Configuration Hardening Assessment PowerShell Script (CHAPS)

Name: Sharvari Sham Dubey.

Group: Group-A

Topic: Project Report on CHAPS

Index

1. Introduction
2. Execute and Screenshots
3. Recommended Remediations
4. Assessment Answers

Introduction

Configuration Hardening Assessment PowerShell Script (CHAPS) is a PowerShell script for checking system security settings where additional software and assessment tools, such as Microsoft Policy Analyzer, cannot be installed.

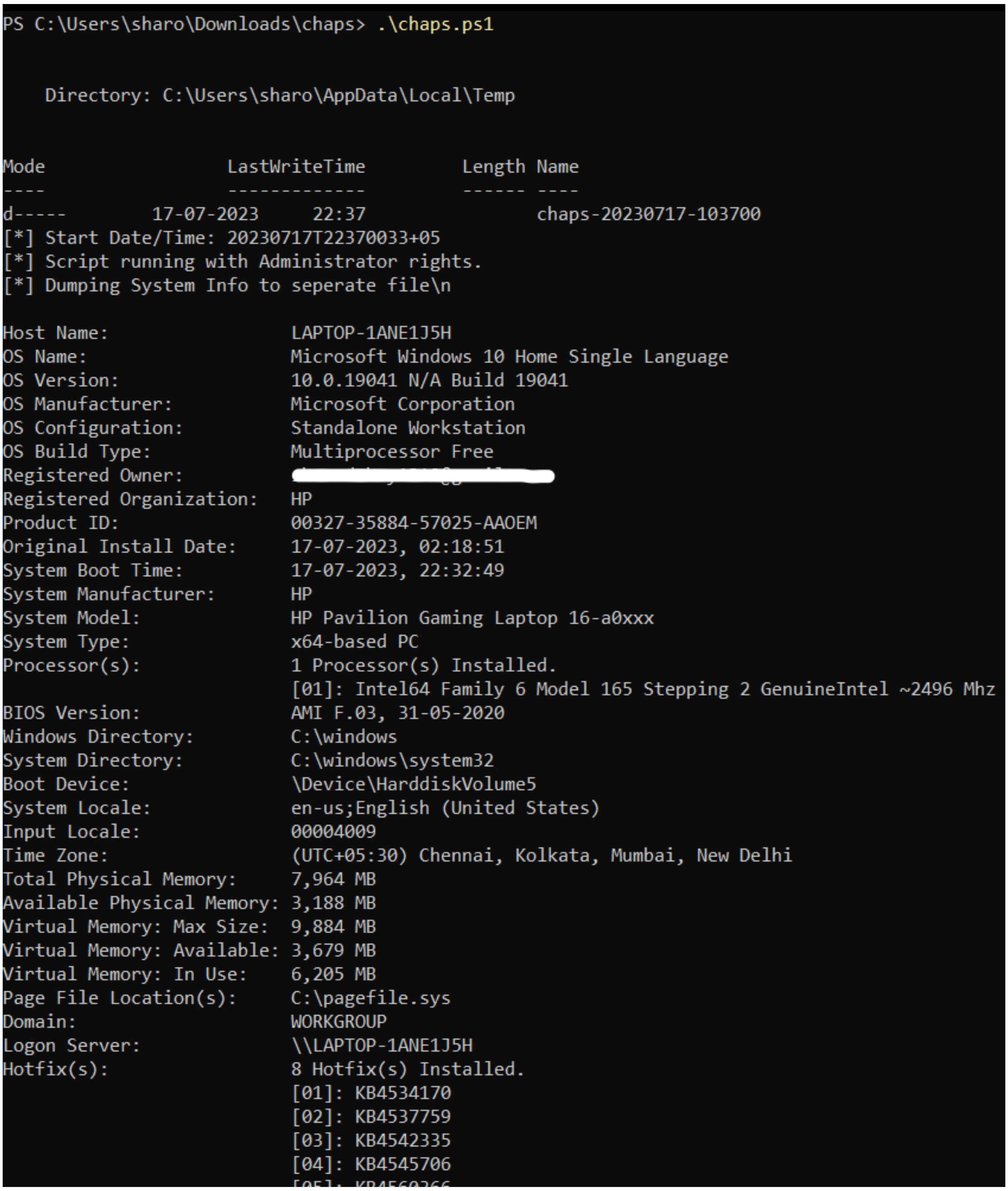
The purpose of this script is to run it on a server or workstation to collect configuration information about that system. The information collected can then be used to provide recommendations (and references) to improve the security of the individual system and systemic issues within the organization's Windows environment. Examples of environments where this script is useful include Industrial Control System (ICS) environments where systems cannot be modified. These systems include Engineer / Operator workstations, Human Machine Interface (HMI) systems, and management servers that are deployed in production environments.

