Internship Assessment 1: CHAPS Configuration

CHAPS (Hardening Assessment PowerShell Script) Assignment Report

Prepared by: Alok Kumar Singh

Date: 24/02/2024

Client: h1k0r

Week 1.

Introduction

Configuration Hardening Assessment PowerShell Scripts (CHAPS) are scripts designed to evaluate the security posture of a Windows system by checking its configuration settings against recommended security best practices. They don't modify the system configuration themselves, but rather report on potential vulnerabilities and suggest remediation steps.

Report-

These are the following steps are taken to complete the assessment.

Step1- Download the Zip file of CHAP from Git repository

Step2- Unzip the file.

Step3- Now open the CMD.exe or window power shell with administration privilege

Step4- Open the CHAPS extracted file in Cmd.

Step5- Run the command **powershell.exe -exec bypass** to being a PowerShell prompt.

Step6- Run the CHAPS command by typing **chaps.ps1** script and execute it.

Step7- Let the command finish it and it will perform the series of checks on the systems configuration and generate the output.

```
C:\Windows\System32\cmd.exe - powershell.exe  -exec bypass

[*] Testing Local Administrator Accounts.
[-] More than one account is in local Administrators group: 2
[*] Account in local Administrator group: DESKTOP-259PJA3\Administrator
[*] Account in local Administrator group: DESKTOP-259PJA3\singh
[*] Testing if AppLocker is configured.
[x] Testing for Microsoft AppLocker failed.
[*] EMET Service components are built into Windows 10.
[*] Testing if Local Administrator Password Solution (LAPS) is installed.
[x] Testing for Microsoft LAPS failed.
[*] Testing if Group Policy Objects.
[*] System may not be assigned GPOs.
[*] Testing Net Session Enumeration configuration using the TechNet script NetSessEnumPerm.ps1
[*] Testing for WPAD entry in C:\Windows\System32\Drivers\etc\hosts
[-] No WPAD entry detected. Should contain: wpad 255.255.255.255
[*] Testing for WPADOverride registry key.
[*] System not configured with the WpadOverride registry key.
[*] Testing WinHttpAutoProxySvc configuration.
[-] WinHttpAutoProxySvc service is: Running
[*] Testing if KB3165191 is installed to harden WPAD by check installation date.
[-] KB3165191 to harden WPAD is not installed.
[*] Testing if Network Adapters are configured to enable WINS Resolution: DNSEnabledForWINSResolution
[+] DNSEnabledForWINSResolution is disabled
[*] Testing if Network Adapters are configured to enable WINS Resolution: WINSEnableLMHostsLookup
[-] WINSEnableLMHostsLookup is enabled
[*] Testing if LLMNR is disabled.
[-] DNSClient.EnableMulticast does not exist or is enabled:
[*] Testing if Computer Browser service is disabled.
[-] Computer Browser service is: Running
[*] Testing if NetBios is disabled.
[-] NetBios is Enabled: 0
[*] Testing if Windows Scripting Host (WSH) is disabled.
[-] WSH Setting Enabled key does not exist.
[*] Testing if security back-port patch KB2871997 is installed by check installation date.
[-] KB2871997 is not installed.
[*] Testing if PowerShell LocalAccountTokenFilterPolicy in Policies is Disabled
[+] LocalAccountTokenFilterPolicy Is Not Set
[*] Testing if PowerShell LocalAccountTokenFilterPolicy in Wow6432Node Policies is Disabled
[+] LocalAccountTokenFilterPolicy in Wow6432Node Is Not Set
[*] Testing if WDigest is disabled.
[-] WDigest UseLogonCredential key does not exist.
[*] Testing if SMBv1 is disabled.
[*] Testing if SMBv1 is disabled.
[-] SMBv1 is Enabled
[*] Testing if system is configured to audit SMBv1 activity.
[+] SMBv1 Auditing should be Enabled: Enabled
[*] Testing if Untrusted Fonts are disabled using the Kernel MitigationOptions.
```

Findings-

Based on the security assessment output of the CHAPS, here are some key security Findings:

Power Shell:

Enable PowerShell auditing: Enable features like script block logging, invocation logging, and transcription to monitor PowerShell activity and identify potential misuse.

Local Administrator Accounts:

Reduce the number of accounts in the local Administrators group: Having multiple accounts in this group increases the attack surface. Ideally, only one account with strong credentials should be in the local Administrators group.

LAPS:

Install and implement LAPS (Local Administrator Password Solution): This Microsoft tool helps manage and secure local administrator passwords on domain-joined machines.

Untrusted Fonts:

Disable untrusted fonts: This can help mitigate the risk of malware injection through font files.

NTLM:

Enforce NTLMv2 and 128-bit encryption: Configure NTLM settings to require NTLMv2 authentication and 128-bit encryption for stronger security.

Additional recommendations:

Consider enabling Credential Guard and Device Guard: These features can provide additional protection against certain attacks, but their implementation may depend on your hardware and software configuration.

Conclusion-

CHAPS is a PowerShell script for checking system security settings. The purpose of this script is to run it on a server or workstation to collect configuration information about that system. The information collected can then be used to provide recommendations (and references) to improve the security of the individual system.

Firstly, I downloaded the file from the Git hub of CHAPS and extracted the file then opened the file in the CMD.exe window with administration privilege. Then run the command the to bypass those connection and after few minutes I got the result and after analysis of that results, some recommendation and findings have been pointed out.

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?

c. Installed software settings, system configuration settings, and network share settings.

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?

d. It may generate false positives or false negatives, depending on the system configuration.

8. What are some ways to improve CHAPS?

b. Add support for vulnerability scanning and penetration testing.

9. What are some alternatives to CHAPS?

(A,b,c,d) all are the alternative of CHAPS, the best will suites according to the requirement.

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

Answer· CHAPS is a valuable tool for assessing the configuration hardening of Windows machines. It provides a quick and automated way to identify potential security weaknesses and helps ensure compliance with security best practices. CHAPS is a free and open·source tool, making it accessible to organizations of all sizes. It can be easily customized to meet the specific needs of an organization. CHAPS can be integrated with other security tools and processes.

Report   by·
Alok   Kumar   Singh
9971203753
alok.mbcs12213@nfsu.ac.in