8 gives guidelines to collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack. Benchmark 2.2.30 ensures 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE', ensures 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled', ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled', ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log', ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes', and Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' There are a few more logs that the CIS benchmark recommends updating including the one mentioned above.

● Oracle Linux (POS Servers)

Oracle Linux provides a complete security stack, from network firewall control to access control security policies. While Oracle Linux is designed "secure by default," there are a few hardening steps I would recommend.

1. CIS Control 8.5, Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. Benchmark provides a variety of ways to harden Linux System Servers including ensuring audit tools are 755 or more restrictive, ensuring successful and unsuccessful attempts to use the usermod, chaco, setfacl, or chcon command are recorded, and ensuring events that modify the system's Mandatory Access Controls are collected.
2. CIS Control 4.8 recommends that we uninstall or Disable Unnecessary Services on Enterprise Assets and Software. We do this by ensuring VSFTPD, TFTP, IMAP, and POP3 Servers are not installed. We would disable the following file systems: squashfs and udf. We also ensure separate partition exists for /var
3. CIS Control 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts. Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user’s primary,

non-privileged account.CIS Benchmark recommends ensuring users must provide a password for escalation.

- **Windows 10**
  - Users using the POS software:

    To harden a system that uses POS software we would utilize the following controls using CIS controls and Benchmark Level 2:

    1. CIS Control 4.8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software. Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file-sharing service, web application module, or service function. Following CIS Benchmark, we must ensure 'Bluetooth Audio Gateway Service (BTAGService)' is set to 'Disabled', ensure 'Bluetooth Support Service (bthserv)' is set to 'Disabled', ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not installed', and ensure 'Peer Networking Grouping (p2psvc)' is set to 'Disabled'. These are just a few of the many other steps we would need to take.
    2. CIS Control 3.10: Encrypt Sensitive Data in Transit: Since POS is going to send customers information including credit card info we need to encrypt the data. To harden the system we want to ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'.
    3. Control 4.3: Configure Automatic Session Locking on Enterprise Assets. Configure automatic session locking on enterprise assets after a defined period of inactivity. For general-purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. We ensure 'Interactive logon: Number of previous logons to cache (in case the domain controller is not available)' is set to '4 or fewer logon(s)'

  - Users not using the POS software:

    To harden a system for users who are not using a POS system, we would implement controls that are level 1 benchmarked. There are lots of controls that we can implement so I will highlight the ones that are significant.

    1. Control 4.3: Configure Automatic Session Locking on Enterprise Assets. Configure automatic session locking on enterprise assets after a defined period of inactivity. For general-purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. We ensure that 'Interactive logon: Machine inactivity limit' is set to ‘900 or fewer second(s), but not 0’. Additionally, ensure that 'Interactive logon: Prompt user to change the password before expiration' is set to 'between 5 and 14 days'.
    2. Control 3.3: 3 Configure Data Access Control Lists. Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. We must ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'. Additionally, we ensure that 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow

3. Control 5.2: Use Unique Password: Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. We ensure 'Enforce password history' is set to '24 or more password(s)', 'Maximum password age' is set to '365 or fewer days, but not 0', and 'Minimum password age' is set to '1 or more day(s).'