Hardening

Objectives:

- 2.5 - Explain the purpose of mitigation techniques used to secure the enterprise
- 4.1 - Given a scenario, you must be able to apply common security techniques to computing resources
- 4.5 - Given a scenario, you must be able to modify enterprise capabilities to enhance security

- **Hardening**
    - *Hardening*
        - Process of enhancing system, application, or network security
        - Measures
            - Apply security patches, configure access controls, disable unnecessary services
        - Purpose
            - Strengthen overall security posture and resilience against cyberattacks
    - Study Topics
        - Default Configurations
            - Definition and identification of default configurations
            - Changing default passwords, open ports, and insecure configurations
        - Restricting Applications
            - Application restriction approach
            - Allow listing, blocking unauthorized software
        - Disabling Unnecessary Services
            - Identifying unnecessary services

        - Risks and consequences of running unnecessary services
        - Disabling unnecessary services to reduce the attack surface
    - Trusted Operating Systems
        - Definition and characteristics of trusted operating systems
        - Rigorous security evaluations and certifications
    - Updates and Patches
        - Understanding updates vs. patches
        - Importance of regular software updates
        - Systematic process of patch management
    - Group Policies
        - Role of Group Policies in Windows environments
        - Central management and control of user and computer settings
    - SELinux (Security-Enhanced Linux)
        - Role and implementation of SELinux
        - Mandatory access controls for enhanced security
    - Data Encryption Levels
        - Different levels of data encryption
            - Full-disk
            - Partition
            - File
            - Volume
            - Database
            - Record Level Encryption
    - Secure Baselines
        - Definition and purpose of secure baselines
        - Establishing a secure starting point for minimizing security risks

- **Changing Default Configurations**
    - Default passwords
        - Preset authentication details
        - Should be immediately changed
        - Rotate every 90 days
        - Rely on password manager
    - Unneeded ports and protocols
        - Close any ports that aren’t needed
        - Audit ports and protocols that are enabled
        - Look for secure versions of protocols and use them instead
    - Extra open ports
        - May be open by default
        - Use the more secure ports and close the insecure ones

- **Restricting Applications**
    - *Least Functionality*
        - Involves configuring systems with only essential applications and services
        - Least functionality aims to provide only the necessary applications and services
        - Unneeded applications should be restricted or uninstalled to reduce vulnerabilities
        - Over time, personal computers accumulate unnecessary programs
    - Managing Software
        - Keeping software up-to-date is crucial for security
        - New programs may be installed without removing old versions
        - Large networks require preventive measures to control excessive installations

- Creating Secure Baseline Images
  - Secure baseline images are used to install new computers
  - Images include the OS, minimum required applications, and strict configurations
  - These images should be updated based on evolving business needs
- Preventing Unauthorized Software
  - Unauthorized software installation poses security risks
  - Application allowlisting and blocklisting are used to control which applications can run on a workstation
- *Application Allowlisting*
  - Only applications on the approved list are allowed to run
  - All other applications are blocked from running
  - Similar to an "Explicit Allow" statement in access control
- *Application Blocklisting*
  - Applications placed on the blocklist are prevented from running
  - All other applications are permitted to run
  - Any application on the blocklist is denied
- Choosing Between Allowlisting and Blocklisting
  - Allowlisting is more secure, as everything is denied by default
  - Managing allowlists can be challenging as updates require list adjustments
  - Blocklisting is less secure, as everything is allowed except what's explicitly denied
  - Managing blocklists can be difficult, as every new program variation would be allowed until a rule is created
- Centralized Management
  - Microsoft Active Directory domain controllers allow centralized management of lists
  - Group policies can be used to deploy and manage allowlists and blocklists across

workstations in a network

- **Trusted Operating Systems**
  - Trusted Operating System (TOS)
    - An operating system that is designed to provide a secure computing environment by enforcing stringent security policies that usually rely on mandatory access controls
    - Used where Confidentiality, Integrity, and Availability is essential
  - Evaluation Assurance Level (EAL)
    - A predefined security standard and certification from the Common Criteria for Information Technology Security Evaluation
    - Common criteria standards are used to assess the effectiveness of the security controls in an operating system
      - EAL 1 is the lowest level of assurance
      - EAL 7 is the highest level of assurance
  - Trusted operating systems often include
    - Mandatory Access Control
      - Access permissions are determined by a policy defined by the system administrators and enforced by the operating system
    - Security Auditing
    - Role-based Access Control
  - Examples
    - SELinux (Security-Enhanced Linux)
      - Set of controls that are installed on top of another Linux distribution like CentOS or Red Hat Linux

        - Trusted Solaris
            - Offers secure, multi-level operations with MAC, detailed system audits, and data/process compartmentalization
    - Trusted OS enhances security with microkernels by minimizing the trusted base and reducing attack surface and vulnerabilities
    - Choosing an operating system requires balancing security with usability, performance, and functional requirements