Execute and Screenshots

Commands for execution:

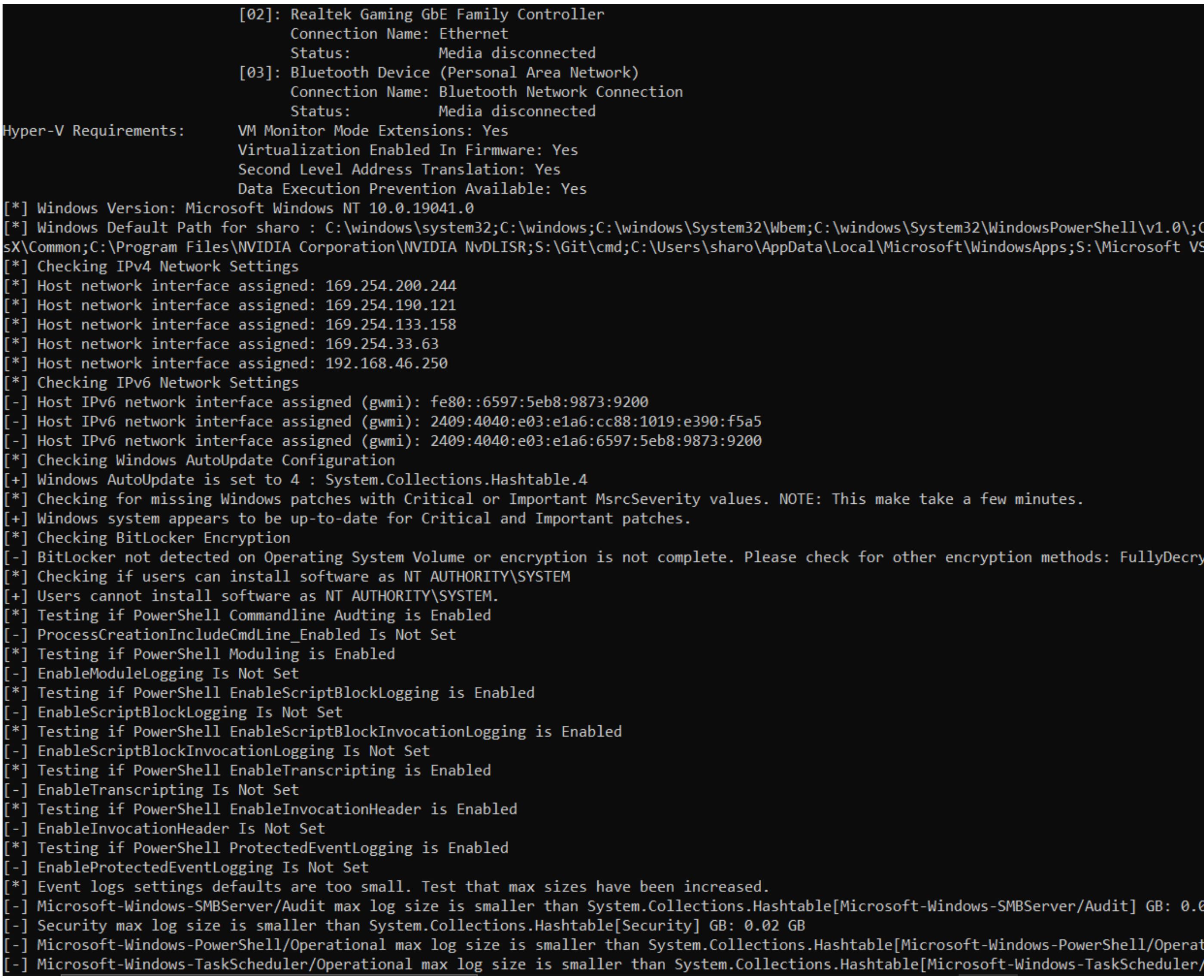
1. Press the Windows key, enter "cmd," and the Command Prompt will appear.
2. The current directory can be changed accordingly for destination of our CHAPS and PowerSploit download.
3. Downloads CHAPS and PowerSploit from GitHub repository.
4. Start the web webserver in the system using following command: python3 -m http.server 8181
5. Once the server is running, you can access it from any system on the same network by using the server's IP address and port number. To find the IP address of the system running the server, you can use the ipconfig command in your target system.
6. On another system connected to the same network, open a web browser and enter the IP address of the system running the server, followed by :8181.
7. You should now see the contents of the current directory (including the CHAPS and PowerSploit directories) listed in the web browser.
8. On the target system open a CMD.exe window, preferably as an Administrator. Run the command powershell.exe -exec bypass to being a PowerShell prompt.
9. From this prompt, run the following command to execute the chaps.ps1 script: PS C:\Windows\system32> IEX (New-Object Net.WebClient).DownloadString('http://192.168.29.201:8181/chaps/chaps.ps1')

