Lab 8

Implement Access Control Systems and Compliance

Identify and authenticate access to system components:

Summary:

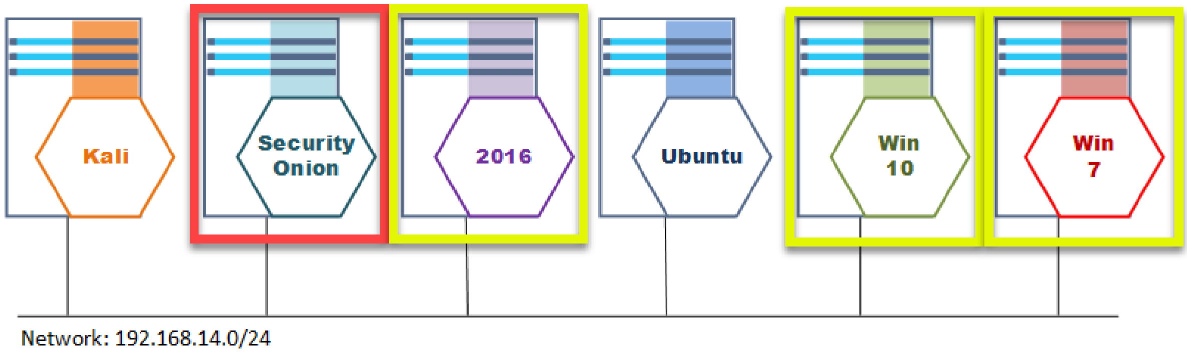
The ability to identify individual users not only ensures that system access is limited to those with the proper authorization; it also establishes an audit trail that can be analyzed following an incident. Documented policies and procedures must therefore be implemented to ensure proper user identification 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 out 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:

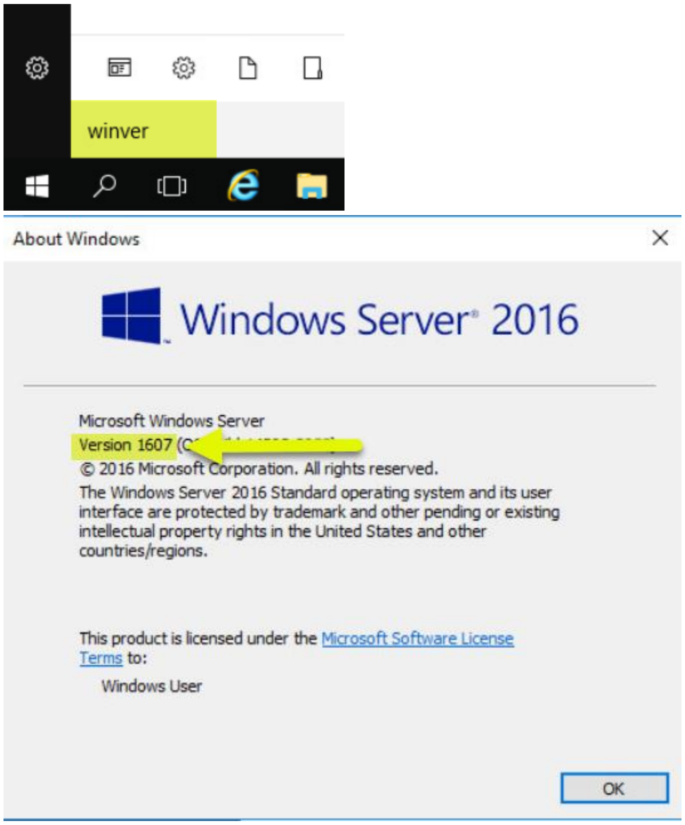
- Require a minimum length of at least seven characters.
  - **MinimumPasswordLength >= 7**
- Contain both numeric and alphabetic characters.
  - **PasswordComplexity = 1**
- Change user passwords/passphrases at least every 90 days.
  - **MaximumPasswordAge < 90**
- Do not allow an individual to submit 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:

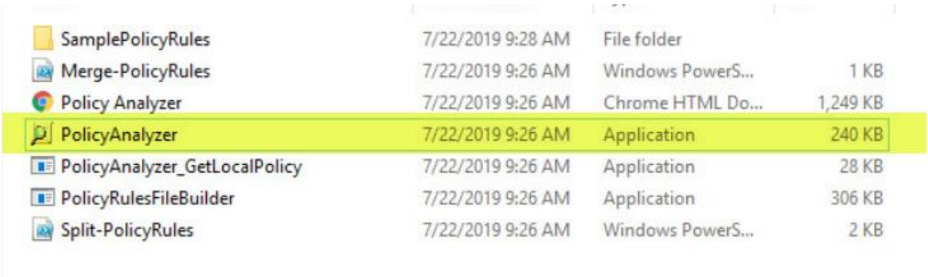
Step 1) Get the version information about the current OS you are running. We need this to select the correct “SamplePolicyRules” file for the next step. In the search bar enter “winver”.



Microsoft Windows Server
Version 1607 (O
© 2016 Microsoft Corporation. All rights reserved.
The Windows Server 2016 Standard operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the Microsoft Software License Terms to:
Windows User

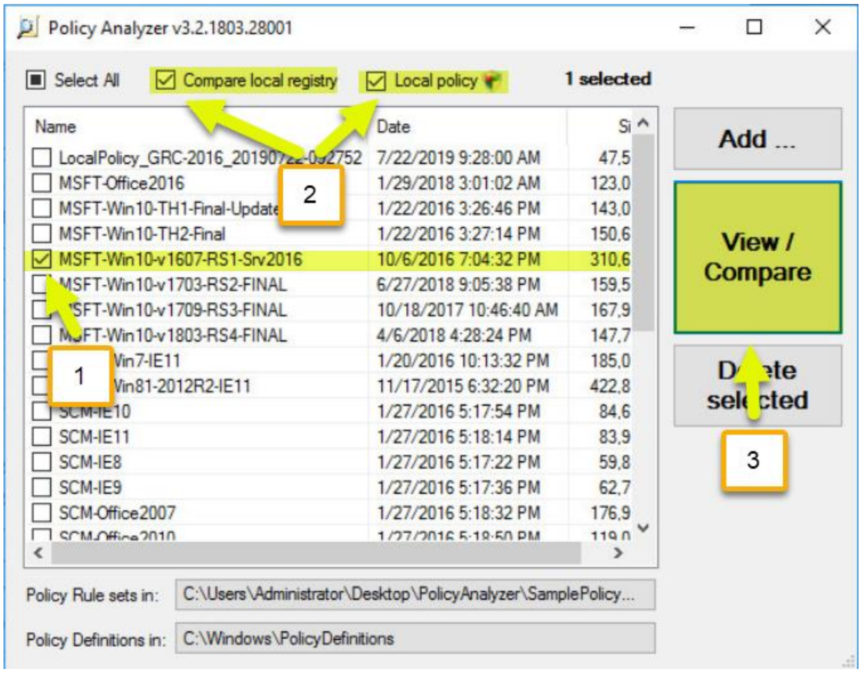
Step 2) Open the “PolicyAnalyzer” folder on the desktop of the Server2016 Machine and select the “PolicyAnalyzer” Application.



SamplePolicyRules	7/22/2019 9:28 AM	File folder	
Merge-PolicyRules	7/22/2019 9:26 AM	Windows PowerS...	1 KB
Policy Analyzer	7/22/2019 9:26 AM	Chrome HTML Do...	1,249 KB
PolicyAnalyzer	7/22/2019 9:26 AM	Application	240 KB
PolicyAnalyzer_GetLocalPolicy	7/22/2019 9:26 AM	Application	28 KB
PolicyRulesFileBuilder	7/22/2019 9:26 AM	Application	306 KB
Split-PolicyRules	7/22/2019 9:26 AM	Windows PowerS...	2 KB

