



Hardening TTC6050-3004

Lab 2: Windows 11 Hardening

Michael Herman

Toni Peltola

Karri Päivärinta

Project report

Instructor: Jarmo Viinikanoja

Return date: 6.9.2023

Group: TIC21S1

Contents

1	Introduction	4
2	Theoretical background	5
2.1	Security Baselines.....	5
2.2	Group Policy Objects.....	5
2.3	Policy modification.....	6
2.4	Security policy management.....	7
2.4.1	Access control.....	7
2.4.2	Script execution permissions.....	7
2.5	General policy management.....	8
2.5.1	Installation privileges.....	8
2.5.2	File-sharing.....	8
2.6	Advantages of central management.....	9
3	Environment.....	9
3.1	Initial status.....	10
3.2	Security Compliance Toolkit.....	11
3.2.1	Script execution.....	11
3.2.2	GPO creation.....	12
3.2.3	Updated workstation GPOs	13
4	Manual policy modification.....	14
4.1	Security-related modifications.....	14
4.1.1	Workstation access.....	14
4.1.2	Script execution permissions.....	15
4.2	General modifications.....	16
4.2.1	Installation permissions.....	16
4.2.2	Prevent file-sharing.....	16
4.2.3	Login message.....	17
5	Conclusion.....	18
6	Sources.....	20
7	Tools	22

Figures

Figure 1: Workflow.....	9
Figure 2: Preliminary analysis	10
Figure 3: Import scripts	11
Figure 4: New GPOs imported	12
Figure 5: Credential Guard	12
Figure 6: GPOs moved.....	13
Figure 7: Command execution and confirmation	13
Figure 8: Policy Viewer conflict	14
Figure 9: Restrict workstation access	14
Figure 10: Scripting permissions	15
Figure 11: Always install with escalated privileges disabled	16
Figure 12: Prevent file-sharing.....	17
Figure 13: Login text.....	17
Figure 14: Authorized users only	18

1 Introduction

This report examines the process of remotely hardening a Windows 11 workstation. Hardening is defined here as the process of modifying system configurations to render them more secure (Krause, 2018). It was performed using Windows Group Policy Editor. Configuration changes were implemented on the basis of recommendations from Microsoft's Security Baselines. The report examines both automated hardening using the Security Compliance Toolkit and manual hardening processes.

It begins with a theoretical discussion of the practical advantages of using baselines instead of ad hoc tinkering. It introduces the basic building block of the Windows network management system: the Group Policy Object (GPO). The report then examines how GPOs can be used in administrative tasks. A theoretical justification for the configuration changes made in the environment follows. The theoretical section concludes with a discussion of the practical advantages of centralized administration in Windows environments.

The practical section of the report demonstrates how policy modifications are made. Policies are adjusted using the Security Compliance Toolkit and Group Policy Management applications. Standardized changes are implemented using Microsoft baselines. Changes requiring non-standard policy states are implemented manually. Both security-related and general policies are modified. Manual policy modifications are made in both categories.

Policies are identified on the basis of criticality. Changes are made in areas in which smooth network operations are absolute requirements. Security-related changes tighten network access controls and script execution permissions. General changes concern installation privileges and file-sharing. These changes were implemented without strictly considering the security implications. There is nevertheless considerable overlap between the two categories.

There are clear security implications associated with loose controls in these areas. These are noted in the discussion. The login message was also modified. It is an unambiguously general policy with no meaningful security implications. The report concludes by highlighting the challenges faced and insights generated during the completion of the task.

2 Theoretical background

2.1 Security Baselines

Many organizations find it necessary to have precise control over their security configurations. Guidance on configuring various security features is frequently required owing to the abundance of security controls to manage (Microsoft 2023a). Microsoft provides an extensive range of baseline configuration capabilities for this reason. Such configurations are rigorously tested and widely recognized as industry-standard. They provide granular control over IT network environments.

Microsoft defines a security baseline as a collection of recommended configuration settings along with explanations of their security implications (2023b). The general aim is to provide a satisfactory level of security against common threats without extensive customization (CSRC, 2020). Implementing recommended settings removes the need for a time-consuming evaluation of configuration changes prior to their incorporation into a production environment. Appropriate values can be determined only after security implications are assessed. This would in most circumstances be highly labor-intensive (Moskowitz, 2019). Baselines are presented in accessible formats to facilitate rapid deployment and simplify the management process.

Baselines are organized according to the following principles:

- Tailored to have a strong emphasis on enterprise security. Relevant in scenarios where standard end users lack administrative privileges.
- Baselines enforce configuration settings only if they mitigate an established security risk and do not negatively affect business operations.
- Enforce default settings if there is a likelihood an authorized user might otherwise configure them to an insecure state.
 - Enforce the default if a non-administrator can set an insecure state.
 - Enforce the default if an administrator with administrative rights could potentially introduce an insecure state (Microsoft 2023a).

2.2 Group Policy Objects

A GPO is a virtual collection of policy settings. Group Policy settings are contained in a GPO. A GPO represents policy settings in the file system and in AD (Microsoft, 2018). Policy settings affect two distinct groups: computers and users. They can also affect both simultaneously. Computer-related settings take precedence over user-related settings. Policies associated with computers define

system behavior, application configurations, security parameters, assigned applications and startup and shutdown scripts. User-related policies govern system behavior, application settings, security configurations, assigned and published applications, user logon and logoff scripts and folder redirection (Simpkins, 2016).

Microsoft's security baselines can be implemented in production environments using the Security Compliance Toolkit. GPOs can then be employed to tailor these to specific security needs. They enable administrators to uniformly enforce security configurations. The centralized management approach efficiently controls access to critical resources and ensures consistency across networks (Lewis & Tammariello, 2016). It enables policies to be enforced on an automated basis. This reduces vulnerabilities and unauthorized access risks. Hardening GPO policies at the enterprise level promotes regulatory compliance and improves the overall security posture (Jillepalli et al., 2018).

GPOs facilitate efficient patch management and robust password policies. They can be deployed for comprehensive audit and logging. They play a pivotal role in safeguarding sensitive data. This is critical when detecting and responding to security incidents (Microsoft, 2023a). Customizing preexisting baselines may sometimes be necessary. Testing in a controlled environment is essential to ensure customization does not negatively impact system functionality (Moskowitz, 2012). Policies can then be linked to specific organizational units or user groups within the AD domain.

