CHAPS (Hardening Assessment PowerShell Script) Assignment Report

Prepared by: Lohitha R

Date: 23/2/2024

Client: LAN Corporation

Executive Summary:

LAN Corporation systems underwent CHAPS analysis to determine their security level and potential vulnerabilities. This paper summarizes the findings and makes recommendations for strengthening the security of the systems.

Assessment Overview:

<u>The assessment covered the following areas:</u>

1. Windows Security Settings and Configurations

2. Patch Management

3. User Account Settings and Permissions

4. Group Policy Settings

5. Firewall Configurations

6. Common Security Vulnerabilities

7. Findings and Recommendations

1.Windows Security Settings and Configurations

Host Information:

- ✓ The system runs Windows 11 (Version 10.0.22631)
- ✓ Administrator rights are required for more accurate findings.
- ✓ x64-based PC

Recommendations:

- ➢ **Use a Standard User Account for Daily Activities:** For daily activities, use a standard user account rather than an administrator account. Instead, utilize a conventional user account for day-to-day tasks to reduce the effect of potential security issues.
- ➢ **Enable User Account Control (UAC):** UAC protects your computer from unwanted changes by prompting you for permission when a task requires administrator capabilities. Keep UAC enabled at the default level or customize it to meet your security requirements.

2.Patch Management:

Findings:

- ✓ The system has 5 hotfixes installed and appears to be up to current.

Recommendations:

- ➢ **Patch Compliance:** Ensure that all systems are up to date with the most recent security patches and updates. This can be accomplished using built-in Windows utilities or third-party patch management software.
- ➢ **Third-Party Patch Management Tools:** Consider using third-party patch management tools to automate updates throughout your Windows installation.

3.User Account Settings and Permissions:

Findings:

- ✓ More than one account is in the local Administrators group : 2

Recommendations:

- ➢ **Implement Network Access Control (NAC):** Use NAC solutions to control network access based on the security posture of the devices and users that connect to the network.
- ➢ **Implement the Least Privilege Principle:** Assign permissions according to the concept of least privilege, which states that users should only have the minimum level of access required to fulfill their job tasks.

4.Group Policy Settings:

Findings:

- ✓ System may not assigned any GPOs (Group Policy Objects)

Recommendations:

- ➢ **GPO Assignment:** Investigate and address any issues with GPO assignment to ensureconsistent security policy application across the system.

5.Firewall Configurations:

Findings:

- ✓ WinRM Firewall rules for remote connections are disabled.

Recommendations:

- ➢ **WinRM Configuration:** Review and configure WinRM Firewall rules for secure remoteconnections, enhancing the overall system security posture.

6.Common Security Vulnerabilities:

Findings:

- ✓ App Locker is not configured.
- ✓ LAPS (Local Administrator Password Solution) is not installed.
- ✓ SMBv1 is enabled.

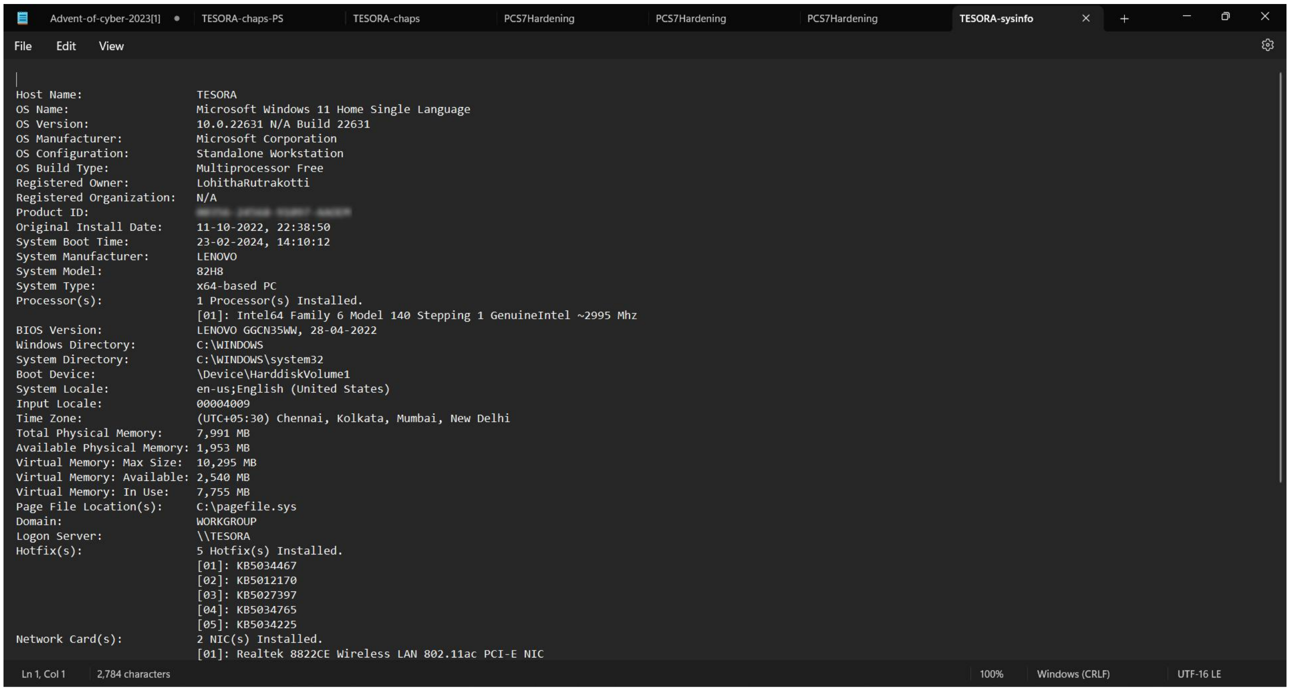
Recommendations:

- ➢ **App Locker Implementation:** Consider implementing App Locker for application control,preventing unauthorized software execution.
- ➢ **LAPS Installation:** Investigate the installation of LAPS for managing local administratorpasswords securely.
- ➢ **SMBv1 Disabling:** Disable SMBv1 to mitigate the risk associated with this outdated vulnerable protocol

General Recommendations:

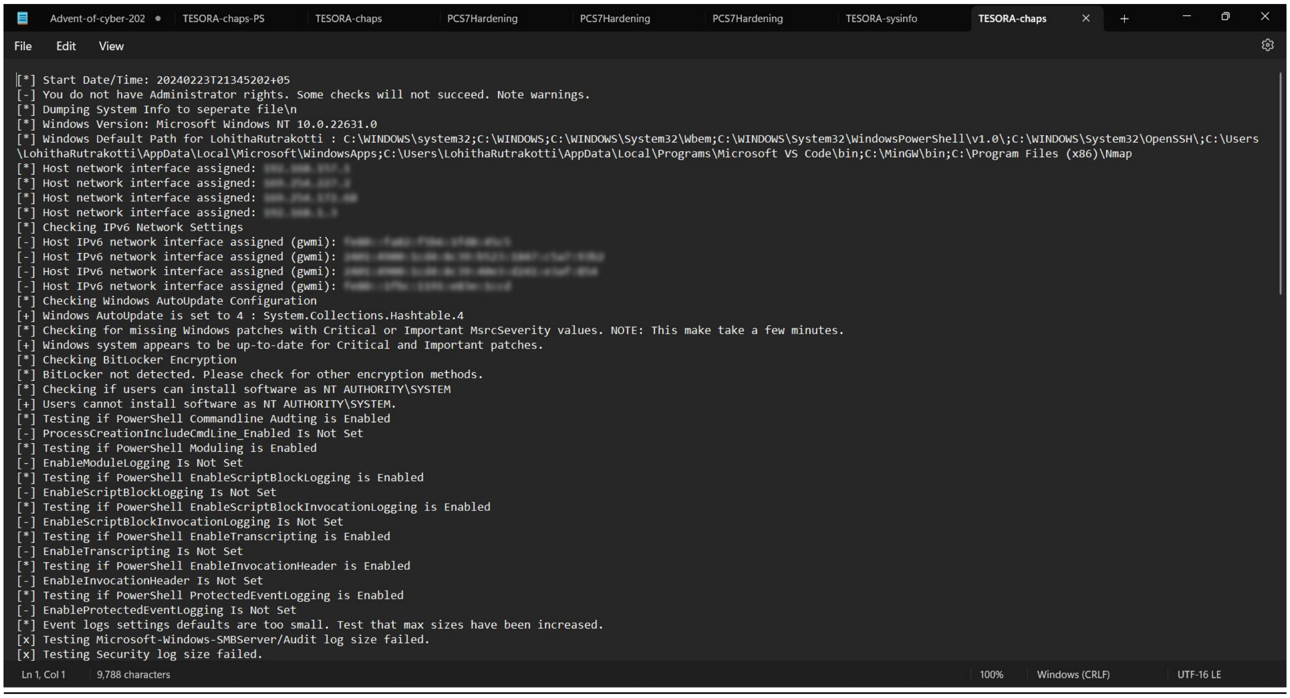
- **Consider PowerShell version 2:** If not needed, drop support for PowerShell version 2 to clean up the attack surface.
- **Keep Windows Updated:** Enable automatic Windows updates to acquire the latest security patches and fixes.
- **Use a Strong Password:** Set a strong password and utilize multi-factor authentication to increase security.
- **Enable Firewall:** Enable Windows Firewall to monitor and manage network traffic and prevent unauthorized access.
- **Disable Unused Services:** Reduce your system's vulnerability by disabling superfluous services and functionality.
- **Regular Backups:** Regular backups might help restore data in case of ransomware or device issues.
- **Disable Auto run:** Disable auto run for removable media to prevent malware execution when connecting external devices.
- **Review and Adjust Privacy Settings:** Review and update privacy settings to restrict information shared with Microsoft and third-party apps.
- **Regularly Scan for Malware:** Regularly scan for viruses with Windows Defender or a trusted third-party antivirus tool.