Step 3)

1. Select the “SamplePolicyRules” file that lines up with your Operating System (in this case “MSFT-Win10-v1607-RS1-Srv2016.PolicyRules”).
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/Compair” button to see the results of the comparison.
4. Just click “Run” each time it pops up (should be twice)



Policy Analyzer v3.2.1803.28001

▣ Select All ☑ Compare local registry ☑ Local policy 1 selected

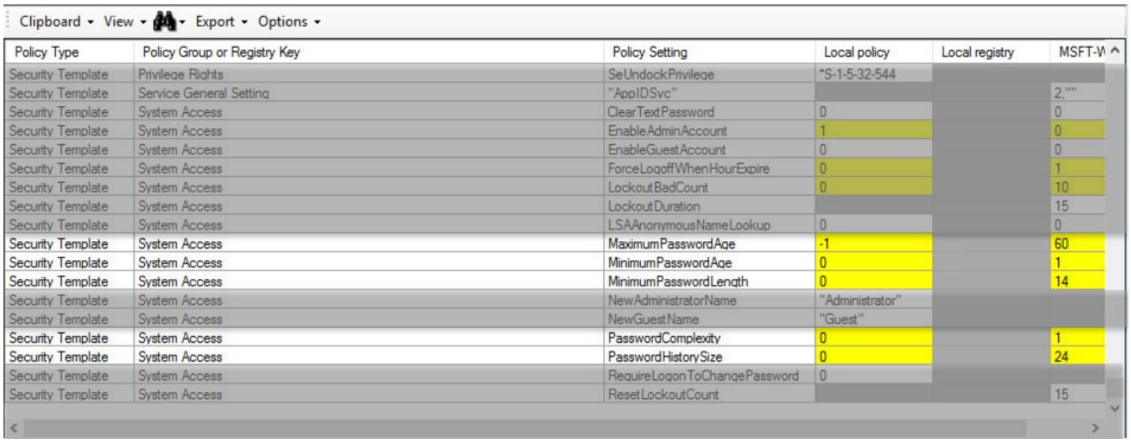
Name	Date	Si
□ LocalPolicy_GRC-2016_20190722-092752	7/22/2019 9:28:00 AM	47,5
□ MSFT-Office2016	1/29/2018 3:01:02 AM	123,0
□ MSFT-Win10-TH1-Final-Update	1/22/2016 3:26:46 PM	143,0
□ MSFT-Win10-TH2-Final	1/22/2016 3:27:14 PM	150,6
☑ MSFT-Win10-v1607-RS1-Srv2016	10/6/2016 7:04:32 PM	310,6
□ MSFT-Win10-v1703-RS2-FINAL	6/27/2018 9:05:38 PM	159,5
□ MSFT-Win10-v1709-RS3-FINAL	10/18/2017 10:46:40 AM	167,9
□ MSFT-Win10-v1803-RS4-FINAL	4/6/2018 4:28:24 PM	147,7
□ MSFT-Win7-IE11	1/20/2016 10:13:32 PM	185,0
□ MSFT-Win81-2012R2-IE11	11/17/2015 6:32:20 PM	422,8
□ SCM-IE10	1/27/2016 5:17:54 PM	84,6
□ SCM-IE11	1/27/2016 5:18:14 PM	83,9
□ SCM-IE8	1/27/2016 5:17:22 PM	59,8
□ SCM-IE9	1/27/2016 5:17:36 PM	62,7
□ SCM-Office2007	1/27/2016 5:18:32 PM	176,9
□ SCM-Office2010	1/27/2016 5:18:50 PM	119,0

Policy Rule sets in: C:\Users\Administrator\Desktop\PolicyAnalyzer\SamplePolicy...

Policy Definitions in: C:\Windows\PolicyDefinitions

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.

