**Security Hardening Report**

**Name: FMJ2**

**Date: 6/23/23**

Executive summary: The purpose of the security hardening reports is to outline the security measures implemented to strengthen the security system of Design World. This report provides an overview of the hardening activities performed, the reasoning behind each measure, and the expected impact on the system's security. It is intended for review and approval by the configuration control boards (CCB) So ensure compliance with the established security standards and guidelines.

**WINDOWS**

Microsoft Windows 10 STIG SCAP Benchmark :: Version 2, Release: 8 Benchmark Date: 11 May 2023

**CAT 1**

1. Data Execution Prevention (DEP) Configuration:

Finding ID: V-220726

STIG ID: WN 10-00-000145

Severity: High

A screenshot of a computer error

Description automatically generated with medium confidence

A blue screen with white text

Description automatically generated with low confidence

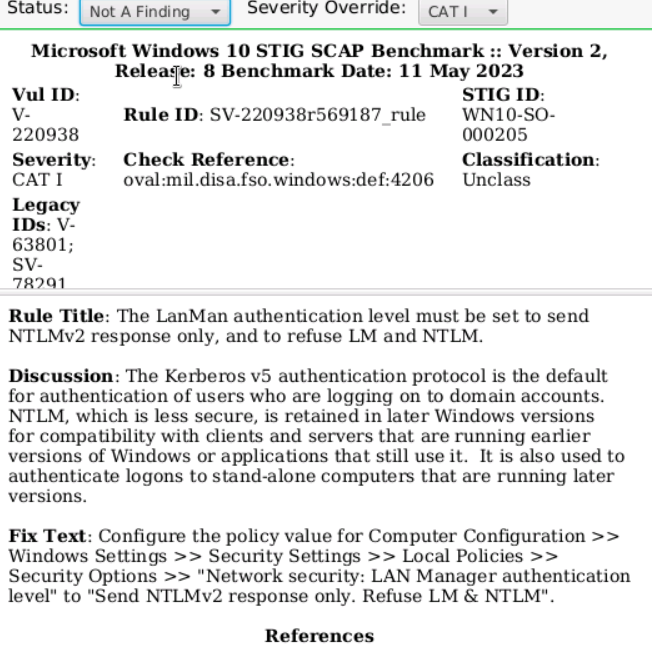
The following security hardening activity has been performed to address the Windows vulnerability related to (Data Execution Prevention) DEP configuration. DEP prevents harmful code from running and protects memory locations reserved for Windows and other programs. This vulnerability is considered CAT 1 and a high severity. To verify and configure the DEP setting, the following steps were taken: a command prompt was opened, and the following command was executed: “BCDEdit/ enum “current” to view the current DEP configuration. This verified that the value for “nx” was not “OptOut”, the necessary changes were made to set it to “OptOut”. This will prevent harmful code from running in memory locations reserved for Windows and other programs. This will also mitigate potential vulnerabilities and reduce the risk of code execution attacks or any attempts to exploit memory-based vulnerabilities.

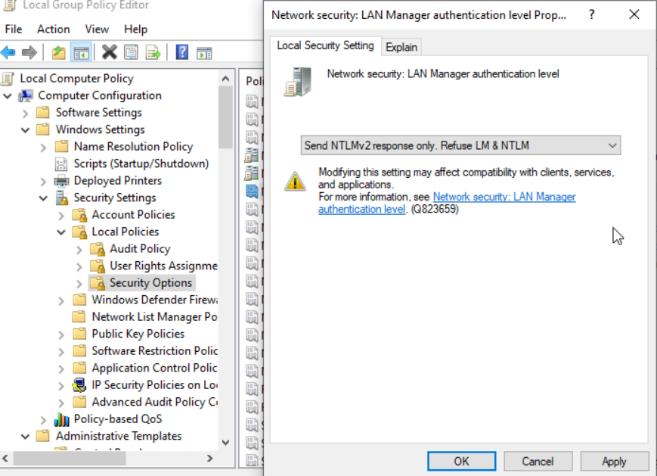
1. LanMan Authentication Level Configuration:

Finding ID: V-220938

STIG ID: WN10-S0-000205

Severity: High





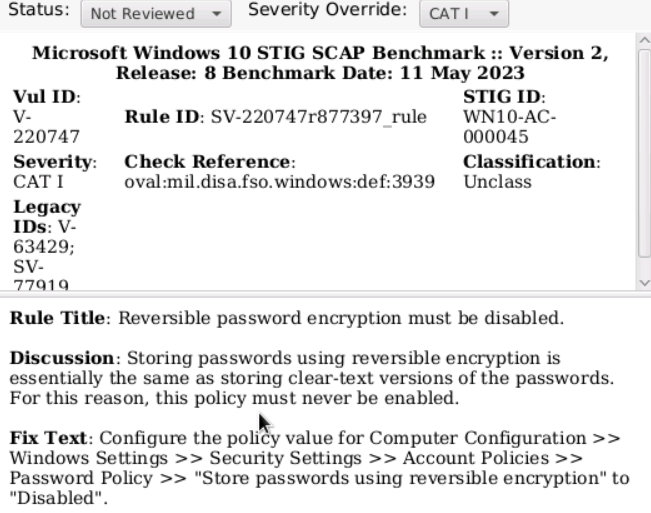
The following security hardening activity has been performed to address the Windows vulnerability related to the LanMAN authentication level, or NTLM. The NTLM is less secure and is retained in later Windows versions for compatibility with clients and servers that are running earlier versions of Windows or applications that still use it. It is also used to authenticate logons to standalone computers that are running later versions. LanMan authentication level must be set to send NTLMv2 response only and refuse LM and NTLM. To configure the LanMan authentication level, the following steps were taken: FMJ2 configured the policy value for computer configuration, Windows settings, security settings, local policies, security options, then navigated to “network security calling land manager authentication level” to “send NTLMv2 response only. Refuse LM and NTLM”. This one has the system security of the authentication process by sending NTLM V2 response only, while mitigating the risks associated with weak authentication protocols.

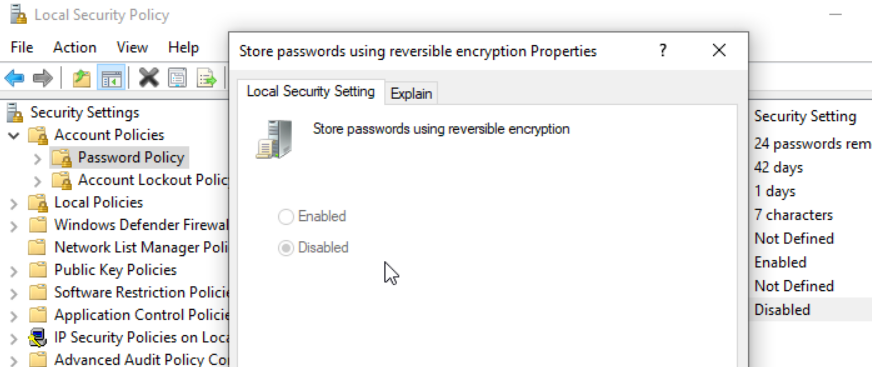
1. Reversible Password Encryption Configuration:

Finding ID: V-220747

STIG ID: WN 10-00-000045

Severity: High





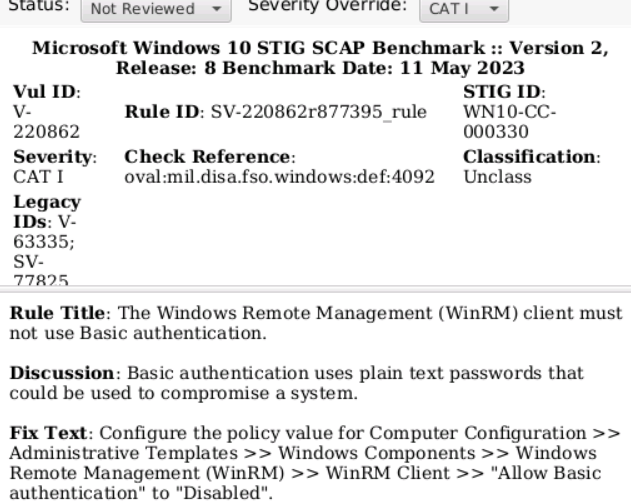
The following security hardening activity has been performed to address the windows vulnerability related to reversible password encryption. A vulnerability that is categorized as CAT 1 and the severity level is considered high. In short, storing passwords using reversible encryption is essentially the same as storing clear text versions of the passwords. For this reason, this policy must never be enabled. To configure reversible password encryption, the following steps were taken: we navigated to the local computer policy, computer configuration, Windows settings, security settings, account policies, and password policy. Then we verified the setting for “store password using reversible encryption”, configured the setting to “Disabled”. Implementing the reversible password encryption configuration will Prevent unauthorized access to clear text passwords in the event of a breach or unauthorized access to the password database.

