Assignment Report

CHAPS (Configuration Hardening Assessment PowerShell Script)

Prepared by: Saifur Rehman
Date: 22/02/2023
Client: Saifur Rehman PC

Contents

Executive Summary

The Configuration Hardening Assessment PowerShell Script (CHAPS) was executed on the system to evaluate its security posture and identify potential vulnerabilities.

The assessment revealed a combination of strengths and weaknesses in various security aspects. While certain measures such as Windows AutoU-pdate configuration and protocol security demonstrate proactive steps towards mitigating risks, critical areas such as encryption status, PowerShell security features, and event log sizes require immediate attention. Recommendations have been provided to address these weaknesses and enhance the overall security posture of the system.

This assessment report provides a comprehensive analysis of the security posture of a Windows system. Through a series of checks, we identified both strengths and weaknesses in the system's security configuration. Key findings include:

- Adequate Windows Auto-Update configuration.
- Lack of BitLocker encryption.
- Inadequate configuration of PowerShell security features.
- Event log sizes smaller than recommended.
- Presence of multiple accounts in the local Administrators group.
- Enabling of outdated protocols like Net-Bios and SMBv1.
- Absence of advanced security features such as Device Guard and Credential Guard.

Assessment Overview

The assessment covered the following areas

- System Information
- Windows Update Configuration
- Encryption Status
- PowerShell Security Features
- Event Log Sizes
- Local Administrator Accounts
- Protocol Security
- Advanced Security Features

System Information

Operating System: Microsoft Windows NT 10.0.22631.0

Default Path: The default path for system executables includes various directories such as

- C:\Program Files\Microsoft\jdk-11.0.16.101-hotspot\bin,
- C:\Program Files (x86)\VMware\VMware Workstation\bin\,
- C:\Windows\system32, and others.

Network Interfaces: The host has multiple network interfaces assigned with IP addresses

- 192.168.56.1,
- 192.168.142.1,
- 192.168.66.1,
- 192.168.1.73,
- 169.254.X.X and so on

Windows Version: Windows_NT
PowerShell Version: 5.1.22621.2506
Processor Architecture: AMD64
Number of Processors: 32
System Drive: C:
System Root: C:\Windows

Windows Update Configuration

Auto-Update Setting: The Auto-Update setting is configured with the value 4.

Meaning of Auto-Update Value 4: Value **4** typically corresponds to automatic download and scheduled installation of updates every day. This setting ensures that critical and important updates are downloaded and installed automatically on the system without user intervention.

Implication: With Auto-Update set to value 4, the system is configured to maintain up-to-date security patches by automatically downloading and installing critical and important updates on a daily basis.

Advantages:

- Ensures timely installation of critical and important updates, reducing the risk of vulnerabilities being exploited.
- Minimizes the burden on users or administrators to manually check for and install updates regularly.
- Enhances overall system security by keeping the operating system and software components up-to-date with the latest security patches.

Considerations:

- While automatic updates are convenient for ensuring system security, they may occasionally cause system reboots or disrupt ongoing work if not scheduled appropriately.
- It's important to monitor the update process to ensure that updates are applied successfully without any errors or compatibility issues.

Recommendations:

- Regularly review the update process and monitor system performance after updates to address any issues promptly.
- Ensure that critical and important updates are being installed successfully and that there are no pending updates or failures in the update process.
- Consider configuring maintenance windows or scheduling updates during off-peak hours to minimize disruptions to users or critical business operations.

Encryption Status

BitLocker Encryption:

- BitLocker encryption was not detected on the system.
- BitLocker is a feature in Windows that provides full disk encryption to protect data stored on the system's hard drives.
- Its absence suggests that the system's data is not encrypted using BitLocker.

Other Encryption Methods:

- The assessment report does not provide information about other encryption methods.
- It only mentions the absence of BitLocker encryption.

Implications:

- Without BitLocker or any other disk encryption mechanism in place, the data stored on the system's hard drives may be vulnerable to unauthorized access if the physical storage devices are compromised or stolen.
- Sensitive information stored on the system, such as personal files, credentials, or business data, may be at risk of exposure in the event of a security breach.

Recommendations:

- Consider implementing disk encryption using BitLocker or another reputable encryption solution to protect sensitive data on the system's hard drives.
- Ensure that encryption keys are securely managed and stored to prevent unauthorized access to encrypted data.
- Regularly review and update encryption policies and practices to align with security best practices and compliance requirements.
- BitLocker encryption is not detected, leaving data vulnerable to unauthorized access. Implementation of BitLocker is recommended to enhance data security.

PowerShell Security Features

PowerShell Command-line Auditing:

- The report indicates that the PowerShell commandline auditing feature is not enabled (‘**ProcessCreationIncludeCmdLine_Enabled**’ is not set). This feature allows organizations to log detailed information about PowerShell commands executed on the system, enabling better visibility into potential security incidents or malicious activities.

PowerShell Script Logging:

- Various PowerShell script logging features are not enabled such as
  - **EnableModuleLogging**
  - **EnableScriptBlockLogging**
  - **EnableScriptBlockInvocationLogging**
  - **EnableTranscripting**
  - **EnableInvocationHeader**
  - **EnableProtectedEventLogging**

- These features help in tracking and logging PowerShell script activities, including script blocks executed, module usage, and transcripts of PowerShell sessions, enhancing the ability to detect and investigate suspicious behavior.

PowerShell Version:

- The system is running PowerShell version **5.1.22621.2506**. It's essential to keep PowerShell updated to leverage the latest security enhancements and features provided by newer versions.

PowerShell Constrained Language Mode:

- The assessment indicates that PowerShell is not configured to use Constrained Language mode (**Execution Langugage Mode Is Not ConstrainedLanguage: FullLanguage**).
- Constrained Language mode restricts the use of certain PowerShell language elements and cmdlets to enhance security by reducing the attack surface for malicious scripts.

PowerShell Execution Policy:

- The PowerShell execution policy preference is set to Bypass, which allows the execution of scripts without any restrictions.
- This setting may increase the risk of running malicious scripts and should be reviewed to ensure scripts are executed securely.

Event Log Sizes

Microsoft-Windows-SMBServer/Audit Log:

- The log size test failed, indicating that the log size may be insufficient for recording SMB Server audit events.
- Adequate log size is crucial for capturing detailed information about SMB Server activities, including file and folder access, authentication attempts, and other security-related events.

Security Log:

- The test for the Security log size failed, suggesting that the log size may be too small. The Security log records security-related events such as authentication, authorization, and access control events.
- Insufficient log size may lead to the loss of critical security event data, hindering incident detection and response efforts.

Microsoft-Windows-PowerShell/Operational Log:

- The maximum log size for the PowerShell Operational log is smaller than recommended (**GB: 0.015 GB**).

- This log captures detailed information about PowerShell script execution, including script block logging and module usage.
- Increasing the log size ensures that all relevant PowerShell activities are recorded for security analysis and troubleshooting purposes.