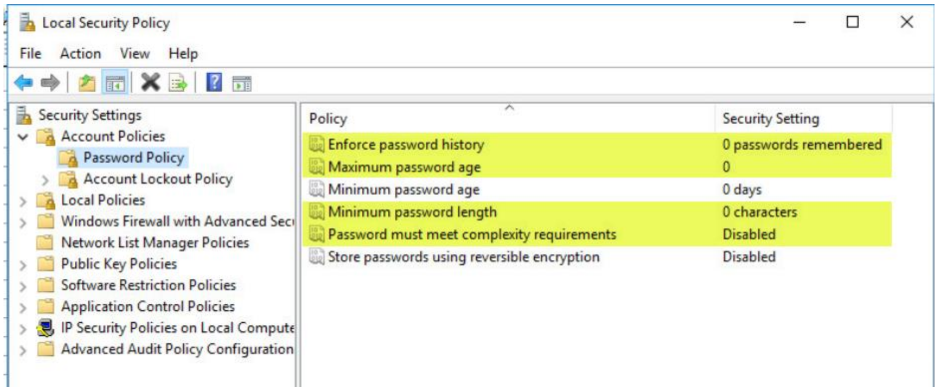
- Yellow = Conflicting settings
- Gray = Settings are absent
- White = Settings match or are not conflicting



Policy Type	Policy Group or Registry Key	Policy Setting	Local policy	Local registry	MSFT-W
Security Template	Privilege Rights	SeUndockPrivilege	*S-1-5-32-544		
Security Template	Service General Setting	"AppIDSvc"			2,""
Security Template	System Access	ClearTextPassword	0		0
Security Template	System Access	EnableAdminAccount	1		0
Security Template	System Access	EnableGuestAccount	0		0
Security Template	System Access	ForceLogoffWhenHourExpire	0		1
Security Template	System Access	LockoutBadCount	0		10
Security Template	System Access	LockoutDuration			15
Security Template	System Access	LSAAnonymousNameLookup	0		0
Security Template	System Access	MaximumPasswordAge	-1		60
Security Template	System Access	MinimumPasswordAge	0		1
Security Template	System Access	MinimumPasswordLength	0		14
Security Template	System Access	NewAdministratorName	"Administrator"		
Security Template	System Access	NewGuestName	"Guest"		
Security Template	System Access	PasswordComplexity	0		1
Security Template	System Access	PasswordHistorySize	0		24
Security Template	System Access	RequireLogonToChangePassword	0		
Security Template	System Access	ResetLockoutCount			15

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.