- **Updates and Patches**
    - Patch management can be
        - Manual
            - Rare for fully manual patch management these days
        - Automated
            - More reliable and most often used
    - Hackers can reverse engineer patches to find the underlying vulnerability
    - *Hotfix*
        - A software patch that solves a security issue and should be applied immediately after being tested in a lab environment
    - *Update*
        - Provides a system with additional functionality, but it doesn't usually provide any patching of security related issues
        - Often introduce new vulnerabilities
    - *Service Pack*
        - Includes all the hotfixes and updates since the release of the operating system
    - Effective Patch Management involves
        - Assigning a dedicated team to track vendor security patches

    - Establishing automated system-wide patching for OS and applications
    - Including cloud resources in patch management
    - Categorizing patches as urgent, important, or non-critical for prioritization
    - Create a test environment to verify critical patches before production deployment
    - Maintaining comprehensive patching logs for program evaluation and monitoring
    - Establishing a process for evaluating, testing, and deploying firmware updates
    - Developing a technical process for deploying approved urgent patches to production
    - Periodically assessing non-critical patches for combined rollout

- **Patch Management**
  - *Patch Management*
    - Planning, testing, implementing, and auditing of software patches
  - Important for compliance
  - Four Step Process
    - Planning
      - Creating policies, procedures, and systems to track and verify patch compatibility
      - A good patch management tool confirms patch deployment, installation, and functional verification on servers or clients
    - Testing
      - Do this to prevent the patch from causing additional problems
    - Implementing
      - Deploy to all devices that need it
      - Can be done manually or automated

            - Large organizations should use a central update server instead of Windows Update or other tool
            - Mobile devices can be patched using an MDM
            - Patch Rings
                - Implement patches one group (or ring) at a time
        - Auditing
            - Scan network to ensure the patch was installed correctly
            - Determine if there are any unexpected problems as a result of the patch
    - Firmware versions should also be monitored and patched
        - Companies will have centralized resources to help keep firmware patched

- **Group Policies**
    - *Group Policy*
        - A set of rules and policies that can be applied to users or computer accounts within an operating system
    - Accessing Group Policy Editor
        - Access the Group Policy Editor by entering "gpedit" in the run prompt
        - The local Group Policy Editor is used to create and manage policies within a Windows environment
    - Group Policies Overview
        - Each policy acts as a security template applying rules such as
            - Password complexity requirements,
            - Account lockout policies
            - Software restrictions
            - Application restrictions
        - In a Windows environment with an Active Directory domain controller, you have

access to an advanced Group Policy Editor

- *Security Templates*
    - A group of policies that can be loaded through one procedure
    - In corporate environments, create security templates with predefined rules based on administrative policies
    - *Security Template*
        - A group of policies that can be loaded through the Group Policy Editor
    - *Group Policy Objective (GPO)*
        - Used to harden the operating system and establish secure baselines
- *Baselining*
    - A process of measuring changes in the network, hardware, or software environment
    - Helps establish what "normal" is for the organization
    - Identifies abnormal or deviations for investigation
- Group Policy Editor in Windows
    - Access the Group Policy Editor by entering "gpedit" in the run prompt
    - Create allow or block list rules for application control policies

- Creating a Rule in Group Policy Editor
    - Launch the Group Policy Editor
    - Navigate to "Computer Configuration" > "Windows Settings" > "Security Settings" > "Application Control Policies" > "App Locker”
    - Create an executable rule
    - Choose to allow or deny
    - Select who the rule applies to (e.g., everyone)
    - Define the rule based on conditions like publisher, path, or file hash.

        - Specify the path to be blocked (e.g., the temp directory)
        - Name the rule and provide a description
        - Decide whether to create default rules (allow or deny) and save the policy
        - Deploy the policy across the environment for system hardening
    - Rules in Group Policy Editor
        - *Allow Rules (Default)*
            - Allow files in the "Program Files" directory to launch
            - Allow files in the "Windows" folder to launch
            - Allow administrators to launch any file
        - *Deny Rule (Custom)*
            - Block all files from running in the "temp directory"
    - By following these steps, you can establish a secure baseline for your Windows systems, improving overall security and policy management

- **SELinux**
    - SELinux and MAC Basics
        - *SELinux (Security Enhanced Linux)*
            - A security mechanism that provides an additional layer of security for Linux distributions
            - Enforces Mandatory Access Control (MAC)
        - *Mandatory Access Control (MAC)*
            - Restricts access to system resources based on subject clearance and object labels
        - *Context-based permissions*
            - Permission schemes that consider various properties to determine whether to grant or deny access to a user