Issues found:



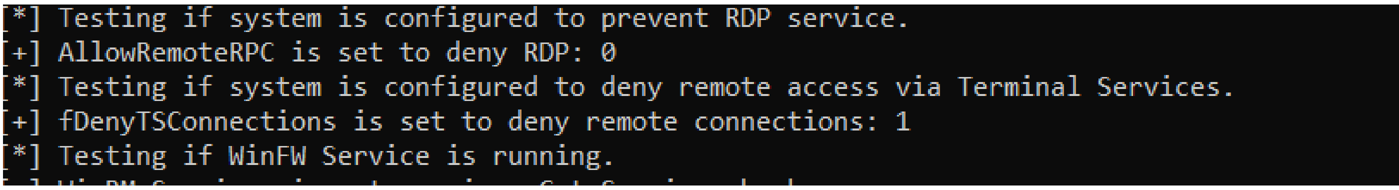
```
PS C:\Users\sharo\Downloads\chaps> .\chaps.ps1


    Directory: C:\Users\sharo\AppData\Local\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        17-07-2023     22:37                chaps-20230717-103700
[*] Start Date/Time: 20230717T22370033+05
[*] Script running with Administrator rights.
[*] Dumping System Info to seperate file\n

Host Name:                 LAPTOP-1ANE1J5H
OS Name:                   Microsoft Windows 10 Home Single Language
OS Version:                10.0.19041 N/A Build 19041
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          [redacted]
Registered Organization:   HP
Product ID:                00327-35884-57025-AAOEM
Original Install Date:     17-07-2023, 02:18:51
System Boot Time:          17-07-2023, 22:32:49
System Manufacturer:       HP
System Model:              HP Pavilion Gaming Laptop 16-a0xxx
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 165 Stepping 2 GenuineIntel ~2496 Mhz
BIOS Version:              AMI F.03, 31-05-2020
Windows Directory:         C:\windows
System Directory:          C:\windows\system32
Boot Device:               \Device\HarddiskVolume5
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     7,964 MB
Available Physical Memory: 3,188 MB
Virtual Memory: Max Size:  9,884 MB
Virtual Memory: Available: 3,679 MB
Virtual Memory: In Use:    6,205 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LAPTOP-1ANE1J5H
Hotfix(s):                 8 Hotfix(s) Installed.
                           [01]: KB4534170
                           [02]: KB4537759
                           [03]: KB4542335
                           [04]: KB4545706
```

