Internship Assessment: CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS) - Week 1

Name: Oihik Mitra

Contact

Phone No: 9836129803

Email ID: mitraoihik1@gmail.com

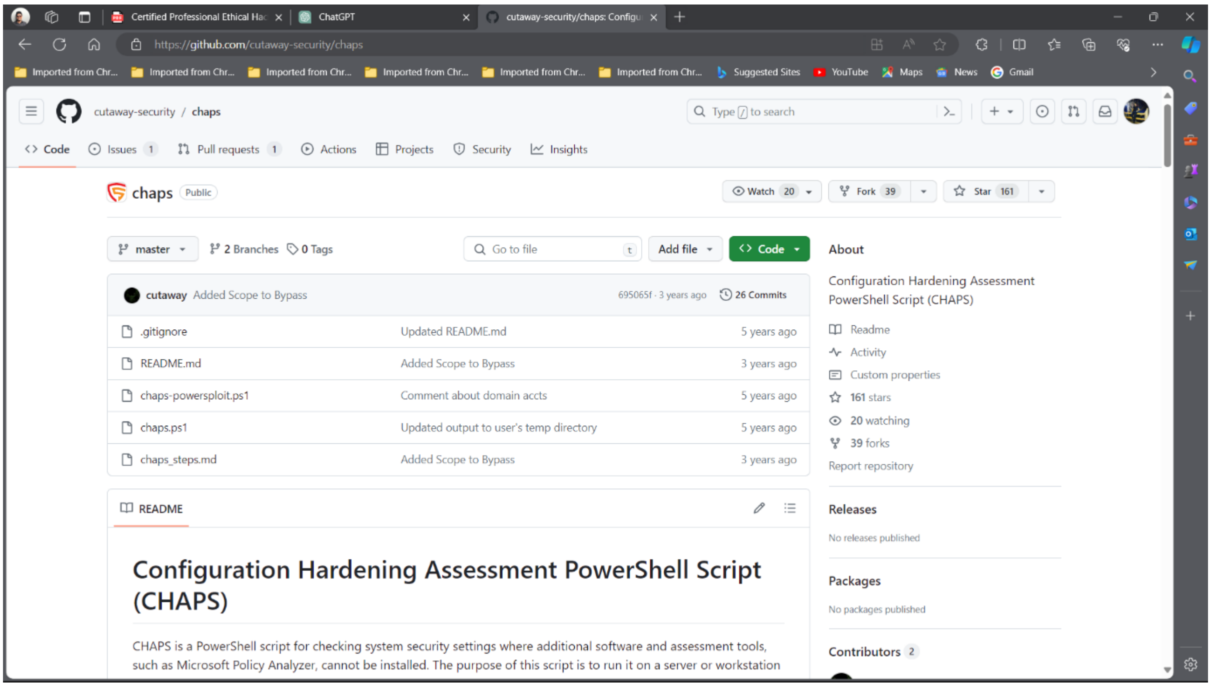
LinkedIn ID: https://www.linkedin.com/in/oihikmitra/

Introduction to CHAPS

The Configuration Hardening Assessment PowerShell Script (CHAPS) is a powerful tool used in cybersecurity for evaluating and strengthening the security configuration of Windows systems. Developed as a PowerShell script, CHAPS automates the assessment process by scanning system configurations against industry best practices and security benchmarks. It identifies potential security vulnerabilities and provides recommendations for remediation, enabling organizations to proactively harden their systems against cyber threats. With its simplicity and efficiency, CHAPS is an invaluable asset in enhancing the security posture of Windows environments, ensuring robust protection against various cyber risks.

Steps to use CHAPS

1. Download CHAPS from GitHub (https://github.com/cutaway-security/chaps.git)



cutaway Added Scope to Bypass 695065f · 3 years ago 26 Commits

.gitignore	Updated README.md	5 years ago
README.md	Added Scope to Bypass	3 years ago
chaps-powersploit.ps1	Comment about domain accts	5 years ago
chaps.ps1	Updated output to user's temp directory	5 years ago
chaps_steps.md	Added Scope to Bypass	3 years ago

About

Configuration Hardening Assessment PowerShell Script (CHAPS)

Readme
Activity
Custom properties
161 stars
20 watching
39 forks
Report repository

Releases

No releases published

Packages

No packages published

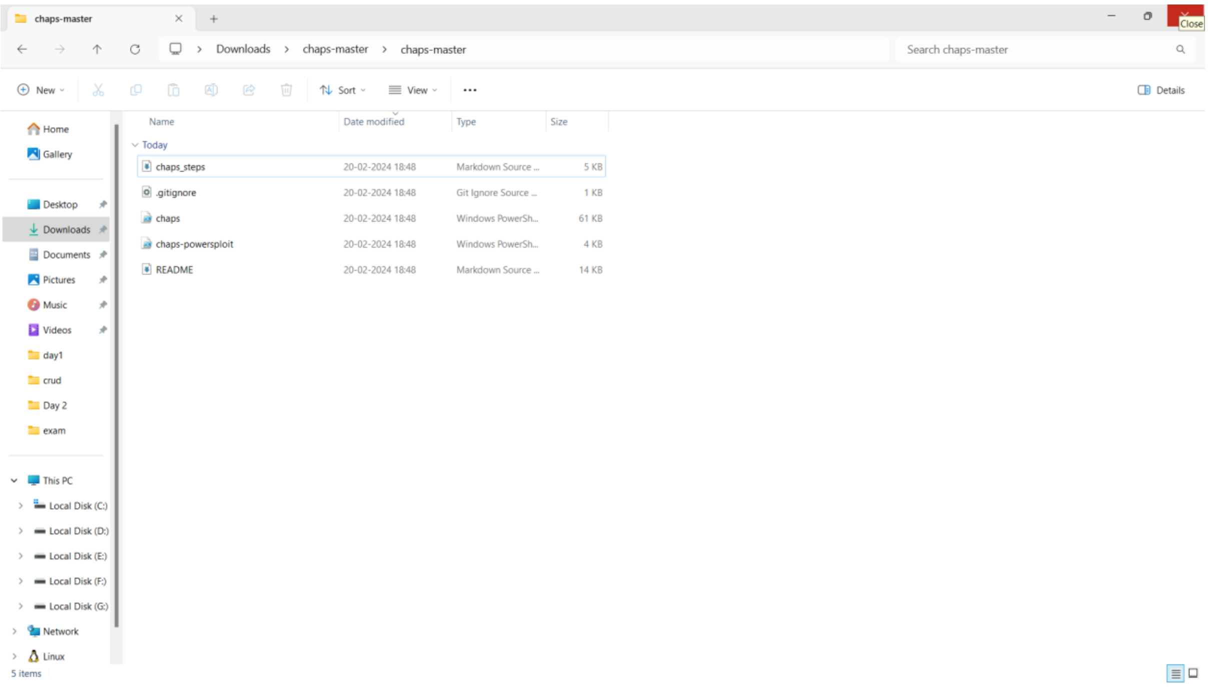
Contributors 2

README

Configuration Hardening Assessment PowerShell Script (CHAPS)

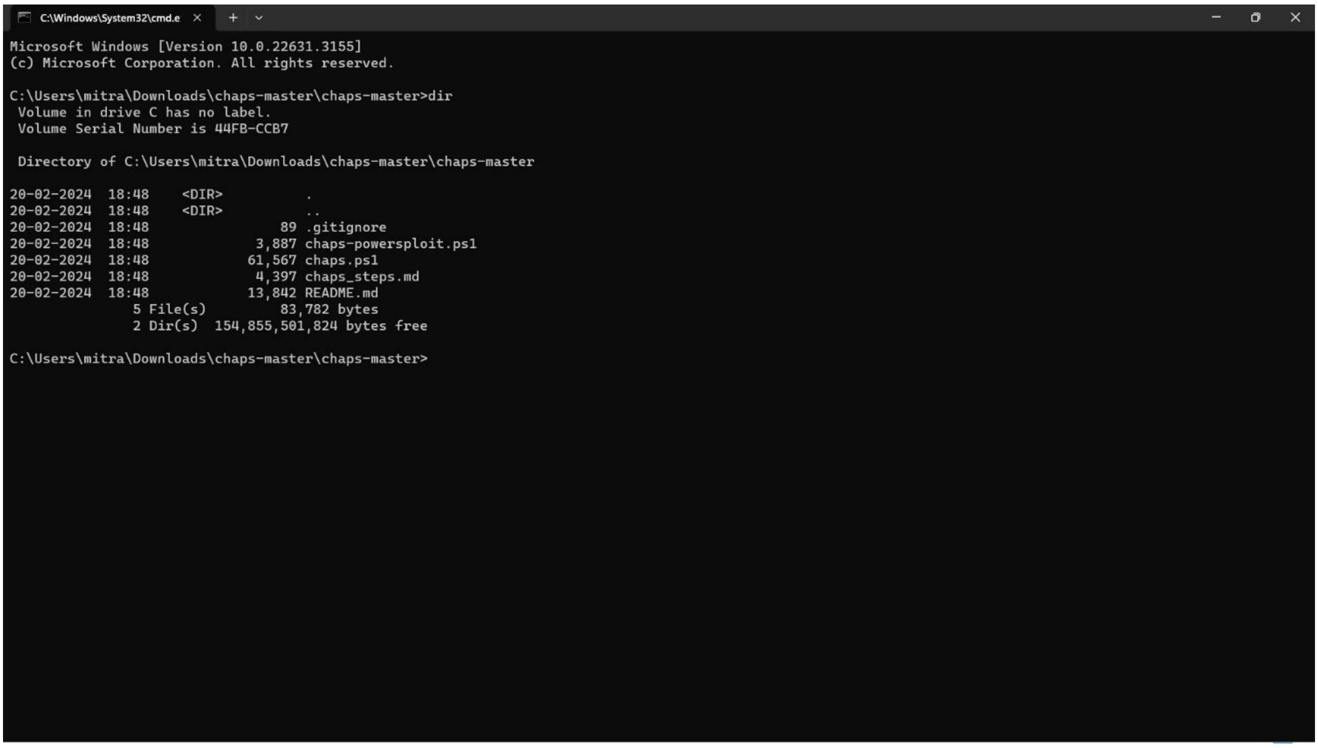
CHAPS is a PowerShell script for checking system security settings where additional software and assessment tools, such as Microsoft Policy Analyzer, cannot be installed. The purpose of this script is to run it on a server or workstation

2. Extract the zip file.



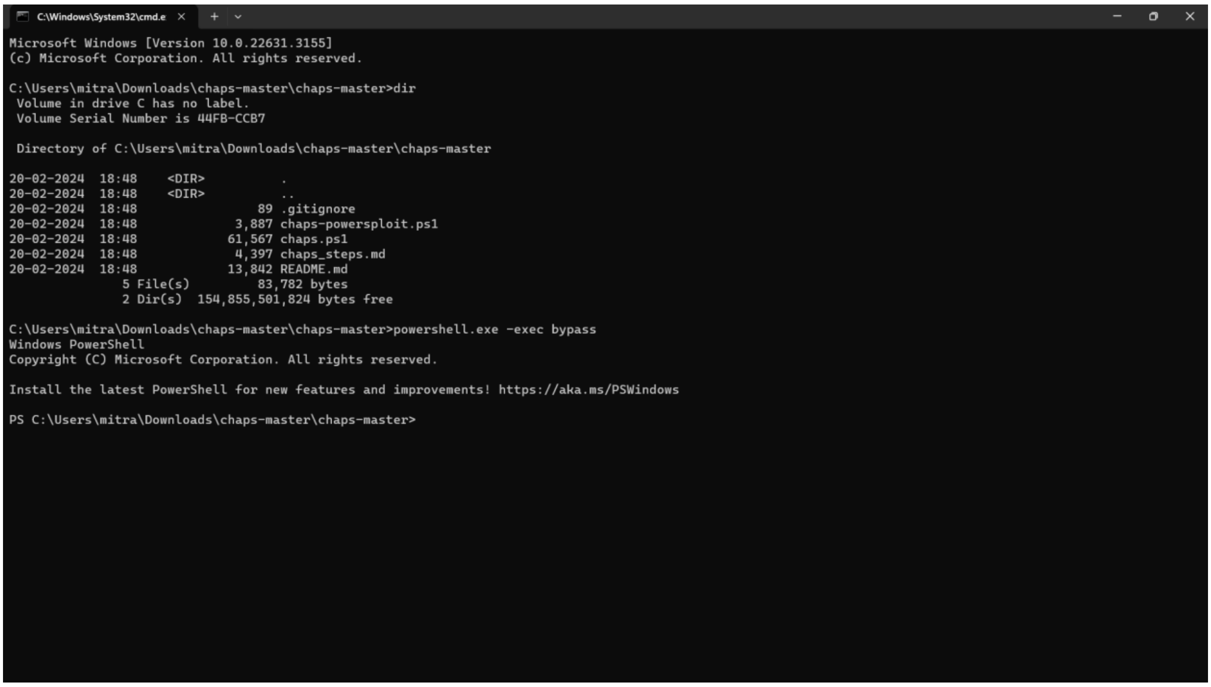
Name	Date modified	Type	Size
chaps_steps	20-02-2024 18:48	Markdown Source ...	5 KB
.gitignore	20-02-2024 18:48	Git Ignore Source ...	1 KB
chaps	20-02-2024 18:48	Windows PowerSh...	61 KB
chaps-powersploit	20-02-2024 18:48	Windows PowerSh...	4 KB
README	20-02-2024 18:48	Markdown Source ...	14 KB

3. Open CMD from the CHAPS directory and list the files ‘dir’ command.



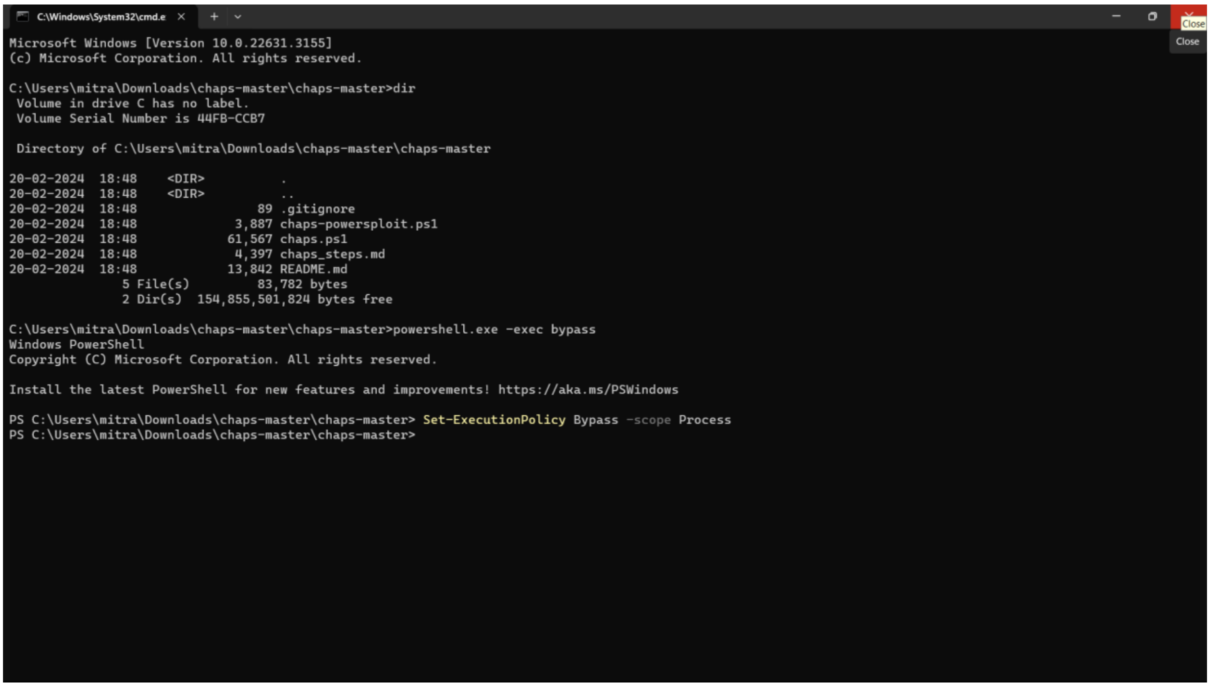
```
Microsoft Windows [Version 10.0.22631.3155]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mitra\Downloads\chaps-master\chaps-master>dir
 Volume in drive C has no label.
 Volume Serial Number is 44FB-CCB7

 Directory of C:\Users\mitra\Downloads\chaps-master\chaps-master

20-02-2024  18:48    <DIR>          .
20-02-2024  18:48    <DIR>          ..
20-02-2024  18:48                89 .gitignore
20-02-2024  18:48             3,887 chaps-powersploit.ps1
20-02-2024  18:48            61,567 chaps.ps1
20-02-2024  18:48             4,397 chaps_steps.md
20-02-2024  18:48            13,842 README.md
               5 File(s)         83,782 bytes
               2 Dir(s)  154,855,501,824 bytes free

C:\Users\mitra\Downloads\chaps-master\chaps-master>
```

4. Run `powershell.exe -exec bypass` to being a PowerShell prompt. We got the PowerShell.



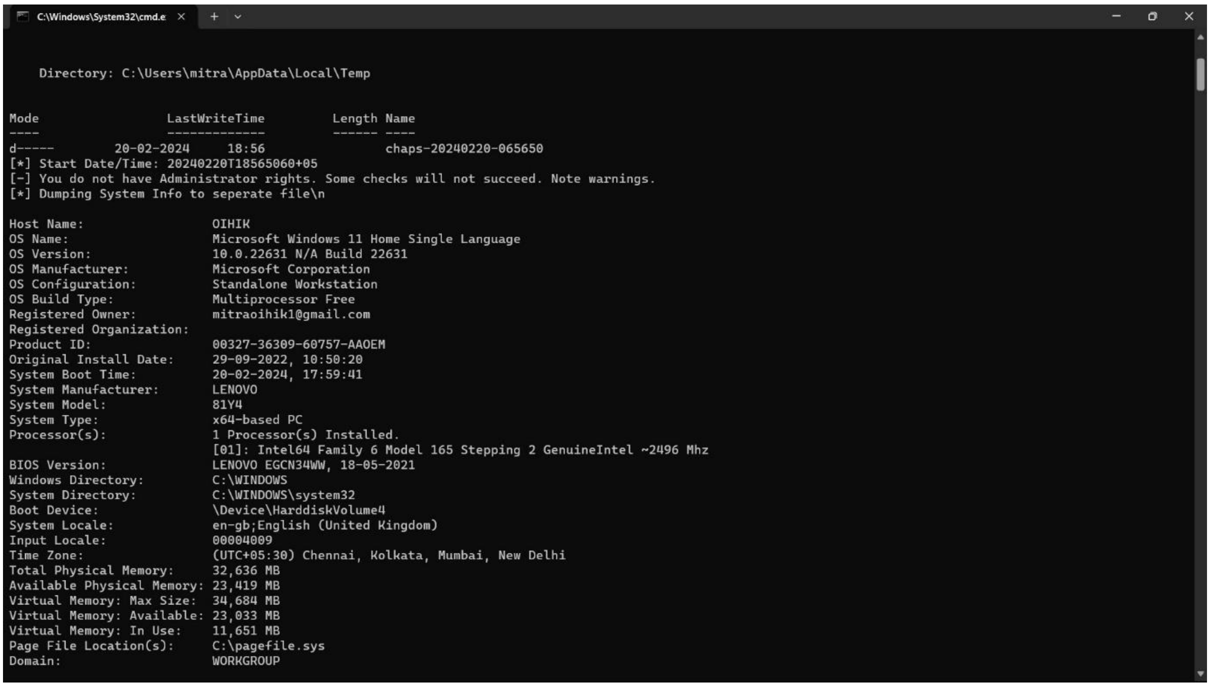
```
Microsoft Windows [Version 10.0.22631.3155]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mitra\Downloads\chaps-master\chaps-master>dir
 Volume in drive C has no label.
 Volume Serial Number is 44FB-CCB7

 Directory of C:\Users\mitra\Downloads\chaps-master\chaps-master

20-02-2024  18:48    <DIR>          .
20-02-2024  18:48    <DIR>          ..
20-02-2024  18:48                89 .gitignore
20-02-2024  18:48             3,887 chaps-powersploit.ps1
20-02-2024  18:48            61,567 chaps.ps1
20-02-2024  18:48             4,397 chaps_steps.md
20-02-2024  18:48            13,842 README.md
               5 File(s)         83,782 bytes
               2 Dir(s)  154,855,501,824 bytes free

C:\Users\mitra\Downloads\chaps-master\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 C:\Users\mitra\Downloads\chaps-master\chaps-master>
```

5. Now we will run `Set-ExecutionPolicy Bypass -scope Process` to allow scripts to execute.

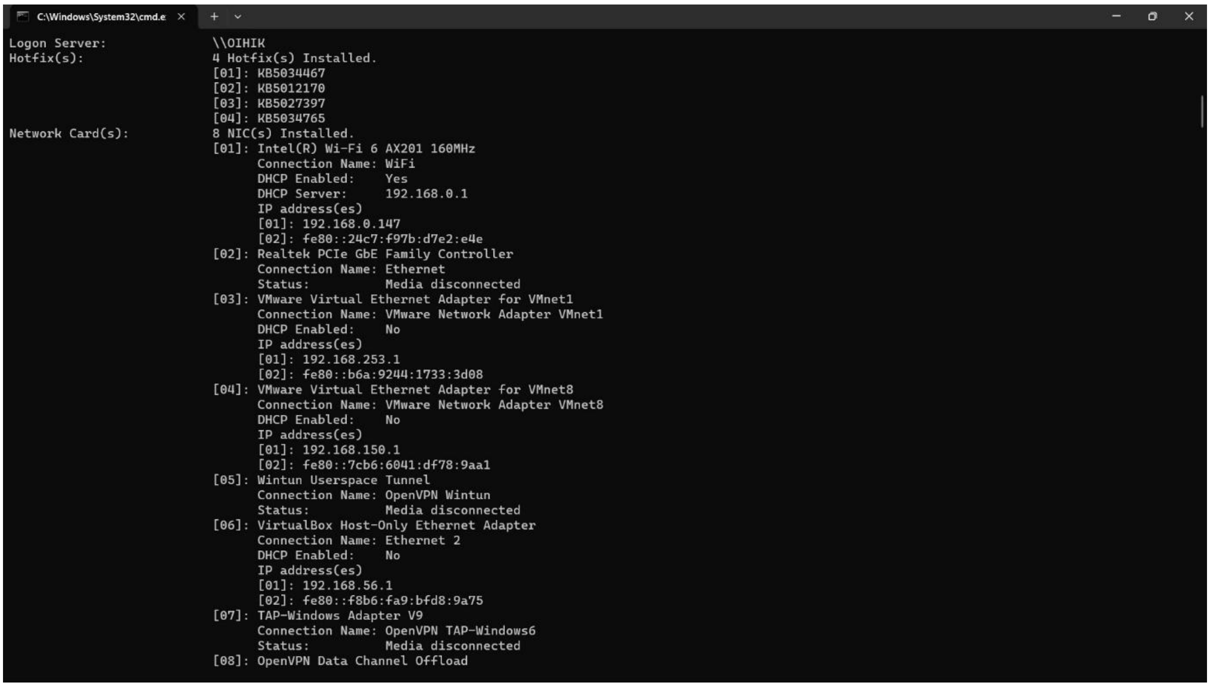


```
Microsoft Windows [Version 10.0.22631.3155]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mitra\Downloads\chaps-master\chaps-master>dir
 Volume in drive C has no label.
 Volume Serial Number is 44FB-CCB7

 Directory of C:\Users\mitra\Downloads\chaps-master\chaps-master

20-02-2024  18:48    <DIR>          .
20-02-2024  18:48    <DIR>          ..
20-02-2024  18:48                89 .gitignore
20-02-2024  18:48             3,887 chaps-powersploit.ps1
20-02-2024  18:48            61,567 chaps.ps1
20-02-2024  18:48             4,397 chaps_steps.md
20-02-2024  18:48            13,842 README.md
               5 File(s)         83,782 bytes
               2 Dir(s)  154,855,501,824 bytes free

C:\Users\mitra\Downloads\chaps-master\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 C:\Users\mitra\Downloads\chaps-master\chaps-master> Set-ExecutionPolicy Bypass -scope Process
PS C:\Users\mitra\Downloads\chaps-master\chaps-master>
```

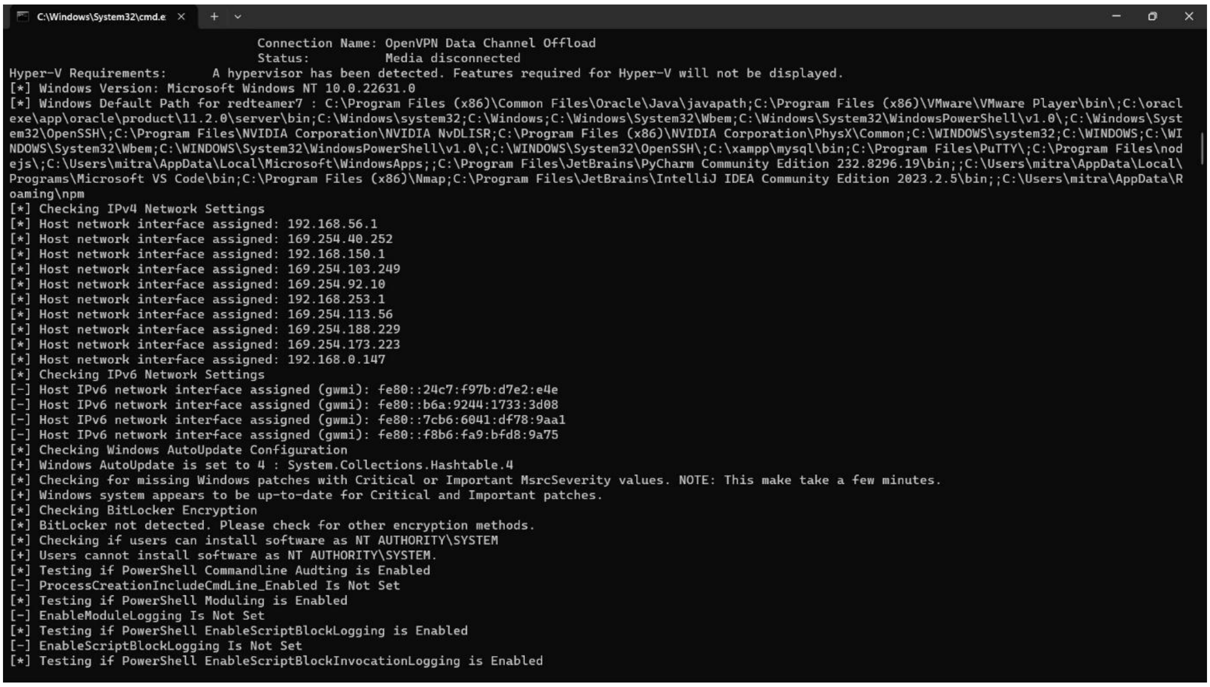
6. Now we will run `chaps.ps1`



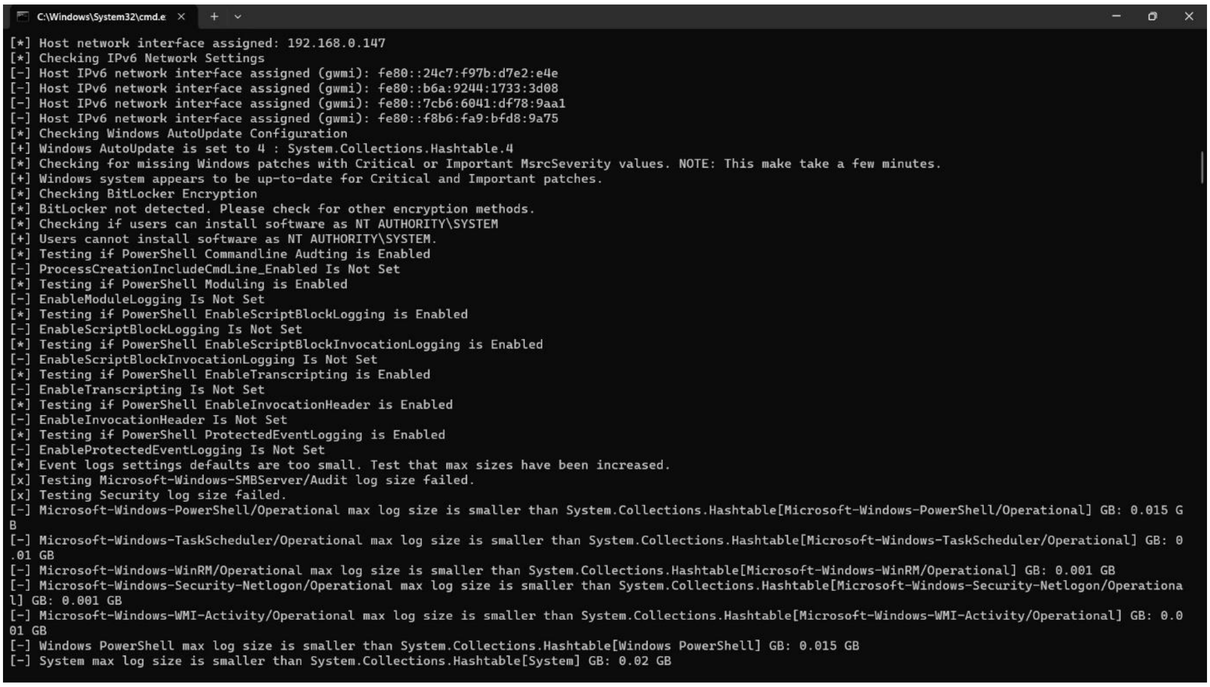
```

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


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        20-02-2024     18:56                chaps-20240220-065650
[*] Start Date/Time: 20240220T18565060+05
[-] You do not have Administrator rights. Some checks will not succeed. Note warnings.
[*] Dumping System Info to seperate file\n

Host Name:                 OIHIK
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:          mitraoihik1@gmail.com
Registered Organization:
Product ID:                00327-36309-60757-AAOEM
Original Install Date:     29-09-2022, 10:50:20
System Boot Time:          20-02-2024, 17:59:41
System Manufacturer:       LENOVO
System Model:              81Y4
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 165 Stepping 2 GenuineIntel ~2496 Mhz
BIOS Version:              LENOVO EGCN34WW, 18-05-2021
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume4
System Locale:             en-gb;English (United Kingdom)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     32,636 MB
Available Physical Memory: 23,419 MB
Virtual Memory: Max Size:  34,684 MB
Virtual Memory: Available: 23,033 MB
Virtual Memory: In Use:    11,651 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
```



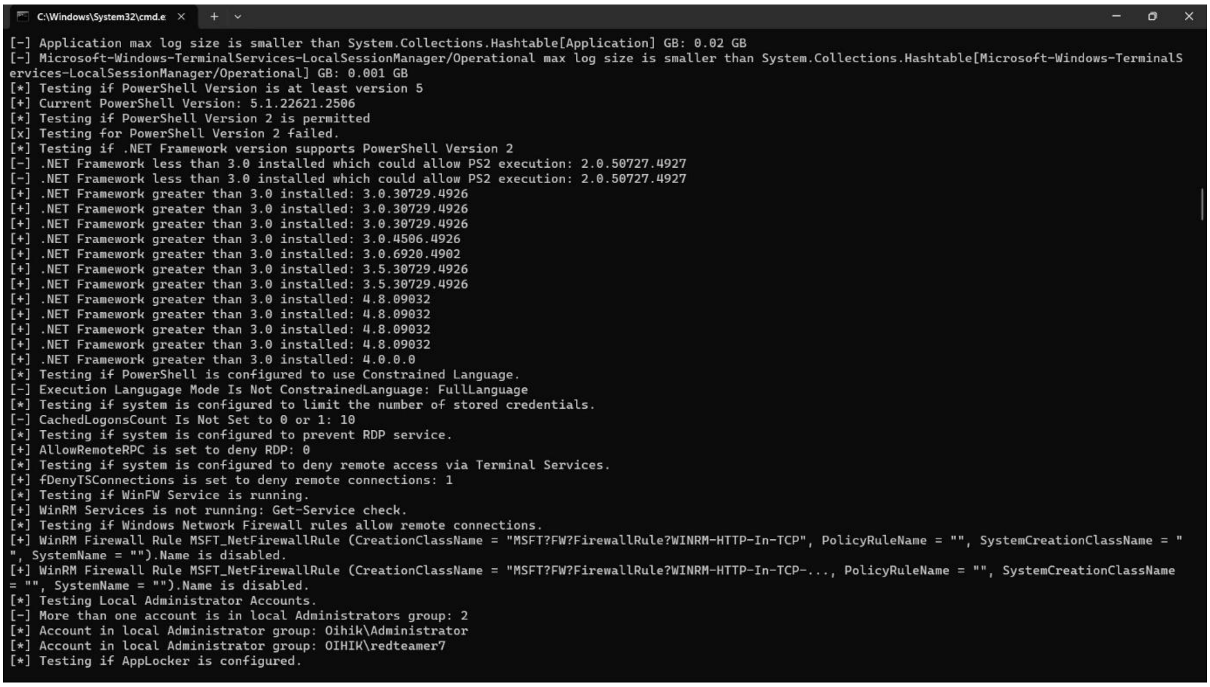
```
Logon Server:              \\OIHIK
Hotfix(s):                 4 Hotfix(s) Installed.
                           [01]: KB5034467
                           [02]: KB5012170
                           [03]: KB5027397
                           [04]: KB5034765
Network Card(s):           8 NIC(s) Installed.
                           [01]: Intel(R) Wi-Fi 6 AX201 160MHz
                                 Connection Name: WiFi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.0.1
                                 IP address(es)
                                 [01]: 192.168.0.147
                                 [02]: fe80::24c7:f97b:d7e2:e4e
                           [02]: Realtek PCIe GbE Family Controller
                                 Connection Name: Ethernet
                                 Status:          Media disconnected
                           [03]: VMware Virtual Ethernet Adapter for VMnet1
                                 Connection Name: VMware Network Adapter VMnet1
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.253.1
                                 [02]: fe80::b6a:9244:1733:3d08
                           [04]: VMware Virtual Ethernet Adapter for VMnet8
                                 Connection Name: VMware Network Adapter VMnet8
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.150.1
                                 [02]: fe80::7cb6:6041:df78:9aa1
                           [05]: Wintun Userspace Tunnel
                                 Connection Name: OpenVPN Wintun
                                 Status:          Media disconnected
                           [06]: VirtualBox Host-Only Ethernet Adapter
                                 Connection Name: Ethernet 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.56.1
                                 [02]: fe80::f8b6:fa9:bfd8:9a75
                           [07]: TAP-Windows Adapter V9
                                 Connection Name: OpenVPN TAP-Windows6
                                 Status:          Media disconnected
                           [08]: OpenVPN Data Channel Offload
```



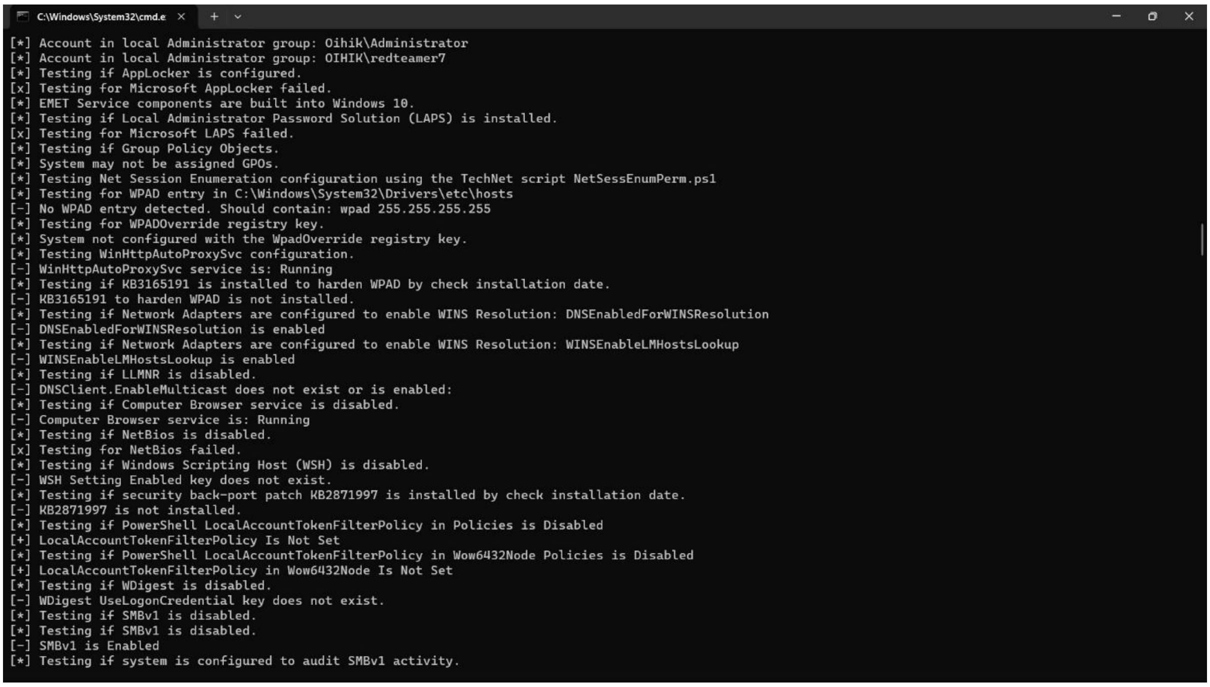
```
                                 Connection Name: OpenVPN Data Channel Offload
                                 Status:          Media disconnected
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
[*] Windows Version: Microsoft Windows NT 10.0.22631.0
[*] Windows Default Path for redteamer7 : C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Program Files (x86)\VMware\VMware Player\bin\;C:\oracl
exe\app\oracle\product\11.2.0\server\bin;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\Syst
em32\OpenSSH\;C:\Program Files\NVIDIA Corporation\NVIDIA NvDLISR;C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common;C:\WINDOWS\system32;C:\WINDOWS;C:\WI
NDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\xampp\mysql\bin;C:\Program Files\PuTTY\;C:\Program Files\nod
ejs\;C:\Users\mitra\AppData\Local\Microsoft\WindowsApps;;C:\Program Files\JetBrains\PyCharm Community Edition 232.8296.19\bin;;C:\Users\mitra\AppData\Local\
Programs\Microsoft VS Code\bin;C:\Program Files (x86)\Nmap;C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2023.2.5\bin;;C:\Users\mitra\AppData\R
oaming\npm
[*] Checking IPv4 Network Settings
[*] Host network interface assigned: 192.168.56.1
[*] Host network interface assigned: 169.254.40.252
[*] Host network interface assigned: 192.168.150.1
[*] Host network interface assigned: 169.254.103.249
[*] Host network interface assigned: 169.254.92.10
[*] Host network interface assigned: 192.168.253.1
[*] Host network interface assigned: 169.254.113.56
[*] Host network interface assigned: 169.254.188.229
[*] Host network interface assigned: 169.254.173.223
[*] Host network interface assigned: 192.168.0.147
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi): fe80::24c7:f97b:d7e2:e4e
[-] Host IPv6 network interface assigned (gwmi): fe80::b6a:9244:1733:3d08
[-] Host IPv6 network interface assigned (gwmi): fe80::7cb6:6041:df78:9aa1
[-] Host IPv6 network interface assigned (gwmi): fe80::f8b6:fa9:bfd8:9a75
[*] 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
```



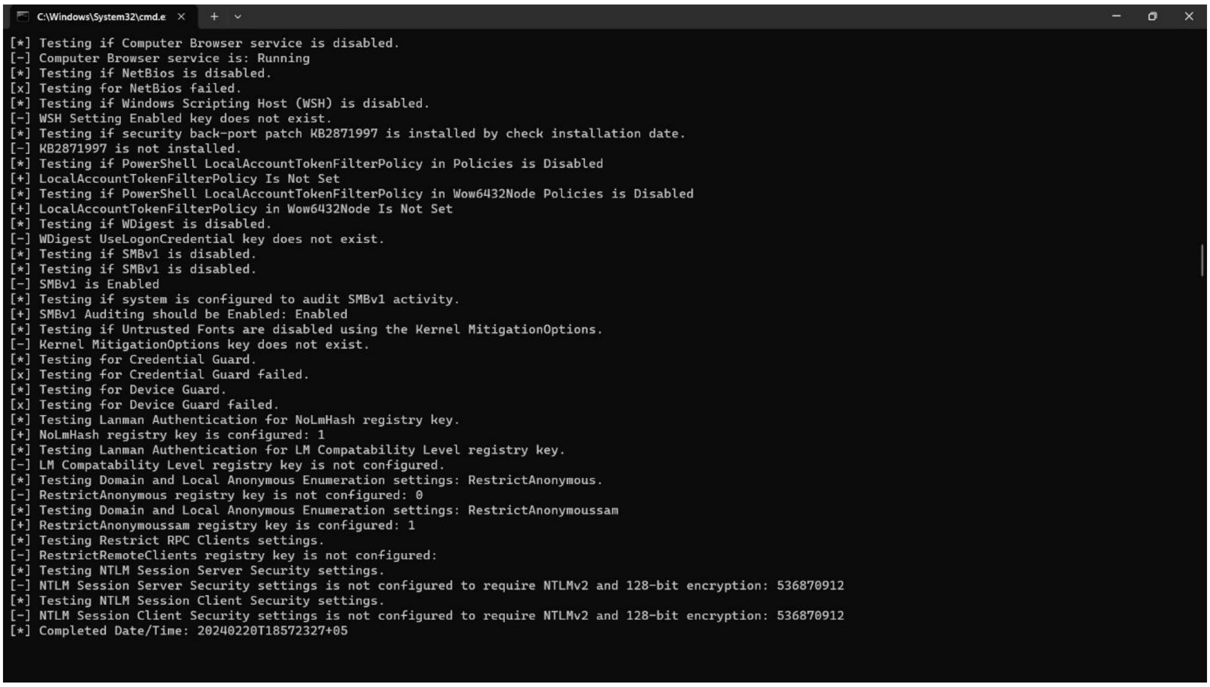
```
[*] Host network interface assigned: 192.168.0.147
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi): fe80::24c7:f97b:d7e2:e4e
[-] Host IPv6 network interface assigned (gwmi): fe80::b6a:9244:1733:3d08
[-] Host IPv6 network interface assigned (gwmi): fe80::7cb6:6041:df78:9aa1
[-] Host IPv6 network interface assigned (gwmi): fe80::f8b6:fa9:bfd8:9a75
[*] 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.
[-] Microsoft-Windows-PowerShell/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-PowerShell/Operational] GB: 0.015 G
B
[-] 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/Operationa
l] GB: 0.001 GB
[-] Microsoft-Windows-WMI-Activity/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-WMI-Activity/Operational] GB: 0.0
01 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-TerminalS
ervices-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
[x] Testing for PowerShell Version 2 failed.
[*] 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
[*] 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: Oihik\Administrator
[*] Account in local Administrator group: OIHIK\redteamer7
[*] Testing if AppLocker is configured.
```

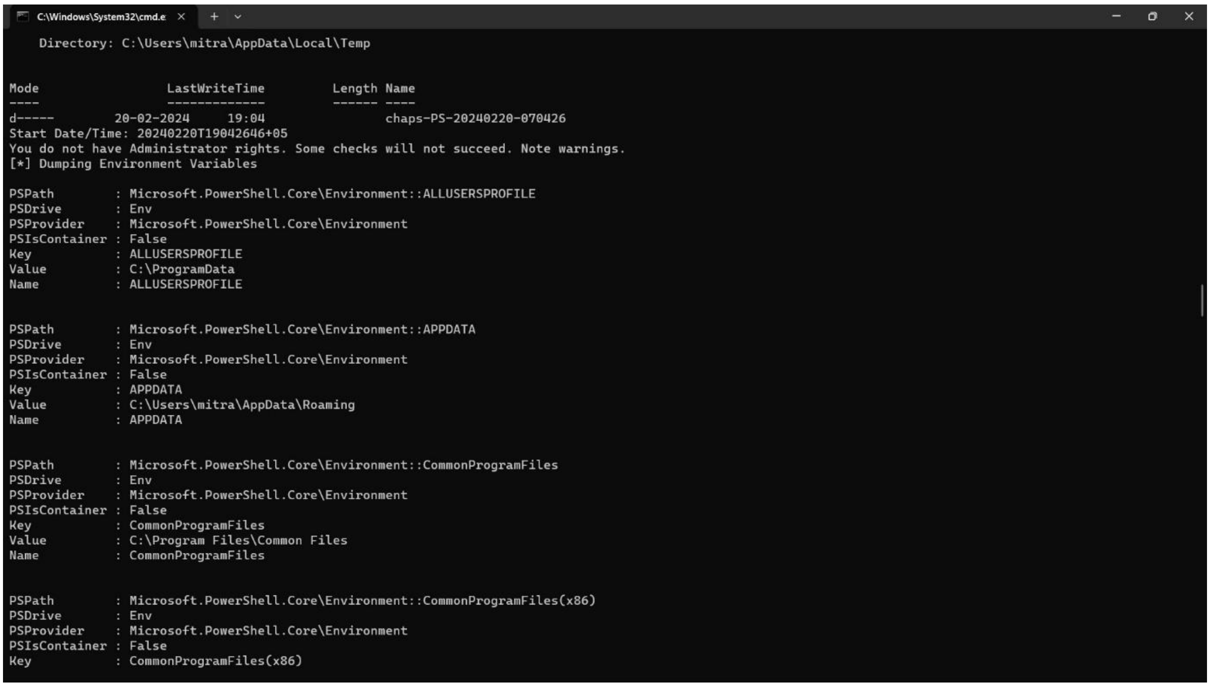


```
[*] Account in local Administrator group: Oihik\Administrator
[*] Account in local Administrator group: OIHIK\redteamer7
[*] Testing if AppLocker is configured.
[x] Testing for Microsoft AppLocker failed.
[*] EMET Service components are built into Windows 10.
[*] Testing if Local Administrator Password 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
[*] Testing if WDigest is disabled.
[-] WDigest UseLogonCredential key does not exist.
[*] Testing if SMBv1 is disabled.
[*] Testing if SMBv1 is disabled.
[-] SMBv1 is Enabled
[*] Testing if system is configured to audit SMBv1 activity.
```

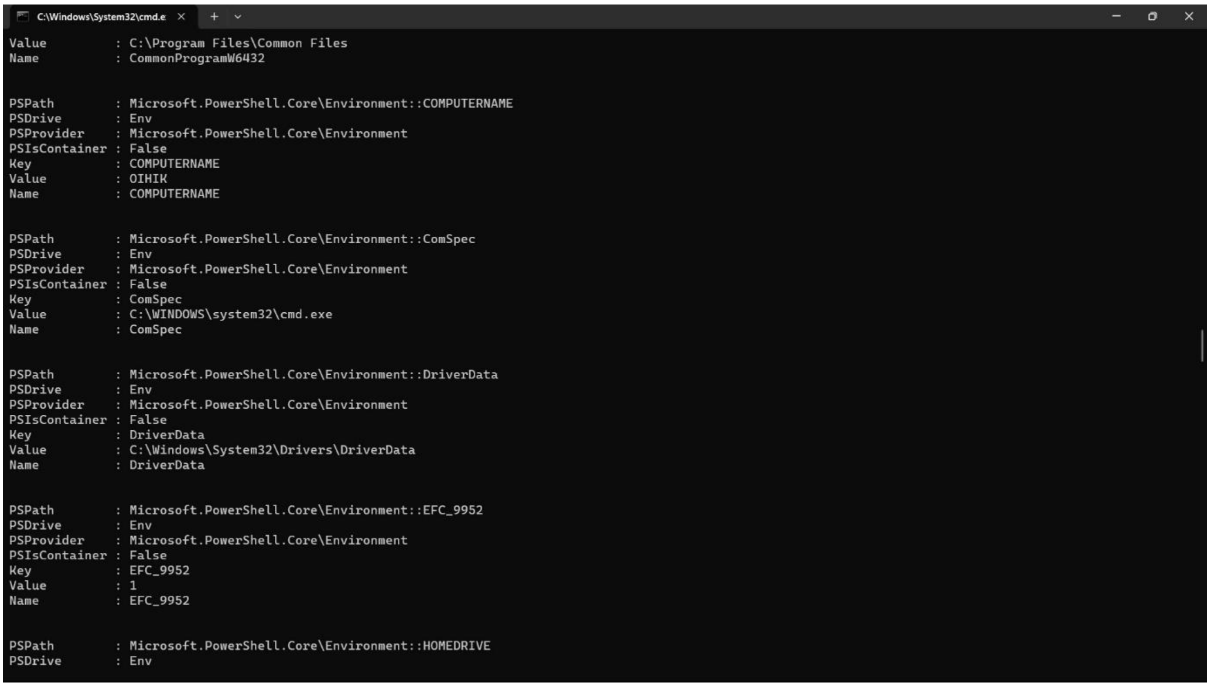


```
[*] Testing if Computer Browser service is disabled.
[-] Computer Browser service is: Running
[*] Testing if NetBios is disabled.
[x] Testing for NetBios failed.
[*] Testing if Windows Scripting Host (WSH) is disabled.
[-] WSH Setting Enabled key does not exist.
[*] Testing if security back-port 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
[*] Testing if WDigest is disabled.
[-] WDigest UseLogonCredential key does not exist.
[*] 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: 20240220T18572327+05
```

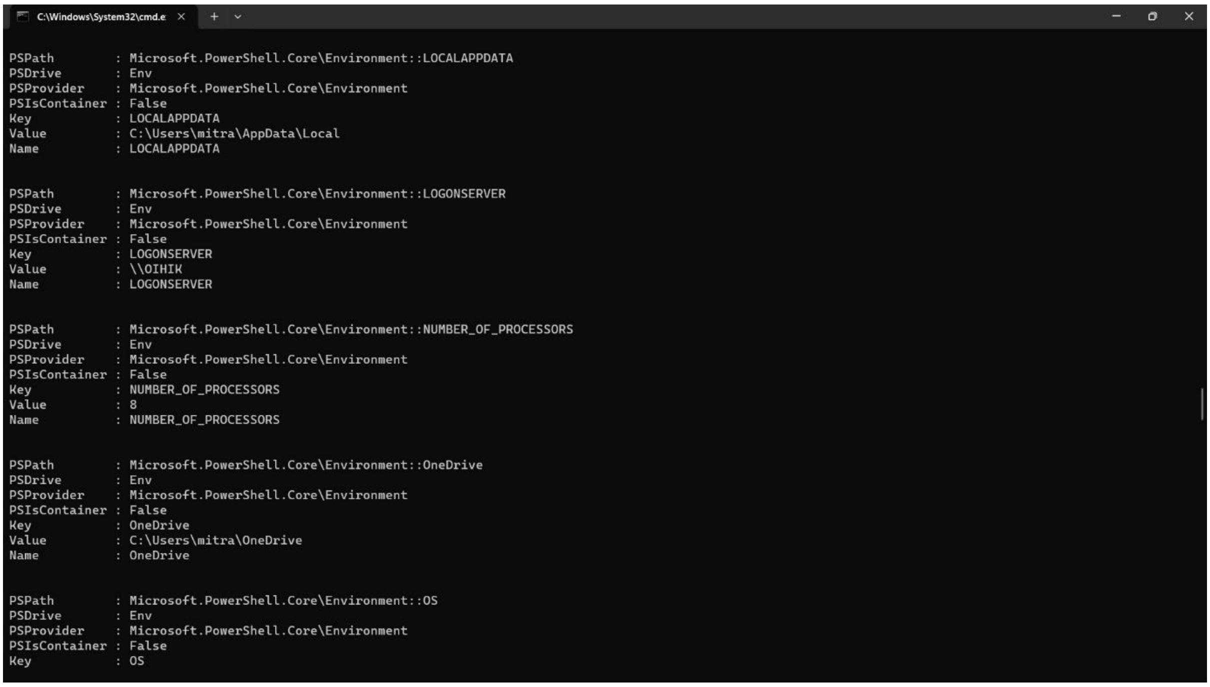
7. Now we will run `chaps-powershell.ps1` to import the appropriate PowerSploit scripts



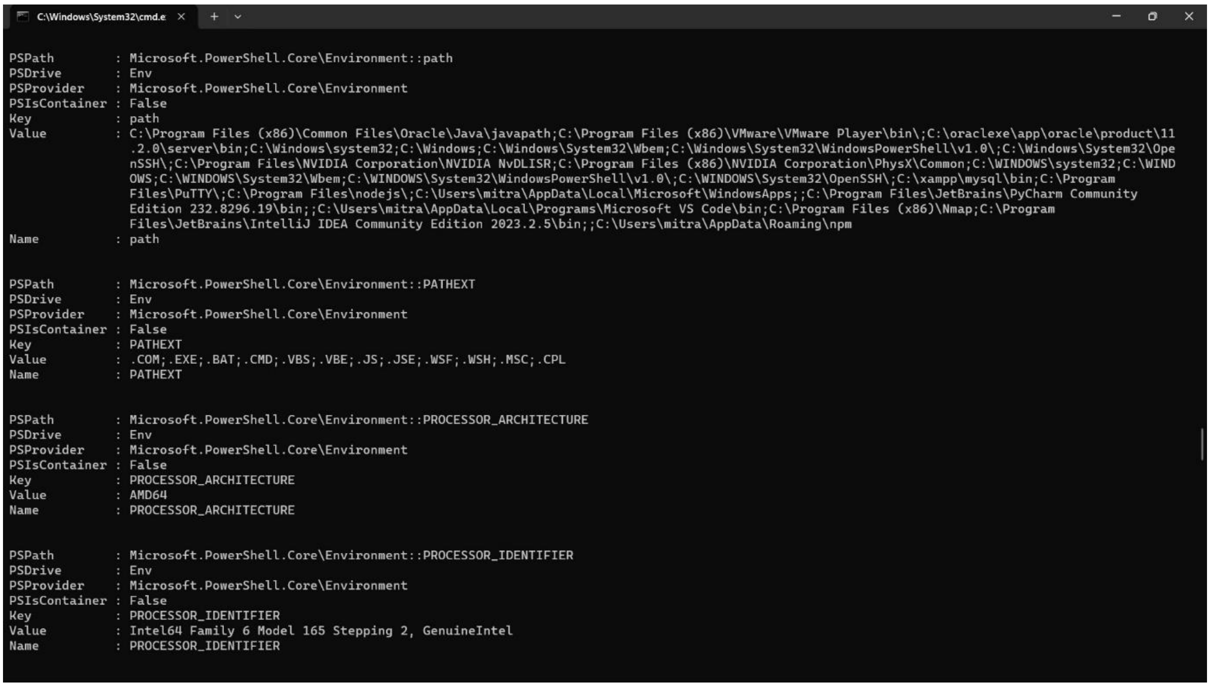
```
    Directory: C:\Users\mitra\AppData\Local\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        20-02-2024     19:04                chaps-PS-20240220-070426
Start Date/Time: 20240220T19042646+05
You do not have Administrator rights. Some checks will not succeed. Note warnings.
[*] Dumping Environment Variables

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


PSPath        : Microsoft.PowerShell.Core\Environment::APPDATA
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : APPDATA
Value         : C:\Users\mitra\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)
```



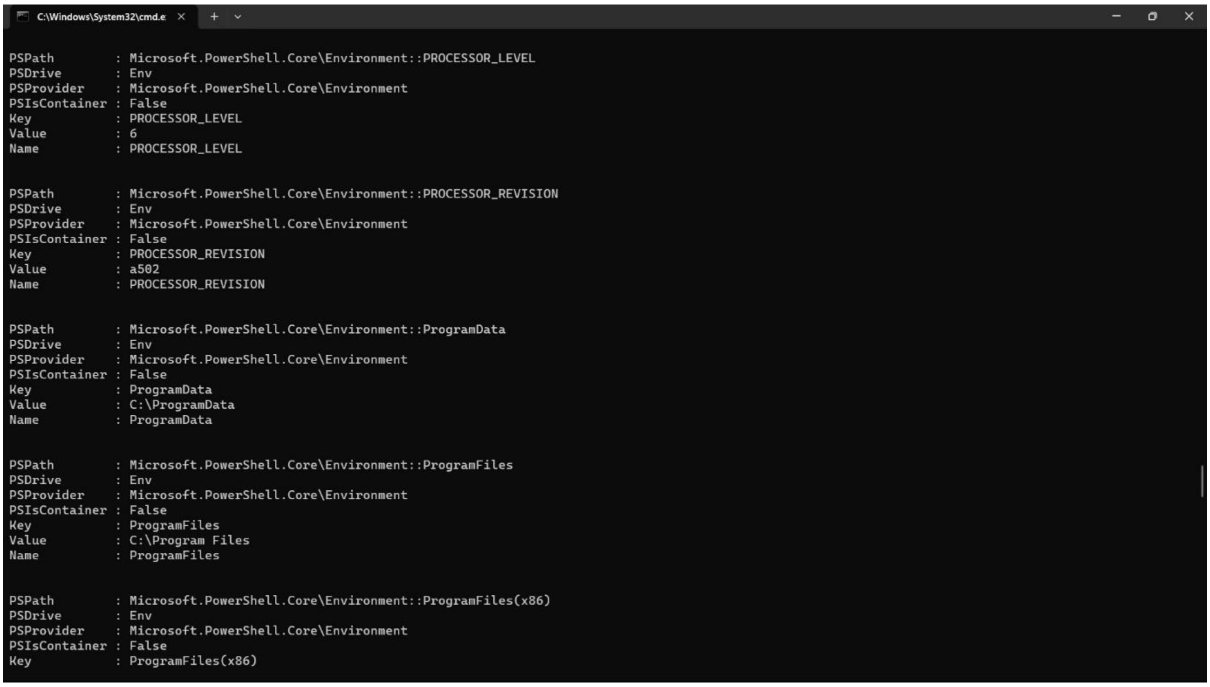
```
Value        : C:\Program Files\Common Files
Name         : CommonProgramW6432


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


PSPath       : Microsoft.PowerShell.Core\Environment::ComSpec
PSDrive      : Env
PSProvider   : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key          : ComSpec
Value        : C:\WINDOWS\system32\cmd.exe
Name         : ComSpec


PSPath       : Microsoft.PowerShell.Core\Environment::DriverData
PSDrive      : Env
PSProvider   : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key          : DriverData
Value        : C:\Windows\System32\Drivers\DriverData
Name         : DriverData


PSPath       : Microsoft.PowerShell.Core\Environment::EFC_9952
PSDrive      : Env
PSProvider   : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key          : EFC_9952
Value        : 1
Name         : EFC_9952


PSPath       : Microsoft.PowerShell.Core\Environment::HOMEDRIVE
PSDrive      : Env
```



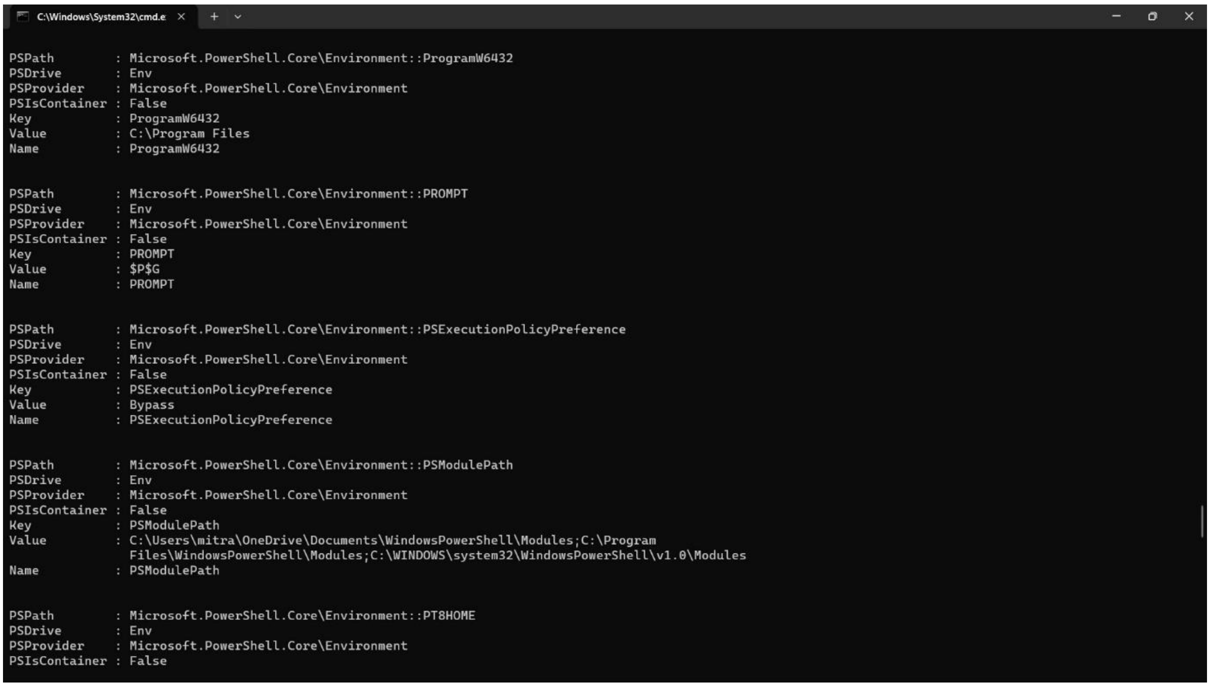
```
PSPath       : Microsoft.PowerShell.Core\Environment::LOCALAPPDATA
PSDrive      : Env
PSProvider   : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key          : LOCALAPPDATA
Value        : C:\Users\mitra\AppData\Local
Name         : LOCALAPPDATA


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


PSPath       : Microsoft.PowerShell.Core\Environment::NUMBER_OF_PROCESSORS
PSDrive      : Env
PSProvider   : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key          : NUMBER_OF_PROCESSORS
Value        : 8
Name         : NUMBER_OF_PROCESSORS


PSPath       : Microsoft.PowerShell.Core\Environment::OneDrive
PSDrive      : Env
PSProvider   : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key          : OneDrive
Value        : C:\Users\mitra\OneDrive
Name         : OneDrive


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



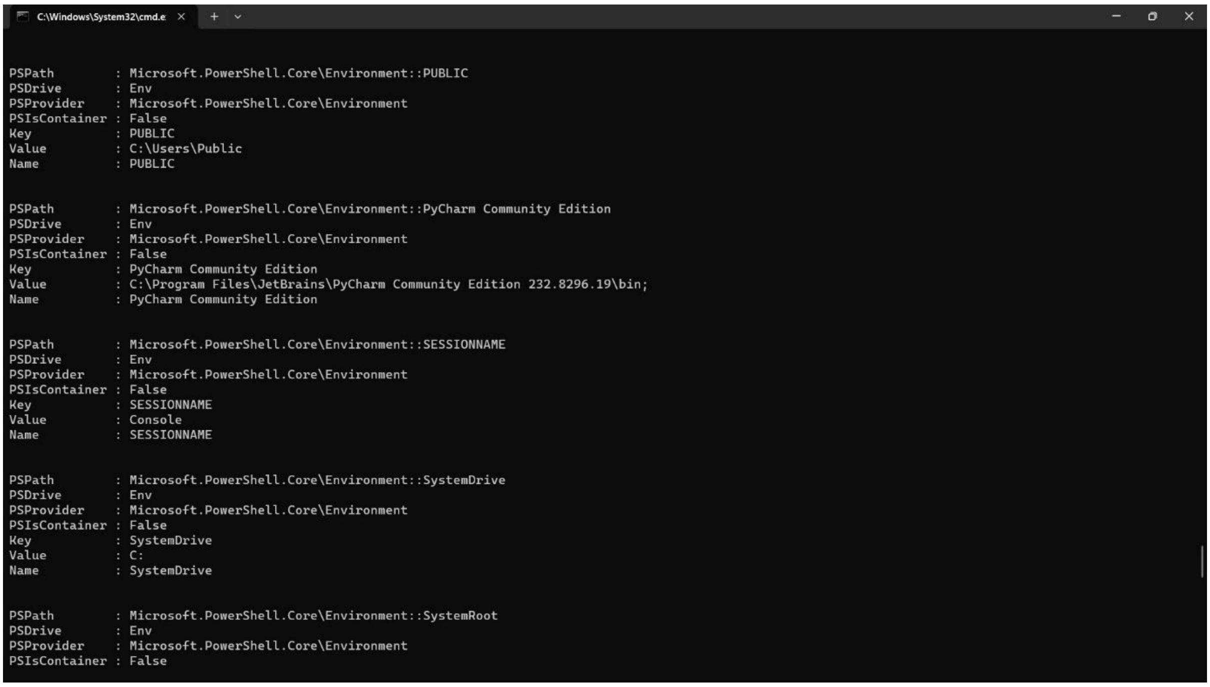
```
PSPath        : Microsoft.PowerShell.Core\Environment::path
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : path
Value         : C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Program Files (x86)\VMware\VMware Player\bin\;C:\oraclexe\app\oracle\product\11
                .2.0\server\bin;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\Ope
                nSSH\;C:\Program Files\NVIDIA Corporation\NVIDIA NvDLISR;C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common;C:\WINDOWS\system32;C:\WIND
                OWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\xampp\mysql\bin;C:\Program
                Files\PuTTY\;C:\Program Files\nodejs\;C:\Users\mitra\AppData\Local\Microsoft\WindowsApps;;C:\Program Files\JetBrains\PyCharm Community
                Edition 232.8296.19\bin;;C:\Users\mitra\AppData\Local\Programs\Microsoft VS Code\bin;C:\Program Files (x86)\Nmap;C:\Program
                Files\JetBrains\IntelliJ IDEA Community Edition 2023.2.5\bin;;C:\Users\mitra\AppData\Roaming\npm
Name          : path


PSPath        : Microsoft.PowerShell.Core\Environment::PATHEXT
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : PATHEXT
Value         : .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.CPL
Name          : PATHEXT


PSPath        : Microsoft.PowerShell.Core\Environment::PROCESSOR_ARCHITECTURE
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : PROCESSOR_ARCHITECTURE
Value         : AMD64
Name          : PROCESSOR_ARCHITECTURE


PSPath        : Microsoft.PowerShell.Core\Environment::PROCESSOR_IDENTIFIER
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : PROCESSOR_IDENTIFIER
Value         : Intel64 Family 6 Model 165 Stepping 2, GenuineIntel
Name          : PROCESSOR_IDENTIFIER
```



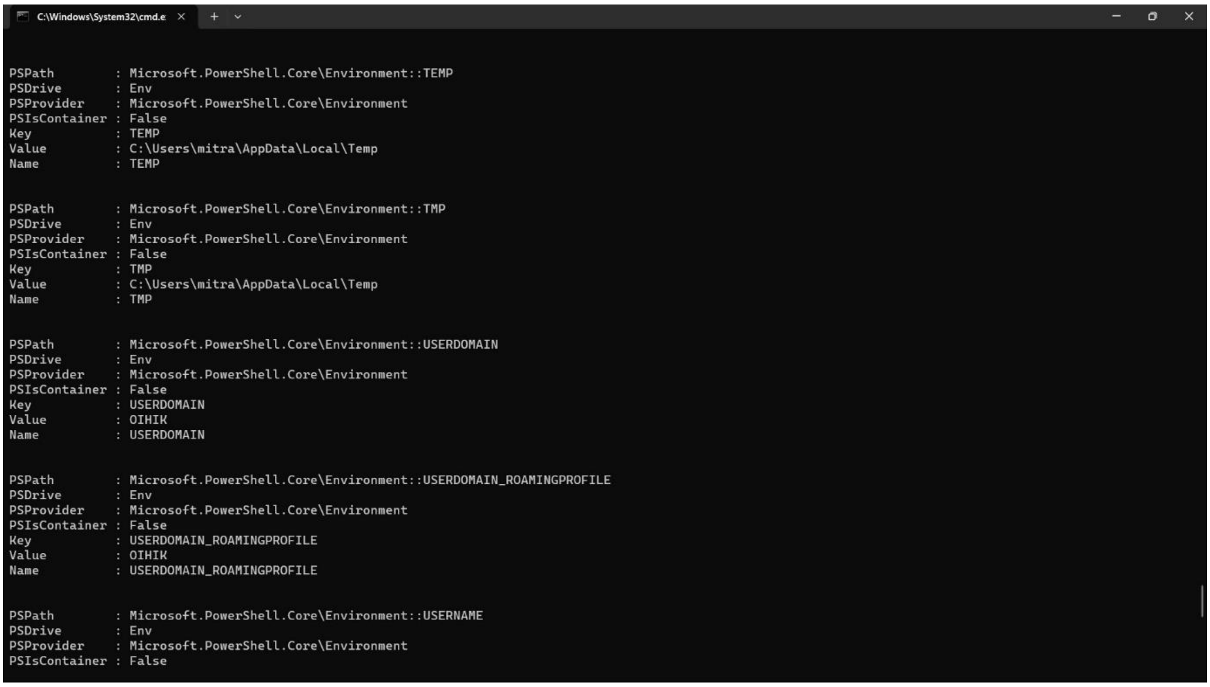
```
PSPath        : Microsoft.PowerShell.Core\Environment::PROCESSOR_LEVEL
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : PROCESSOR_LEVEL
Value         : 6
Name          : PROCESSOR_LEVEL


PSPath        : Microsoft.PowerShell.Core\Environment::PROCESSOR_REVISION
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : PROCESSOR_REVISION
Value         : a502
Name          : PROCESSOR_REVISION


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


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


PSPath        : Microsoft.PowerShell.Core\Environment::ProgramFiles(x86)
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : ProgramFiles(x86)
```



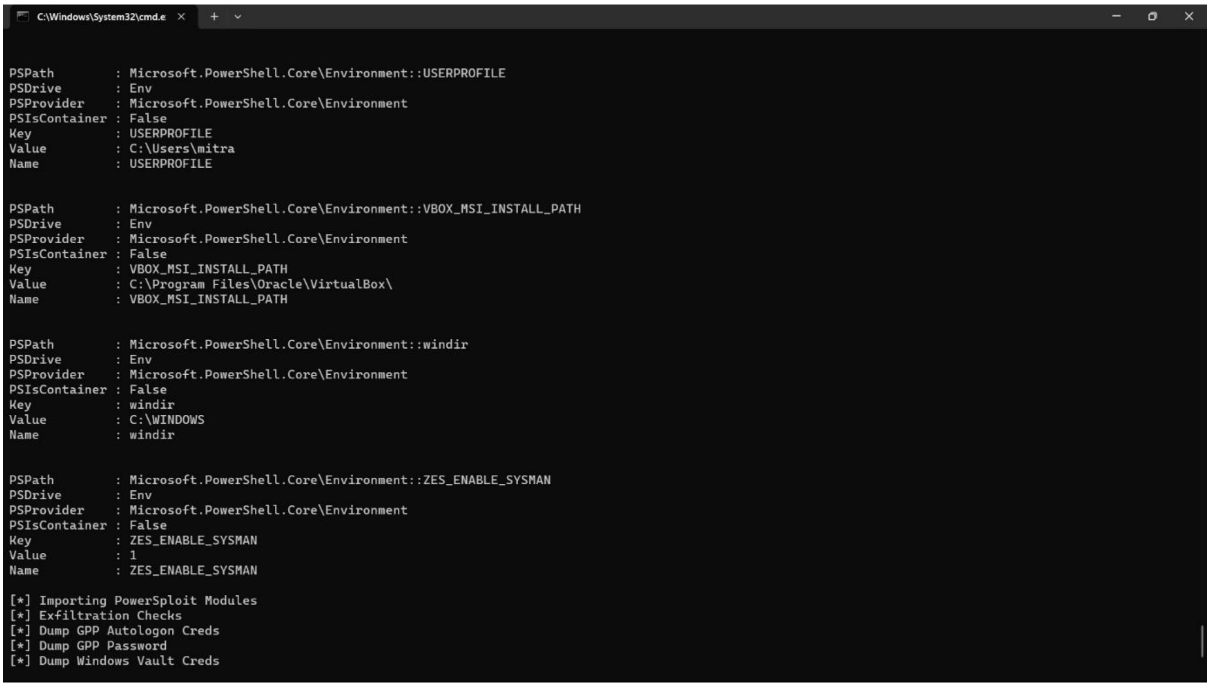
```
PSPath        : Microsoft.PowerShell.Core\Environment::ProgramW6432
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : ProgramW6432
Value         : C:\Program Files
Name          : ProgramW6432


PSPath        : Microsoft.PowerShell.Core\Environment::PROMPT
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : PROMPT
Value         : $P$G
Name          : PROMPT


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


PSPath        : Microsoft.PowerShell.Core\Environment::PSModulePath
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : PSModulePath
Value         : C:\Users\mitra\OneDrive\Documents\WindowsPowerShell\Modules;C:\Program
                Files\WindowsPowerShell\Modules;C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules
Name          : PSModulePath


PSPath        : Microsoft.PowerShell.Core\Environment::PT8HOME
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
```



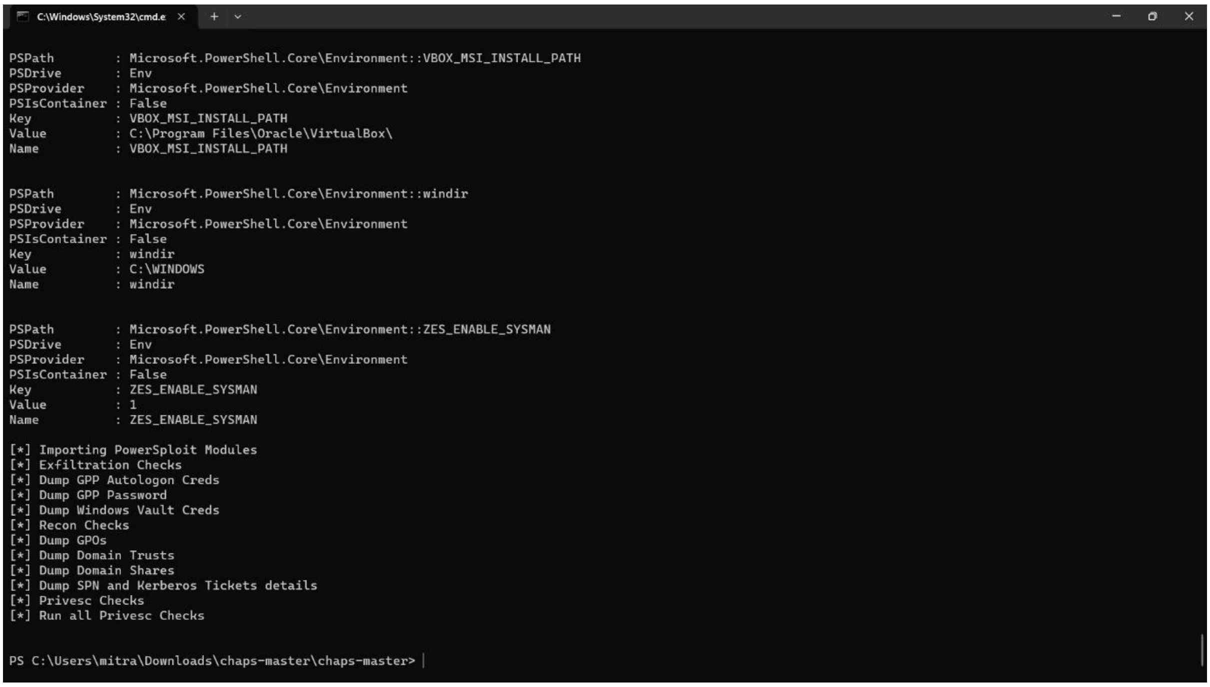
```
PSPath        : Microsoft.PowerShell.Core\Environment::PUBLIC
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : PUBLIC
Value         : C:\Users\Public
Name          : PUBLIC


PSPath        : Microsoft.PowerShell.Core\Environment::PyCharm Community Edition
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : PyCharm Community Edition
Value         : C:\Program Files\JetBrains\PyCharm Community Edition 232.8296.19\bin;
Name          : PyCharm Community Edition


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


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


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



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


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


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


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



```
PSPath        : Microsoft.PowerShell.Core\Environment::USERPROFILE
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : USERPROFILE
Value         : C:\Users\mitra
Name          : USERPROFILE


PSPath        : Microsoft.PowerShell.Core\Environment::VBOX_MSI_INSTALL_PATH
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : VBOX_MSI_INSTALL_PATH
Value         : C:\Program Files\Oracle\VirtualBox\
Name          : VBOX_MSI_INSTALL_PATH


PSPath        : Microsoft.PowerShell.Core\Environment::windir
PSDrive       : Env
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
```



```
PSPath        : Microsoft.PowerShell.Core\Environment::VBOX_MSI_INSTALL_PATH
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : VBOX_MSI_INSTALL_PATH
Value         : C:\Program Files\Oracle\VirtualBox\
Name          : VBOX_MSI_INSTALL_PATH


PSPath        : Microsoft.PowerShell.Core\Environment::windir
PSDrive       : Env
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


PS C:\Users\mitra\Downloads\chaps-master\chaps-master>
```

These are the system vulnerabilities which need to be mitigated to strength the security configuration of Windows systems.

Remediations

1. Keep the System Updated

Ensure that Windows operating systems, as well as all installed software and applications, are regularly updated with the latest security patches and updates. Enable automatic updates where possible to ensure timely protection against known vulnerabilities.

2. Use Strong Authentication

Implement strong authentication mechanisms, such as multi-factor authentication (MFA), to enhance user authentication and access control. This adds an extra layer of security beyond passwords.

3. User Account Management

Enforce the principle of least privilege by restricting user permissions to only those necessary for their job functions. Regularly review and audit user accounts to remove unnecessary privileges and disable or remove inactive accounts.

4. Enable Windows Firewall

Activate and configure the built-in Windows Firewall to control inbound and outbound network traffic. Define rules to allow only essential services and applications to communicate over the network.

5. Implement Endpoint Protection

Deploy robust antivirus and anti-malware software on all Windows systems to detect and prevent malicious software infections. Regularly update virus definitions and perform full system scans.

6. Encrypt Data

Utilize encryption technologies such as BitLocker to encrypt data on disk drives and ensure data confidentiality, especially for sensitive information. Additionally, implement encryption for data transmitted over networks using protocols like TLS.

7. Secure Remote Access

Secure remote access to Windows systems by using VPNs (Virtual Private Networks) with strong encryption and authentication methods. Implement remote desktop solutions securely, such as Remote Desktop Gateway, and restrict access based on user roles and permissions.

8. Enable Auditing and Logging

Configure Windows auditing policies to monitor and log security-relevant events, such as login attempts, privilege changes, and file access. Centralize logs to a secure location and regularly review them for suspicious activities.

9. Application Whitelisting

Implement application whitelisting to allow only authorized and trusted applications to execute on Windows systems. This helps prevent the execution of malicious software and unauthorized programs.

10. Secure Configuration Baselines

Utilize security configuration baselines provided by Microsoft or industry standards (such as CIS benchmarks) to apply recommended security settings consistently across Windows systems. Regularly review and update these baselines to align with evolving threats and best practices.

11. User Training and Awareness

Educate users about security best practices, such as recognizing phishing emails, avoiding suspicious websites, and safeguarding sensitive information. Regular security awareness training can help mitigate the risk of human error leading to security incidents.

12. Implement Group Policies

Utilize Group Policy Objects (GPOs) to enforce security settings and restrictions across Windows domains and organizational units. Configure GPOs to enforce password policies, restrict USB access, and control other security-related settings.

Assessment Questions

1. a. A PowerShell script for assessing the configuration hardening of Windows machines.
2. a. To provide an automated way to assess the configuration hardening of Windows machines.
3. a. Password policy settings, local security policy settings, and user rights assignments.
4. a. By querying the Windows registry and security policy settings.
5. a. A report in CSV format that lists the security settings assessed and their status (enabled/disabled).
6. a. It can help identify security vulnerabilities and assist in hardening the configuration of Windows machines.
7. a. It only assesses security settings related to configuration hardening and does not perform vulnerability scanning or penetration testing.
8. c. Improve the accuracy of the assessments to minimize false positives and false negatives.
9. a. Microsoft Baseline Security Analyzer (MBSA)
10. In my opinion, CHAPS is quite useful for assessing the configuration hardening of Windows machines. Its automation capabilities streamline the process of evaluating security settings, such as password policies and user rights assignments, across multiple systems. By providing a structured approach to security configuration assessment, CHAPS helps administrators quickly identify potential vulnerabilities and areas for improvement. While it may have some limitations, such as focusing solely on configuration hardening and requiring administrative privileges to run, its ability to generate detailed reports facilitates informed decision-making and enhances overall security posture. Overall, CHAPS serves as a valuable tool in the arsenal of security professionals tasked with safeguarding Windows environments.