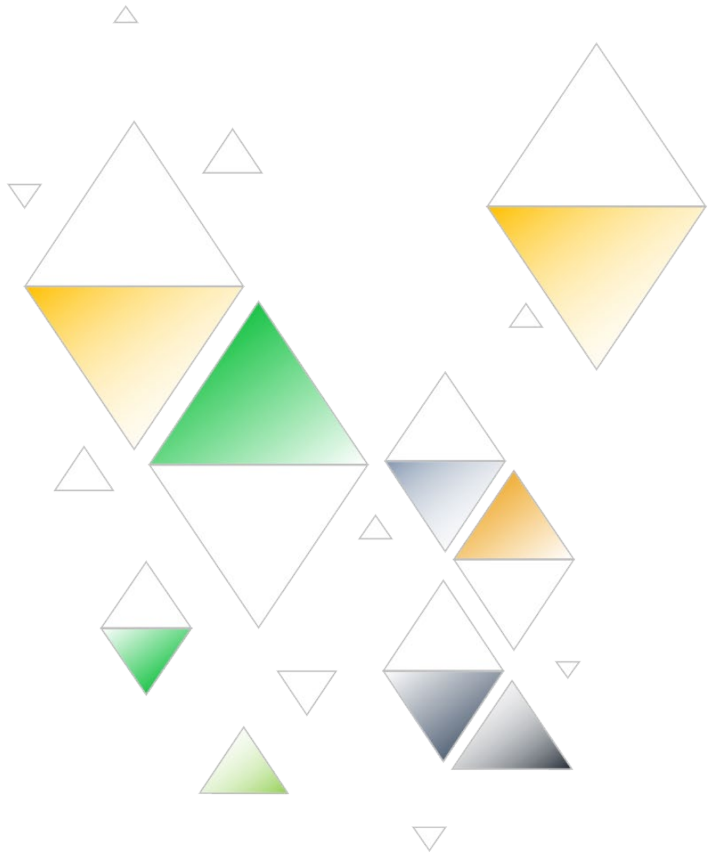
CIS-5017
Hands-on OS Hardening

EXECUTIVE REPORT

OMAR ALZUBAIR

04/29/2024



OVERVIEW

This executive report provides details of the OS hardening work done to address security vulnerabilities in our virtual machine environment. Focusing on the account security controls identified in the CIS Microsoft Windows 10 Benchmark, the report outlines the problem statement, security risks identified prior to implementation, solutions implemented to mitigate these risks, numerical findings, and conclusions.

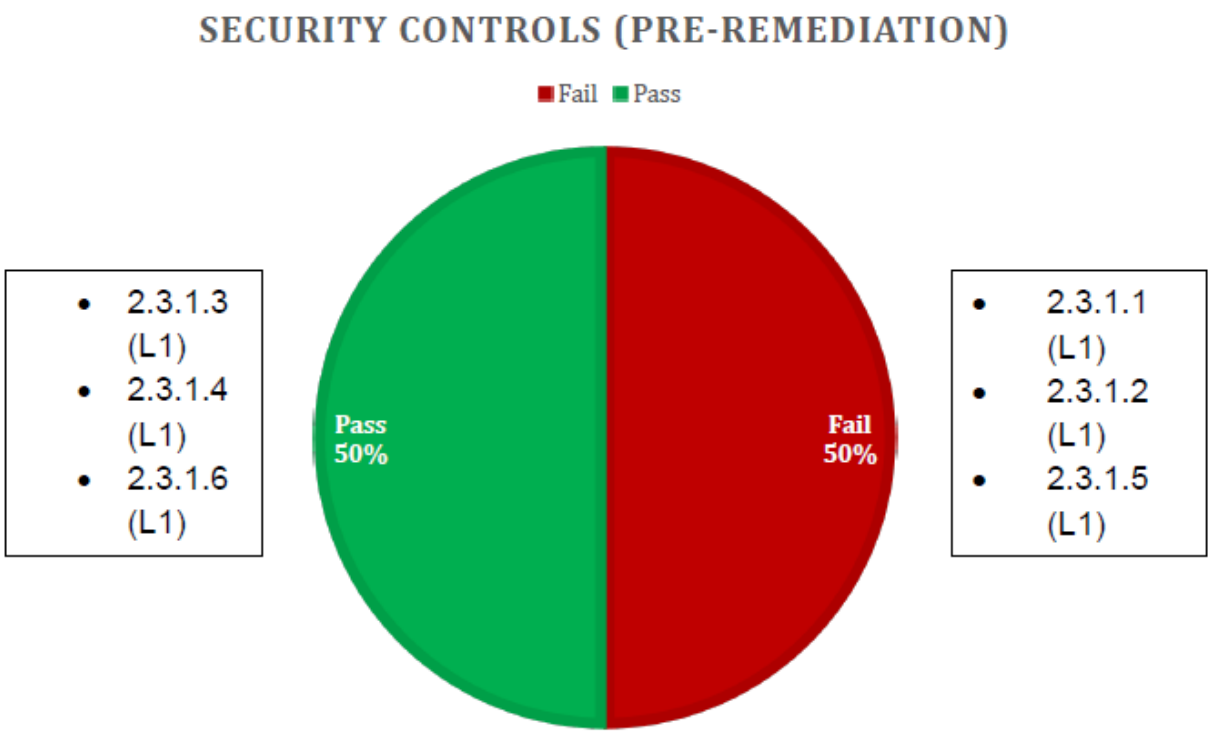
PROBLEM SUMMARY

The operating system (OS) of our virtual machines presented security vulnerabilities that needed addressing. I chose the Accounts Security Options Control to ensure that account security options are secure which helps protect against unauthorized access, mitigates the risk of various types of threats, ensures compliance with regulations such as NIST, and prevents privilege escalation. I discovered that on the virtual machine the Accounts security options were not sufficiently hardened according to the CIS Microsoft Windows 10 Benchmark. These vulnerabilities posed significant risks to the overall security posture of our systems.

SECURITY RISKS BEFORE IMPLEMENTATION:

Before implementing security controls, the OS exhibited vulnerabilities across various Accounts Security Options including:

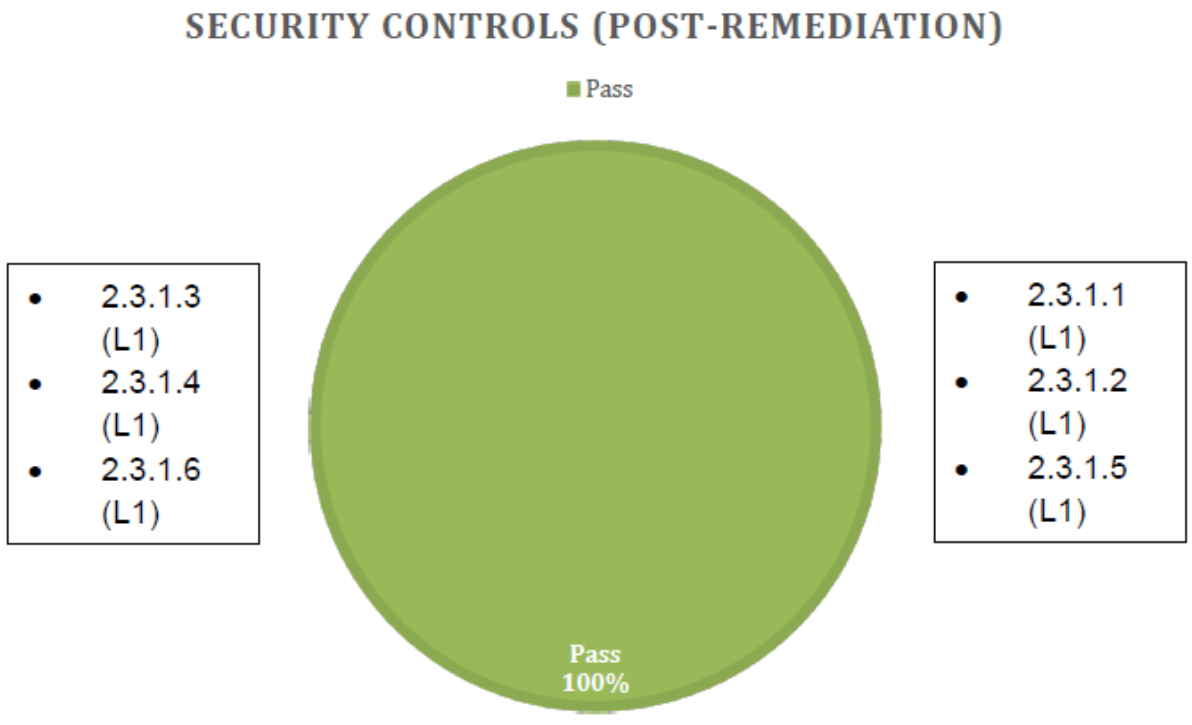
2.3.1.1 - The Administrator account status was not disabled, leaving it susceptible to brute force attacks.
2.3.1.2 - Users could add or log on with Microsoft accounts, potentially compromising identity management policies.
2.3.1.3 - The Guest account status was enabled, allowing unauthenticated access to the system. (Guest account was disabled in this specific machine)
2.3.1.4 - Local accounts with blank passwords could log on from remote client computers, posing a serious security threat so make sure to limit it. (Limiting local accounts use of blank password is enabled)
2.3.1.5 / 2.3.1.6 - The default names of the Administrator and Guest accounts made them prime targets for attackers.



THE SOLUTION

To mitigate these risks and align with the CIS benchmark recommendations, the following security controls were implemented:

2.3.1.1 - Disabled the Administrator account to prevent unauthorized access and brute force attacks.
2.3.1.2 - Blocked Microsoft accounts to maintain firm control over user logins and comply with identity management policies.(Users can't add or log on with Microsoft accounts.)
2.3.1.3 - Disabled the Guest account to restrict unauthenticated access and prevent potential data exposure or corruption. (No remediations needed)
2.3.1.4 - Limited local account use of blank passwords to console logon only, eliminating the threat posed by unprotected accounts. (No remediations needed)
2.3.1.5 - Renamed the Administrator account to mitigate the risk associated with its default name.
2.3.1.6 - Renamed the Guest account for added security, even though it was disabled by default.



ANALYSIS 

Pre-remediation, the security controls exhibited a 50% failure rate, indicating significant vulnerabilities. The pie chart presented showcases a balanced distribution of security controls, with an equal split between those meeting the recommendations and those not meeting the CIS benchmark recommendations. This indicates a balance in the default system configurations before our remediation efforts.

However, post-remediation efforts led to a complete alignment with the CIS benchmark recommendations, marking a notable 50% increase in secure configurations. Post-remediation, there is a notable transformation, with 100% of the configurations aligning with the security control recommendations, marking a significant 50% increase from the initial state. This underscores our successful enhancement of account configurations, ensuring robust security measures are now firmly in place.

The pie chart demonstrates a balanced distribution of security controls, with all controls meeting the recommendations post-remediation. This transformation underscores the successful enhancement of account configurations, ensuring robust security measures are now firmly in place.

CONCLUSION

In summary, we have undergone a transformative process of strengthening our system's security posture. Through diligent remediation efforts, we have successfully aligned with the CIS benchmark and NIST recommendations, effectively eliminating vulnerabilities and fortifying our defenses against potential threats. This initiative not only safeguards our systems but also ensures compliance with industry standards, safeguarding our organization's assets and reputation. Moving forward, these enhancements will play a pivotal role in maintaining a secure and resilient infrastructure, essential for the sustained success of our business operations.