In the above screenshot you can see all the details of the windows system in which it has performed the scan. All the details like OS name, version, product ID, time zone, etc.



```
                           [02]: Realtek Gaming GbE Family Controller
                                 Connection Name: Ethernet
                                 Status:          Media disconnected
                           [03]: Bluetooth Device (Personal Area Network)
                                 Connection Name: Bluetooth Network Connection
                                 Status:          Media disconnected
Hyper-V Requirements:      VM Monitor Mode Extensions: Yes
                           Virtualization Enabled In Firmware: Yes
                           Second Level Address Translation: Yes
                           Data Execution Prevention Available: Yes
[*] Windows Version: Microsoft Windows NT 10.0.19041.0
[*] Windows Default Path for sharo : C:\windows\system32;C:\windows;C:\windows\System32\Wbem;C:\windows\System32\WindowsPowerShell\v1.0\;C
sX\Common;C:\Program Files\NVIDIA Corporation\NVIDIA NvDLISR;S:\Git\cmd;C:\Users\sharo\AppData\Local\Microsoft\WindowsApps;S:\Microsoft VS
[*] Checking IPv4 Network Settings
[*] Host network interface assigned: 169.254.200.244
[*] Host network interface assigned: 169.254.190.121
[*] Host network interface assigned: 169.254.133.158
[*] Host network interface assigned: 169.254.33.63
[*] Host network interface assigned: 192.168.46.250
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi): fe80::6597:5eb8:9873:9200
[-] Host IPv6 network interface assigned (gwmi): 2409:4040:e03:e1a6:cc88:1019:e390:f5a5
[-] Host IPv6 network interface assigned (gwmi): 2409:4040:e03:e1a6:6597:5eb8:9873:9200
[*] Checking Windows AutoUpdate Configuration
[+] Windows AutoUpdate is set to 4 : System.Collections.Hashtable.4
[*] Checking for missing Windows patches with Critical or Important MsrcSeverity values. NOTE: This make take a few minutes.
[+] Windows system appears to be up-to-date for Critical and Important patches.
[*] Checking BitLocker Encryption
[-] BitLocker not detected on Operating System Volume or encryption is not complete. Please check for other encryption methods: FullyDecry
[*] Checking if users can install software as NT AUTHORITY\SYSTEM
[+] Users cannot install software as NT AUTHORITY\SYSTEM.
[*] Testing if PowerShell Commandline Audting is Enabled
[-] ProcessCreationIncludeCmdLine_Enabled Is Not Set
[*] Testing if PowerShell Moduling is Enabled
[-] EnableModuleLogging Is Not Set
[*] Testing if PowerShell EnableScriptBlockLogging is Enabled
[-] EnableScriptBlockLogging Is Not Set
[*] Testing if PowerShell EnableScriptBlockInvocationLogging is Enabled
[-] EnableScriptBlockInvocationLogging Is Not Set
[*] Testing if PowerShell EnableTranscripting is Enabled
[-] EnableTranscripting Is Not Set
[*] Testing if PowerShell EnableInvocationHeader is Enabled
[-] EnableInvocationHeader Is Not Set
[*] Testing if PowerShell ProtectedEventLogging is Enabled
[-] EnableProtectedEventLogging Is Not Set
[*] Event logs settings defaults are too small. Test that max sizes have been increased.
[-] Microsoft-Windows-SMBServer/Audit max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-SMBServer/Audit] GB: 0.0
[-] Security max log size is smaller than System.Collections.Hashtable[Security] GB: 0.02 GB
[-] Microsoft-Windows-PowerShell/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-PowerShell/Operat
[-] Microsoft-Windows-TaskScheduler/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-TaskScheduler/
```

1) As you can see in the above screenshot it shows, Bitlocker not detected on Operating System Volume or encryption is not complete. It could pose a security risk as Bitlocker provides encryption on entire volume or a drive helping it protect the data from theft.
2) Many settings related to powershell such as auditing, ModuleLogging, ScriptLogging, etc. are not enabled.
3) Cached Logons Count: The log reveals that the CachedLogonsCount is set to 10, which allows for the caching of multiple logon credentials.
4) Credential Guard and Device Guard: The log indicates that testing for Credential Guard and Device Guard failed. Credential Guard and Device Guard are security features designed to protect against various types of attacks



```
[*] Testing if system is configured to prevent RDP service.
[+] AllowRemoteRPC is set to deny RDP: 0
[*] Testing if system is configured to deny remote access via Terminal Services.
[+] fDenyTSConnections is set to deny remote connections: 1
[*] Testing if WinFW Service is running.
```

Here, Testing if a system is configured to deny remote access via Terminal Services involves checking the settings and configurations related to Remote Desktop Services (RDS) or Remote Desktop Protocol (RDP) on a Windows system. The goal is to ensure that remote access to the system is properly restricted and denied if necessary, to prevent unauthorized access and potential security risks. If "fDenyTSConnections" is set to 1: Remote access via Terminal Services (RDP) is denied. This means that users cannot remotely connect to the system using Remote Desktop Protocol. And it is a good practice to disable the RDP protocol.

Recommended Remediations:

1) It is a good practice to enable the BitLocker as it helps in protecting your data.
2) Enabling PowerShell Settings could help improve the security and auditability of PowerShell usage.
3) It is recommended to set the CachedLogonsCount to either 0 or 1 to limit the number of stored credentials and reduce the potential impact of compromised credentials.
4) Credential Guard and Device Guard: Verify if these features are supported on the system and configure them accordingly if required.

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?

b. A log file that lists all the files scanned and their status (infected/clean).

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 only assesses security settings related to configuration hardening and does not perform vulnerability scanning or penetration testing.

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. 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?

a. It is a very useful tool to perform scans on windows target system and get info about its policy, security, and everything. There are various advantages of using it like there's no need of installing chaps we have to just download and run the script. Also, we can customise the script according to our needs and specifications. And it has it disadvantages too like, Comprehensive Assessment: While CHAPS can check various security settings, it might not provide a comprehensive assessment like dedicated security tools designed explicitly for configuration hardening.