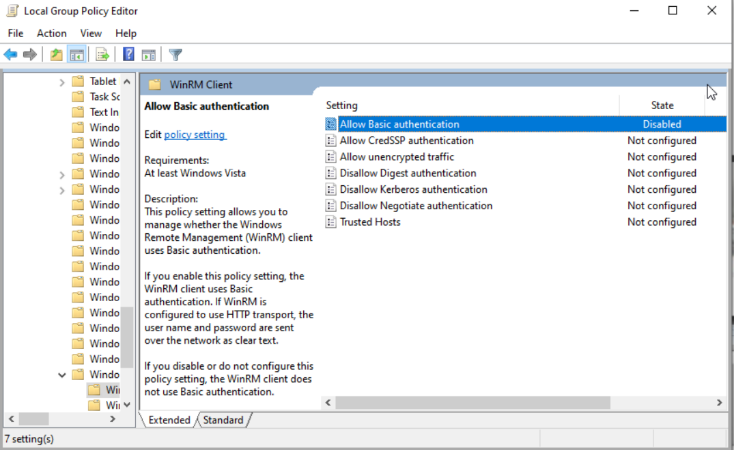
1. WinRm Client Basic Authentication Configuration:

Finding ID: V-220862

STIG ID: WN 10-CC-000330

Severity: High

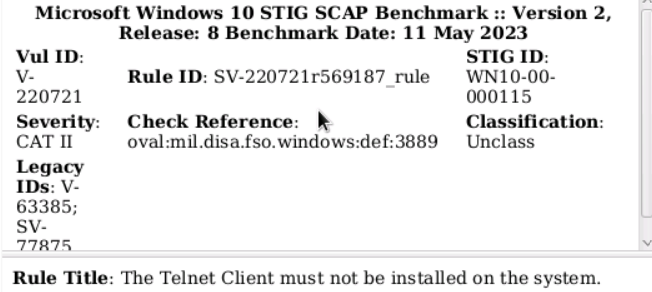


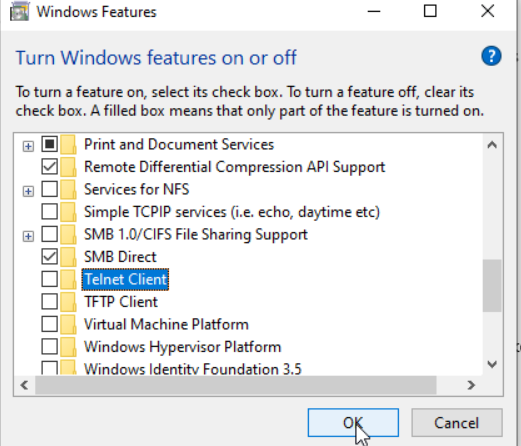


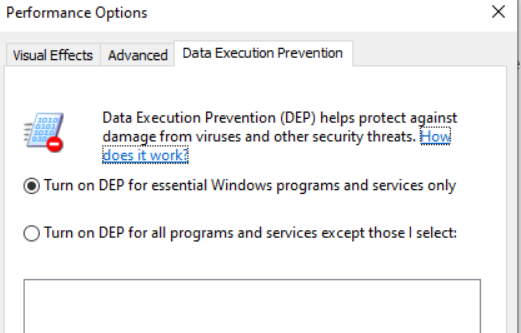
The following security hardening activity has been performed to address the Windows vulnerability related to the Windows Remote Management (WinRM) client’s usage of basic authentication. Basic authentication uses plaintext passwords that could be used to compromise the system. This is why it's important to disable basic authentication because it will reduce the risk of an attack. It is categorized as a CAT 1, and the severity level is considered high. To configure WinRM client basic authentication, the following steps were taken: FMJ2 navigated to computer configuration, administrative templates, Windows components, Windows remote management (WinRM), and finally WinRM Client. We then configure the policy value for “allow basic authentication” to “Disabled”. The rationale behind the configuration is to protect the security of the win RM client by disabling basic authentication, which uses plain text passwords. Mitigating this risk will prevent unauthorized access to the system using plaintext passwords.

**CAT 2**

1. STIG ID: WN 10-00-000115 & Vul ID: V-220721







The following security hardening activity has been performed to address the Windows vulnerability related to the telnet client. Unnecessary services like telnet increases the attack surface of a system. Some of these services may not support the required levels of authentication or encryption or may provide unauthorized access to the system. This is a vulnerability that is considered a CAT 2, and the severity level is deemed medium. To remove the tonic client, the following steps were taken: we navigated to the server manager, from the drop-down task list, setup we then selected the appropriate server on the server selection page and clicked next. Finally, “telnet client” was deselected on the features page.