2.3 Policy modification

Policies are modified with the Group Policy Editor. Group Policy Editor is a management tool designed for system administrators. It is used to centrally configure and administer policies and settings across Windows-based computers in a networked environment. It empowers administrators to enforce security measures, deploy software, manage Windows Updates, customize user desktops and control various system settings (Arya, 2016). It offers extensive control and streamlines administrative tasks. Misconfigurations can produce unintended consequences for the network. The editor therefore requires careful handling (Bauer, Garriss, & Reiter, 2011). A solid grasp of policy settings and their implications is necessary to utilize the tool effectively.

2.4 Security policy management

2.4.1 Access control

A common group policy modification performed with the editor concerns access control. One such case is restricting network access to administrators only. This is in keeping with the principle of least privilege. There are compelling reasons to restrict network access to specific computers within a network environment. It can be done to isolate infected or compromised devices. It could also simply be to safeguard against unauthorized access or external attacks. Access restrictions ensure compliance with data protection regulations and enable efficient resource management (Arya, 2016).

Access controls can be used to control bandwidth usage, prioritize traffic and balance loads to maintain optimal network performance (Zang, Brody & Jajodia, 2006). They can be used to manage remote work systems and adhere to geographical restrictions. They can also facilitate testing and development. They can be used to prevent the unauthorized setup of services (Martin & Xie, 2007). It is also possible use access control to manage guest Wi-Fi usage. This makes it easier to fulfill statutory privacy requirements (Cheng et al., 2013). Such restrictions protect vulnerable systems by segregating guest networks and conserving resources. Access restrictions are critical during security incident responses.

2.4.2 Script execution permissions

Scripting permissions dictate who can run scripts and under what conditions. Disabling scripting for ordinary users in enterprise Windows environments is a widely-recommended best practice (Arya, 2016; Moskowitz, 2012; Niemimaa & Niemimaa, 2017). It is closely related to the principle of least privilege (Ma et al., 2011). The principle dictates individuals or processes should be granted the minimum level of access and permissions necessary to perform tasks effectively. Disabling scripting reduces the risk of users inadvertently running or downloading malicious scripts. It prevents unauthorized access to sensitive data and system resources and aligns with a wide range of statutory obligations (Chari et al., 2013).

Scripting languages often provide extensive control over system resources. Permission to run scripts should therefore be limited. Scripting environments should be strictly controlled and monitored

(Arya, 2016). This reduces the potential for system disruptions resulting from scripting-related errors. An array risks can be minimized by ensuring only qualified personnel have this capability. Disabling scripts reduces the attack surface, reduces the risk of security incidents and promotes system security (Moskowitz, 2012).

2.5 General policy management

2.5.1 Installation privileges

It is advisable to set the 'Always install with elevated privileges' group policy to *Disabled* in networked environments (Krause, 2018). Disabling this policy is desirable from both the security and administrative perspectives. The ability for software installations to occur with full administrative permissions introduces security risks associated with unauthorized or potentially malicious software installations.

Disabling this helps prevent malware from exploiting elevated privileges to infiltrate systems and maintains control over software installations. This will enhance both network security and compliance efforts (Moskovitz, 2012). Disabling this policy promotes system stability, minimizes compatibility issues and once again aligns with the principle of least privilege. This ensures software installations are a deliberate and controlled process rather than a default setting (Arya, 2016). This produces a more stable and well-managed network.

2.5.2 File-sharing

Enabling the 'Prevent users from sharing files within their profile' group policy is common practice in networked Windows environments (Kralicek, 2016). This also follows the least privilege principle. The policy helps safeguard sensitive data from unauthorized sharing or access within a user's profile (Arya, 2016). This is necessary to maintain data security as well as compliance with regulatory requirements. Mitigating the risk of malware distribution and unauthorized data exposure ensures better control over data flow. It channels file sharing through managed and monitored platforms while reducing the likelihood of inadvertent data leaks (Krause, 2018). The policy contributes to more effective data loss prevention and results in a more secure environment.

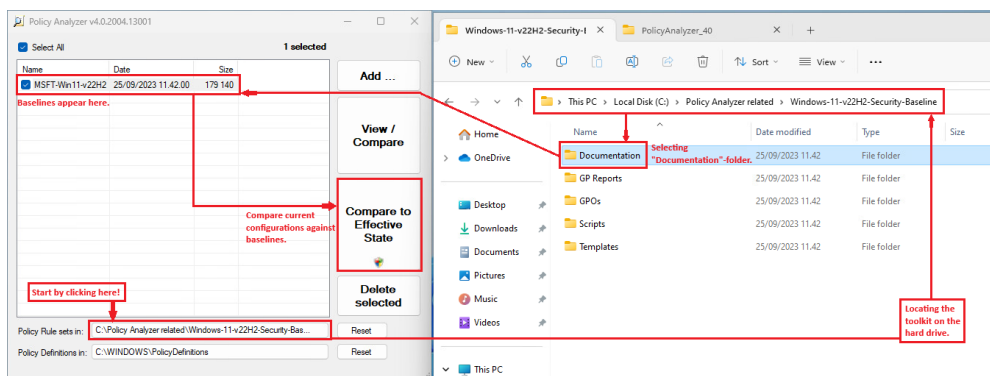
2.6 Advantages of central management

Group Policy provides a centralized and granular approach to managing a wide array of network elements. It has the capability to efficiently apply global changes to networks in all of the cases above. Central management promotes consistency in security settings and simplifies policy management in large-scale environments (Arya, 2016). Centrally managed networks are easier to monitor and audit. Doing so with Group Policy empowers administrators by introducing reversibility and version control to their network management suite (de Leon et al., 2018). This means no single failure can bring the network down. It also makes it easier to correct configuration errors. The benefits of such an approach are self-evident.

3 Environment

Hardening is performed on DC01. Changes would apply in principle to all machines located in WS-net. In this case the network is comprised of a single machine, WS01. Hardening is effectively directed at this machine alone. It is executed with the abovementioned theoretical considerations in mind. Policy configurations are verified and compared to security baselines using Microsoft's Policy Analyzer tool.¹ The workflow is illustrated in Figure 1.

Figure 1: Workflow



¹ The toolkit and baselines are downloadable at <https://www.microsoft.com/en-us/download/details.aspx?id=55319>

3.1 Initial status

Forty-four items are found in the initial comparison after conflicts are filtered out. Conflicts can be resolved with the toolkit's ready-made GPOs. It is first necessary to log in to the workstation in order to create a new domain administrator account. The account is used to apply and verify configuration changes after they take effect. It has been named *g3_domadmin*. It is necessary to log in to the new account before it can be used to make changes in the system. This will also serve to confirm if it is configured with appropriate administrative privileges.

