Alok Kumar Singh 9971203753 alok.mbcs12213@nfsu.ac.in

Internship Assessment 1: CHAPS Configuration

Hardening Assessment Power Shell script (CHAPS)

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.

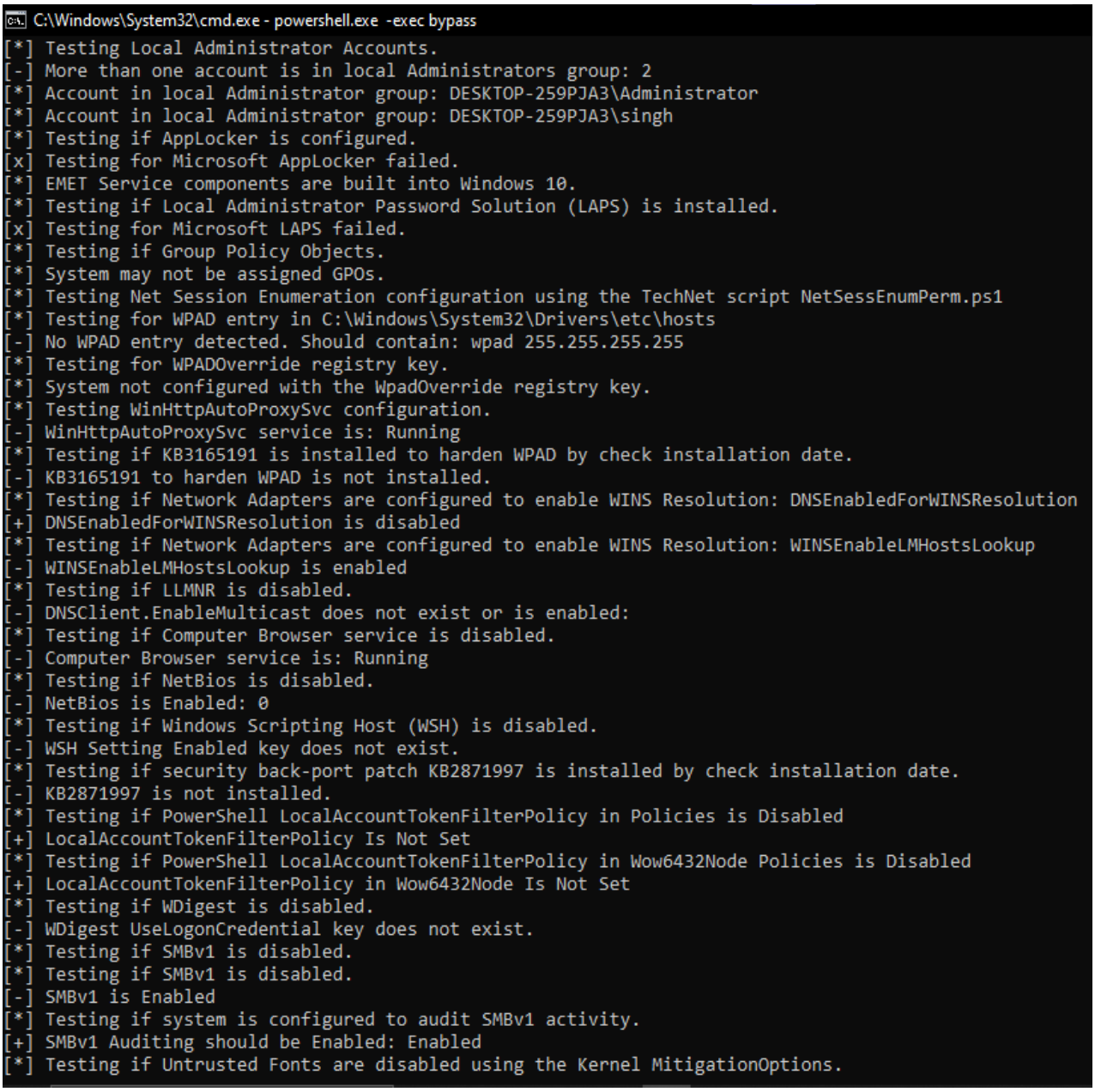
Step3- Now open the CMD.exe or window power shell with administration privilege

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.



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