Other Event Logs:

- Similar findings were observed for other event logs such as
  - **Microsoft-Windows-TaskScheduler/Operational**
  - **Microsoft-Windows-WinRM/Operational**
  - **Microsoft-Windows-Security-Netlogon/Operational**
  - **Microsoft-Windows-WMI-Activity/Operational**
- In each case, the maximum log size was smaller than recommended, potentially limiting the amount of event data that can be stored.

Local Administrator Accounts

Number of Accounts: The assessment identified two accounts that belong to the local Administrators group.

Account Details:

- **Saifur\Administrator:** This account is a member of the local Administrators group. The "**Administrator**" account is a default built-in account in Windows systems and typically holds elevated privileges.
- **SAIFUR\saifr:** Another account named "**saifr**" is also part of the local Administrators group. This account appears to be a user-specific account with administrative privileges.

Implications:

- Having multiple accounts with administrative privileges increases the potential attack surface and poses security risks.
- Malicious actors could compromise any of these accounts to gain elevated privileges and potentially carry out unauthorized actions on the system.
- It's crucial to regularly review the membership of the local Administrators group and remove any unnecessary accounts to minimize the risk of privilege escalation attacks.

Recommendations:

- Conduct a thorough review of the accounts in the local Administrators group and ensure that only essential accounts have administrative privileges.
- Remove any unnecessary or unused accounts from the local Administrators group to reduce the risk of unauthorized access.

- Implement the principle of least privilege (**PoLP**) by assigning administrative privileges only to accounts that require them for specific tasks.
- Monitor the activity of administrative accounts closely and implement strong password policies to enhance security. Regularly audit and rotate passwords for these accounts to mitigate the risk of credential compromise.

Protocol Security

WinRM Firewall Rules:

- The assessment identified disabled WinRM Firewall rules, indicating that certain WinRM (Windows Remote Management) traffic may be blocked.
- WinRM is Microsoft's implementation of the WS-Management Protocol, which allows remote management of Windows systems over HTTP(S).
- The presence of disabled WinRM Firewall rules suggests that specific configurations or restrictions are in place regarding remote management protocols.

SMBv1 Configuration:

- The assessment tested for the status of SMBv1 (Server Message Block version 1), an older network file-sharing protocol.
- It revealed that SMBv1 is enabled on the system.
- SMBv1 is known to have security vulnerabilities, and its usage is discouraged due to the risk of exploitation by malware such as WannaCry and NotPetya.

SMBv1 Auditing:

- The assessment also checked if auditing for SMBv1 activity is enabled.
- It indicated that SMBv1 auditing should be enabled but did not specify whether it is actually configured as such.
- Enabling auditing for SMBv1 activity can provide visibility into file-sharing activities and help in detecting and investigating potential security incidents.

Implications:

- Enabling outdated or insecure protocols like SMBv1 can expose the system to known vulnerabilities and increase the risk of exploitation by malicious actors.
- Proper configuration and auditing of network protocols are essential for maintaining a secure network environment and protecting sensitive data from unauthorized access or exfiltration.

Recommendations:

- Disable SMBv1 protocol if not required for compatibility reasons and migrate to newer, more secure versions such as SMBv2 or SMBv3.
- Regularly review and update firewall rules to ensure that only necessary network traffic is allowed, and disable unused or unnecessary protocols.
- Implement network segmentation and access controls to restrict the communication between different network segments and mitigate the impact of potential protocol-based attacks.
- Enable auditing for critical network protocols to monitor for suspicious activities and facilitate incident response and forensic investigations.

Advanced Security Features

PowerShell Security Features:

- The assessment tested various PowerShell security features such as Commandline Auditing, Module Logging, Script Block Logging, Script Block Invocation Logging, Transcripting, Invocation Header, and Protected Event Logging.
- These features are designed to enhance PowerShell script and command security by providing detailed logging and auditing capabilities, which can help in identifying and investigating potential security incidents involving PowerShell scripts.

LocalAccountTokenFilterPolicy:

- The assessment checked if the LocalAccountTokenFilterPolicy is disabled. This policy controls whether administrative accounts can remotely access the system over the network without having their credentials filtered out.
- Disabling this policy enhances security by requiring administrative users to authenticate with full credentials when accessing the system remotely, reducing the risk of unauthorized access.

AppLocker:

- The assessment tested for AppLocker configuration, which is a security feature that allows administrators to control which applications are allowed to run on a system.
- AppLocker helps prevent unauthorized software from running and can mitigate the risk of malware infections and other security threats.

Windows Scripting Host (WSH):

- The assessment checked if Windows Scripting Host (WSH) is disabled. WSH is a Windows administration tool that allows scripts to automate tasks.

- Disabling WSH can enhance security by preventing malicious scripts from executing on the system, reducing the risk of script-based attacks.

Kernel MitigationOptions:

- The assessment checked for the presence of the Kernel MitigationOptions key, which can be used to enable various security mitigations in the Windows kernel.
- These mitigations include protections against certain types of exploits and attacks, such as DEP (Data Execution Prevention) and ASLR (Address Space Layout Randomization).

Credential Guard and Device Guard:

- The assessment tested for the presence of Credential Guard and Device Guard, which are advanced security features available in Windows that protect against credential theft and malware attacks.
- These features use virtualization-based security to isolate sensitive processes and code, reducing the risk of unauthorized access and malware infections.
- Advanced security features such as Device Guard and Credential Guard are not detected, indicating a lack of defense against advanced threats.

