CyberPatriot Guide by Image

Windows Image Guide

1. User Accounts:

   - Remove unnecessary users (e.g., Guest).

   - Enforce strong passwords via Local Security Policy.

2. Windows Updates:

   - Ensure all updates are installed via Windows Update.

3. Disable Unnecessary Services:

   - Use 'services.msc' to disable Telnet, Remote Registry, etc.

4. Installed Programs:

   - Uninstall unauthorized or outdated software.

5. Group Policy Changes:

   - Configure password policies and enable auditing.

   - Check event log sizes and policies.

Linux Image Guide

1. User Accounts:

   - Remove unnecessary users by reviewing /etc/passwd.

   - Enforce password complexity via PAM settings.

2. Apply Updates:

   - Use 'sudo apt update && sudo apt upgrade -y' for Ubuntu/Debian systems.

3. Secure SSH:

   - Disable root login and password authentication in /etc/ssh/sshd_config.

4. World-Writable Files:

   - Use 'find / -perm /o=w -type f' to identify and fix permissions.

5. Firewall:

   - Enable UFW and configure rules to block unnecessary ports.

Cisco Image Guide

1. Secure Console and Remote Access:

   - Set console and VTY passwords.

   - Configure SSH for secure remote access.

2. Disable Unnecessary Services:

   - Disable HTTP, HTTPS, and CDP if not needed.

3. Banner:

   - Set a login banner with 'banner motd'.

4. Basic Interface Configuration:

   - Assign IP addresses and shut down unused interfaces.

5. ACLs:

   - Create ACLs to block Telnet or other unwanted traffic.

6. Verify and Save Configuration:

   - Use 'show running-config', 'show ip ssh', etc., to verify settings.

   - Save with 'copy running-config startup-config'.