

# CHAPS (Configuration Hardening Assessment PowerShell Script) Assignment Report

Prepared By: Ashish Bharambe

Date: 23/02/2024

Client: Personal System

## Executive Summary:

The CHAPS assessment was conducted on the personal system 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:

In this assessment, CHAPS (Configuration Hardening Assessment PowerShell Script) is used to understand CHAPS and its use in assessing the security configuration of Windows Operating Systems. CHAPS is used to identify the security configuration issues if present any in operating system.

## 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: Some Windows security settings are misconfigured and missing.

Recommendations: Configure good security settings or as according to windows security policies.

#### Patch Management:

Findings: Some critical or vulnerable system security patches are missing, they can be exploit.

Recommendations: Always do regularly installation of security updates and also patches on time.

#### User Account Settings and Permissions:

Findings: Having a good administrative privileges.

Recommendations: Administrative privileges and some permissions can be better than current.

#### Group Policy Settings:

Findings: Some group policies are disabled and not set.

Recommendations: Set the group policies as standard for better consistencies.

#### Firewall Configurations:

Findings: Some firewall rules are allowing unnecessary traffic.

Recommendations: Make strong firewall rules to restrict unnecessary traffic.

#### Common Security Vulnerabilities:

Findings: Some systems found vulnerable and some security settings not configured as required, such as NTLMv2.

Recommendations: Apply security patches and configure required security settings.

#### Conclusion:

The CHAPS assessment identified several areas where improvements can be made to enhance the security posture of system. By implementing the recommendations as given in this report, user can reduce the risk of security breaches and protect sensitive data from unauthorized access.

## Assessment Questions:

### 1. What is CHAPS?

- a. A PowerShell script for assessing the configuration hardening of Windows machines.

### 2. What is the purpose of CHAPS?

- a. To provide an automated way to assess the configuration hardening of Windows machines.

### 3. What are some of the security settings assessed by CHAPS?

- a. Password policy settings, local security policy settings, and user rights assignments.

### 4. How does CHAPS assess the security settings of Windows machines?

- a. By querying the Windows registry and security policy settings.

### 5. What is the output of CHAPS?

- a. A report in CSV format that lists the security settings assessed and their status (enabled/disabled).

### 6. How can CHAPS be useful in a corporate environment?

- a. It can help identify security vulnerabilities and assist in hardening the configuration of Windows machines.

### 7. What are some limitations of CHAPS?

- a. It requires administrative privileges to run.

8. What are some ways to improve CHAPS?

- a. Provide an automated way to remediate security vulnerabilities found during the assessment.

9. What are some alternatives to CHAPS?

- a. Microsoft Baseline Security Analyzer (MBSA)

10. In your opinion, how useful do you think CHAPS is for assessing the configuration hardening of Windows machines? Why?

Answer: CHAPS is very useful for assessing the configuration hardening of windows machines.

Because, user get all security related issues at one place. It also shows which patch is missing in target windows machine. It also shows all other logs configurations, RDP, User groups, Accounts settings, that's why CHAPS is very useful in my opinion.