Lab 8
Implement Access Control Systems and Compliance

**Identify and authenticate access to system components:**

**Summary:**

The ability to identify individual users not only ensures that system access is limited to those with the proper authorization; it also establishes an audit trail that can be analyzed following an incident. Documented policies and procedures must therefore be implemented to ensure proper user identification management for non-consumer users and administrators on all system components. All users must be assigned a unique ID, which must be managed according to specific guidelines. Controlled user authentication management (e.g. the use of passwords, smart cards or biometrics) should also be implemented and, as three-quarters of all network intrusions exploited weak or stolen passwords, 2FA (two-factor authentication) must be used for remote network access.
Lab Setup:

Our goal here is to test if the current security policies in place on our Windows machines match up with a security policy that is predetermined by our organization. In the case of this lab we are going to check our password policies against Microsoft's recommended best practices (We could however generate a test policy of our own design and use that as our source of security best practices). We are going to be using the “Microsoft Security Compliance Toolkit” for this job.

PCI_DSS Mapping:

8.2.3 Passwords/phrases must meet the following:
• Require a minimum length of at least seven characters.
• Contain both numeric and alphabetic characters.
Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.
8.2.4 Change user passwords/passphrases at least every 90 days.
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.
Microsoft Security Compliance Toolkit

Policy Analyzer is a utility for analyzing and comparing sets of Group Policy Objects (GPOs). It can highlight when a set of Group Policies has redundant settings or internal inconsistencies, and can highlight the differences between versions or sets of Group Policies. It can also compare GPOs against current local policy settings and against local registry settings. And you can export its findings to a Microsoft Excel spreadsheet.

Policy Analyzer lets you treat a set of GPOs as a single unit. This makes it easy to determine whether particular settings are duplicated across the GPOs or are set to conflicting values. It also lets you capture a baseline and then compare it to a snapshot taken at a later time to identify changes anywhere across the set.

For example, the US Government Configuration Baseline (USGCB) for Windows 7 includes seven different GPOs. Policy Analyzer can treat them as a single set, and show all the differences between them and the Microsoft recommended baselines for Windows 10 and Internet Explorer 11 with a single comparison. You can also use it to verify changes that were made to your production GPOs.
Audit:

Policy options we need to confirm:

The policy we are going to confirm for this lab involves ensuring that all machines are enforcing password best practices. In this case we can not use Kibana to check for live changes in the log files. Rather we need to apply another tool that can compare a set of known good static values against our current static “Local Security Policy” settings. As you will see the tool allows us to view all of the settings involved in setting up security policies and compare them against a defined policy file but we will focus on just the password policy here. So what we will be looking at:

- Require a minimum length of at least seven characters.
  - MinimumPasswordLength $\geq 7$
- Contain both numeric and alphabetic characters.
  - PasswordComplexity = 1
- Change user passwords/passphrases at least every 90 days.
  - MaximumPasswordAge < 90
- Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.
  - PasswordHistorySize > 4

Note: These settings are not stored in the System registry like some of the other policy settings. These are stored in a binary format in:
- C:\Windows\security\database\secedit.sdb
Audit HowTo:

Step 1) Get the version information about the current OS you are running. We need this to select the correct “SamplePolicyRules” file for the next step. In the search bar enter “winver”.

![Windows Server 2016 Version](image)

Step 2) Open the “PolicyAnalyzer” folder on the desktop of the Server2016 Machine and select the “PolicyAnalyzer” Application.

![PolicyAnalyzer Folder](image)
Step 3)  
2. We want to check our current Local System Registry and Local Policy against the Sample policy so we need to select the checkboxes.  
3. Click the “View/Compare” button to see the results of the comparison.  
4. Just click “Run” each time it pops up (should be twice)
Step 4) Show the output comparing current “Local Policy” and “Local Registry” against the “MSFT-Win10-v1607-RS1-Srv2016.PolicyRules” settings. The settings that do not match will be highlighted in yellow. Note: For the purposes of this lab we are focused on analyzing a few settings we defined in “Policy options we need to confirm” above, so I have grayed out any of the settings we are not concerned with. In a real audit all of the yellow should be corrected if possible.

- Yellow = Conflicting settings
- Gray = Settings are absent
- White = Settings match or are not conflicting

Step 5) Go into the security policy editor and bring the settings into line with the policy and then rerun the test.

1. In the search bar “Local Security Policy”.
2. Edit the out of policy values.
ToDo:

It is important to make sure that you are logging key pieces of information that give you visibility into things that are happening in your infrastructure.

Apply what you have learned to bringing the “Logon/Logoff” “Audit Policy” into spec with the “MSFT-Win10-v1607-RS1-Srv2016.PolicyRules”.

Note: Audit policies are configured in the “Local Security Policy” tool under “Advanced Audit Policy Configuration”
References:

To configure:
Microsoft Security Compliance Toolkit 1.0

To get current version of Windows OS: