CHAPS (Hardening Assessment PowerShell Script) Assignment Report

Prepared by:RUTTALA DEEPAK KUMAR

Date: 2/22/2024

Client: Momen Corporation

Executive Summary:

The CHAPS assessment was conducted on the systems belonging to Momen 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
7. Findings and Recommendations

1. **Windows Security Settings and Configurations**

- Host Information:

- The system runs Windows 11 (Version 10.0.2200).

- Administrator rights are required 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 6 installed hotfixes.

- Recommendations:

- **Ongoing Monitoring:** Continue regular monitoring and updating to maintain patch compliance, ensuring the system is protected against known vulnerabilities.

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 unauthorized access and privilege escalation.

4. **Group Policy Settings:**

- Findings:

- GPOs (Group Policy Objects) may not be assigned to the system.

- Recommendations:

- GPO Assignment: Investigate and address any issues with GPO assignment to ensure consistent security policy application across the system.

5. **Firewall Configurations:**

- Findings:

- WinRM Firewall rules for remote connections are disabled.

- **Recommendations:**

- **WinRM Configuration:** 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:**

- **AppLocker Implementation:** Consider implementing AppLocker for application control, preventing unauthorized software execution.

- **LAPS Installation:** Investigate the installation of LAPS for managing local administrator passwords securely.

- **SMBv1 Disabling:** Disable SMBv1 to mitigate the risk associated with this outdated and vulnerable protocol.

General Recommendations:

- **Administrator Rights:** Ensure Administrator rights are obtained for more comprehensive security checks, addressing issues that require elevated privileges.

- **Ongoing Patch Management:** Regularly monitor and update the system for the latest security patches to mitigate potential vulnerabilities.

- **Event Log Size Adjustment:** Review and adjust event log sizes to accommodate log data and facilitate effective security monitoring.

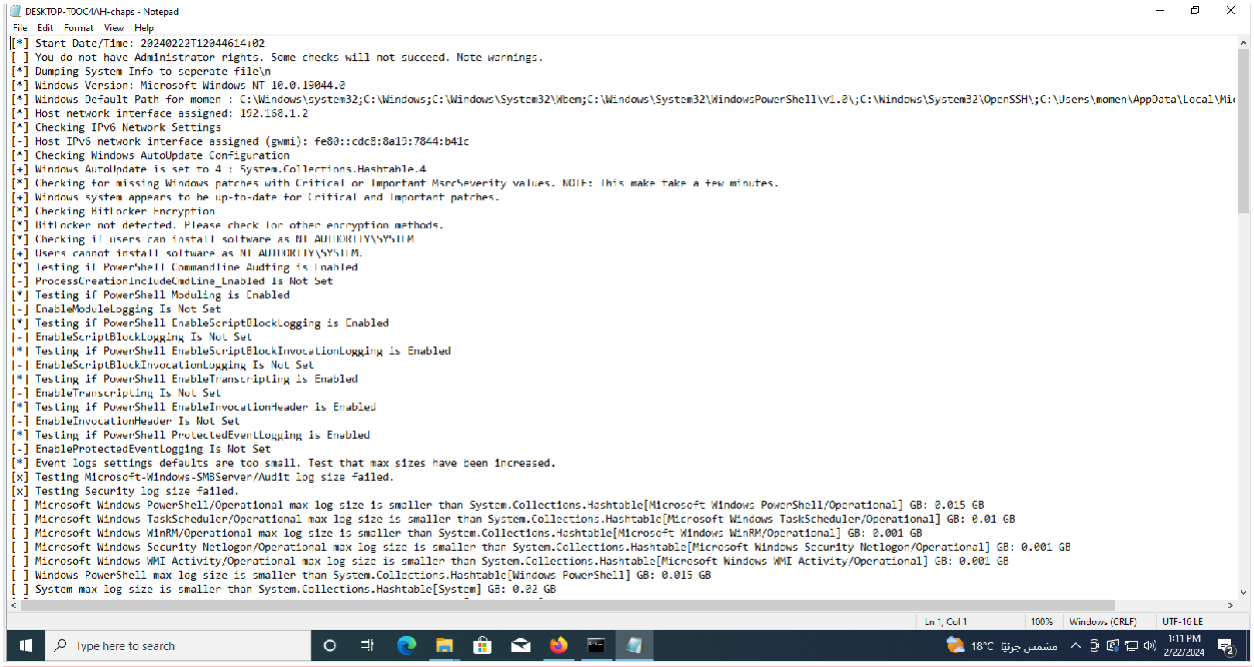
- **PowerShell Version 2 Support:** Consider disabling PowerShell version 2 support if not needed, reducing the attack surface.

- **Remote Access Security:** Implement security best practices for remote access configurations to protect against unauthorized access.

- **Additional Security Measures:** Address other identified security issues based on organizational policies, ensuring a holistic approach to system security.

There is Screenshots :

1- DESKTOP-T0OC4AH-chaps



2.SKTOP-T0OC4AH-sysinfo