  - Two main context-based permission schemes in Linux that use MAC
    - SELinux
    - AppArmor
  - DAC vs. MAC
    - *DAC (Discretionary Access Control)*
      - Each object has a list of entities that are allowed to access it
      - Allows object owners to directly control access using tools like 'chown' and 'chmod'
    - SELinux relies on MAC for permissions and access control, not DAC
- *SELinux*
  - The default context-based permission scheme in CentOS and Red Hat Enterprise Linux created by NSA
  - Used to enforce MAC on processes and resources
  - Enables information to be classified and protected
  - Enhances file system and network security, preventing unauthorized access, security breaches, and execution of untrustworthy programs
- Three Main Contexts in SELinux
  - *User Context*
    - Defines which users can access an object, including common contexts like 'unconfined_u,' 'user_u,' 'sysadm_u,' and 'root'
  - *Role Context*
    - Determines which roles can access an object, using 'object_r' for files and directories
  - *Type Context*
    - Essential for fine-grained access control, grouping objects with similar security characteristics

- Optional Context
    - *Level Context*
        - Describes the sensitivity level of a file, directory, or process
        - Known as a multi-level security context, allowing further access control refinement
- SELinux Modes
    - *Disabled Mode*
        - Turns off SELinux, relying on default DAC for access control
    - *Enforcing Mode*
        - Enforces all SELinux security policies, preventing policy violations
    - *Permissive Mode*
        - Enables SELinux but doesn't enforce policies, allowing processes to bypass security policies

- SELinux Policies
    - *SELinux Policy*
        - Describes access permissions for users, programs, processes, files, and devices
    - Two Main Policy Types
        - *Targeted Policies*
            - Only specific processes are confined to a domain, while others run unconfined
        - *Strict Policies*
            - Every subject and object operates under MAC, but it's more complex to set up

- Violation Messages
  - SELinux captures violation messages in an audit log
  - Violations can occur when someone tries to access an unauthorized object, or an action contradicts an existing policy
- Policy Configuration
  - Initial SELinux setup may result in false violations, requiring policy tweaking and fine-tuning
  - Strong security depends on creating effective restricted profiles and hardening applications to prevent malicious attacks

- **Data Encryption Levels**
  - *Data Encryption*
    - Process of converting data into a secret code to prevent unauthorized access
  - Levels
    - *Full-disk*
      - Encrypts the entire hard drive to protect all of the data being stored on it
    - *Partition*
      - Similar to full-disk encryption but it is only applied to a specific partition on the storage device
      - *VeraCrypt*
        - Tool that selectively encrypts partitions, like sensitive documents, while leaving the OS partition unencrypted
    - *Volume*
      - Used to encrypt a set space on the storage medium
      - Creates an encrypted container that can house various files and folders

        - *File-level Encryption*
            - Used to encrypt an individual file instead of an entire partition or an entire disk drive
            - *GNU Privacy Guard*
                - A tool that provides cryptographic privacy and authentication for data communication
        - *Database*
            - Secures the entire database
            - Can extend the encryption across multiple storage devices or cloud storage
            - Similar to full-disk encryption
        - *Record*
            - Encrypts individual records or rows within a database

- **Secure Baselines**
    - *Secure Baseline*
        - Standard set of security configurations and controls applied to systems, networks, or applications to ensure a minimum level of security
        - Helps organizations maintain consistent security postures and mitigate common vulnerabilities
    - Establishing a Secure Baseline
        - The process begins with a thorough assessment of the system, network, or application that requires protection
        - Identify the type of data involved, understand data workflows, and evaluate potential vulnerabilities and threats
        - Best practices, industry standards, and compliance requirements (e.g., ISO

27001, NIST SP 800-53) are used as starting points for defining the secure baseline

- Create a secure baseline configuration by securing the operating system on a reference device (e.g., a laptop)

- Configuring a Secure Baseline
  - Install, update, configure, and secure the operating system on the reference device
  - Check the device against baseline configuration guides and scan for known vulnerabilities or misconfigurations
  - Install required applications (e.g., Microsoft Office suite, endpoint detection and response agents)
  - Scan for vulnerabilities in the installed applications and remediate them
  - Create an image of the reference device as the "known good and secure baseline”
- Deployment
  - Configure firewalls, set up user permissions, implement encryption protocols, and ensure antivirus and anti-malware solutions are properly installed and updated
  - Use automated tools and scripts to ensure consistent application of the secure baseline across devices
  - In a Windows environment, Group Policy Objects (GPO) can be used to dictate policies, user rights, and audit settings
  - In cloud environments (e.g., AWS), services like AWS Config are employed to define and deploy secure configurations
- Maintenance
  - Lock down systems to prevent unauthorized software installation or

configuration changes

    - Regular audits, monitoring, and continuous assessment are required to keep the baseline up-to-date
    - Continuous monitoring tools help identify deviations from the baseline and trigger alerts for immediate remediation
    - Periodically review and update the secure baseline to adapt to changes in organizational infrastructure, business needs, and emerging threats
- Employee Training and Awareness
    - Conduct training sessions to educate employees about the importance of adhering to secure baseline configurations
    - Raise awareness about the potential risks of deviating from the baseline
    - Encourage employees to report any suspicious activities they notice when using their systems