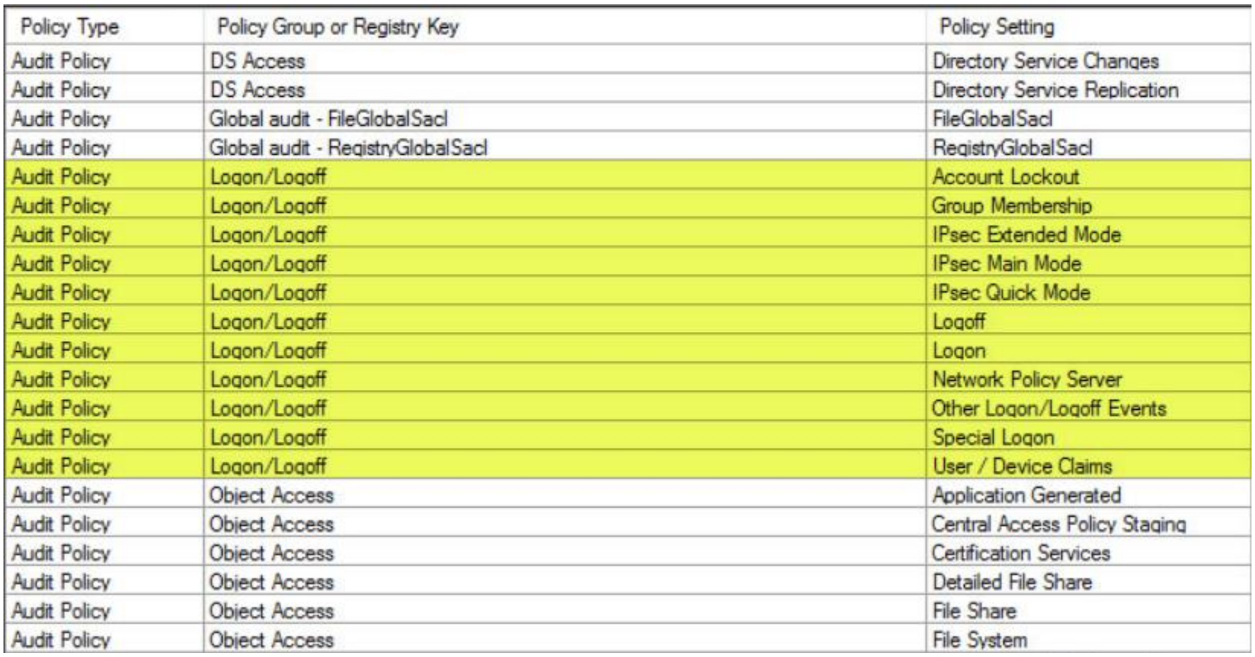

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

ToDo:

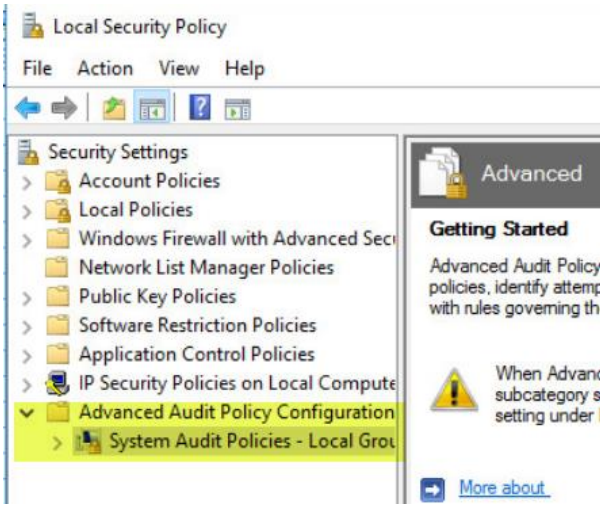
It is important to make sure that you are logging key pieces of information that give you visibility into things that are happening in your infrastructure.

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



Policy Type	Policy Group or Registry Key	Policy Setting
Audit Policy	DS Access	Directory Service Changes
Audit Policy	DS Access	Directory Service Replication
Audit Policy	Global audit - FileGlobalSacl	FileGlobalSacl
Audit Policy	Global audit - RegistryGlobalSacl	RegistryGlobalSacl
Audit Policy	Logon/Logoff	Account Lockout
Audit Policy	Logon/Logoff	Group Membership
Audit Policy	Logon/Logoff	IPsec Extended Mode
Audit Policy	Logon/Logoff	IPsec Main Mode
Audit Policy	Logon/Logoff	IPsec Quick Mode
Audit Policy	Logon/Logoff	Logoff
Audit Policy	Logon/Logoff	Logon
Audit Policy	Logon/Logoff	Network Policy Server
Audit Policy	Logon/Logoff	Other Logon/Logoff Events
Audit Policy	Logon/Logoff	Special Logon
Audit Policy	Logon/Logoff	User / Device Claims
Audit Policy	Object Access	Application Generated
Audit Policy	Object Access	Central Access Policy Staging
Audit Policy	Object Access	Certification Services
Audit Policy	Object Access	Detailed File Share
Audit Policy	Object Access	File Share
Audit Policy	Object Access	File System

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


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
System Audit Policies - Local Grou
Advanced
Getting Started
More about

Advanced Audit Policy
policies, identify attemp
with rules governing th

When Advanc
subcategory s
setting under

References:

To configure:
Microsoft Security Compliance Toolkit 1.0
https://blogs.technet.microsoft.com/secguide/2016/01/22/new-tool-policy-analyzer/

To get current version of Windows OS: