CHAPS (Hardening Assessment PowerShell Script) Assignment Report

***Prepared by*: <u>Tejas Pachpile</u>** **Date:** February 21, 2024

Executive Summary:

Note: few data is redacted or is changed

The system under review, identified as "IAMTEJAS," is running Microsoft Windows 11 Home Single Language with Build 22621 on a LENOVO model 82K2, featuring an AMD64 processor. The system was originally installed on February 8, 2023, and last booted on February 19, 2024. Notable hardware includes 7,020 MB of total physical memory and various network adapters, including Realtek PCIe GbE and MediaTek Wi-Fi 6 MT7921.

This assessment was conducted using the Configuration Hardening Assessment PowerShell Script (CHAPS) tool, which provides detailed insights into the system's security posture. The tool identified several areas where the system could be strengthened to better defend against potential threats.

In terms of security, the system has received several critical and important hotfixes, ensuring it is up-to-date with patches. However, some security configurations require attention. Notably, BitLocker encryption is not detected, and PowerShell logging and scripting features are not fully enabled, leaving the system potentially vulnerable to unauthorized software installations and insufficient logging of PowerShell activity.

Furthermore, the absence of SMBv1, AppLocker, and LAPS poses security risks, and the presence of multiple local administrator accounts raises concerns about privilege escalation. Although some security best practices are followed, such as enabling PowerShell Version 2 and Windows Scripting Host, there is room for improvement in hardening the system against potential threats.

In conclusion, while the system has received critical and important patches and follows some security best practices, there are areas that require attention to enhance its security posture. Recommendations include implementing encryption measures, enabling PowerShell logging, disabling unnecessary services, and regularly monitoring and updating security configurations to mitigate potential risks and vulnerabilities, as suggested by the CHAPS tool assessment.

Assessment Overview:

The Configuration Hardening Assessment PowerShell Script (CHAPS) tool provides a comprehensive assessment of the security configuration of the "IAMTEJAS" system running Microsoft Windows 11 Home Single Language. The assessment aims to evaluate the system's security posture by analyzing various parameters, including patch management, encryption status, user privileges, network configurations, and adherence to security best practices.

During the assessment, CHAPS checks for the presence of critical and important patches to ensure the system is up-to-date with security updates. It also evaluates encryption status, PowerShell logging and scripting configurations, user privilege settings, network firewall rules, and adherence to security guidelines such as disabling SMBv1 and enabling AppLocker.

The assessment aims to provide actionable insights and recommendations to enhance the system's security posture, mitigate potential risks, and improve overall resilience against cyber threats. By identifying security gaps and vulnerabilities, organizations can proactively address weaknesses, strengthen security controls, and ensure compliance with industry standards and best practices.

The assessment covered the following areas:

Operating System Details:

- Host name, OS name, version, and build information.
- System manufacturer, model, and type.
- BIOS version and installation date.

User Account Settings and Permissions:

Patch Management:

- Identification of installed hotfixes and their respective KB numbers.
- Verification of Windows AutoUpdate configuration.

Network Configurations:

- Details of installed network cards including connection names and IP addresses.
- Verification of DHCP status and DHCP server information.

Security Settings:

- Detection of BitLocker encryption status.
- Analysis of user privileges and ability to install software.
- Evaluation of PowerShell logging and scripting configurations.

Event Logs Settings:

- Assessment of event logs' maximum sizes and verification if they have been appropriately configured.

PowerShell Configuration:

- Testing PowerShell version and permissions for PowerShell Version 2.
- Verification of PowerShell execution language mode and transcription settings.

Other Security Configurations:

- Analysis of SMBv1 settings, AppLocker configuration, and Remote Desktop Protocol (RDP) access permissions.
- Examination of firewall rules, NetBIOS, Windows Scripting Host (WSH), and WINS resolution settings.

Finding of OS and configurations:

Host Name: IAMTEJAS

OS Name: Microsoft Windows 11 Home Single Language

OS Version: 10.0.22621 N/A Build 22621

OS Manufacturer: Microsoft Corporation

OS Configuration: Standalone Workstation

OS Build Type: Multiprocessor Free

Registered Owner: redacted@gmail.com

Registered Organization: N/A

Product ID: 00123-42309-51526-AASEM

Original Install Date: 02-08-2023, 04:07:06 PM

System Boot Time: 19-02-2024, 08:42:22 PM

System Manufacturer: LENOVO

System Model: 82K2

System Type: x64-based PC

Processor(s):

- AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3301 Mhz

BIOS Version: LENOVO H3CG32AA(V2.02), 23-02-2022

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: 7,020 MB

Available Physical Memory: 897 MB

Virtual Memory:

- Max Size: 16,236 MB
- Available: 2,807 MB
- In Use: 13,429 MB

Recommendations:

Update OS: Ensure that the operating system is regularly updated with the latest patches and security updates to mitigate vulnerabilities and improve system stability.

Monitor Memory Usage: Monitor and manage memory usage to ensure that the system has sufficient available physical memory for optimal performance.

BIOS Update: Consider updating the BIOS to the latest version to access new features, enhance system compatibility, and address potential security vulnerabilities.

System Locale: Confirm that the system locale settings are appropriate for the user's location and language preferences to ensure a seamless user experience.

Time Zone Settings: Verify that the time zone settings are accurate to reflect the correct local time and prevent discrepancies in time-sensitive operations and logs.

Security Measures: Implement additional security measures such as encryption (e.g., BitLocker) to protect sensitive data and enhance system security against unauthorized access.

Patch Management:

1. Hotfixes Installed: Four hotfixes have been installed on the system, namely KB5034467, KB5034765, KB5032393, and KB5034225. These hotfixes indicate that some patch management activities have been performed on the system to address known security vulnerabilities or improve system stability.

2. Windows AutoUpdate Configuration: The Windows AutoUpdate is set to 4, suggesting that automatic updates are enabled. This configuration ensures that the system can receive and install important updates and patches from Microsoft automatically, enhancing the system's security posture by keeping it up-to-date with the latest fixes and improvements.

3.BitLocker Encryption: The assessment indicates that BitLocker encryption is not detected on the operating system volume or encryption is not complete. While BitLocker provides enhanced security by encrypting data on the disk, its absence may pose a risk, especially for sensitive data. The recommendation would be to consider enabling BitLocker encryption for improved data protection.

Recommendations:

* Enable BitLocker Encryption: Safeguard data with BitLocker encryption on the OS volume.

* Review Windows Firewall Rules: Ensure proper configuration to control network access.

* Limit Local Administrator Accounts: Minimize security risks by reducing admin privileges.

* Regular Patch Management: Apply critical updates promptly to address vulnerabilities.

* Enhance PowerShell Security: Enable logging and Constrained Language Mode.

* Review Event Log Settings: Increase log sizes for comprehensive monitoring.

* Disable SMBv1 and Enable Auditing: Mitigate risks associated with outdated protocols.

* Implement Credential and Device Guard: Strengthen credential protection and code execution security.

*Security Awareness Training: Educate users on security best practices regularly.

By implementing these recommendations, the system can significantly improve its security posture, reduce the risk of security breaches, and enhance resilience against evolving cyber threats. Regular monitoring, maintenance, and updates are also crucial to ensuring continued effectiveness of the security measures implemented.

User Account Settings and Permissions:

FINDINGS:

Multiple accounts are in the local Administrators group: WINDOWS SYSTEM\Administrator and IAMTEJAS\tejas.

CachedLogonsCount is not set to 0 or 1, allowing caching of multiple logon credentials.

fDenyTSConnections is set to deny remote connections, which might restrict remote access via Terminal Services.

Recommendations:

Review and restrict membership in the local Administrators group to essential users only.

Set CachedLogonsCount to 0 or 1 to limit cached logon credentials.

Ensure remote access configurations align with organizational security policies and requirements.

Implementing these recommendations helps mitigate unauthorized access and strengthens overall security posture. Regular review and maintenance of user account settings are essential for maintaining a secure environment.

Group Policy Settings:

FINDINGS:

Group Policy settings were assessed to determine the configuration of security-related policies within the Windows environment. These settings govern various aspects of system behavior, user privileges, and security configurations.

1. AppLocker Configuration: The assessment failed to retrieve information regarding the configuration of Microsoft AppLocker, a feature that allows administrators to control which applications are allowed to run on the system.

2. Lack of AppLocker configuration could potentially lead to increased risk from unauthorized or malicious software execution.

3. Local Administrator Accounts: The assessment identified multiple accounts within the local Administrators group, including "iamtejas\Administrator" and "WINDOWS SYSTEM\tejas." This configuration increases the risk of privilege escalation and unauthorized access to critical system resources.

Recommendations:

1. Implement AppLocker Policies: Configure and enforce AppLocker policies to restrict the execution of unauthorized or potentially malicious applications. Define rules based on trusted publishers, file hashes, or file paths to control application whitelisting and blacklisting effectively.

2. Review Local Administrator Accounts: Regularly review and audit the membership of the local Administrators group to ensure that only authorized individuals have elevated privileges on the system. Remove unnecessary accounts from the Administrators group to minimize the risk of privilege misuse or exploitation.

Firewall Configurations:

FINDINGS:

The assessment evaluated the configuration of Windows Firewall settings to determine the level of network security controls implemented on the system. Windows Firewall is a built-in feature that helps protect the system by controlling inbound and outbound network traffic based on predefined rules.

- WinRM Firewall Rules: The assessment identified two WinRM (Windows Remote Management) firewall rules named "WINRM-HTTP-In-TCP" and "WINRM-HTTP-In-TCP-..., " both of which were disabled. These rules govern the communication protocol used by WinRM for remote management tasks. While the rules being disabled may indicate intentional configuration, it's important to ensure that remote management capabilities are properly secured and restricted to authorized users and systems.

Recommendations:

* Review and Enable WinRM Firewall Rules: Evaluate the necessity of WinRM firewall rules based on organizational requirements for remote management. If WinRM functionality is required, enable the necessary firewall rules while adhering to the principle of least privilege. Configure specific IP address or subnet restrictions to restrict access to trusted sources only.

* Implement Additional Firewall Rules: Consider implementing additional firewall rules to restrict inbound and outbound network traffic based on organizational security policies and requirements. Define rules to allow or block specific protocols, ports, and applications as needed to minimize the attack surface and mitigate potential security risks.

Common Security Vulnerabilities:

The assessment examined the system for common security vulnerabilities that could potentially be exploited by malicious actors to compromise system integrity, confidentiality, or availability. Identifying and addressing these vulnerabilities is crucial for maintaining a secure computing environment and mitigating the risk of unauthorized access or data breaches.

1. SMBv1 Enabled: Server Message Block version 1 (SMBv1) was found to be enabled on the system. SMBv1 is an outdated and vulnerable protocol known for various security weaknesses, including susceptibility to remote code execution exploits such as WannaCry and NotPetya. Continuing to support SMBv1 poses significant security risks and should be avoided whenever possible.

2. CVE-2017-0144 (also known as EternalBlue): This vulnerability is associated with the exploit used by the WannaCry ransomware in 2017. It allows remote attackers to execute arbitrary code on vulnerable systems via crafted packets.

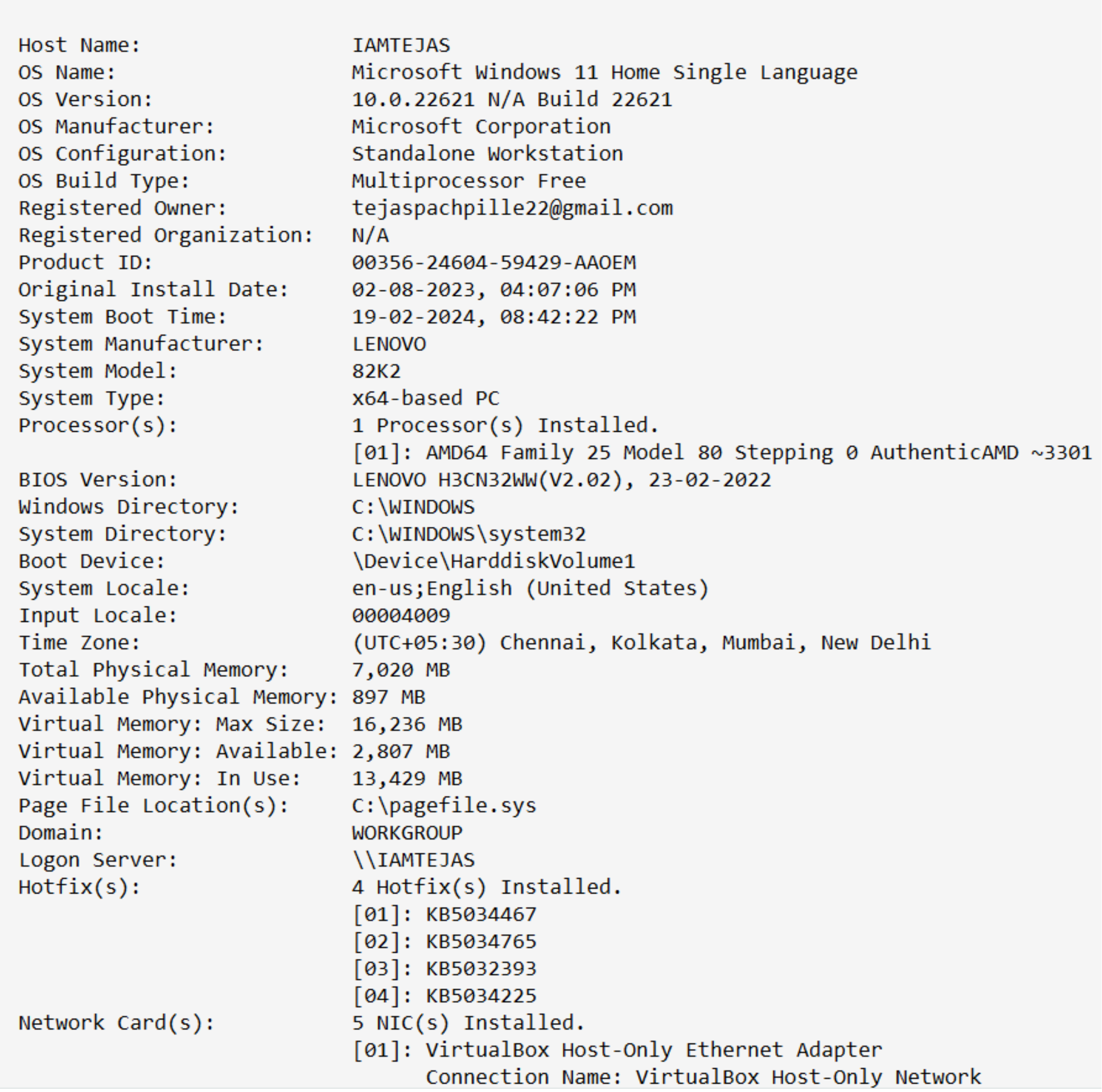
Recommendations:

Disable SMBv1: Immediately disable SMBv1 on the system to eliminate the associated security risks. Modern versions of Windows and other networked devices support newer SMB versions (e.g., SMBv2 or SMBv3), which offer improved security features and protection against known vulnerabilities. Ensure compatibility with other networked devices before disabling SMBv1 and consider upgrading legacy systems that rely on SMBv1.

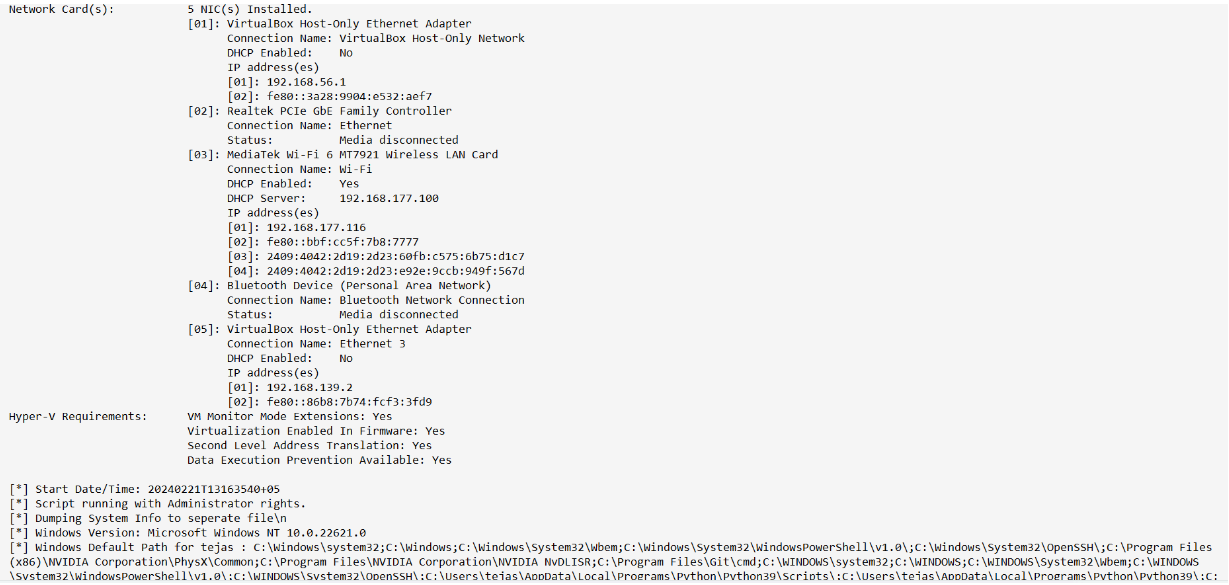
CONCLUSIONS:

In conclusion, while the system demonstrates some adherence to security best practices, there are areas for improvement identified through the CHAPS Hardening Assessment. Addressing these findings, such as enabling BitLocker encryption, enhancing PowerShell logging, reviewing Group Policy settings, and disabling SMBv1, can strengthen the system's security posture and mitigate potential risks. Ongoing monitoring and maintenance of security configurations are essential to ensure the system remains resilient against evolving threats.

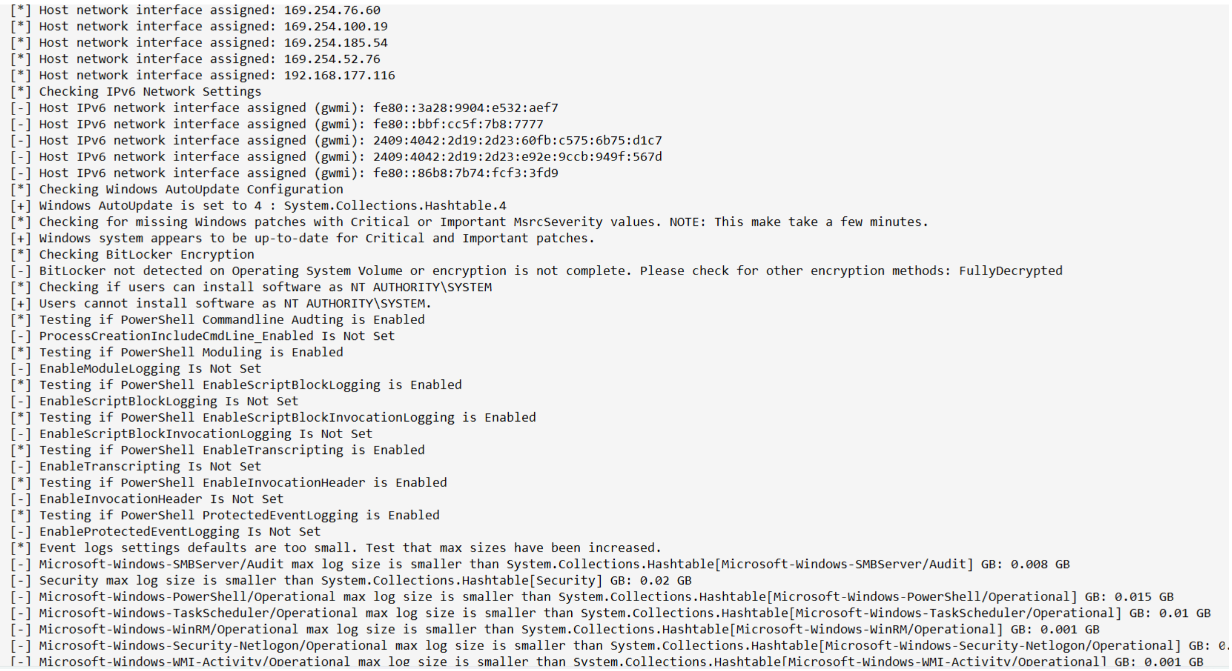
THERE ARE THE FINDINGS BELOW:



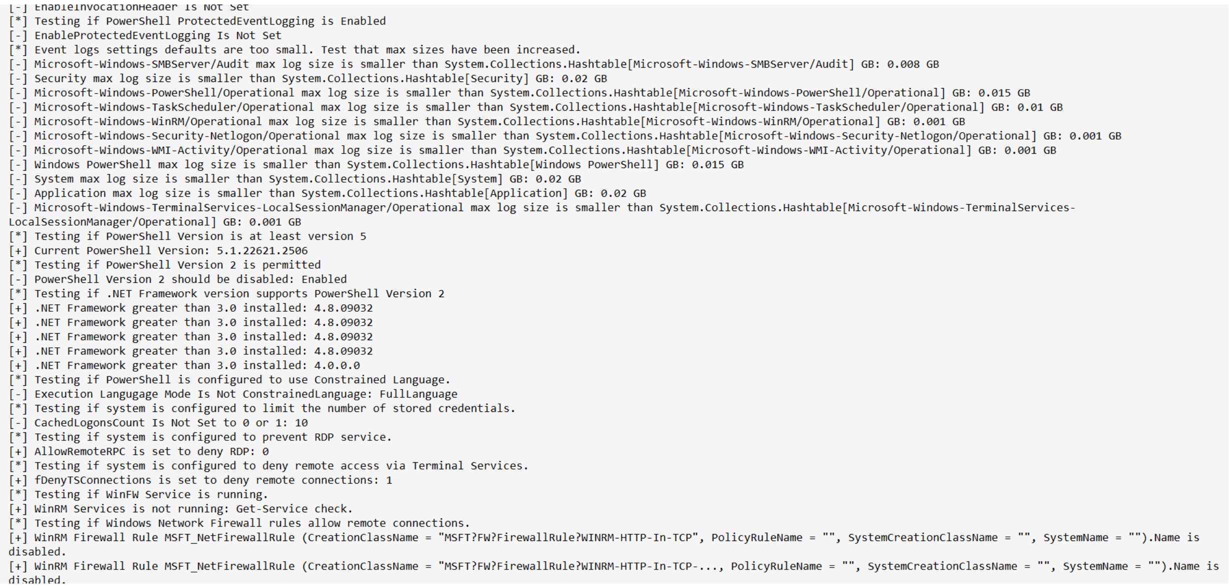
```
Host Name:                 IAMTEJAS
OS Name:                   Microsoft Windows 11 Home Single Language
OS Version:                10.0.22621 N/A Build 22621
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          tejaspachpille22@gmail.com
Registered Organization:   N/A
Product ID:                00356-24604-59429-AAOEM
Original Install Date:     02-08-2023, 04:07:06 PM
System Boot Time:          19-02-2024, 08:42:22 PM
System Manufacturer:       LENOVO
System Model:              82K2
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3301
BIOS Version:              LENOVO H3CN32WW(V2.02), 23-02-2022
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:     7,020 MB
Available Physical Memory: 897 MB
Virtual Memory: Max Size:  16,236 MB
Virtual Memory: Available: 2,807 MB
Virtual Memory: In Use:    13,429 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\IAMTEJAS
Hotfix(s):                 4 Hotfix(s) Installed.
                           [01]: KB5034467
                           [02]: KB5034765
                           [03]: KB5032393
                           [04]: KB5034225
Network Card(s):           5 NIC(s) Installed.
                           [01]: VirtualBox Host-Only Ethernet Adapter
                                 Connection Name: VirtualBox Host-Only Network
```



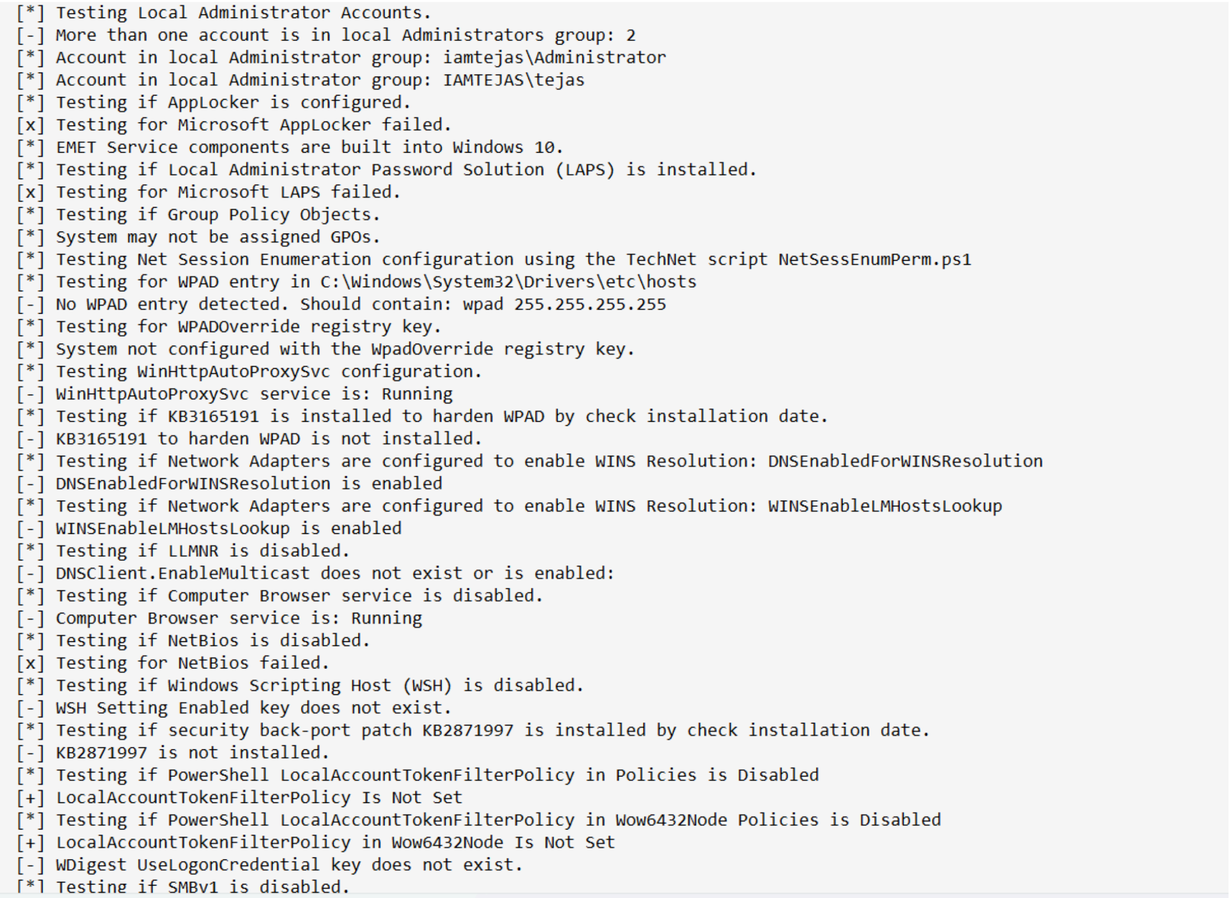
```
Network Card(s):           5 NIC(s) Installed.
                           [01]: VirtualBox Host-Only Ethernet Adapter
                                 Connection Name: VirtualBox Host-Only Network
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.56.1
                                 [02]: fe80::3a28:9904:e532:aef7
                           [02]: Realtek PCIe GbE Family Controller
                                 Connection Name: Ethernet
                                 Status:          Media disconnected
                           [03]: MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
                                 Connection Name: Wi-Fi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.177.100
                                 IP address(es)
                                 [01]: 192.168.177.116
                                 [02]: fe80::bbf:cc5f:7b8:7777
                                 [03]: 2409:4042:2d19:2d23:60fb:c575:6b75:d1c7
                                 [04]: 2409:4042:2d19:2d23:e92e:9ccb:949f:567d
                           [04]: Bluetooth Device (Personal Area Network)
                                 Connection Name: Bluetooth Network Connection
                                 Status:          Media disconnected
                           [05]: VirtualBox Host-Only Ethernet Adapter
                                 Connection Name: Ethernet 3
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.139.2
                                 [02]: fe80::86b8:7b74:fcf3:3fd9
Hyper-V Requirements:      VM Monitor Mode Extensions: Yes
                           Virtualization Enabled In Firmware: Yes
                           Second Level Address Translation: Yes
                           Data Execution Prevention Available: Yes

[*] Start Date/Time: 20240221T13163540+05
[*] Script running with Administrator rights.
[*] Dumping System Info to seperate file\n
[*] Windows Version: Microsoft Windows NT 10.0.22621.0
[*] Windows Default Path for tejas : 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:\Program Files\Git\cmd;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS
\System32\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\Users\tejas\AppData\Local\Programs\Python\Python39\Scripts\;C:\Users\tejas\AppData\Local\Programs\Python\Python39\;C:
```



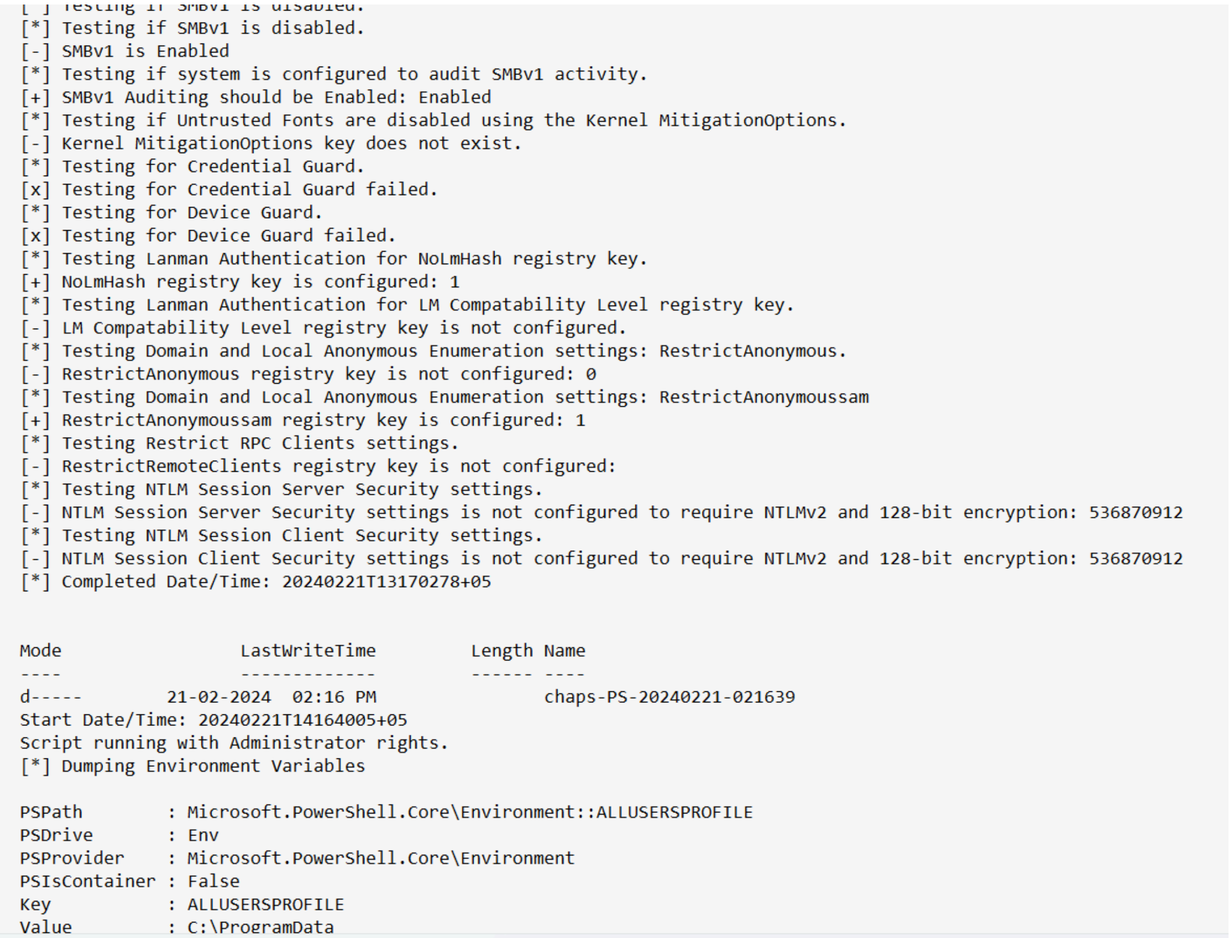
```
[*] Host network interface assigned: 169.254.76.60
[*] Host network interface assigned: 169.254.100.19
[*] Host network interface assigned: 169.254.185.54
[*] Host network interface assigned: 169.254.52.76
[*] Host network interface assigned: 192.168.177.116
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi): fe80::3a28:9904:e532:aef7
[-] Host IPv6 network interface assigned (gwmi): fe80::bbf:cc5f:7b8:7777
[-] Host IPv6 network interface assigned (gwmi): 2409:4042:2d19:2d23:60fb:c575:6b75:d1c7
[-] Host IPv6 network interface assigned (gwmi): 2409:4042:2d19:2d23:e92e:9ccb:949f:567d
[-] Host IPv6 network interface assigned (gwmi): fe80::86b8:7b74:fcf3:3fd9
[*] 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: FullyDecrypted
[*] 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: 0.008 GB
[-] 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/Operational] GB: 0.015 GB
[-] Microsoft-Windows-TaskScheduler/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-TaskScheduler/Operational] GB: 0.01 GB
[-] Microsoft-Windows-WinRM/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-WinRM/Operational] GB: 0.001 GB
[-] Microsoft-Windows-Security-Netlogon/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-Security-Netlogon/Operational] GB: 0.
[-] Microsoft-Windows-WMI-Activity/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-WMI-Activity/Operational] GB: 0.001 GB
```



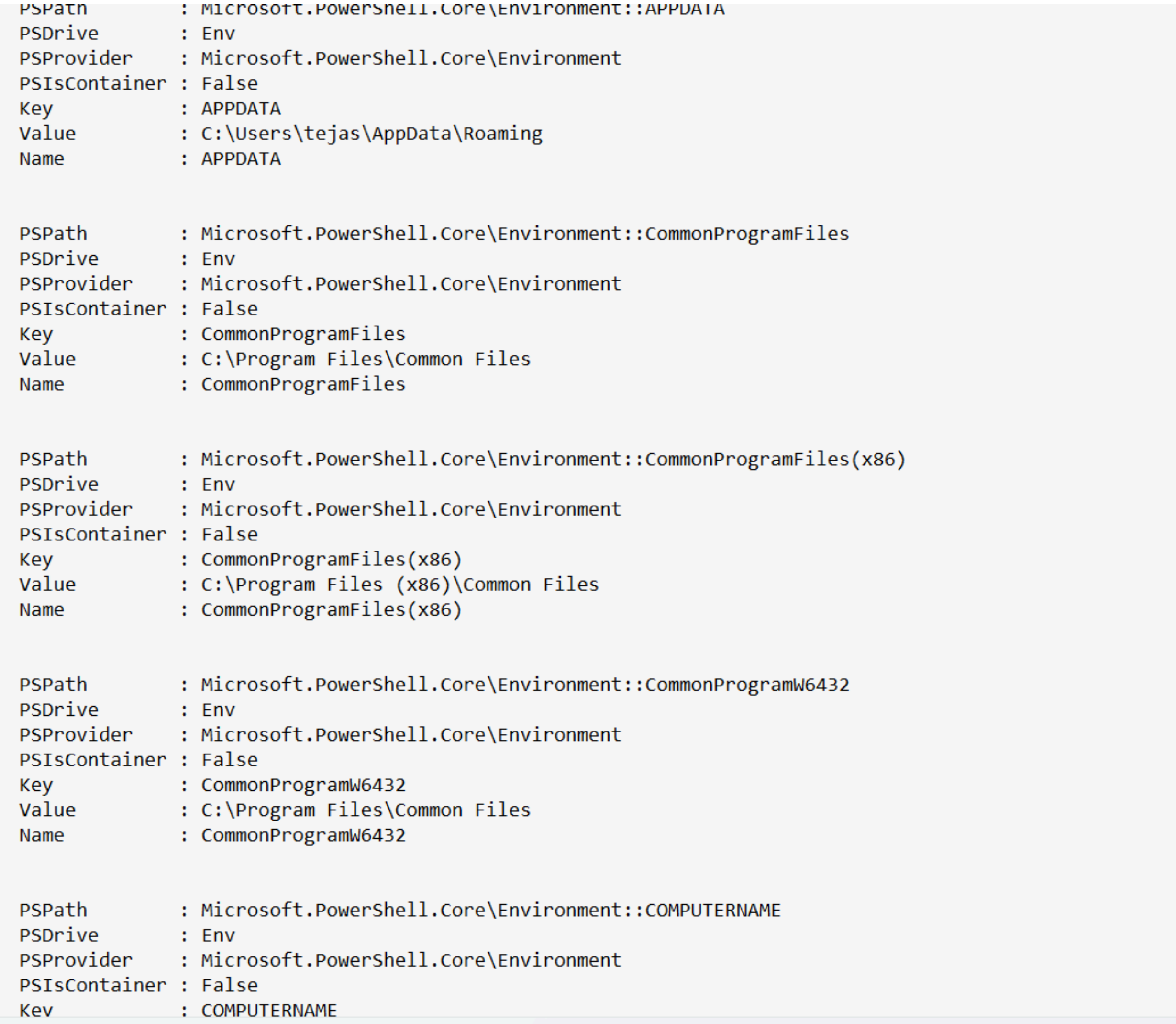
```
[-] EnableInvocationHeader Is Not Set
[*] Testing if PowerShell ProtectedEventLogging is Enabled
[-] EnableProtectedEventLogging Is Not Set
[*] Event logs settings defaults are too small. Test that max sizes have been increased.
[-] Microsoft-Windows-SMBServer/Audit max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-SMBServer/Audit] GB: 0.008 GB
[-] 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/Operational] GB: 0.015 GB
[-] Microsoft-Windows-TaskScheduler/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-TaskScheduler/Operational] GB: 0.01 GB
[-] Microsoft-Windows-WinRM/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-WinRM/Operational] GB: 0.001 GB
[-] Microsoft-Windows-Security-Netlogon/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-Security-Netlogon/Operational] GB: 0.001 GB
[-] Microsoft-Windows-WMI-Activity/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-WMI-Activity/Operational] GB: 0.001 GB
[-] Windows PowerShell max log size is smaller than System.Collections.Hashtable[Windows PowerShell] GB: 0.015 GB
[-] System max log size is smaller than System.Collections.Hashtable[System] GB: 0.02 GB
[-] Application max log size is smaller than System.Collections.Hashtable[Application] GB: 0.02 GB
[-] Microsoft-Windows-TerminalServices-LocalSessionManager/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-TerminalServices-
LocalSessionManager/Operational] GB: 0.001 GB
[*] Testing if PowerShell Version is at least version 5
[+] Current PowerShell Version: 5.1.22621.2506
[*] Testing if PowerShell Version 2 is permitted
[-] PowerShell Version 2 should be disabled: Enabled
[*] Testing if .NET Framework version supports PowerShell Version 2
[+] .NET Framework greater than 3.0 installed: 4.8.09032
[+] .NET Framework greater than 3.0 installed: 4.8.09032
[+] .NET Framework greater than 3.0 installed: 4.8.09032
[+] .NET Framework greater than 3.0 installed: 4.8.09032
[+] .NET Framework greater than 3.0 installed: 4.0.0.0
[*] Testing if PowerShell is configured to use Constrained Language.
[-] Execution Langugage Mode Is Not ConstrainedLanguage: FullLanguage
[*] Testing if system is configured to limit the number of stored credentials.
[-] CachedLogonsCount Is Not Set to 0 or 1: 10
[*] 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.
[+] WinRM Services is not running: Get-Service check.
[*] Testing if Windows Network Firewall rules allow remote connections.
[+] 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.
```



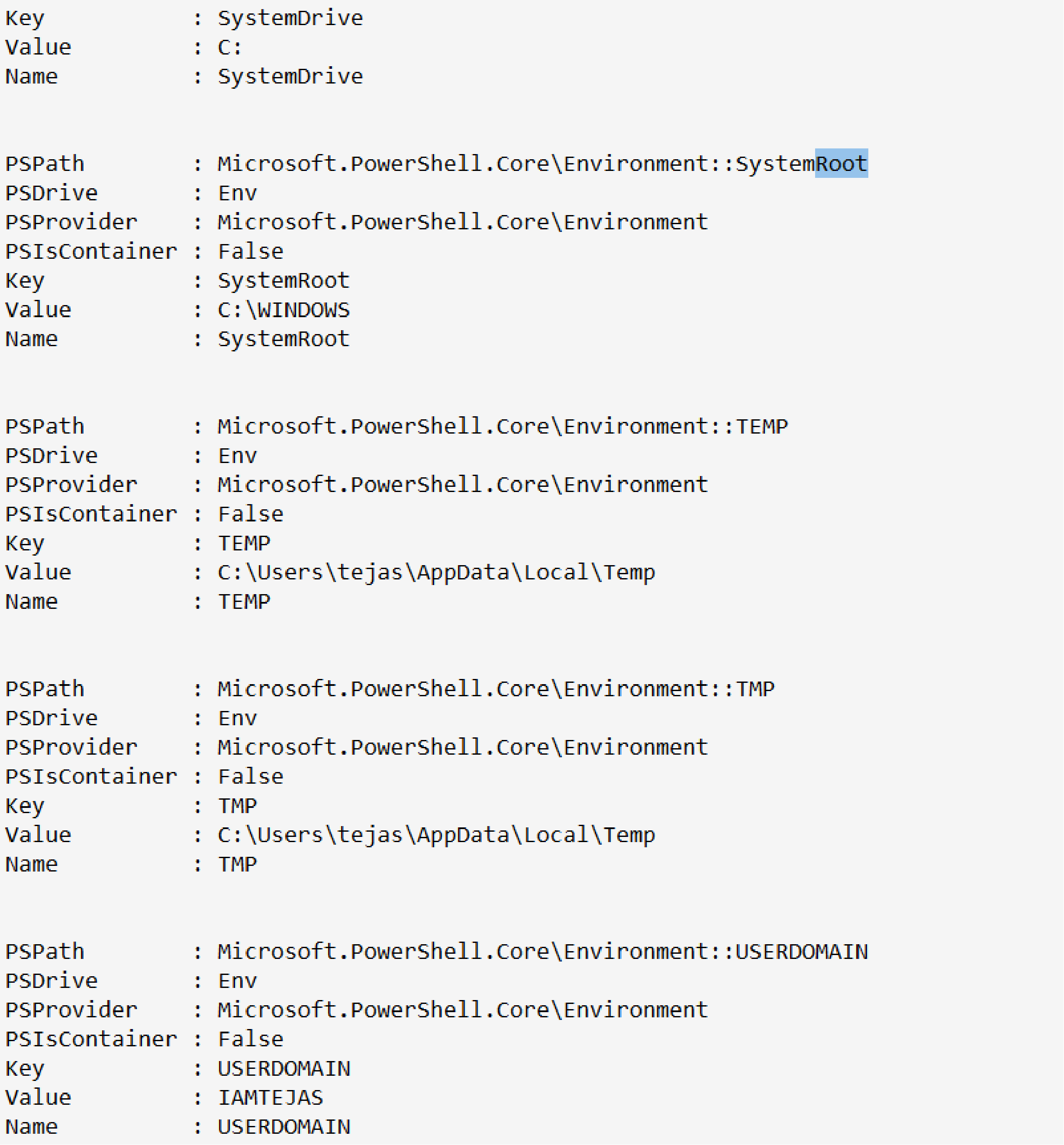
```
[*] Testing Local Administrator Accounts.
[-] More than one account is in local Administrators group: 2
[*] Account in local Administrator group: iamtejas\Administrator
[*] Account in local Administrator group: IAMTEJAS\tejas
[*] Testing if AppLocker is configured.
[x] Testing for Microsoft AppLocker failed.
[*] EMET Service components are built into Windows 10.
[*] Testing if Local Administrator Password Solution (LAPS) is installed.
[x] Testing for Microsoft LAPS failed.
[*] Testing if Group Policy Objects.
[*] System may not be assigned GPOs.
[*] Testing Net Session Enumeration configuration using the TechNet script NetSessEnumPerm.ps1
[*] Testing for WPAD entry in C:\Windows\System32\Drivers\etc\hosts
[-] No WPAD entry detected. Should contain: wpad 255.255.255.255
[*] Testing for WPADOverride registry key.
[*] System not configured with the WpadOverride registry key.
[*] Testing WinHttpAutoProxySvc configuration.
[-] WinHttpAutoProxySvc service is: Running
[*] Testing if KB3165191 is installed to harden WPAD by check installation date.
[-] KB3165191 to harden WPAD is not installed.
[*] Testing if Network Adapters are configured to enable WINS Resolution: DNSEnabledForWINSResolution
[-] DNSEnabledForWINSResolution is enabled
[*] Testing if Network Adapters are configured to enable WINS Resolution: WINSEnableLMHostsLookup
[-] WINSEnableLMHostsLookup is enabled
[*] Testing if LLMNR is disabled.
[-] DNSClient.EnableMulticast does not exist or is enabled:
[*] Testing if Computer Browser service is disabled.
[-] Computer Browser service is: Running
[*] Testing if NetBios is disabled.
[x] Testing for NetBios failed.
[*] Testing if Windows Scripting Host (WSH) is disabled.
[-] WSH Setting Enabled key does not exist.
[*] Testing if security back-port patch KB2871997 is installed by check installation date.
[-] KB2871997 is not installed.
[*] Testing if PowerShell LocalAccountTokenFilterPolicy in Policies is Disabled
[+] LocalAccountTokenFilterPolicy Is Not Set
[*] Testing if PowerShell LocalAccountTokenFilterPolicy in Wow6432Node Policies is Disabled
[+] LocalAccountTokenFilterPolicy in Wow6432Node Is Not Set
[-] WDigest UseLogonCredential key does not exist.
[*] Testing if SMBv1 is disabled.
```



```
[*] Testing if SMBv1 is disabled.
[*] Testing if SMBv1 is disabled.
[-] SMBv1 is Enabled
[*] Testing if system is configured to audit SMBv1 activity.
[+] SMBv1 Auditing should be Enabled: Enabled
[*] Testing if Untrusted Fonts are disabled using the Kernel MitigationOptions.
[-] Kernel MitigationOptions key does not exist.
[*] Testing for Credential Guard.
[x] Testing for Credential Guard failed.
[*] Testing for Device Guard.
[x] Testing for Device Guard failed.
[*] Testing Lanman Authentication for NoLmHash registry key.
[+] NoLmHash registry key is configured: 1
[*] Testing Lanman Authentication for LM Compatability Level registry key.
[-] LM Compatability Level registry key is not configured.
[*] Testing Domain and Local Anonymous Enumeration settings: RestrictAnonymous.
[-] RestrictAnonymous registry key is not configured: 0
[*] Testing Domain and Local Anonymous Enumeration settings: RestrictAnonymoussam
[+] RestrictAnonymoussam registry key is configured: 1
[*] Testing Restrict RPC Clients settings.
[-] RestrictRemoteClients registry key is not configured:
[*] Testing NTLM Session Server Security settings.
[-] NTLM Session Server Security settings is not configured to require NTLMv2 and 128-bit encryption: 536870912
[*] Testing NTLM Session Client Security settings.
[-] NTLM Session Client Security settings is not configured to require NTLMv2 and 128-bit encryption: 536870912
[*] Completed Date/Time: 20240221T13170278+05


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        21-02-2024  02:16 PM                chaps-PS-20240221-021639
Start Date/Time: 20240221T14164005+05
Script running with Administrator rights.
[*] Dumping Environment Variables

PSPath        : Microsoft.PowerShell.Core\Environment::ALLUSERSPROFILE
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : ALLUSERSPROFILE
Value         : C:\ProgramData
```



```
PSPath        : Microsoft.PowerShell.Core\Environment::APPDATA
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : APPDATA
Value         : C:\Users\tejas\AppData\Roaming
Name          : APPDATA


PSPath        : Microsoft.PowerShell.Core\Environment::CommonProgramFiles
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : CommonProgramFiles
Value         : C:\Program Files\Common Files
Name          : CommonProgramFiles


PSPath        : Microsoft.PowerShell.Core\Environment::CommonProgramFiles(x86)
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : CommonProgramFiles(x86)
Value         : C:\Program Files (x86)\Common Files
Name          : CommonProgramFiles(x86)


PSPath        : Microsoft.PowerShell.Core\Environment::CommonProgramW6432
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : CommonProgramW6432
Value         : C:\Program Files\Common Files
Name          : CommonProgramW6432


PSPath        : Microsoft.PowerShell.Core\Environment::COMPUTERNAME
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : COMPUTERNAME
```



```
Key           : SystemDrive
Value         : C:
Name          : SystemDrive


PSPath        : Microsoft.PowerShell.Core\Environment::SystemRoot
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : SystemRoot
Value         : C:\WINDOWS
Name          : SystemRoot


PSPath        : Microsoft.PowerShell.Core\Environment::TEMP
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : TEMP
Value         : C:\Users\tejas\AppData\Local\Temp
Name          : TEMP


PSPath        : Microsoft.PowerShell.Core\Environment::TMP
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : TMP
Value         : C:\Users\tejas\AppData\Local\Temp
Name          : TMP


PSPath        : Microsoft.PowerShell.Core\Environment::USERDOMAIN
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : USERDOMAIN
Value         : IAMTEJAS
Name          : USERDOMAIN
```

This concludes the CHAPS Hardening Assessment Report