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

Name- Tiasha Saha

Email ID- tiashasaha1999@gmail.com

LinkedIn ID- https://www.linkedin.com/in/tiasha-gbs

Phone NO.- 7980871490

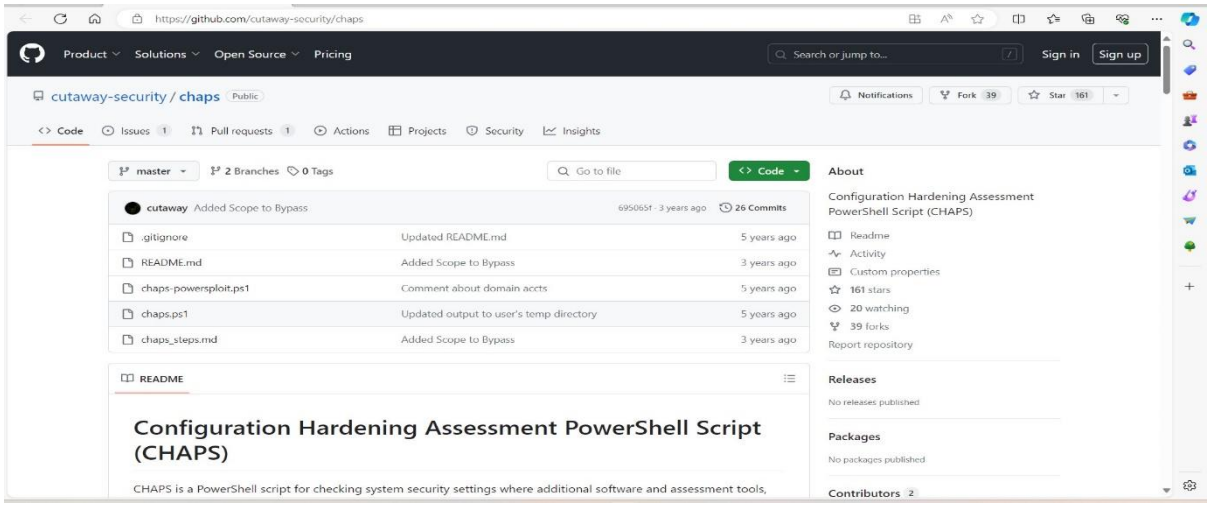
Introduction

Configuration Hardening Assessment PowerShell Script (CHAPS) is designed to verify the security settings of a system in situations where installing extra software or assessment tools, like Microsoft Policy Analyzer, is not possible. This script is meant to be launched on a workstation or server to gather configuration data about that particular system. The gathered data can then be utilized to offer suggestions (and references) for enhancing the security of each system as well as systemic problems with the Windows environment inside the company. Situations involving Industrial Control Systems (ICS) where system modifications are not possible are circumstances where this script can be helpful. These systems, installed in production settings, consist of management servers, engineer/operator workstations, and Human Machine Interface (HMI) systems.

Steps to use chaps

Step 1

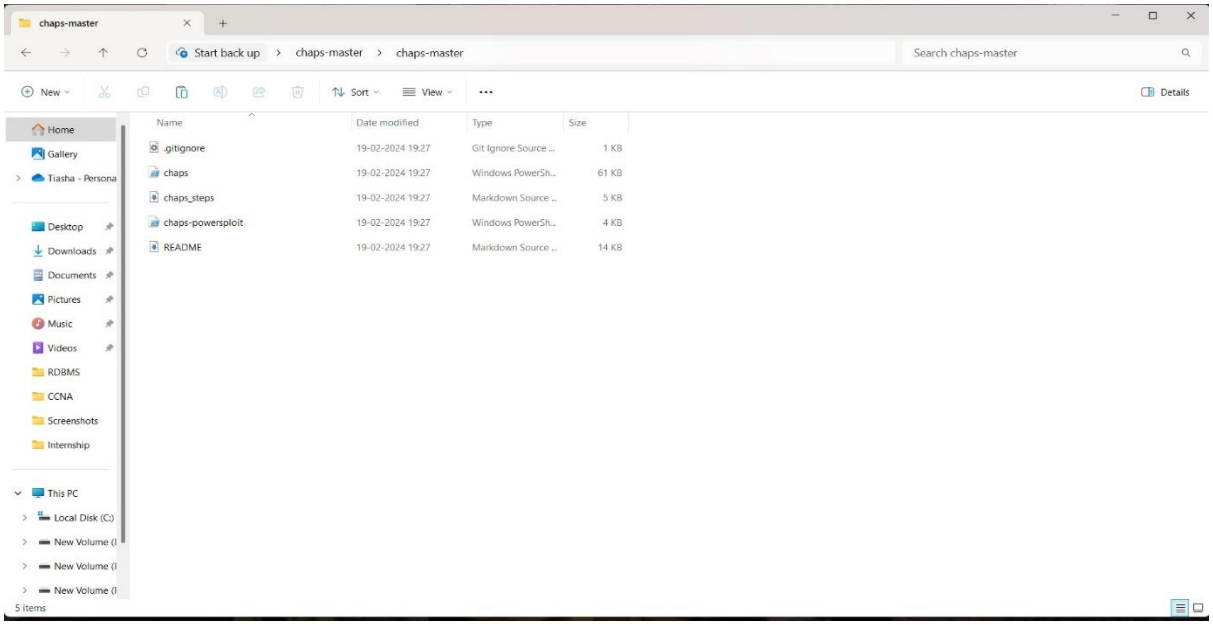
First, we have to download CHAPS from GitHub (https://github.com/cutawaysecurity/chaps)



By clicking the above link, the above page will open the go to the code and download the zip file of CHAPS

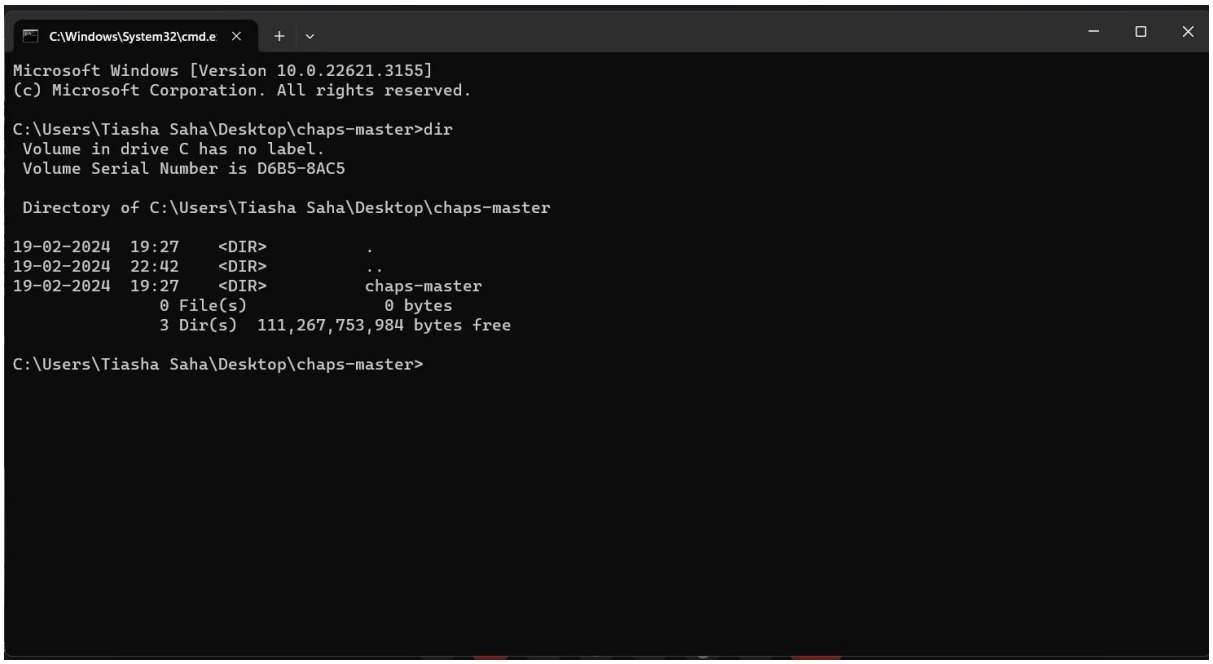
Step 2

Then extract the zip file



Step 3

Then open CMD in the CHAPS directory and list the files by clicking **'dir'** command.



Step 4

Next step is to run the command **'powershell.exe -exec bypass'** to being a PowerShell prompt. Then we got the PowerShell Script by using this command.

```
C:\Users\Tiasha Saha\Desktop\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
```

Step 5

Now we have to run the command **'Set-ExecutionPolicy Bypass -scope Process'** to allow scripts to execute.'

```
PS C:\Users\Tiasha Saha\Desktop\chaps-master\chaps-master> Set-ExecutionPolicy Bypass -scope Process
PS C:\Users\Tiasha Saha\Desktop\chaps-master\chaps-master>
```

Step 6

Now again we have to use the **'dir'** command to get the list, and use the third command from the list.

```
C:\Windows\System32\cmd.e

PS C:\Users\Tiasha Saha\Desktop\chaps-master\chaps-master> dir


    Directory: C:\Users\Tiasha Saha\Desktop\chaps-master\chaps-master


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        19-02-2024     19:27             89 .gitignore
-a----        19-02-2024     19:27           3887 chaps-powersploit.ps1
-a----        19-02-2024     19:27          61567 chaps.ps1
-a----        19-02-2024     19:27           4397 chaps_steps.md
-a----        19-02-2024     19:27          13842 README.md


PS C:\Users\Tiasha Saha\Desktop\chaps-master\chaps-master>
```