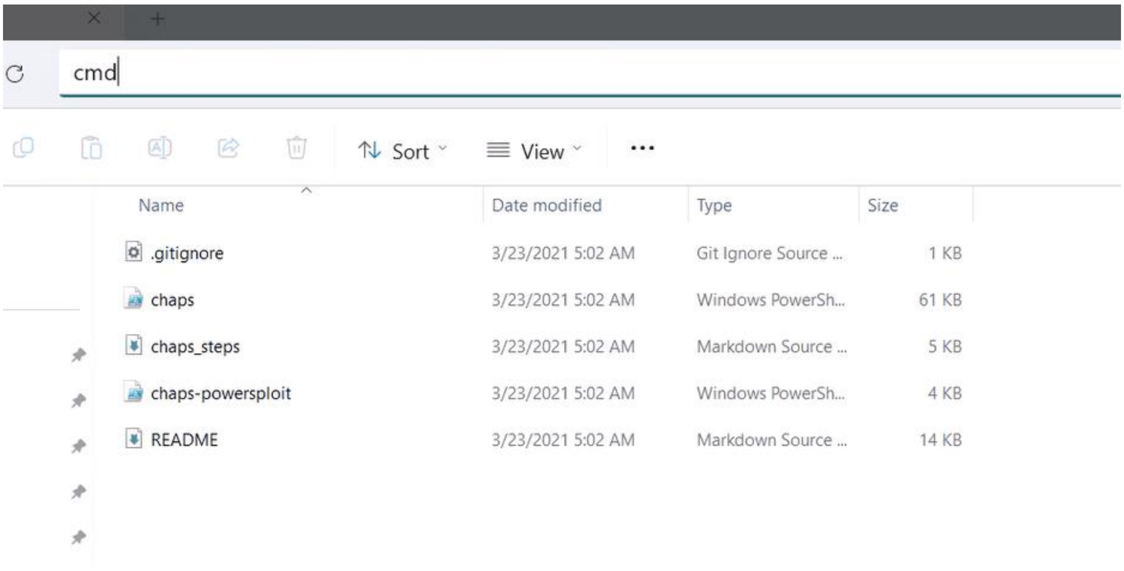
Conclusion

The assessment report highlights both strengths and weaknesses in the system's security posture. While certain measures such as Windows Auto-Update configuration and protocol security demonstrate proactive steps towards mitigating risks, critical areas such as encryption status, PowerShell security features, and event log sizes require immediate attention. By addressing these weaknesses and implementing recommended measures, the system can enhance its overall security posture and better defend against a wide range of cyber threats.

Annexture I

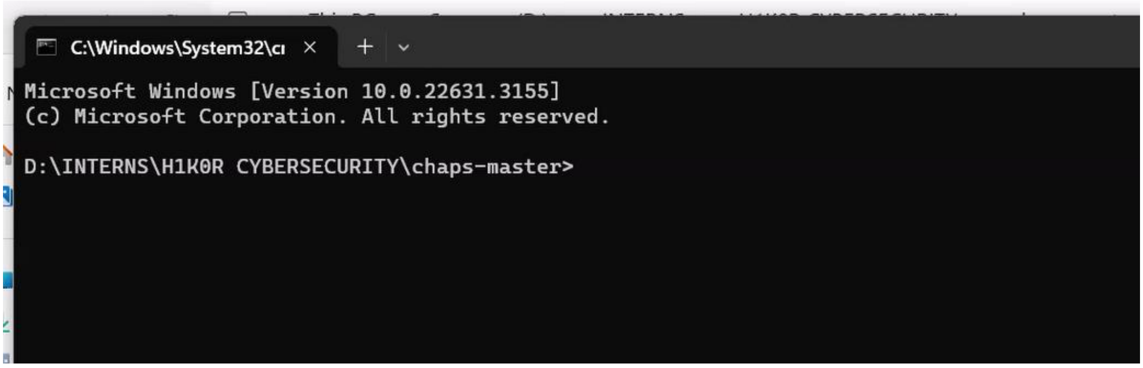
STAPES FOLLOWED IN ASSESSMENT

Step 1: Open the CHAPS-MASTER Folder then Run CMD or Open CMD and enter into CHAPS Directory



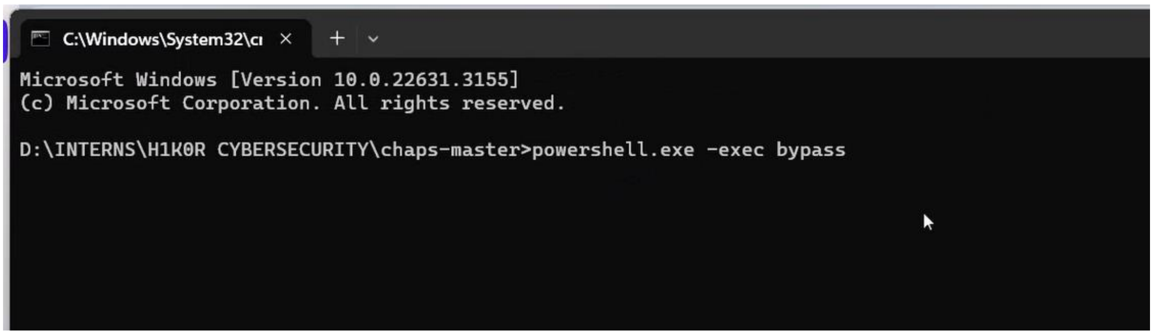
cmd

Name	Date modified	Type	Size
.gitignore	3/23/2021 5:02 AM	Git Ignore Source ...	1 KB
chaps	3/23/2021 5:02 AM	Windows PowerSh...	61 KB
chaps_steps	3/23/2021 5:02 AM	Markdown Source ...	5 KB
chaps-powersploit	3/23/2021 5:02 AM	Windows PowerSh...	4 KB
README	3/23/2021 5:02 AM	Markdown Source ...	14 KB



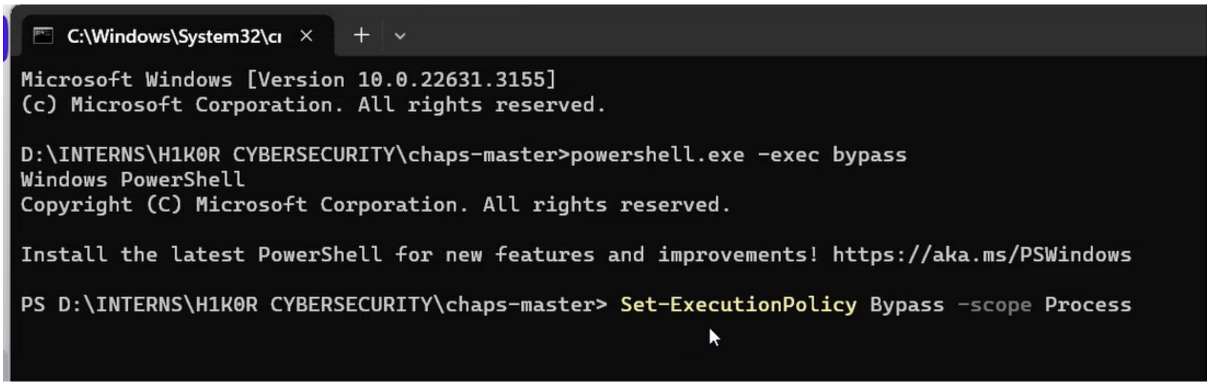
```
Microsoft Windows [Version 10.0.22631.3155]
(c) Microsoft Corporation. All rights reserved.

D:\INTERNS\H1K0R CYBERSECURITY\chaps-master>
```

Step 2: Run the command: ***powershell.exe -exec bypass***



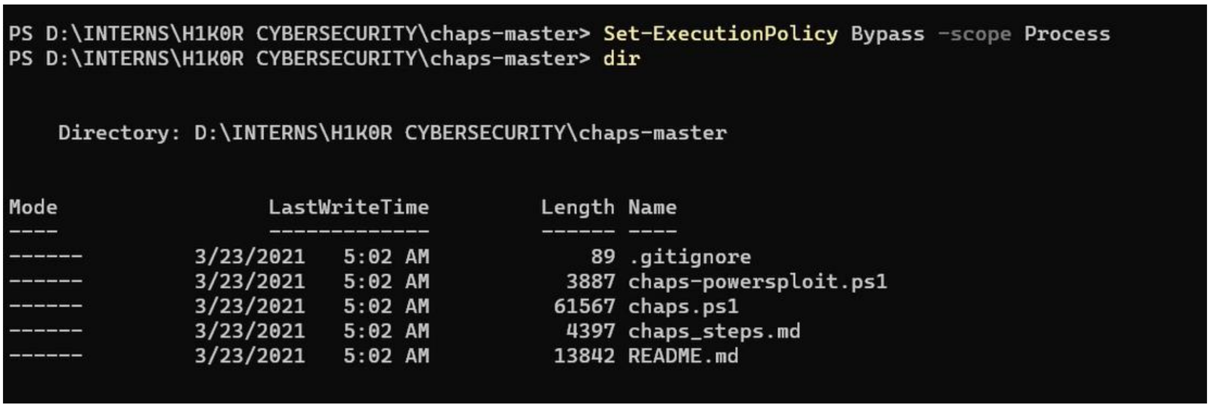
```
Microsoft Windows [Version 10.0.22631.3155]
(c) Microsoft Corporation. All rights reserved.

D:\INTERNS\H1K0R CYBERSECURITY\chaps-master>powershell.exe -exec bypass
```

Step 3: Run the command: ***Set-ExecutionPolicy Bypass -scope Process***



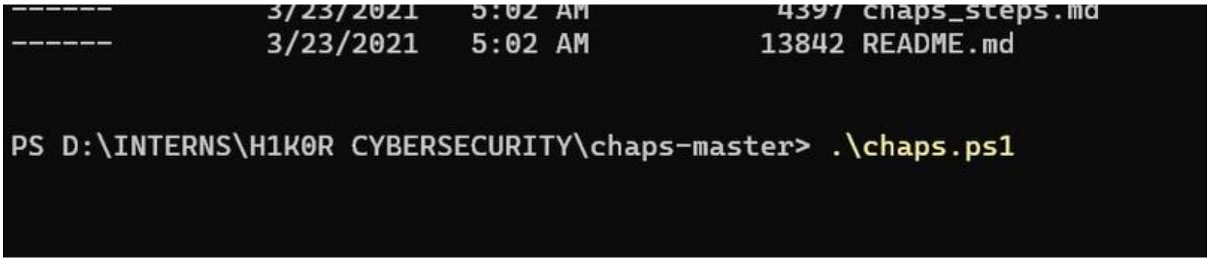
```
Microsoft Windows [Version 10.0.22631.3155]
(c) Microsoft Corporation. All rights reserved.

D:\INTERNS\H1K0R CYBERSECURITY\chaps-master>powershell.exe -exec bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS D:\INTERNS\H1K0R CYBERSECURITY\chaps-master> Set-ExecutionPolicy Bypass -scope Process
```

Step 4: Then To view the contents (Files/Directories) within the CHAPS-MASTER Directory use ***DIR*** Command

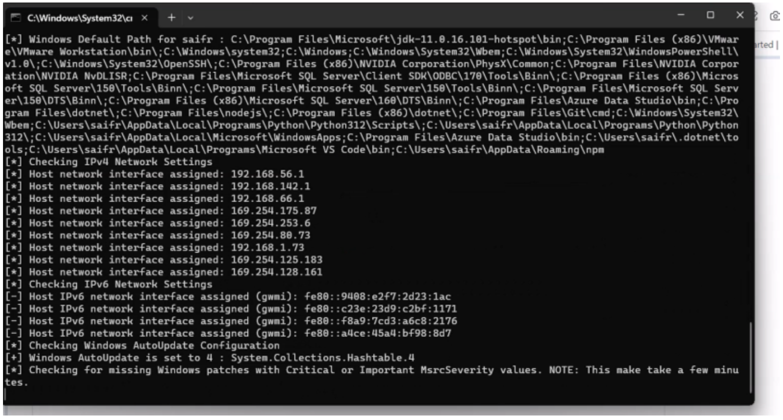


```
PS D:\INTERNS\H1K0R CYBERSECURITY\chaps-master> Set-ExecutionPolicy Bypass -scope Process
PS D:\INTERNS\H1K0R CYBERSECURITY\chaps-master> dir


    Directory: D:\INTERNS\H1K0R CYBERSECURITY\chaps-master


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
------         3/23/2021   5:02 AM             89 .gitignore
------         3/23/2021   5:02 AM           3887 chaps-powersploit.ps1
------         3/23/2021   5:02 AM          61567 chaps.ps1
------         3/23/2021   5:02 AM           4397 chaps_steps.md
------         3/23/2021   5:02 AM          13842 README.md
```

Step 5: Now Run the **chaps.ps1** file using ***.\chaps.ps1*** Command.

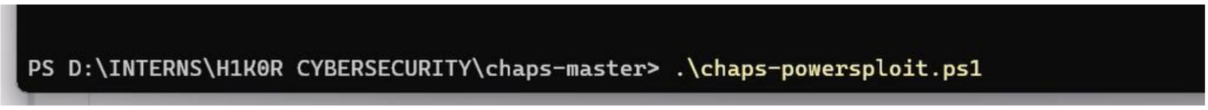


```
------         3/23/2021   5:02 AM           4397 chaps_steps.md
------         3/23/2021   5:02 AM          13842 README.md


PS D:\INTERNS\H1K0R CYBERSECURITY\chaps-master> .\chaps.ps1
```

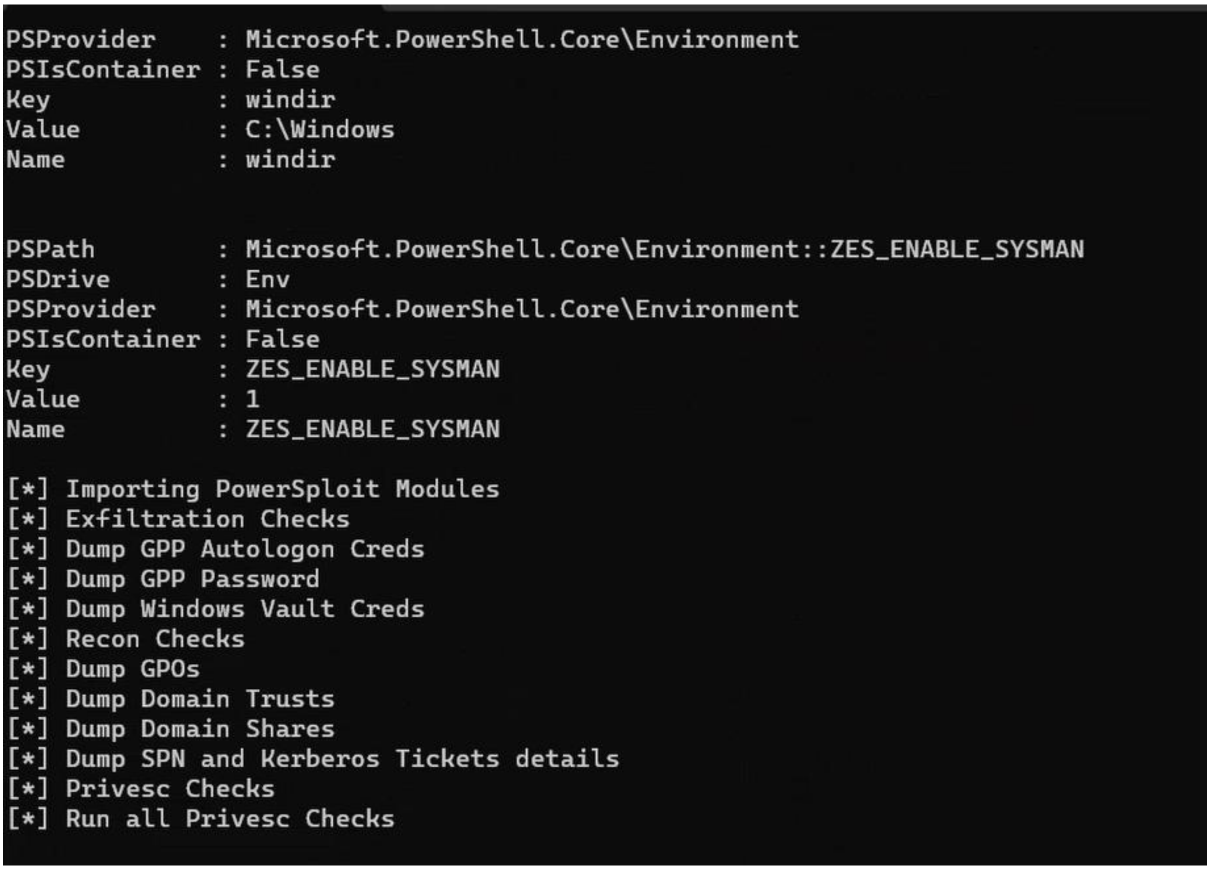


```
[*] Windows Default Path for saifr : C:\Program Files\Microsoft\jdk-11.0.16.101-hotspot\bin;C:\Program Files (x86)\VMwar
e\VMware Workstation\bin\;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\
v1.0\;C:\Windows\System32\OpenSSH\;C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common;C:\Program Files\NVIDIA Corpor
ation\NVIDIA NvDLISR;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\;C:\Program Files (x86)\Micros
oft SQL Server\150\Tools\Binn\;C:\Program Files\Microsoft SQL Server\150\Tools\Binn\;C:\Program Files\Microsoft SQL Serv
er\150\DTS\Binn\;C:\Program Files (x86)\Microsoft SQL Server\160\DTS\Binn\;C:\Program Files\Azure Data Studio\bin;C:\Pro
gram Files\dotnet\;C:\Program Files\nodejs\;C:\Program Files (x86)\dotnet\;C:\Program Files\Git\cmd;C:\Windows\System32\
Wbem;C:\Users\saifr\AppData\Local\Programs\Python\Python312\Scripts\;C:\Users\saifr\AppData\Local\Programs\Python\Python
312\;C:\Users\saifr\AppData\Local\Microsoft\WindowsApps;C:\Program Files\Azure Data Studio\bin;C:\Users\saifr\.dotnet\to
ols;C:\Users\saifr\AppData\Local\Programs\Microsoft VS Code\bin;C:\Users\saifr\AppData\Roaming\npm
[*] Checking IPv4 Network Settings
[*] Host network interface assigned: 192.168.56.1
[*] Host network interface assigned: 192.168.142.1
[*] Host network interface assigned: 192.168.66.1
[*] Host network interface assigned: 169.254.175.87
[*] Host network interface assigned: 169.254.253.6
[*] Host network interface assigned: 169.254.80.73
[*] Host network interface assigned: 192.168.1.73
[*] Host network interface assigned: 169.254.125.183
[*] Host network interface assigned: 169.254.128.161
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi): fe80::9408:e2f7:2d23:1ac
[-] Host IPv6 network interface assigned (gwmi): fe80::c23e:23d9:c2bf:1171
[-] Host IPv6 network interface assigned (gwmi): fe80::f8a9:7cd3:a6c8:2176
[-] Host IPv6 network interface assigned (gwmi): fe80::a4ce:45a4:bf98:8d7
[*] 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 minu
tes.
```

Step 6: Then Run the **chaps-powersploit.ps1** file using ***.\chaps-powersploit .ps1*** Command.



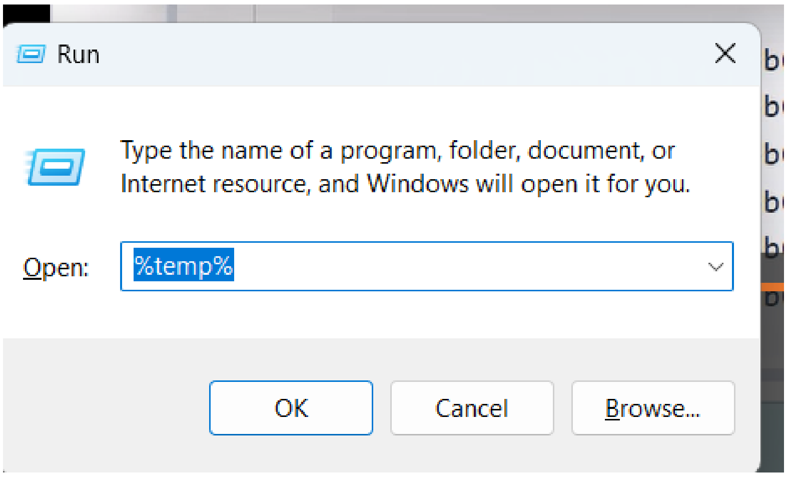
```
PS D:\INTERNS\H1K0R CYBERSECURITY\chaps-master> .\chaps-powersploit.ps1
```



```
PSProvider     : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key            : windir
Value          : C:\Windows
Name           : windir


PSPath         : Microsoft.PowerShell.Core\Environment::ZES_ENABLE_SYSMAN
PSDrive        : Env
PSProvider     : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key            : ZES_ENABLE_SYSMAN
Value          : 1
Name           : ZES_ENABLE_SYSMAN

[*] Importing PowerSploit Modules
[*] Exfiltration Checks
[*] Dump GPP Autologon Creds
[*] Dump GPP Password
[*] Dump Windows Vault Creds
[*] Recon Checks
[*] Dump GPOs
[*] Dump Domain Trusts
[*] Dump Domain Shares
[*] Dump SPN and Kerberos Tickets details
[*] Privesc Checks
[*] Run all Privesc Checks
```

Step 7: To view the report go to TEMP Directory as follows:

Windows Key +R (Run) >> ***Type %temp%***

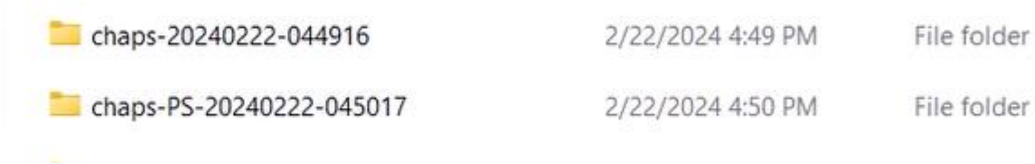


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

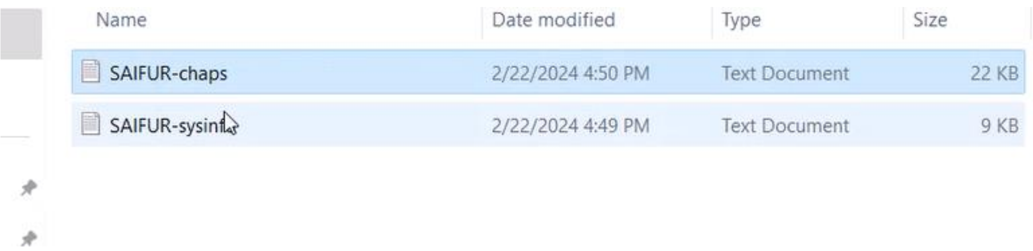
Open: %temp%

Step 8: Find below three Files within **chap-[date-time]** Folders in TEMP Directory and Observe the Assessment Report for Vulnerabilities or system hardening.

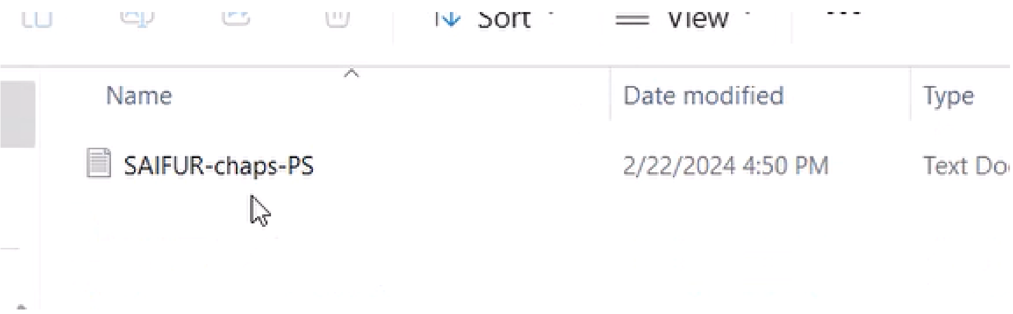
[systemName]-chaps
[systemName]-sysinfo
[systemName]-chaps-PS



chaps-20240222-044916	2/22/2024 4:49 PM	File folder
chaps-PS-20240222-045017	2/22/2024 4:50 PM	File folder



Name	Date modified	Type	Size
SAIFUR-chaps	2/22/2024 4:50 PM	Text Document	22 KB
SAIFUR-sysinfo	2/22/2024 4:49 PM	Text Document	9 KB

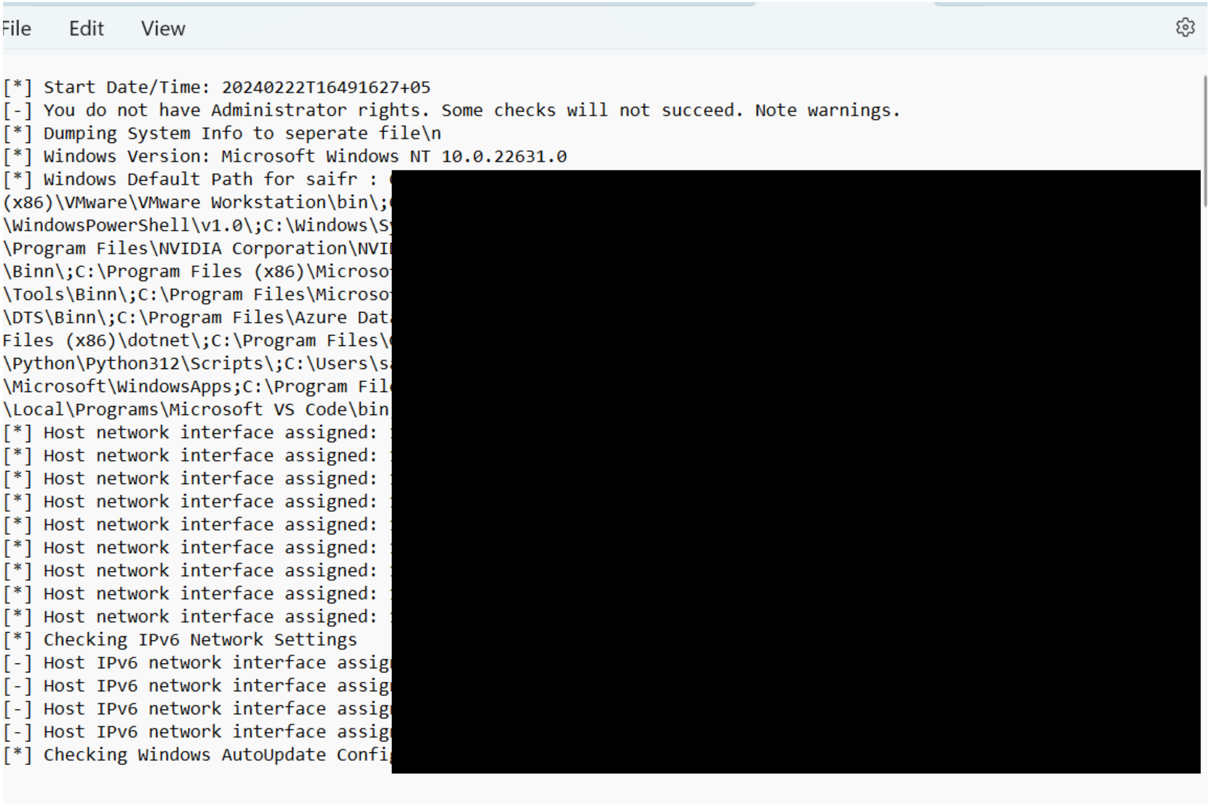


Name	Date modified	Type
SAIFUR-chaps-PS	2/22/2024 4:50 PM	Text Do

ANNEXTURE II

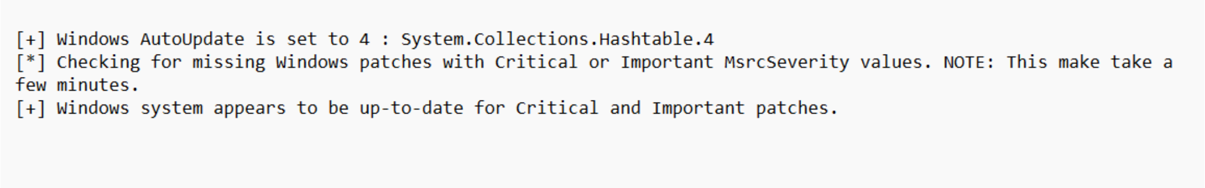
ASSESMENT REPORT OBSERVATION

1. System Information



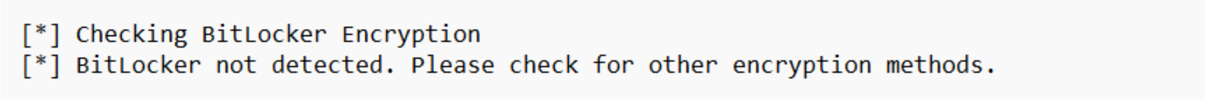
```
[*] Start Date/Time: 20240222T16491627+05
[-] You do not have Administrator rights. Some checks will not succeed. Note warnings.
[*] Dumping System Info to seperate file\n
[*] Windows Version: Microsoft Windows NT 10.0.22631.0
[*] Windows Default Path for saifr : [redacted]
(x86)\VMware\VMware Workstation\bin\;
\WindowsPowerShell\v1.0\;C:\Windows\S
\Program Files\NVIDIA Corporation\NVI
\Binn\;C:\Program Files (x86)\Microso
\Tools\Binn\;C:\Program Files\Microso
\DTS\Binn\;C:\Program Files\Azure Dat
Files (x86)\dotnet\;C:\Program Files\
\Python\Python312\Scripts\;C:\Users\s
\Microsoft\WindowsApps;C:\Program Fil
\Local\Programs\Microsoft VS Code\bin
[*] Host network interface assigned:
[*] Host network interface assigned:
[*] Host network interface assigned:
[*] Host network interface assigned:
[*] 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 assig
[-] Host IPv6 network interface assig
[-] Host IPv6 network interface assig
[-] Host IPv6 network interface assig
[*] Checking Windows AutoUpdate Confi
```

2. Windows Update



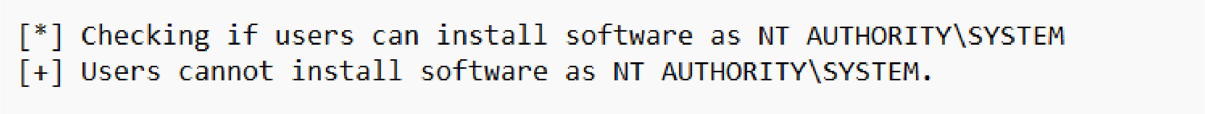
```
[+] Windows AutoUpdate is set to 4 : System.Collections.Hashtable.4
[*] Checking for missing Windows patches with Critical or Important MsrcSeverity values. NOTE: This make take a
few minutes.
[+] Windows system appears to be up-to-date for Critical and Important patches.
```

3. Checking BitLocker Encryption



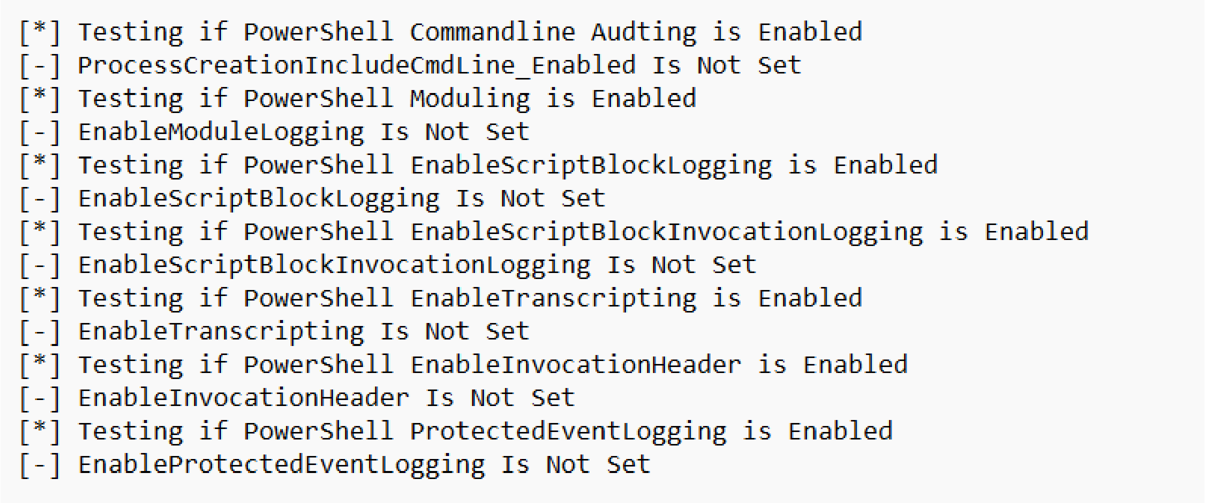
```
[*] Checking BitLocker Encryption
[*] BitLocker not detected. Please check for other encryption methods.
```

4. Checking if users can install software as NT AUTHORITY\SYSTEM



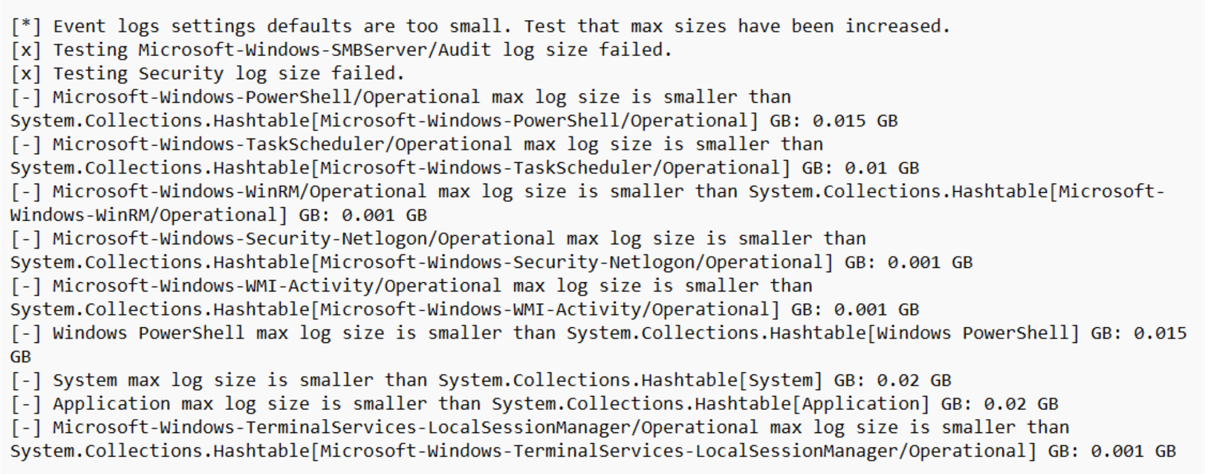
```
[*] Checking if users can install software as NT AUTHORITY\SYSTEM
[+] Users cannot install software as NT AUTHORITY\SYSTEM.
```

5. Testing if PowerShell Scripts are Enabled



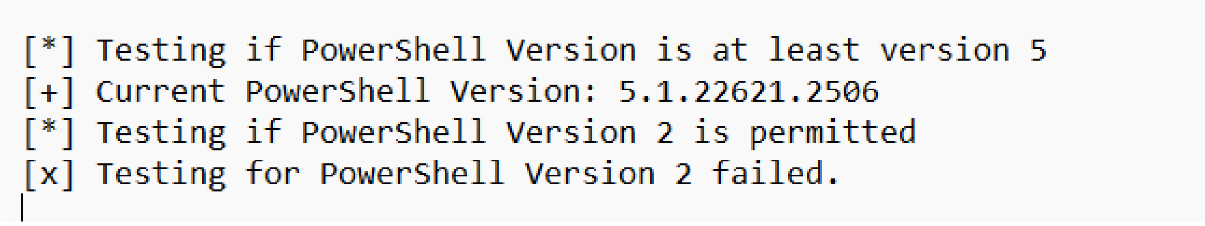
```
[*] Testing if PowerShell Commandline Audting is Enabled
[-] ProcessCreationIncludeCmdLine_Enabled Is Not Set
[*] Testing if PowerShell Moduling is Enabled
[-] EnableModuleLogging Is Not Set
[*] Testing if PowerShell EnableScriptBlockLogging is Enabled
[-] EnableScriptBlockLogging Is Not Set
[*] 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
```

6. Checking for Event and other log size



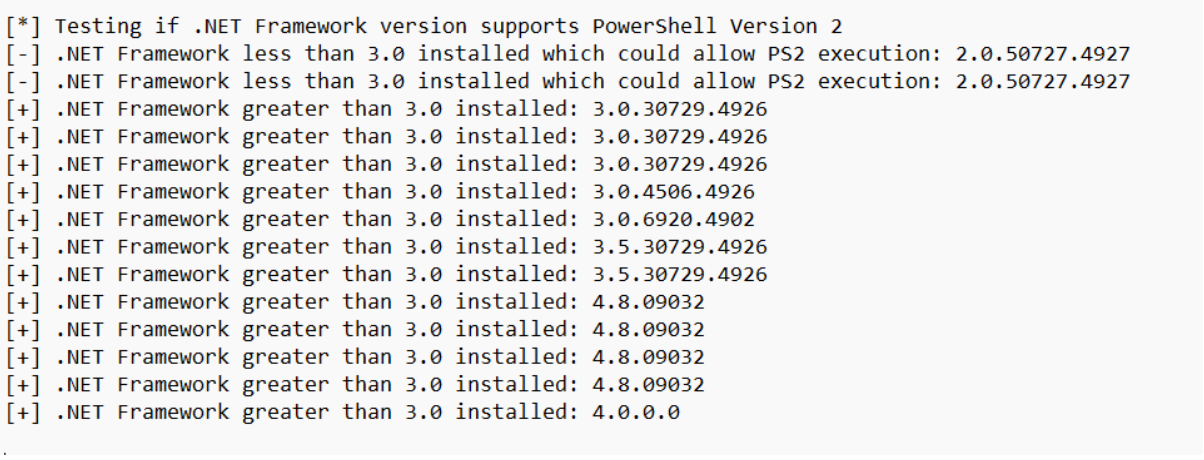
```
[*] Event logs settings defaults are too small. Test that max sizes have been increased.
[x] Testing Microsoft-Windows-SMBServer/Audit log size failed.
[x] Testing Security log size failed.
[-] Microsoft-Windows-PowerShell/Operational max log size is smaller than
System.Collections.Hashtable[Microsoft-Windows-PowerShell/Operational] 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
```

7. Testing for PowerShell version



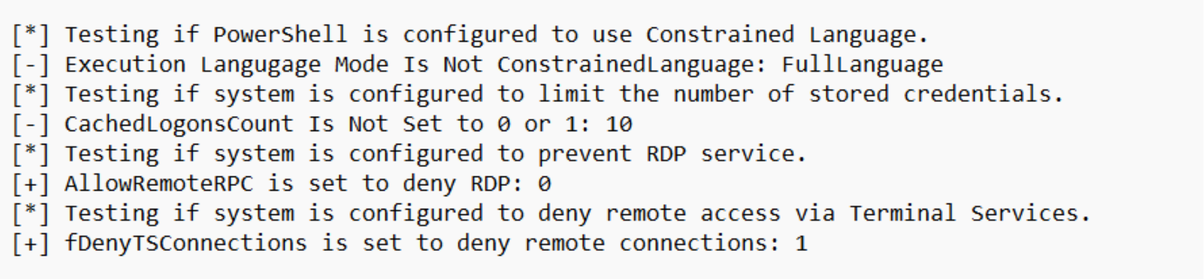
```
[*] Testing if PowerShell Version is at least version 5
[+] Current PowerShell Version: 5.1.22621.2506
[*] Testing if PowerShell Version 2 is permitted
[x] Testing for PowerShell Version 2 failed.
```

8. Testing .Net Framework version compatible with PowerShell version 2



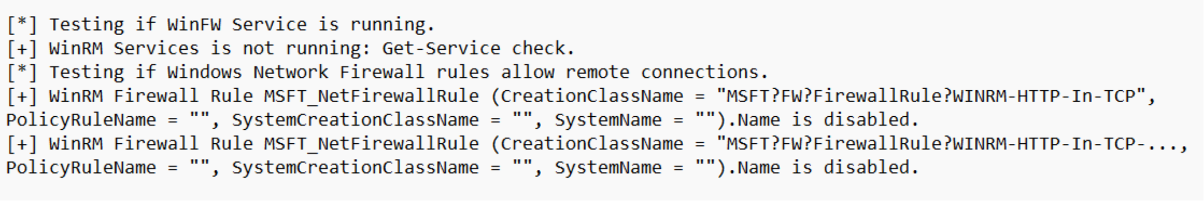
```
[*] Testing if .NET Framework version supports PowerShell Version 2
[-] .NET Framework less than 3.0 installed which could allow PS2 execution: 2.0.50727.4927
[-] .NET Framework less than 3.0 installed which could allow PS2 execution: 2.0.50727.4927
[+] .NET Framework greater than 3.0 installed: 3.0.30729.4926
[+] .NET Framework greater than 3.0 installed: 3.0.30729.4926
[+] .NET Framework greater than 3.0 installed: 3.0.30729.4926
[+] .NET Framework greater than 3.0 installed: 3.0.4506.4926
[+] .NET Framework greater than 3.0 installed: 3.0.6920.4902
[+] .NET Framework greater than 3.0 installed: 3.5.30729.4926
[+] .NET Framework greater than 3.0 installed: 3.5.30729.4926
[+] .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
```

9. Testing for System Configuration



```
[*] 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
```

10. Testing for Windows Firewall running



```
[*] 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.
```