Internship Assessment: CHAPS Configuration

Hardening Assessment PowerShell Scripts (CHAPS) REPORT- Week 1

Prepared by: Kamlesh Jat

Date: 23/02/2024

Client: h1k0r Corporation

INTRODUCTION:

CHAPS is a PowerShell script for checking system security settings where additional software and assessment tools, such as Microsoft Policy Analyzer, cannot be installed. 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 and systemic issues within the organization's Windows environment. The script does not make any modifications in the system. This is particularly valuable for systems, such as master and support servers.

STEPS:

1. FIRSTLY, I have downloaded VMware and install windows 11 pro
2. Now I have cloned the zip file of CHAPS github for this link GitHub - cutaway-security/chaps: Configuration Hardening Assessment PowerShell Script (CHAPS)
3. Now I have extract that file
4. Now I have opened cmd with the path of chaps-master
5. In cmd type dir to view the all directory and type chaps-master
6. Next type the powershell.exe -exec bypass
7. Next command type Set-ExecutionPolicy Bypass -scope Process
8. Now type .\chaps.ps1 -this command will start scanning it
9. Then type .\chaps.powersploit.psl

10. For to see output of the result go to temp file through Run type in RUN : %temp% and enter it

11. Open that file Name with chaps-with today’s date present

there. And we can see both txt file save it and convert it into pdf

# Windows Security Settings and Configurations

Findings: Windows AutoUpdate is set to 4 : System.Collections.Hashtable.4

System not configured with the WpadOverride registry key.

Recommendations: Should set the WpadOverride registry key not that much big problem

/

Findings: Windows system appears to be up-to-date for Critical and Important patches.

Recommendations: Set to good

# User Account Settings and Permissions

Findings: Account in local Administrator group: DESKTOP-0520P8I\Administrator Account in local Administrator group: DESKTOP-0520P8I\LENOVO

Recommendations: Should set user permissions principles for Administrator Privilege

# Group Policy Settings:

Findings: RestrictAnonymous registry key is not configured

Recommendations: Set the registry key to restrict the Anonymous login

# Firewall Configurations:

Findings: WinRM Firewall Rule MSFT_NetFirewallRule (CreationClassName = "MSFT?FW?FirewallRule?WINRM-HTTP-In-TCP", PolicyRuleName = "", SystemCreationClassName = "", SystemName = "").Name is disabled. [+] WinRM Firewall Rule MSFT_NetFirewallRule (CreationClassName = "MSFT?FW?FirewallRule?WINRM-HTTP-In-TCP-..., PolicyRuleName = "", SystemCreationClassName = "", SystemName = "").Name is disabled.

Recommendations: Firewall is configured well

# Common Security Vulnerabilities:

Findings: Several Systems is not vulnerable to common exploits, Such as EternalBlue and MS08-617.

Recommendations: Patched with good patches.

This concludes the CHAPS Hardening Assessment Report for h1k0r Corporation