Figure 2: Preliminary analysis

Policy Viewer - 44 items				
Clipboard View Export Options				
Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Audit Policy	Account Logon	Credential Validation	Success and Fail...	No Auditing
Audit Policy	Account Management	User Account Management	Success and Fail...	Success
Audit Policy	Detailed Tracking	PNP Activity	Success	No Auditing
Audit Policy	Detailed Tracking	Process Creation	Success	No Auditing
Audit Policy	Logon/Logoff	Account Lockout	Failure	Success
Audit Policy	Logon/Logoff	Group Membership	Success	No Auditing
Audit Policy	Logon/Logoff	Other Logon/Logoff Events	Success and Fail...	No Auditing
Audit Policy	Object Access	Detailed File Share	Failure	No Auditing
Audit Policy	Object Access	File Share	Success and Fail...	No Auditing
Audit Policy	Object Access	Other Object Access Events	Success and Fail...	No Auditing
Audit Policy	Object Access	Removable Storage	Success and Fail...	No Auditing
Audit Policy	Policy Change	MPSSVC Rule-Level Policy Change	Success and Fail...	No Auditing
Audit Policy	Policy Change	Other Policy Change Events	Failure	No Auditing
Audit Policy	Privilege Use	Sensitive Privilege Use	Success and Fail...	No Auditing
Audit Policy	System	Security System Extension	Success	No Auditing
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	ConsentPromptBehaviorAdmin	2	5
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	ConsentPromptBehaviorUser	0	3
HKLM	SYSTEM\CurrentControlSet\Control\Lsa	RestrictAnonymous	1	0
HKLM	System\CurrentControlSet\Control\Lsa\MSV1_0	NTLMMinClientSec	537395200	536870912
HKLM	System\CurrentControlSet\Control\Lsa\MSV1_0	NTLMMinServerSec	537395200	536870912
HKLM	SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	requiresecuritysignature	1	0
HKLM	System\CurrentControlSet\Services\LanmanWorkstation\Parameters	RequireSecuritySignature	1	0
HKLM	SYSTEM\CurrentControlSet\Services\Tcpip\Parameters	EnableICMPRedirect	0	1
Security Template	Privilege Rights	SeBackupPrivilege	*S-1-5-32-544	*S-1-5-32-544,*S-...
Security Template	Privilege Rights	SeCreateGlobalPrivilege	*S-1-5-19,*S-1-5-...	*S-1-5-19,*S-1-5-...
Security Template	Privilege Rights	SeDenyNetworkLogonRight	*S-1-5-113	Guest
Security Template	Privilege Rights	SeDenyRemoteInteractiveLogonR...	*S-1-5-113	*S-1-5-21-853918...
Security Template	Privilege Rights	SeInteractiveLogonRight	*S-1-5-32-544,*S-...	*S-1-5-32-544,*S-...
Security Template	Privilege Rights	SeNetworkLogonRight	*S-1-5-32-544,*S-...	*S-1-1-0,*S-1-5-3...
Security Template	Privilege Rights	SeRemoteShutdownPrivilege	*S-1-5-32-544	*S-1-5-21-853918...
Security Template	Privilege Rights	SeRestorePrivilege	*S-1-5-32-544	*S-1-5-32-544,*S-...
Security Template	Privilege Rights	SeSecurityPrivilege	*S-1-5-32-544	*S-1-5-21-853918...
Security Template	Privilege Rights	SeSystemEnvironmentPrivilege	*S-1-5-32-544	*S-1-5-21-853918...
Security Template	Privilege Rights	SeTakeOwnershipPrivilege	*S-1-5-32-544	*S-1-5-21-853918...
Security Template	Service General Setting	"XblAuthManager"	4,""	3,""
Security Template	Service General Setting	"XblGameSave"	4,""	3,""
Security Template	Service General Setting	"XboxGipSvc"	4,""	3,""
Security Template	Service General Setting	"XboxNetApiSvc"	4,""	3,""
Security Template	System Access	AllowAdministratorLockout	1	0
Security Template	System Access	LockoutBadCount	10	5
Security Template	System Access	LockoutDuration	10	15
Security Template	System Access	MinimumPasswordLength	14	7
Security Template	System Access	PasswordHistorySize	24	0
Security Template	System Access	ResetLockoutCount	10	15

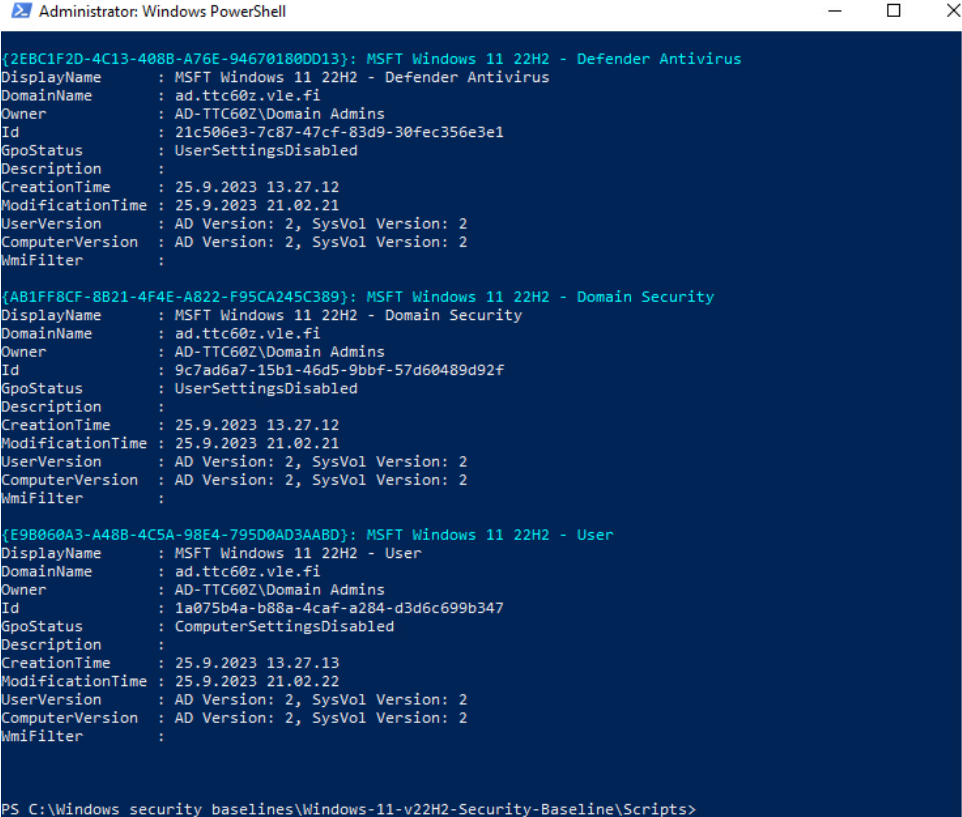
3.2 Security Compliance Toolkit

The Security Compliance Toolkit's baselines should be downloaded and extracted on the server. The most convenient way to do this was to install Firefox directly on DC01. It is not advisable to do this in a production environment. This would typically be done through a remote connection to the DC. The required files should be downloaded elsewhere and copied onto the machine (Arya, 2016). Here the Windows 11 Security Baselines are downloaded from the same location as WS01 and extracted on the server.

3.2.1 Script execution

The next step is to import the downloaded policies using PowerShell scripts in the pre-defined server location (`C:\Windows security baselines\Windows-11-v22H2-Security-Baseline\Scripts`). Script execution policy should be set to *ByPass* or they will not run. The policy was once again set to *Restricted* after the GPOs were imported. Figure 3 shows the three new GPOs.

Figure 3: Import scripts



```
Administrator: Windows PowerShell

{2EBC1F2D-4C13-408B-A76E-94670180DD13}: MSFT Windows 11 22H2 - Defender Antivirus
DisplayName      : MSFT Windows 11 22H2 - Defender Antivirus
DomainName       : ad.ttc60z.vle.fi
Owner            : AD-TTC60Z\Domain Admins
Id               : 21c506e3-7c87-47cf-83d9-30fec356e3e1
GpoStatus        : UserSettingsDisabled
Description       :
CreationTime     : 25.9.2023 13.27.12
ModificationTime : 25.9.2023 21.02.21
UserVersion      : AD Version: 2, SysVol Version: 2
ComputerVersion  : AD Version: 2, SysVol Version: 2
WmiFilter        :

{AB1FF8CF-8B21-4F4E-AB22-F95CA245C389}: MSFT Windows 11 22H2 - Domain Security
DisplayName      : MSFT Windows 11 22H2 - Domain Security
DomainName       : ad.ttc60z.vle.fi
Owner            : AD-TTC60Z\Domain Admins
Id               : 9c7ad6a7-15b1-46d5-9bbf-57d60489d92f
GpoStatus        : UserSettingsDisabled
Description       :
CreationTime     : 25.9.2023 13.27.12
ModificationTime : 25.9.2023 21.02.21
UserVersion      : AD Version: 2, SysVol Version: 2
ComputerVersion  : AD Version: 2, SysVol Version: 2
WmiFilter        :

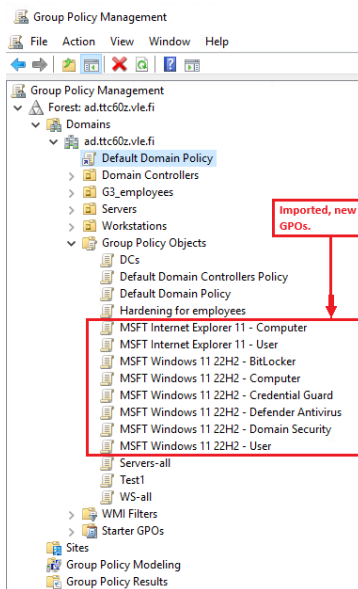
{E9B060A3-A48B-4C5A-98E4-795D0AD3AABD}: MSFT Windows 11 22H2 - User
DisplayName      : MSFT Windows 11 22H2 - User
DomainName       : ad.ttc60z.vle.fi
Owner            : AD-TTC60Z\Domain Admins
Id               : 1a075b4a-b88a-4caf-a284-d3d6c699b347
GpoStatus        : ComputerSettingsDisabled
Description       :
CreationTime     : 25.9.2023 13.27.13
ModificationTime : 25.9.2023 21.02.22
UserVersion      : AD Version: 2, SysVol Version: 2
ComputerVersion  : AD Version: 2, SysVol Version: 2
WmiFilter        :

PS C:\Windows security baselines\Windows-11-v22H2-Security-Baseline\Scripts>
```

3.2.2 GPO creation

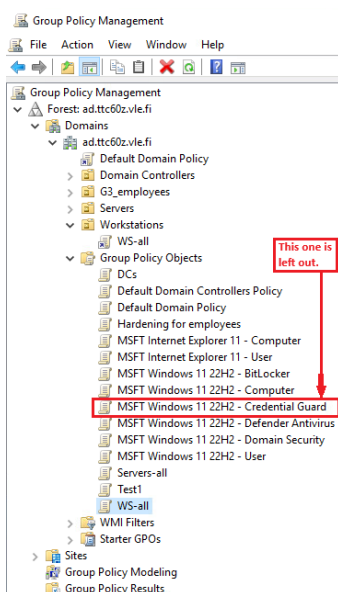
The new GPOs appear under Group Policy Objects in the Group Policy Management tool after refreshing the view (*Action -> Refresh*).

Figure 4: New GPOs imported



All new GPOs are now applied to workstations save one. The GPO in the image below does not work when applied through AD management. It appears to break the WS01 workstation unless applied locally. It was therefore removed.

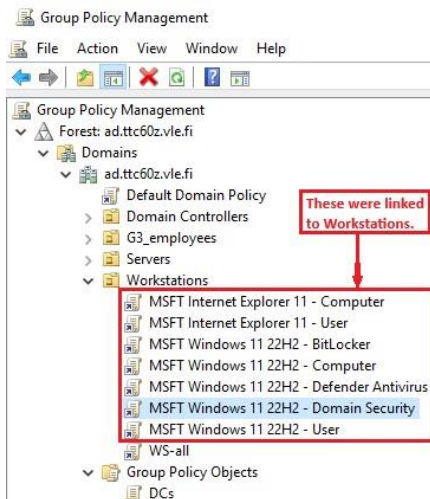
Figure 5: Credential Guard



3.2.3 Updated workstation GPOs

Figures 6 and 7 show the newly linked GPOs located in the Workstations repository. Figure 6 shows the updated policies on WS01 after being moved and linked to the Workstations repository.

Figure 6: GPOs moved



Policies are activated by logging in to WS01 and running the `gpupdate /force` command. The command execution and confirmation of success appear below.

Figure 7: Command execution and confirmation

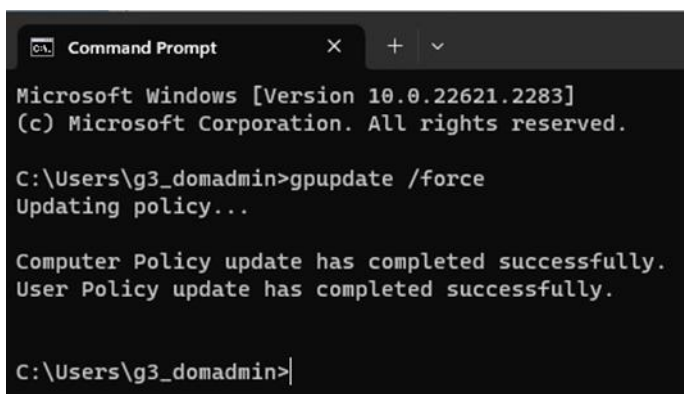


Figure 8 illustrates the changes after the new GPOs were updated and Policy Analyzer was run again. Only one conflict remains. This concerns administrator account lockout policy. The policy is disabled for security reasons. Few circumstances can be envisioned in which this would be desirable in the VLE. The policy cannot in any case be found on the server without running Windows updates. It has been added after the previous server update.

Figure 8: Policy Viewer conflict

Policy Viewer - 1 items				
Clipboard ▾ View ▾ Export ▾ Options ▾				
Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Security Template	System Access	AllowAdministratorLockout	1	0

4 Manual policy modification

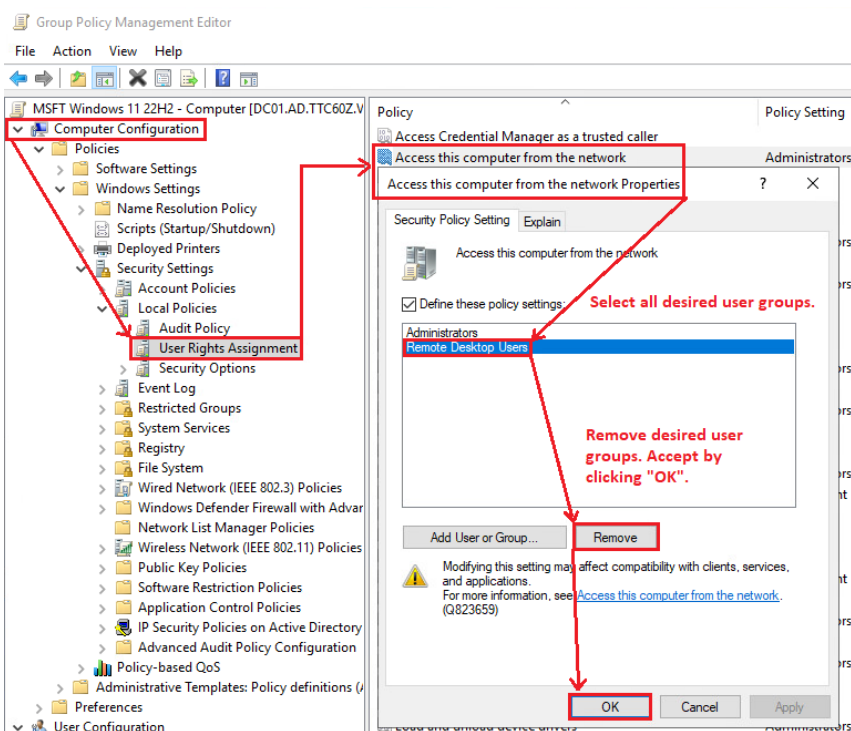
The Security Compliance Toolkit facilitates network configuration according to established baselines. This is in most cases the most desirable outcome. But manual modification of baselines may occasionally be necessary. Section 4 demonstrates how this can be approached.

4.1 Security-related modifications

The first example concerns network access. In this scenario a workstation should be accessible only to administrators. This requires all other user groups be removed from the policy. Changes can be made using the Group Policy Management Editor.

4.1.1 Workstation access

Figure 9: Restrict workstation access

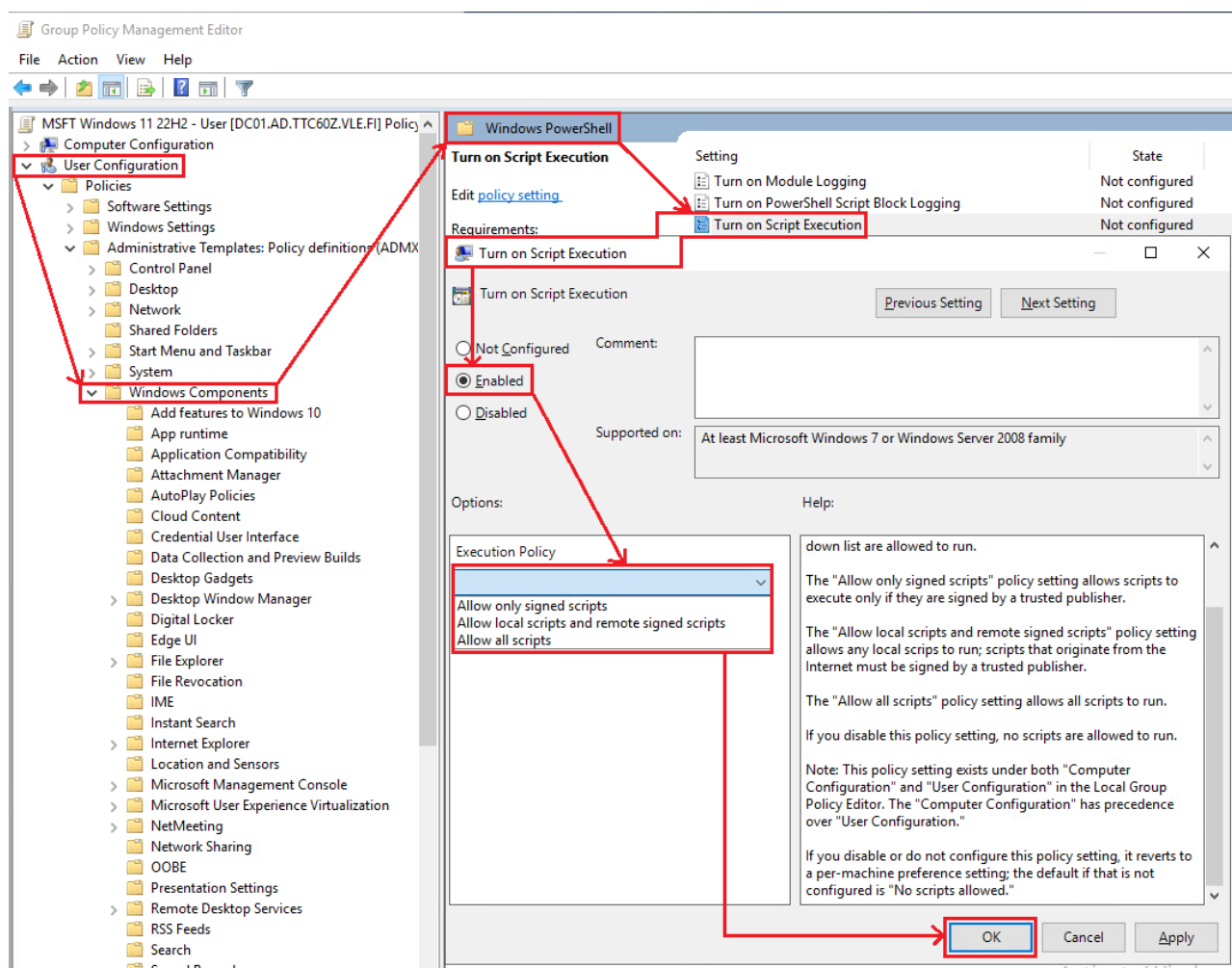


4.1.2 Script execution permissions

Scripting permissions can be modified in two places. The configuration is found in the *Computer Configuration* and *User Configuration* sections of the editor. Configurations in Computer Configurations take precedence over those in User Configuration.

Granting script execution permissions to ordinary users is widely considered bad practice. Administrators themselves may not need this privilege enabled at all times. Figure 10 illustrates where this configuration can be modified in any case. It is enabled for demonstration purposes only. The *Not Configured* state will be reverted to its default value. In this environment this is *No Scripts Allowed / Restricted*.

Figure 10: Scripting permissions



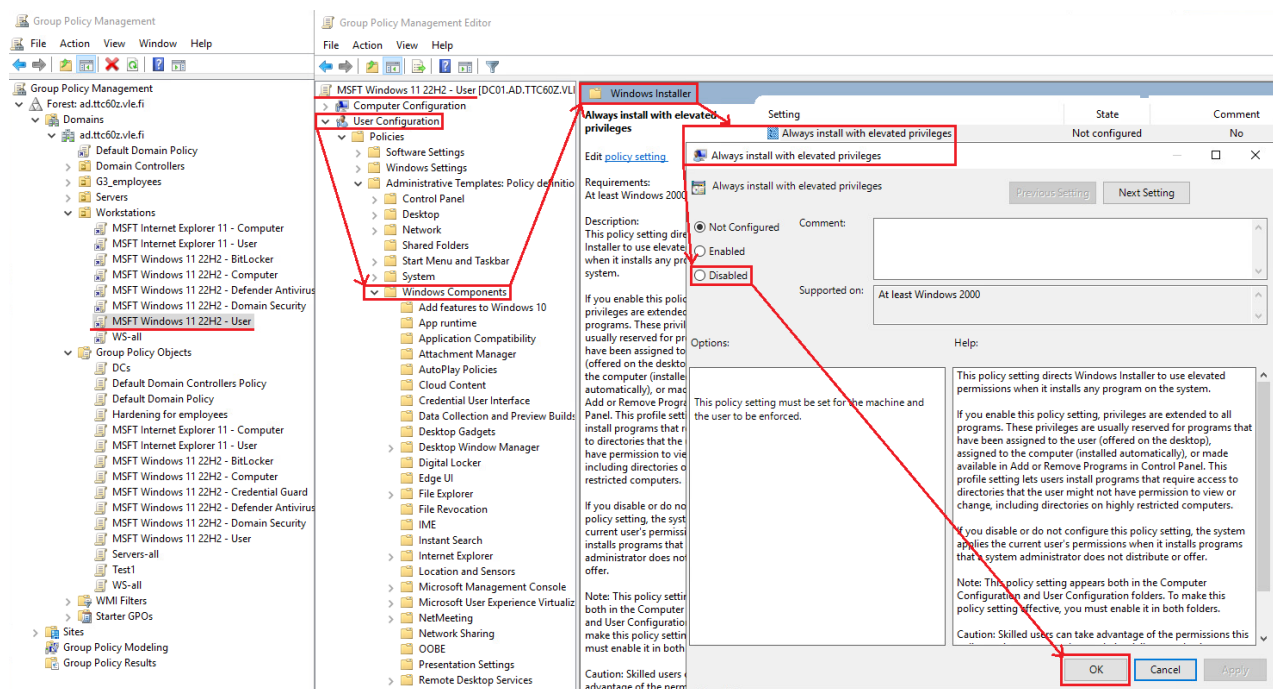
4.2 General modifications

The examples provided in this section fall outside the scope of the Security Compliance Toolkit. Hardening was performed using Group Policy Management tool as before. The examples below are taken from CIS benchmarks for Windows 11 (2023).

4.2.1 Installation permissions

Here 'Always install with elevated privileges' should be set to *Disabled*. This prevents Windows Installer installing programs with system permissions. Allowing programs to be installed with system privileges runs the risk of privilege escalation in case of a breach. The policy needs to be configured for both computer and user configurations to be enforced. The policy was disabled in Computer Configuration but not User Configuration. Figure 11 shows the steps taken to disable the policy for users.

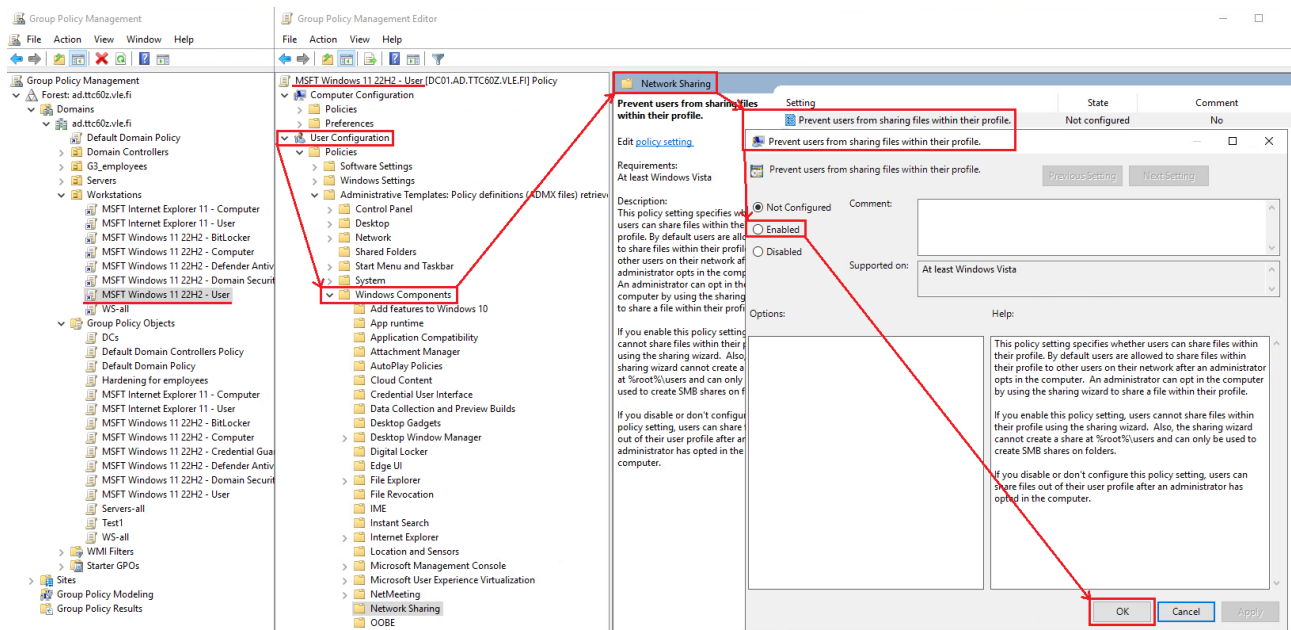
Figure 11: Always install with escalated privileges disabled



4.2.2 Prevent file-sharing

The second example concerns ensuring the 'Prevent users from sharing files within their profile' setting is enabled. Users can potentially share sensitive or malicious data by accident if this is not enabled. How to implement the policy is demonstrated below.

Figure 12: Prevent file-sharing



4.2.3 Login message

The final example is setting a login message. The message typically warns users their actions might be monitored. It can also be a general disclaimer. Another policy was required to be enabled for this to work correctly. The second policy sets a message title when users are trying to log on. Figure 12 illustrates this process.

Figure 13: Login text

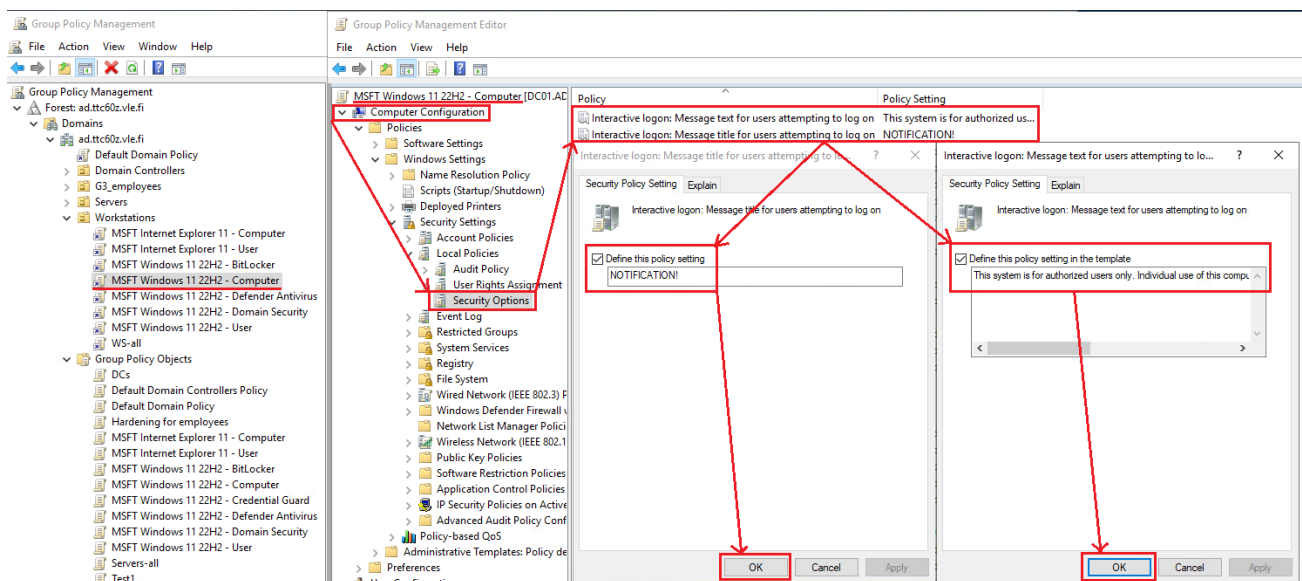
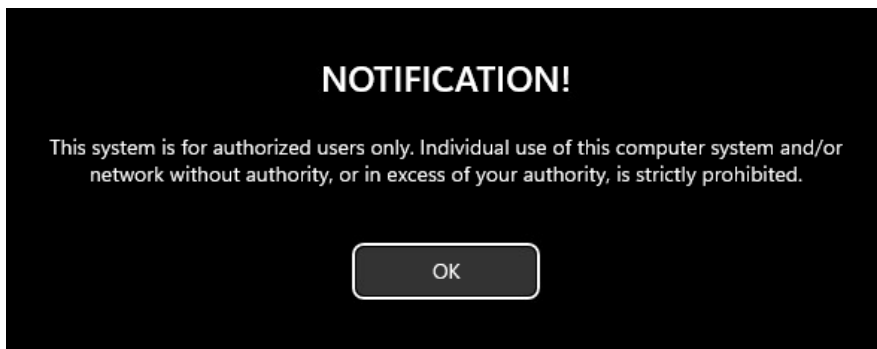


Figure 13 displays the message seen when logging on.

Figure 14: Authorized users only



5 Conclusion

The second lab built on the first lab. Hardening measures performed in the second lab were similar to previous efforts. The first lab was challenging primarily owing to a lack of experience. Having already gone through the trials and tribulations of learning the new system made this task easier. But there is still a lot to understand when it comes to navigating the tools, their menus and structure. Most of the hardening measures performed in this lab were from Microsoft's Security Compliance Toolkit. The GPOs linked to workstations were script-based and could be automatically applied. Less manual work was required than in the first lab.

Lab 2 required implementing hardening measures outside the Security Compliance Toolkit. CIS hardening benchmarks ended up being the source for these. CIS benchmark guides are extensive. The guides are relatively easy to read. Finding appropriate policies to harden nevertheless took time. Locating the relevant policies in the Group Policy Management Editor was frequently like searching for a needle in a haystack. Google and the benchmark guides were used extensively. This made the process somewhat manageable. But it was neither easy nor painless to find the relevant information using these methods.

Understanding and finding even remotely relevant hardening procedures / configurations was a challenge. The sheer number of configurations available in the Policy Management Editor was intimidating. Hardening measures by other means were excluded for practical reasons. The focus was instead on managing policies with the default tools. It was a conscious decision to perform

hardening measures using existing Security Compliance Toolkit GPOs. They were proven to work. Additional policies described in this report were added for demonstration purposes only. This was preferable to making custom GPOs given their potential to produce configuration problems down the road. Troubleshooting was still required in some cases.

Script-created GPOs frequently did not work as expected out of the box. This was mostly due to configuring a policy in the wrong GPO. This was a surprisingly easy mistake to make. Two policies had to be enabled for the disclaimer / notification text modification to display correctly. Relevant information was not found in Microsoft's official documentation. The solution was gleaned through testing and experimentation. An effort to find a list of intertwined policies lead nowhere. This would have been useful resource had it been available.

The lab was a lot of work. The group consensus is that the points allocated for the task were not commensurate with the time and effort required to complete it satisfactorily. But the result is a clear advancement of our knowledge of Windows AD, its hardening policies and how to apply them. Our ability to troubleshoot problems in Windows environments has also improved considerably. The choices faced were perhaps not as existential as those confronting Indiana Jones in the climactic final scene of *The Last Crusade*; we nevertheless believe our hardening measures were chosen wisely. They will be of clear relevance in a production environment. Regretfully our reward in this case will not be eternal life.

6 Sources

Arya, K. (2016). Managing Microsoft Office with Group Policy. In: *Windows Group Policy Troubleshooting: A Best Practice Guide for Managing Users and PCs Through Group Policy*. Springer, New York. https://doi.org/10.1007/978-1-4842-1886-0_4

Bauer, L., Garriss, S., & Reiter, M. K. (2011). Detecting and resolving policy misconfigurations in access-control systems. *ACM Transactions on Information and System Security (TISSEC)*, 14(1), 1-28. <https://doi.org/10.1145/1952982.1952984>

Cheng, N., Wang, X. O., Cheng, W., Mohapatra, P., & Seneviratne, A. (2013, April). Characterizing privacy leakage of public wifi networks for users on travel. In *2013 Proceedings IEEE INFOCOM* (pp. 2769-2777). IEEE. <https://doi.org/10.1109/INFCOM.2013.6567086>

Computer Security Resource Center. (2020). *Security and privacy controls for information systems and organizations*. National Institute of Standards and Technology. <https://doi.org/10.6028/nist.sp.800-53r5>

de Leon, D. C., Jillepalli, A. A., House, V. J., Alves-Foss, J., & Sheldon, F. T. (2018). Tutorials and laboratory for hands-on OS cybersecurity instruction. *Journal of Computing Sciences in Colleges*, 34(1), 242-254. Retrieved September 28, 2023, from https://www.researchgate.net/publication/327857881_Tutorials_and_laboratory_for_hands-on_OS_cybersecurity_instruction/link/607aefb78ea909241e0972cb/download

Jillepalli, A. A., de Leon, D. C., Sheldon, F. T., & Haney, M. A. (2018). Enterprise-level hardening of web browsers for Microsoft Windows. *International Journal of Computing and Digital Systems (IJCDS)*. <http://dx.doi.org/10.12785/ijcds/070501>

Kralicek, E. (2016). Directory Services and Central Account Management. In: *The Accidental SysAdmin Handbook*. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-1817-4_10

Krause, J. (2018). *Mastering Windows Group Policy: Control and secure your Active Directory environment with Group Policy*. Packt Publishing Ltd.

Lewis, C., & Tammariello, J. (2016). *Creating centralized reporting for Microsoft host protection technologies: The enhanced mitigation experience toolkit*. Retrieved September 27, 2023, from <https://apps.dtic.mil/sti/pdfs/AD1045014.pdf>

Ma, X., Li, R., Lu, Z., Lu, J., & Dong, M. (2011). Specifying and enforcing the principle of least privilege in role-based access control. *Concurrency and Computation: Practice and Experience*, 23(12), 1313-1331. <https://doi.org/10.1002/cpe.1731>

Martin, E., & Xie, T. (2007, May). A fault model and mutation testing of access control policies. In *Proceedings of the 16th international conference on World Wide Web* (pp. 667-676). <https://doi.org/10.1145/1242572.1242663>

Microsoft. (2018, May 31). *Group policy objects*. Microsoft Learn. Retrieved September 27, 2023, from <https://learn.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-objects>

Microsoft. (2022, September 20). *Windows 11, version 22H2 Security baseline*. Microsoft Security Baselines Blog. Retrieved September 27, 2023, from <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/windows-11-version-22h2-security-baseline/ba-p/3632520>

Microsoft. (2023a, March 3). *Securing privileged access overview*. Microsoft Learn. Retrieved September 27, 2023, from <https://learn.microsoft.com/en-us/security/privileged-access-workstations/overview>

Microsoft. (2023b, July 11). *Security baselines guide - Windows Security*. Microsoft Learn. Retrieved September 27, 2023, from <https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines>

Moskowitz, J. (2012). *Group Policy: Fundamentals, Security, and the Managed Desktop*. John Wiley & Sons.

Moskowitz, J. (2019). Security with Baselines, BitLocker, AppLocker, and Conditional Access. In: *MDM: Fundamentals, Security, and the Modern Desktop: Using Intune, Autopilot, and Azure to Manage, Deploy, and Secure Windows 10* (pp. 395–437). Wiley & Sons.

<https://doi.org/10.1002/9781119564362.ch10>

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European journal of information systems*, 26(1), 1-20. <https://doi.org/10.1057/s41303-016-0025-y>

Plachkinova, M., & Knapp, K. (2022). Least Privilege across People, Process, and Technology: Endpoint Security Framework. *Journal of Computer Information Systems*, 1-13.

<https://doi.org/10.1080/08874417.2022.2128937>

Simpkins, S. (2016). Group Policy. In: *Building a SharePoint 2016 Home Lab*. Apress, Berkeley, CA.

https://doi.org/10.1007/978-1-4842-2170-9_7

Zhang, L., Brodsky, A., & Jajodia, S. (2006, June). Toward information sharing: Benefit and risk access control (barac). In *Seventh IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'06)* (pp. 9-pp). IEEE. <https://doi.org/10.1109/POLICY.2006.36>

7 Tools

Center for Internet Security. (2023, April 14). *CIS Microsoft Windows Server 2019 Benchmark v2.0.0 - 04-14-2023*. National Institute of Standards and Technology.

<https://learn.cisecurity.org/l/799323/2023-04-05/4sv5vy>

Microsoft. (2023). *Microsoft Security Compliance Toolkit*. Microsoft.

<https://www.microsoft.com/en-us/download/details.aspx?id=55319>