7.4.4 Hardening Enforcement Facts

A *Group Policy Object (GPO)* is a collection of policy settings that enables policy-based administration using Active Directory. GPOs can provide a security administrator with an effective way to ensure the consistent application of controls on Windows servers and workstations throughout the system. In addition, GPOs can significantly reduce the effort involved in implementing and maintaining the hardening of servers and workstations.

Use GPOs to perform these specific hardening tasks:

- Secure local admin accounts
- Standardize user access to computers throughout the network
- Enforce workstation and server security settings
- Remove unnecessary services
- Enforce the password policy
- Set an audit policy
- Create restricted local groups
- Set permissions on local files
- Enforce firewall settings
- Enforce Windows Update settings
- Restrict use of physical inputs and outputs like USB ports

The Security Configuration and Analysis snap-in allows you to apply a template or compare a template to the existing security settings on your computer. This snap-in works only on the local system that is running the snap-in. This snap-in can be used for auditing to see if security settings configured in the past have been changed. A good security practice is to check the security setting frequently (every day if possible) to ensure that the controls set are still in effect and the system stays hardened.

Be aware of the following about GPOs:

- Granular control of the security configuration is achieved by setting GPO attributes.
- GPOs ensure that security policies are enforced each time a user logs in.
- GPOs can be managed using Microsoft Management Console (MMC) snap-ins.
- Security templates are predefined security settings.
- Security templates allow an administrator to easily and consistently apply security settings across GPOs.
- A security administrator can create a template or:
  - Get templates for other Windows systems.
  - Obtain templates from websites.
  - Obtain templates from the NSA. The templates have predefined security settings that the NSA considers appropriate for various Windows operating systems.
- GPOs can be easily changed to reflect changes to an organization's security policies.
- Changes made using Group Policy Management on a domain controller take place after the background refresh interval, which is five minutes on domain controllers and 90 minutes on client workstations.
- GPOs can be linked to Active Directory domains, organizational units (OUs), and containers.

  Built-in containers (such as the Computers container) and folders cannot have GPOs linked to them.

  - A GPO applied to an OU affects the objects in the OU and sub-OUs.
  - A GPO applied to a domain affects all objects in all OUs in the domain.
  - A local GPO is stored on a local machine. Computers that are not part of a domain use the Local Group Policy settings to control security settings and other restrictions on the computer.
- GPOs are applied in the following order:
  1. The Local Group Policy on the computer.
  2. GPOs linked to the domain that contains the user or computer object.
  3. GPOs linked to the organizational unit(s) that contain(s) the object (from the highest-level OU to the lowest-level OU).
- A specific setting in a GPO can be:
  - Undefined, meaning that the GPO has no value for that setting and does not change the current setting.
  - Defined, meaning that the GPO identifies a value to enforce.
- Individual settings within all GPOs are combined to form the effective Group Policy setting as follows:
  - If a setting is defined in one GPO and undefined in another, the defined setting will be enforced (regardless of the position of the GPO in the application order).
  - If a setting is configured in two GPOs, the setting in the last applied GPO will be used.

    The Local Group Policy is applied only when there are no GPOs linked to a domain or GPOs linked to an OU applied. GPOs linked to an OU override GPOs linked to a domain when both are applied.

- The default domain policy is separated into two areas, computer configuration and user configuration. Computer policies are applied as soon as the system is booted. User policies are not applied until the user logs in.
  - Computer policies include:
    - Software that should be installed on a specific computer.
    - Scripts that should run at startup or shutdown.

- Password restrictions that must be met for all user accounts.
- Network communication security settings.
- Registry settings that apply to the computer (the HKEY_LOCAL_MACHINE subtree).

- User policy settings include:
  - Software that should be installed for a specific user.
  - Scripts that should run at login or logoff.
  - Internet Explorer user settings (such as favorites and security settings).
  - Registry settings that apply to the current user (the HKEY_CURRENT_USER subtree).
