Unit 2

Windows Security Policy

Applying security templates

Employing the Security Configuration and Analysis snap

What is security template ?

The Security Templates is a standalone snap-in tool that users can use to define computer-independent security configurations. These configurations are saved as text-based .inf files.

Predefined security templates are used to increase the level of security on your network. You can modify security templates to suit your requirements by using Security Templates in Microsoft Management Console (MMC).

Applying security templates

Employing the Security Configuration and Analysis snap

How to define security templates ?

https://support.microsoft.com/en-us/topic/53ab83b8-4bb2-f8a7-a076-4aa5fbc93e58 (accessed on 6-1-22)

Predefined Security Templates

https://support.microsoft.com/en-us/topic/1e6e0ffb-02eb-deae-e895-b457faa35445
(accessed on 6-1-22)

Understanding

Local Group Policy Objects

https://www.minitool.com/news/windows-10-open-local-group-policy-editor.html

Understanding Local Group Policy Objects

Group Policy Objects Definition

Group Policy is a feature within Windows used to control configuration and behavior settings. A collection or group of settings are called group policy objects.

Understanding Local Group Policy Objects

Types of Group Policy Objects

A group policy object (GPO) is a collection of policy settings available to define the configuration or behavior of users or computers. A GPO can be used to do many things such as applying application or operating system settings, applying security settings, running scripts, or installing software. There are three types of group policy objects. Let's take a closer look at these in a little more detail.

Understanding Local Group Policy Objects

Types of Group Policy Objects

1. Local Group Policy Objects

A local group policy object refers to the collection of group policy settings that are applied locally on a Windows client. Local GPOs are used when policy settings are needed to apply to a single Windows client or user. Local GPOs exist by default on all Windows clients.

Understanding

Local Group Policy Objects

Types of Group Policy Objects

2. Nonlocal Group Policy Objects

A nonlocal group policy object is used when policy settings are needed to apply to one or more Windows clients or users. Nonlocal GPOs apply to Windows clients or users once they're linked to active directory objects such as sites, domains, or organizational units (OUs).

Understanding Local Group Policy

Objects

Types of Group Policy Objects

3. Starter Group Policy Objects

A starter GPO is a type of nonlocal group policy object that's used as a template when creating a new GPO within ADDS (Active Directory Domain Services). Starter GPOs can be used when an organization has a requirement that certain mandatory settings should always be in place. Having a starter GPO would then ensure that as each GPO is created, the mandatory settings are already pre-populated within it. This helps to save time for administrators.

Understanding Domain Group Policy Objects

Why policy objects shall not be included at domain level ?

Administrative Users

How to create administrative user ?

List of Access given to admin users ?

AppLocker

When and how to use AppLocker ?

AppLocker

AppLocker is capable of blocking different file types. The following are the types of files AppLocker is capable of blocking.

- Executable files like .exe, .com
- Windows installer files like .mst, .msi and .msp
- Executable files like .bat, .ps1, .cmd, .js and .vbs
- DLL executables
- Packaged app installers like .appx

AppLocker

AppLocker can help you:

- Define rules based on file attributes that persist across app updates, such as the publisher name (derived from the digital signature), product name, file name, and file version. You can also create rules based on the file path and hash.

- Assign a rule to a security group or an individual user.
- Create exceptions to rules. For example, you can create a rule that allows all users to run all Windows binaries, except the Registry Editor (regedit.exe).
- Use audit-only mode to deploy the policy and understand its impact before enforcing it.
- Create rules on a staging server, test them, then export them to your production environment and import them into a Group Policy Object.
- Simplify creating and managing AppLocker rules by using Windows PowerShell.

User Account Control

User Account Control (UAC) helps prevent malware from damaging a PC and helps organizations deploy a better-managed desktop. With UAC, apps and tasks always run in the security context of a non-administrator account, unless an administrator specifically authorizes administrator-level access to the system. UAC can block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings.

Checking Recommended GPO settings (template-1)

- Moderating Access to Control Panel
- Prevent Windows from Storing LAN Manager Hash
- Control Access to Command Prompt
- Disable Forced System Restarts
- Disallow Removable Media Drives, DVDs, CDs, and Floppy Drives
- Restrict Software Installations
- Disable Guest Account
- Set Minimum Password Length to Higher Limits
- Set Maximum Password Age to Lower Limits
- Disable Anonymous SID Enumeration

https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches/

Checking Recommended GPO settings (template-2)

- Application Control (AppLocker)
- Manage Windows Update
- Disable SMBv1 Client and Server
- Disable Guest Account and Local Administrator Accounts
- Deny Execute Access on Removable Disks
- Prevent Changes to Proxy Settings

Checking

Recommended GPO settings (template-3)

- Change the Admin Account Name
- Guest Account – Strict NO
- Leverage Fine-Grained Password Policies
- Password Expiration
- Don’t store LM password hash strings on disk
- Use Event Logs for Immediate Recognition of Security Breaches
- Wi-Fi Settings You Need to be Careful With
- User Account Control
- Restrict Sharing of Account Information with Apps

Checking

Recommended GPO settings (template-4)

- Turn off forced restarts
- Make sure access to command prompt is restricted
- Turn off the LM hash storage
- Choose who can access your control panel
- Do not allow removable media drives
- Disable any software installations
- OneDrive – how to deal with it
- Control Windows Update
- Switching Windows Defender off
- Disabling automatic driver updates on your system

GPO settings

(password policies)

- Apply Minimum Password Age policy
- Passwords Must Meet Complexity Requirements policy
- Minimum Password Length policy

Reference: https://linfordco.com/blog/nist-password-policy-guidelines/

Account Lockout Policy

What is Windows Account Lockout Policy?

Windows Account lockout policy is a built-in security policy for Windows which will allow you to determine when and how long your user account should be locked out. This can be configured from the local security policy of the computer if it's not restricted by the network admin or in the Group Policy Management Console by the network administrator.

Account Lockout Policy

How does Account Lockout Policy helps curb security threats?

To protect your computer from unauthorized use, Windows 10/8/7 provides a facility to protect it using Account Lockout policies. A malicious threat actor may try to guess your Windows account password using a trial and error method, known as the Brute Force attack. To prevent him from succeeding in his attempts, you can use Account Lockout Policies to restrict the number of invalid logon attempts, which when exceeded would disable the account for a specified period to delay further attempts.

Account Lockout

Policy

Components of Account Lockout Policy:

Account Lockout Policy comprises of three security settings.

Account lockout threshold: Account lockout threshold allows you to set the number of failed logon attempts after which the user account should be locked out. Learn more.

Account lockout duration: Account lockout duration allows you to set the number of minutes the account should be locked out after the account lockout is triggered. Learn more.

Reset Account lockout counter after: The "Reset account lockout counter after" setting allows you to set the duration that must elapse from the first failed login attempt for the failed logon attempt counter to reset to 0.

Account Lockout

Policy

Location for configuring Account Lockout policy

Security Options (windows)

The Security Options contain the following groupings of security policy settings that allow you to configure the behavior of the local computer. Some of these policies can be included in a Group Policy Object and distributed over your organization.

Following windows security features can be enabled to retain windows security:

Security Options (windows)

- Virus & threat protection
- Account protection
- Firewall & network protection
- App & browser control
- Device security
- Device performance & health
- Family options

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/security-policy-settings

Internet Explorer security

Why Internet Explorer Users Are Vulnerable to Cyber Attacks?

In this lesson, you will learn how the **SmartScreen Filter**, **Security Report**, and **InPrivate Filtering** help protect you while browsing. We will also review **additional Internet Options** you may wish to set, including **Content Controls, Pop-up Blockers, and AutoComplete settings**. In addition, you will learn about **InPrivate Browsing**.

https://edu.gcfglobal.org/en/internetexplorer/security-and-privacy-/1/

Internet Explorer security

Compare IE 11 Vs Ms Edge/ Mozilla firefox/chrome

Miscellaneous Administrative Templates

C

Miscellaneous Administrative Templates

- Microsoft has published the administrative templates for Windows 10
- Professional versions of Windows 10 come with a set of policies that administrators may

configure using the Group Policy Editor.

- These templates **install additional policies on Windows 10 devices**.
- The templates (admx) are available for several languages including English, Russian, German, French, Spanish, Chinese, Portuguese and Polish.

Where to find templates and what it does ?

Miscellaneous Administrative Templates

Determines the minimum password length for which password length audit warning events are issued.

Local Computer Policy > Computer

Configuration > Windows Settings > Security Settings > Account Policies > Password Policy > Minimum Password Length Audit

Defines if the minimum password length setting can be increased beyond the legacy limit of 14.

Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy > Relax minimum password length limits

Miscellaneous Administrative Templates

This policy setting allows you to control whether users can sign in using external security keys.

Local Computer Policy > Computer Configuration > Administrative Templates >

System > Logon > Turn on security key sign-in

Specifies whether applications may access the movement of a user's head, hands, motion controllers, and other tracked objects, while they runs in the background.

Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows Components > App Privacy > Let Windows apps access user movements while running in the background

Miscellaneous Administrative Templates

Prevent the installation of packaged Windows apps by non-administrators.

Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows Components

> App Package Deployment > Prevent non-admin users from installing packaged Windows apps

Set the maximum foreground download bandwidth that the device can use across all concurrent download activities using Delivery Optimization.

Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Delivery Optimization > Maximum Foreground Download Bandwidth in KB/s

Miscellaneous Administrative Templates

Set the maximum background download bandwidth that the device can use across all concurrent download activities using

Delivery Optimization.

Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Delivery Optimization > Maximum Background Download Bandwidth in KB/s

Specifies how clients discover Delivery Optimization in Network Cache servers dynamically. Options are 1=DHCP Option 235, 2=DHCP Option 235 Force.

Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Delivery Optimization > Cache Server Hostname Source

Miscellaneous Administrative Templates

Define which version of Chromium Edge is going to used for opening redirected sites.

Local Computer Policy > Computer

Configuration > Administrative Templates > Windows Components > Internet Explorer > Configure which channel of Microsoft Edge to use for opening redirected sites

Microsoft Defender will compute hash values for files it scans if enabled.

Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows Components > Microsoft Defender Antivirus > MpEngine > Enable file hash for computation feature

Miscellaneous Administrative Templates

Microsoft removed five policies in the new administrative templates:

- Delivery Optimization > Max Upload Bandwidth (in KB/s)
- Delivery Optimization > Maximum Download Bandwidth (in KB/s)
- Delivery Optimization > Maximum Download Bandwidth (percentage)
- Windows Defender Application Guard > Allow users to trust files that open in Windows Defender Application Guard
- Windows Defender Application Guard > Configure additional sources for untrusted files in Windows Defender Application Guard

Other Settings in windows

M