Step 7

Now we will run the command **‘chaps.ps1’** from the above list.

```
C:\Windows\System32\cmd.e

PS C:\Users\Tiasha Saha\Desktop\chaps-master\chaps-master> .\chaps.ps1


    Directory: C:\Users\TIASHA~1\AppData\Local\Temp


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        20-02-2024     19:08                chaps-20240220-070803
[*] Start Date/Time: 20240220T19080338+00
[-] You do not have Administrator rights. Some checks will not succeed. Note warnings.
[*] Dumping System Info to seperate file\n

Host Name:                 DESKTOP-DUBTVL6
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:          Tiasha Saha
Registered Organization:
Product ID:                00327-36325-48881-AAOEM
Original Install Date:     26-03-2023, 21:37:12
System Boot Time:          20-02-2024, 16:26:25
System Manufacturer:       Dell Inc.
System Model:              Inspiron 15 3511
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
Tiasha Saha
```

```
C:\Windows\System32\cmd.e
                           [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~2995 Mhz
BIOS Version:              Dell Inc. 1.25.1, 03-10-2023
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume5
System Locale:             en-gb;English (United Kingdom)
Input Locale:              00004009
Time Zone:                 (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     7,927 MB
Available Physical Memory: 1,740 MB
Virtual Memory: Max Size:  10,999 MB
Virtual Memory: Available: 3,205 MB
Virtual Memory: In Use:    7,794 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\DESKTOP-DUBTVL6
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB5034467
                           [02]: KB5012170
                           [03]: KB5034765
                           [04]: KB5032393
                           [05]: KB5034225
Network Card(s):           4 NIC(s) Installed.
                           [01]: Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC
                                 Connection Name: WiFi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.181.184
                                 IP address(es)
                                 [01]: 192.168.181.159
                                 [02]: fe80::a6b0:79f0:2307:2f
: ProgramFiles(x86)
Tiasha Saha
```

```
C:\Windows\System32\cmd.e

                              [02]: VMware Virtual Ethernet Adapter for VMnet1
                                    Connection Name: VMware Network Adapter VMnet1
                                    DHCP Enabled:    Yes
                                    DHCP Server:     192.168.242.254
                                    IP address(es)
                                    [01]: 192.168.242.1
                                    [02]: fe80::65e3:9f8b:883f:c4e1
                              [03]: VMware Virtual Ethernet Adapter for VMnet8
                                    Connection Name: VMware Network Adapter VMnet8
                                    DHCP Enabled:    Yes
                                    DHCP Server:     192.168.75.254
                                    IP address(es)
                                    [01]: 192.168.75.1
                                    [02]: fe80::8d88:88cc:8dc:a893
                              [04]: Bluetooth Device (Personal Area Network)
                                    Connection Name: Bluetooth Network Connection
                                    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 10.0.22621.0
[*] Windows Default Path for Tiasha Saha : C:\oraclexe\app\oracle\product\11.2.0\server\bin;;C:\Program Files (x86)\VMwa
re\VMware Player\bin\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0
\;C:\WINDOWS\System32\OpenSSH\;c 64;C:\Program Files\CodeBlocks\MinGW\bin;C:\Program Files\nodejs\;C:\Users\Tiasha Saha\
AppData\Local\Microsoft\WindowsApps;;C:\Program Files\JetBrains\PyCharm Community Edition 2023.2.1\bin;;C:\Users\Tiasha
Saha\AppData\Local\Programs\Microsoft VS Code\bin;C:\Users\Tiasha Saha\AppData\Roaming\npm
[*] Checking IPv4 Network Settings
[*] Host network interface assigned: 169.254.209.37
[*] Host network interface assigned: 192.168.75.1
[*] Host network interface assigned: 192.168.242.1
[*] Host network interface assigned: 169.254.102.146
[*] Host network interface assigned: 169.254.83.11
```

```
C:\Windows\System32\cmd.e

[*] Host network interface assigned: 192.168.181.159
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi): fe80::a6b0:79f0:2307:2f
[-] Host IPv6 network interface assigned (gwmi): fe80::65e3:9f8b:883f:c4e1
[-] Host IPv6 network interface assigned (gwmi): fe80::8d88:88cc:8dc:a893
[*] 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.
[+] 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.
```

```
C:\Windows\System32\cmd.e
[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-Wind
ows-TaskScheduler/Operational] GB: 0.01 GB
[-] Microsoft-Windows-WinRM/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-WinR
M/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-Windo
ws-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.H
ashtable[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
[x] Testing for PowerShell Version 2 failed.
[*] 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
```

```
C:\Windows\System32\cmd.e
[*] 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", PolicyRuleNa
me = "", SystemCreationClassName = "", SystemName = "").Name is disabled.
[+] WinRM Firewall Rule MSFT_NetFirewallRule (CreationClassName = "MSFT?FW?FirewallRule?WINRM-HTTP-In-TCP-..., PolicyRul
eName = "", SystemCreationClassName = "", SystemName = "").Name is disabled.
[*] Testing Local Administrator Accounts.
[-] More than one account is in local Administrators group: 2
[*] Account in local Administrator group: DESKTOP-DUBTVL6\Administrator
[*] Account in local Administrator group: DESKTOP-DUBTVL6\Tiasha Saha
[*] 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.
```

```
C:\Windows\System32\cmd.e
[-] 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.
[+] 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.
```

```
C:\Windows\System32\cmd.e
[-] 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: 20240220T19091813+00


PS C:\Users\Tiasha Saha\Desktop\chaps-master\chaps-master>
```

```
C:\Windows\System32\cmd.e
[-] 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: 20240220T19091813+00
```

Step 8

Now again we have to use the **‘dir’** command to get the list, and use the second command from the list.

```
PS C:\Users\Tiasha Saha\Desktop\chaps-master\chaps-master> dir


    Directory: C:\Users\Tiasha Saha\Desktop\chaps-master\chaps-master


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        19-02-2024     19:27             89 .gitignore
-a----        19-02-2024     19:27           3887 chaps-powersploit.ps1
-a----        19-02-2024     19:27          61567 chaps.ps1
-a----        19-02-2024     19:27           4397 chaps_steps.md
-a----        19-02-2024     19:27          13842 README.md


PS C:\Users\Tiasha Saha\Desktop\chaps-master\chaps-master>
```

Step 9

Lastly, we will run the command ‘**chaps-powersploit.ps1**’ to import the appropriate PowerSploit script.

```
C:\Windows\System32\cmd.e

PS C:\Users\Tiasha Saha\Desktop\chaps-master\chaps-master> .\chaps-powersploit.ps1


    Directory: C:\Users\TIASHA~1\AppData\Local\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        20-02-2024     19:19                chaps-PS-20240220-071909
Start Date/Time: 20240220T19190996+00
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\Tiasha Saha\AppData\Roaming
Name          : APPDATA


PSPath        : Microsoft.PowerShell.Core\Environment::c
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : c
Value         : 64
Name          : c
```

```
C:\Windows\System32\cmd.e

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
Value         : DESKTOP-DUBTVL6
Name          : COMPUTERNAME


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

```
C:\Windows\System32\cmd.e

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_12500
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : EFC_12500
Value         : 1
Name          : EFC_12500


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


PSPath        : Microsoft.PowerShell.Core\Environment::HOMEPATH
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : HOMEPATH
Value         : \Users\Tiasha Saha
Name          : HOMEPATH
```

```
C:\Windows\System32\cmd.e

PSPath        : Microsoft.PowerShell.Core\Environment::IGCCSVC_DB
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : IGCCSVC_DB
Value         : AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAI02Y2EwjoUaWNcmXZ1H3AgQAAAACAAAAAAAQZgAAAAEAACAAAAC+agY/1GMaD7DuJ+AxUN+
                uswzft9O2vUFpdUfUzIOMAAAAAAAOgAAAAAIAACAAAAAFl+qMueRGnhaul6beoRxU5rEM0sWLBFWrCQAluSQ9+2AAAAAsuBlwG/wMv/
                ykRC/lmtS+huF1SVT7lpTyLpJp5YyCbU1kUAT2NCW7FnK3f90iuyf16UleCvLZvQ89vDlRsDrP5f695kFka4FlYyg+si4hxtenRmTuW
                33s7UaPGpu0vcVAAAAAMmo+VZXpREGF9vkvTVfpLWcLEdI0o2mspxliGoP8Anzwid7+usXMrpK5dPj7MzwjuB6AX5y6hwlfQtjiTOwt
                vg==
Name          : IGCCSVC_DB


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


PSPath        : Microsoft.PowerShell.Core\Environment::LOGONSERVER
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : LOGONSERVER
Value         : \\DESKTOP-DUBTVL6
Name          : LOGONSERVER


PSPath        : Microsoft.PowerShell.Core\Environment::MOZ_PLUGIN_PATH
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : MOZ_PLUGIN_PATH
Value         : C:\Program Files (x86)\Foxit Software\Foxit Reader\plugins\
Name          : MOZ_PLUGIN_PATH
```

```
C:\Windows\System32\cmd.e

PSPath        : Microsoft.PowerShell.Core\Environment::NUMBER_OF_PROCESSORS
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : NUMBER_OF_PROCESSORS
Value         : 4
Name          : NUMBER_OF_PROCESSORS


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


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


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


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

```
C:\Windows\System32\cmd.e

Key           : Path
Value         : C:\oraclexe\app\oracle\product\11.2.0\server\bin;;C:\Program Files (x86)\VMware\VMware Player\bin\;C:\W
                INDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WIND
                OWS\System32\OpenSSH\;c 64;C:\Program Files\CodeBlocks\MinGW\bin;C:\Program
                Files\nodejs\;C:\Users\Tiasha Saha\AppData\Local\Microsoft\WindowsApps;;C:\Program
                Files\JetBrains\PyCharm Community Edition 2023.2.1\bin;;C:\Users\Tiasha
                Saha\AppData\Local\Programs\Microsoft VS Code\bin;C:\Users\Tiasha Saha\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 140 Stepping 1, GenuineIntel
Name          : PROCESSOR_IDENTIFIER


PSPath        : Microsoft.PowerShell.Core\Environment::PROCESSOR_LEVEL
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
```

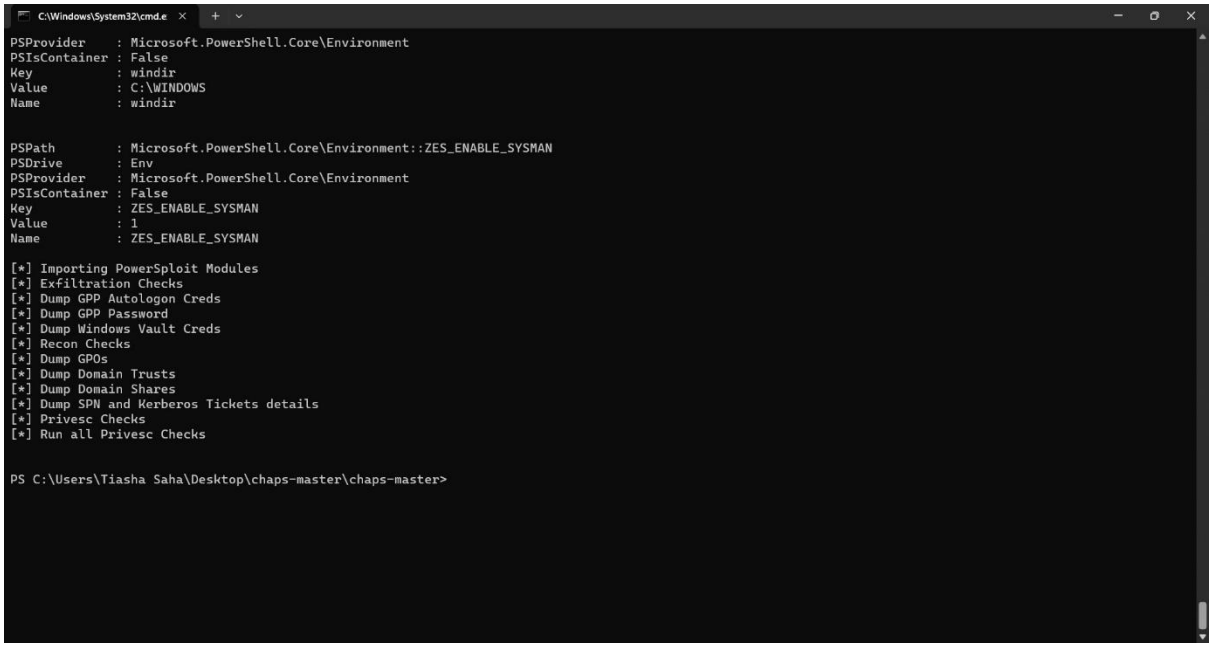
```
C:\Windows\System32\cmd.e

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         : 8c01
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)
Value         : C:\Program Files (x86)
Name          : ProgramFiles(x86)
```

```
C:\Windows\System32\cmd.e

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\Tiasha Saha\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
```

```
C:\Windows\System32\cmd.e

PSIsContainer : False
Key           : PT8HOME
Value         : C:\Program Files\Cisco Packet Tracer 8.2.1
Name          : PT8HOME


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 2023.2.1\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
```

```
C:\Windows\System32\cmd.e

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\TIASHA~1\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\TIASHA~1\AppData\Local\Temp
Name          : TMP


PSPath        : Microsoft.PowerShell.Core\Environment::USERDOMAIN
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : USERDOMAIN
Value         : DESKTOP-DUBTVL6
Name          : USERDOMAIN


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

```
C:\Windows\System32\cmd.e

Key           : USERDOMAIN_ROAMINGPROFILE
Value         : DESKTOP-DUBTVL6
Name          : USERDOMAIN_ROAMINGPROFILE


PSPath        : Microsoft.PowerShell.Core\Environment::USERNAME
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : USERNAME
Value         : Tiasha Saha
Name          : USERNAME


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



```
C:\Windows\System32\cmd.e

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\Tiasha Saha\Desktop\chaps-master\chaps-master>
```

These are the system vulnerabilities that must be fixed in order to strengthen Windows systems' security setup.

Remediations

1. Identify Misconfigurations:

Analyze the results of your configuration hardening assessment to identify specific vulnerabilities or misconfigurations. This could include insecure settings, weak permissions, deprecated protocols, etc.

2. Research Remediation Steps:

Research the remediation steps required to address each identified misconfiguration. This might involve consulting security guidelines, vendor documentation, best practices, or security standards relevant to your environment (e.g., CIS Benchmarks).

3. Develop PowerShell Script:

Write PowerShell script functions to implement the remediation steps for each misconfiguration. Each function should address a specific issue and apply the necessary changes. Use PowerShell cmdlets or modules to interact with system settings, registry keys, file permissions, etc.

4. Test Script:

Test the PowerShell script in a controlled environment to ensure it behaves as expected and successfully mitigates the identified misconfigurations. Test against different configurations and scenarios to validate effectiveness.

5. Implement Logging and Reporting:

Implement logging functionality within the script to record the changes made during the remediation process. This helps in tracking changes and auditing the effectiveness of the mitigation efforts. You may also want to generate a report summarizing the changes made.

6. Execute Script in Production:

Once the script has been tested thoroughly, execute it in your production environment to apply the remediations. Ensure that appropriate permissions are in place to allow the script to make the necessary changes.

7. Monitor and Verify:

Monitor the system after applying the remediations to ensure that the changes have been successfully implemented and have not introduced any new issues. Verify that the system remains compliant with security standards and requirements.

8. Update Documentation:

Update your documentation to reflect the changes made to address the identified misconfigurations. This includes updating configuration management databases, security policies, and procedures.

The above points are the remediations of CHAPS.

Assessment Questions:

1. What is CHAPS?

   Ans: a. A PowerShell script for assessing the configuration hardening of Windows machines.

2. What is the purpose of CHAPS?

   Ans: a. To provide an automated way to assess the configuration hardening of Windows machines.

3. What are some of the security settings assessed by CHAPS?

   Ans: a. Password policy settings, local security policy settings, and user rights assignments.

4. How does CHAPS assess the security settings of Windows machines?

   Ans: a. By querying the Windows registry and security policy settings

5. What is the output of CHAPS?

   Ans: a. A report in CSV format that lists the security settings assessed and their status (enabled/disabled).

6. How can CHAPS be useful in a corporate environment?

   Ans: a. It can help identify security vulnerabilities and assist in hardening the configuration of Windows machines.

7. What are some limitations of CHAPS?

   Ans: a. It only assesses security settings related to configuration hardening and does not perform vulnerability scanning or penetration testing.

8. What are some ways to improve CHAPS?

Ans: c. Improve the accuracy of the assessments to minimize false positives and false negatives.

9. What are some alternatives to CHAPS?

Ans: Microsoft Baseline Security Analyzer (MBSA)

10. In your opinion, how useful do you think CHAPS is for assessing the configuration hardening of Windows machines? Why?

Ans: In my option, CHAPS is a really helpful tool for evaluating how hardened a Windows machine's configuration is. The act of assessing security settings, such as password restrictions and user rights assignments, across numerous networks. CHAPS assists administrators in promptly identifying potential vulnerabilities and areas for improvement by offering an organised method for security configuration review. Its capacity to generate comprehensive reports aids in informed decision-making and improves overall security posture, despite certain constraints such as its exclusive focus on configuration hardening and need for administrative credentials to operate. All things considered; CHAPS is a useful tool in the toolbox of security experts entrusted with protecting Windows systems.