CHAPS (Hardening Assessment PowerShell Script) Assignment Report

# Prepared by: Roshan.M.S.K

Date: 23.02.2024

Client: ABC 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:**

1. Windows Security Settings and Configurations
2. Patch Management
3. User Account Settings and Permissions
4. Group Policy Settings
5. Firewall Configurations
6. Common Security Vulnerabilities

# Conclusion

**Windows Security Settings and Configurations:**

**Host Information:**

* The system runs Microsoft Windows 11 Home Single Language (Version 10.0.22631).
* Administrator rights are needed for more accurate results.

**Recommendations:**

* **Administrator Access**: Obtain Administrator rights for comprehensive security checks, as some checks might not succeed without it.
* **Security Configurations Review**: Review and adjust security configurations based on findings for improved system hardening.

# 2. Patch Management:

**Findings:**

* The system appears up-to-date with 8 installed hotfixes.

**Recommendations:**

* **Ongoing Monitoring:** Regular monitoring and updating to maintain patch compliance, ensuring the system is protected against known vulnerabilities or threads.

# 3.User Account Settings and Permissions:

**Findings:**

* More than one account is in the local Administrators group.

**Recommendations:**

* **Local Administrator Accounts:** Review and secure local Administrator accounts to prevent from unauthorized access and privilege escalation

# 4.Group Policy Settings:

**Findings:**

* Group Policy Objects may not be assigned to the system.

**Recommendations:**

* Investigate and address any issues with GPO assignment to ensure consistency in security policy application across the system.

# 5.Firewall Configurations:

# Findings:

* WinRM Firewall rules for remote connections are disabled

**Recommendations**:

* Review and configure WinRM Firewall rules for secure remote connections, enhancing the overall system security posture

# 6.Common Security Vulnerabilities:

**Findings:**

* AppLocker is not configured.
* LAPS (Local Administrator Password Solution) is not installed.
* SMBv1 is enabled

**Recommendations:**

* Consider implementing AppLocker for application control, preventing unauthorized software execution
* Investigate the installation of LAPS for managing local administrator passwords securely.
* Disable SMBv1 to mitigate the risk associated with this outdated and vulnerable protocol

# 7.Conclusion:

The CHAPS assessment identified several areas where improvements can be made to enhance the security posture of ABC 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.

