CHAPS (Hardening Assessment PowerShell Script) Assignment Report

Prepared by: Shubham More

Date: 22/02/2024

Client: XYZ Corporation

Executive Summary:

The CHAPS assessment was conducted on the systems belonging to XYZ Corporation to evaluate their security posture and identify potential vulnerabilities. This report provides an overview of the findings and recommendations for improving the security of the systems.

Assessment Overview:

The assessment covered the following areas:

Windows Security Settings and Configurations

Patch Management

User Account Settings and Permissions

Group Policy Settings

Firewall Configurations

Common Security Vulnerabilities

Findings and Recommendations:

Windows Security Settings and Configurations:

Findings:

- AutoUpdate: Enabled.
- BitLocker: Not Detected.
- PowerShell Logging: Not Enabled.
- Event Logs: Sizes are smaller than recommended.
- PowerShell Version 2: Not permitted.
- Execution Language Mode: Full Language.
- Cached Logons Count: Greater than recommended.
- Remote Desktop Protocol (RDP): Allowed.
- Terminal Services: Denied for remote access.
- Windows Firewall: Some rules might allow unwanted remote connections.
- Local Administrator Accounts: Multiple accounts present.
- AppLocker and LAPS: Not configured.

Recommendations:

1. Enable BitLocker or alternative encryption methods.
2. Configure PowerShell Logging for better security monitoring.
3. Increase Event Log sizes to recommended levels.
4. Disable PowerShell Version 2 and enforce Constrained Language Mode.
5. Review and limit the number of accounts in the Local Administrators group.
6. Implement AppLocker and LAPS for better application and password management.

Patch Management:

Findings:

- Missing Updates: KB5034441.
- PowerShell Version Compatibility: Not fully configured.
- .NET Framework: Installed but PowerShell Version 2 not supported.

Recommendations:

- Immediately apply missing updates, especially KB5034441.

User Account Settings and Permissions:

Findings:

- NT AUTHORITY\SYSTEM Installation: Restricted.
- PowerShell Constrained Language Mode: Not enforced.
- NetBIOS: Enabled.

Recommendations:

1. Reduce Cached Logons Count to 0 or 1.
2. Disable NetBIOS if not required.

Group Policy Settings:

Findings:

- Possibly Unassigned GPOs.

Recommendations:

- Ensure proper assignment of GPOs to the system.

Firewall Configurations:

Findings:

- AllowRemoteRPC: Set to deny RDP.
- WinHttpAutoProxySvc: Service running.
- SMBv1: Enabled.

Recommendations:

- Review and adjust rules to restrict unwanted remote connections.
- Disable SMBv1 if not required for legacy systems.

Common Security Vulnerabilities:

Findings:

- PowerShell Logging Not Enabled.
- Event Log Sizes Too Small.
- PowerShell Version 2 Permitted.
- Cached Logons Count Too High.
- RDP Allowed and SMBv1 Enabled.

Recommendations:

- Enable PowerShell Logging and increase Event Log sizes.
- Disable PowerShell Version 2 and enforce Constrained Language Mode.
- Review and limit Local Administrator accounts.
- Consider disabling RDP if not necessary for remote administration.

Conclusion:

The CHAPS assessment identified several areas where improvements can be made to enhance the security posture of XYZ Corporation's systems. By implementing the recommendations outlined in this report, XYZ Corporation can reduce the risk of security breaches and protect sensitive data from unauthorized access.

This concludes the CHAPS Hardening Assessment Report for XYZ Corporation.

Immediate action is required to apply missing updates, enforce stronger security configurations, and review system settings to mitigate potential threats. Regular monitoring and proactive security measures are essential to safeguard the system against potential exploits and unauthorized access.