Chicago Hospital-STIG Policy Enforcement Document

Client: Chicago Hospital
Author: Jose Guerrero
Purpose: Enforce least privilege and standardized security baselines on Ubuntu systems using DISA STIG guidelines.

Policy Overview

The following policy establishes controls for **account management, file permissions, group access, service hardening, SSH security, and patch management**. These scripts automate enforcement and support compliance audits.

Purpose: Adapt the STIG automation scripts to protect sensitive data, ensure system integrity, and maintain compliance for Veterans Affairs systems. These scripts can help VA IT teams enforce least privilege, control user and group access, harden SSH and critical system files, and maintain up-to-date patches, supporting HIPAA and federal cybersecurity requirements.

Enforcement Controls & Files

1. **Sticky Bits for Shared Directories** – 01_stig_enforcement_sticky_bits.sh
    - Purpose: Restrict file deletion in shared temporary directories to the file owner.
2. **Secure User Creation** – 02_stig_enforcement_create_user.sh
    - Purpose: Ensure all new users are created with STIG-hardened skeleton directories, enforcing consistent permissions and secure defaults.
3. **Group Directory Permissions** – 03_stig_enforcement_group_permissions.sh
    - Purpose: Restrict access to group directories to authorized members only, supporting least privilege principles.
4. **Audit Users & Groups** – 04_stig_enforcement_audit_users_groups.sh
    - Purpose: Provide visibility of all non-system users and groups to validate compliance with account management controls.
5. **File Permissions Hardening** – 05_stig_enforcement_file_permissions.sh
    - Purpose: Protect sensitive authentication and account data by restricting access to critical system files (/etc/passwd, /etc/shadow, /etc/gshadow).
6. **Remove Insecure Services** – 06_stig_enforcement_remove_services.sh
    - Purpose: Reduce system attack surface by disabling legacy services flagged as insecure.
7. **Secure SSH Configuration** – 07_stig_enforcement_secure_ssh.sh
    - Purpose: Harden SSH to prevent root login and enforce key-based authentication for remote administrative access.
8. **System Update & Patch Management** – 08_stig_enforcement_update_system.sh
    - Purpose: Maintain system security by applying latest updates and patches, supporting STIG compliance.

Usage Guidelines

- All scripts **must be run as root** or with sudo.
- Scripts that require **input parameters**:
    - User creation: provide <username>
    - Group creation: provide <groupname>
- Scripts that do not require input can be run directly.
- Always test in **non-production environments** before deployment.
- Scripts should be run regularly to maintain **ongoing STIG compliance**.