SCREENSHOTS



```
Host Name:                 TESORA
OS Name:                   Microsoft Windows 11 Home Single Language
OS Version:                10.0.22631 N/A Build 22631
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          LohithaRutrakotti
Registered Organization:   N/A
Product ID:                [redacted]
Original Install Date:     11-10-2022, 22:38:50
System Boot Time:          23-02-2024, 14:10:12
System Manufacturer:       LENOVO
System Model:              82H8
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~2995 Mhz
BIOS Version:              LENOVO GGCN35WW, 28-04-2022
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     7,991 MB
Available Physical Memory: 1,953 MB
Virtual Memory: Max Size:  10,295 MB
Virtual Memory: Available: 2,540 MB
Virtual Memory: In Use:    7,755 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\TESORA
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB5034467
                           [02]: KB5012170
                           [03]: KB5027397
                           [04]: KB5034765
                           [05]: KB5034225
Network Card(s):           2 NIC(s) Installed.
                           [01]: Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
```

Fig 1 : TESORA- sys info



```
[*] Start Date/Time: 20240223T21345202+05
[-] You do not have Administrator rights. Some checks will not succeed. Note warnings.
[*] Dumping System Info to seperate file\n
[*] Windows Version: Microsoft Windows NT 10.0.22631.0
[*] Windows Default Path for LohithaRutrakotti : C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\Users
\LohithaRutrakotti\AppData\Local\Microsoft\WindowsApps;C:\Users\LohithaRutrakotti\AppData\Local\Programs\Microsoft VS Code\bin;C:\MinGW\bin;C:\Program Files (x86)\Nmap
[*] Host network interface assigned: [redacted]
[*] Host network interface assigned: [redacted]
[*] Host network interface assigned: [redacted]
[*] Host network interface assigned: [redacted]
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi): [redacted]
[-] Host IPv6 network interface assigned (gwmi): [redacted]
[-] Host IPv6 network interface assigned (gwmi): [redacted]
[-] Host IPv6 network interface assigned (gwmi): [redacted]
[*] 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. Please check for other encryption methods.
[*] 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.
[x] Testing Microsoft-Windows-SMBServer/Audit log size failed.
[x] Testing Security log size failed.
```

Fig 2 : TESORA-chaps