

CHAPS (Hardening Assessment PowerShell Script) Assignment Report

Prepared by: Aadhithiya Narayan S

Date: 23/2/2024

Client: Leo Corporation

Executive Summary:

Leo Corporation systems were subjected to CHAPS analysis to assess their security level and identify potential vulnerabilities. This report provides an overview of the findings and recommendations for improving the security of the systems.

Assessment Overview:

The assessment covered the following areas:

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 is required to get more accurate results.
- x64-based PC

Recommendations:

- **Administrator Access:** Obtain Administrator rights for comprehensive security checks, as some checks might not succeed without it.
- **Security Configurations Review:** Review and adjust security configurations based on findings for improved system hardening.

2.Patch Management:

Findings:

- The system appears up-to-date with 5 installed hotfixes.

Recommendations:

- **Ongoing Monitoring:** Continue regular monitoring and updating to maintain patch compliance, ensuring the system is protected against known vulnerabilities.
- **Establish a Patch Management Policy:** Create a clear and comprehensive patch management policy outlining the procedures, responsibilities, and timelines for applying patches.

-

3.User Account Settings and Permissions:

Findings:

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

Recommendations:

- **Regularly Review and Update User Permissions:** Conduct periodic reviews of user account permissions and adjust them as needed, especially in response to role changes or employee departures.
- **Limit Administrative Privileges:** Restrict administrative privileges to only those users who require them. Regular users should not have unnecessary administrative rights.

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 ensure consistent 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 remote connections, enhancing the overall system security posture

6.Common Security Vulnerabilities:

Findings:

- AppLocker is not configured.
- LAPS (Local Administrator Password Solution) is not installed.
- SMBv1 is enabled.

Recommendations:

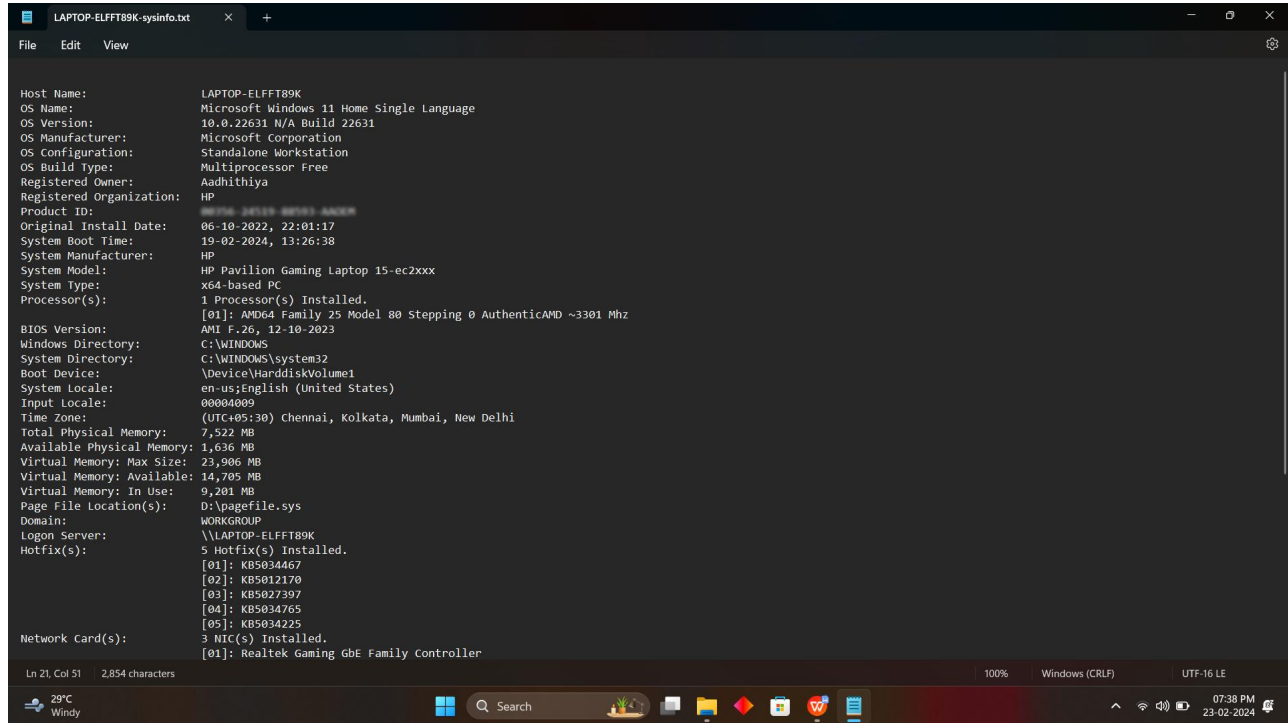
- **AppLocker Implementation:** Consider implementing AppLocker for application control, preventing unauthorized software execution.
- **LAPS Installation:** Investigate the installation of LAPS for managing local administrator passwords securely.
- **SMBv1 Disabling:** Disable SMBv1 to mitigate the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

General Recommendations:

- **Secure administrator rights:** Gain administrator rights to perform comprehensive security audits that address issues that require elevated rights for advanced security.
- **Continuous patch management:** Check and update the system regularly with the latest security patches to minimize potential vulnerabilities.
- **Optimize event log size:** Monitor and adjust event log sizes to better handle log counts and support robust security controls.
- **Consider PowerShell version 2:** If not needed, drop support for PowerShell version 2 to clean up the attack surface.
- **Enhance remote access security:** Implemented best practices for remote access configuration to protect against unauthorized access.
- **Implement new security measures:** Address other security issues identified in the organization's systems, ensuring a comprehensive approach to system security.

-

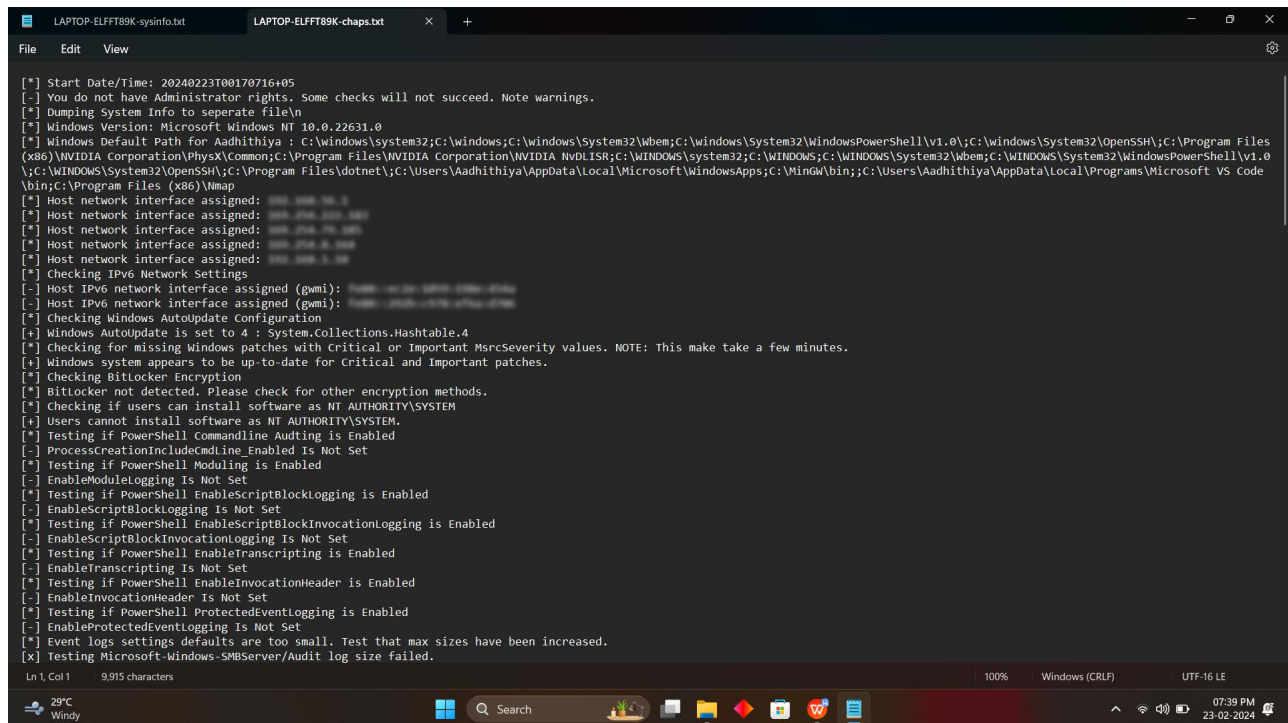
SCREENSHOTS



The screenshot shows a Windows File Explorer window titled "LAPTOP-ELFFT89K-sysinfo.txt". The window displays system information for a laptop. The information is organized into sections: Host Name, OS Name, OS Version, OS Manufacturer, OS Configuration, OS Build Type, Registered Owner, Registered Organization, Product ID, Original Install Date, System Boot Time, System Manufacturer, System Model, System Type, Processor(s), BIOS Version, Windows Directory, System Directory, Boot Device, System Locale, Input Locale, Time Zone, Total Physical Memory, Available Physical Memory, Virtual Memory: Max Size, Virtual Memory: Available, Virtual Memory: In Use, Page File Location(s), Domain, Logon Server, Hotfix(s), and Network Card(s). The system is a Microsoft Windows 11 Home Single Language, installed on 06-10-2022, 22:01:17. The system is a Standalone Workstation, Multiprocessor Free, with a registered owner of Aadithiya and a registered organization of HP. The system is a HP Pavilion Gaming Laptop 15-ec2xxx, x64-based PC, with 1 Processor(s) installed. The processor is an AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3301 Mhz. The system is running Windows 11, version 10.0.22631.0, build 22631. The system is installed on a hard disk volume. The system locale is en-us;English (United States). The input locale is 00004009. The time zone is (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi. The total physical memory is 7,522 MB, and the available physical memory is 1,636 MB. The virtual memory max size is 23,906 MB, and the available virtual memory is 14,705 MB. The virtual memory in use is 9,201 MB. The page file location is D:\pagefile.sys. The domain is WORKGROUP. The logon server is \\LAPTOP-ELFFT89K. There are 5 hotfixes installed: KB5034467, KB5012170, KB5027397, KB5034765, and KB5034225. There are 3 network cards installed: Realtek Gaming GbE Family Controller.

```
Host Name: LAPTOP-ELFFT89K
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: Aadithiya
Registered Organization: HP
Product ID: *****-247129-88703-AADITHIYA
Original Install Date: 06-10-2022, 22:01:17
System Boot Time: 19-02-2024, 13:26:38
System Manufacturer: HP
System Model: HP Pavilion Gaming Laptop 15-ec2xxx
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3301 Mhz
BIOS Version: AMI F.26, 12-10-2023
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: 7,522 MB
Available Physical Memory: 1,636 MB
Virtual Memory: Max Size: 23,906 MB
Virtual Memory: Available: 14,705 MB
Virtual Memory: In Use: 9,201 MB
Page File Location(s): D:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\LAPTOP-ELFFT89K
Hotfix(s): 5 Hotfix(s) Installed.
[01]: KB5034467
[02]: KB5012170
[03]: KB5027397
[04]: KB5034765
[05]: KB5034225
Network Card(s): 3 NIC(s) Installed.
[01]: Realtek Gaming GbE Family Controller
```

Fig 1 : LAPTOP-ELFFT89K-sysinfo



The screenshot shows a Windows File Explorer window titled "LAPTOP-ELFFT89K-sysinfo.txt" and "LAPTOP-ELFFT89K-chaps.txt". The window displays system information for a laptop. The information is organized into sections: Host Name, OS Name, OS Version, OS Manufacturer, OS Configuration, OS Build Type, Registered Owner, Registered Organization, Product ID, Original Install Date, System Boot Time, System Manufacturer, System Model, System Type, Processor(s), BIOS Version, Windows Directory, System Directory, Boot Device, System Locale, Input Locale, Time Zone, Total Physical Memory, Available Physical Memory, Virtual Memory: Max Size, Virtual Memory: Available, Virtual Memory: In Use, Page File Location(s), Domain, Logon Server, Hotfix(s), and Network Card(s). The system is a Microsoft Windows 11 Home Single Language, installed on 06-10-2022, 22:01:17. The system is a Standalone Workstation, Multiprocessor Free, with a registered owner of Aadithiya and a registered organization of HP. The system is a HP Pavilion Gaming Laptop 15-ec2xxx, x64-based PC, with 1 Processor(s) installed. The processor is an AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3301 Mhz. The system is running Windows 11, version 10.0.22631.0, build 22631. The system is installed on a hard disk volume. The system locale is en-us;English (United States). The input locale is 00004009. The time zone is (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi. The total physical memory is 7,522 MB, and the available physical memory is 1,636 MB. The virtual memory max size is 23,906 MB, and the available virtual memory is 14,705 MB. The virtual memory in use is 9,201 MB. The page file location is D:\pagefile.sys. The domain is WORKGROUP. The logon server is \\LAPTOP-ELFFT89K. There are 5 hotfixes installed: KB5034467, KB5012170, KB5027397, KB5034765, and KB5034225. There are 3 network cards installed: Realtek Gaming GbE Family Controller.

```
[*] Start Date/Time: 20240223T00170716+05
[-] You do not have Administrator rights. Some checks will not succeed. Note warnings.
[*] Dumping System Info to separate file\n
[*] Windows Version: Microsoft Windows NT 10.0.22631.0
[*] Windows Default Path for Aadithiya : C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Program Files
(x86)\NVIDIA Corporation\PhysX\Common;C:\Program Files\NVIDIA Corporation\NVIDIA NVDLISR;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0
\;C:\WINDOWS\System32\OpenSSH\;C:\Program Files\dotnet\;C:\Users\Aadithiya\AppData\Local\Microsoft\WindowsApps;C:\Windows\WinSxS;C:\Users\Aadithiya\AppData\Local\Programs\Microsoft VS Code
\bin;C:\Program Files (x86)\Vmap
[*] Host network interface assigned:
[*] Host network interface assigned:
[*] Host network interface assigned:
[*] Host network interface assigned:
[*] Host network interface assigned:
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi):
[-] Host IPv6 network interface assigned (gwmi):
[*] Checking Windows AutoUpdate Configuration
[*] Windows AutoUpdate is set to 4 : System.Collections.Hashtable.4
[*] Checking for missing Windows patches with Critical or Important MsccSeverity 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 Auditing 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.
```

Fig 2 : LAPTOP-ELFFT89K-chaps