Assignment-1

Title: Internship Assessment on CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS)

CHAPS

Configuration Hardening Assessment PowerShell Script (CHAPS) is a PowerShell script for checking system security settings where additional software and assessment tools, such as Microsoft Policy Analyzer, cannot be installed.

Objective:

The objective of this internship assessment is to evaluate the intern's understanding and proficiency in CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS) and its use in assessing the security configuration of Windows operating systems.

Task:

As an intern, your task for the first week of h1k0r ceh Internship is to perform a CHAPS Configuration

Hardening Assessment PowerShell Script (CHAPS) on a Windows system, analyze the results, and provide a report summarizing the findings.

Steps:

- Download the CHAPS PowerShell script from the GitHub repository: https://github.com/cutaway-security/chaps
- Type This Command Git clone https://github.com/cutaway-security/chaps
- Type This Command On Powershell
- Powershell.exe -exec bypass(To Bypass The Execution)
- Type This Command On Powershell
- Set-ExecutionPolicy Bypass -scope Process(To Bypass & Set Execution Policy)

```
PS C:\Users\parag\chaps> 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\parag\chaps> Set-ExecutionPolicy Bypass -scope Process
PS C:\Users\parag\chaps> dir


    Directory: C:\Users\parag\chaps


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        23-01-2024     12:48            100 .gitignore
-a----        23-01-2024     12:48           3972 chaps-powersploit.ps1
-a----        23-01-2024     12:48          62859 chaps.ps1
-a----        23-01-2024     12:48           4481 chaps_steps.md
-a----        23-01-2024     12:48          14027 README.md
```

- Type This Command On Powershell

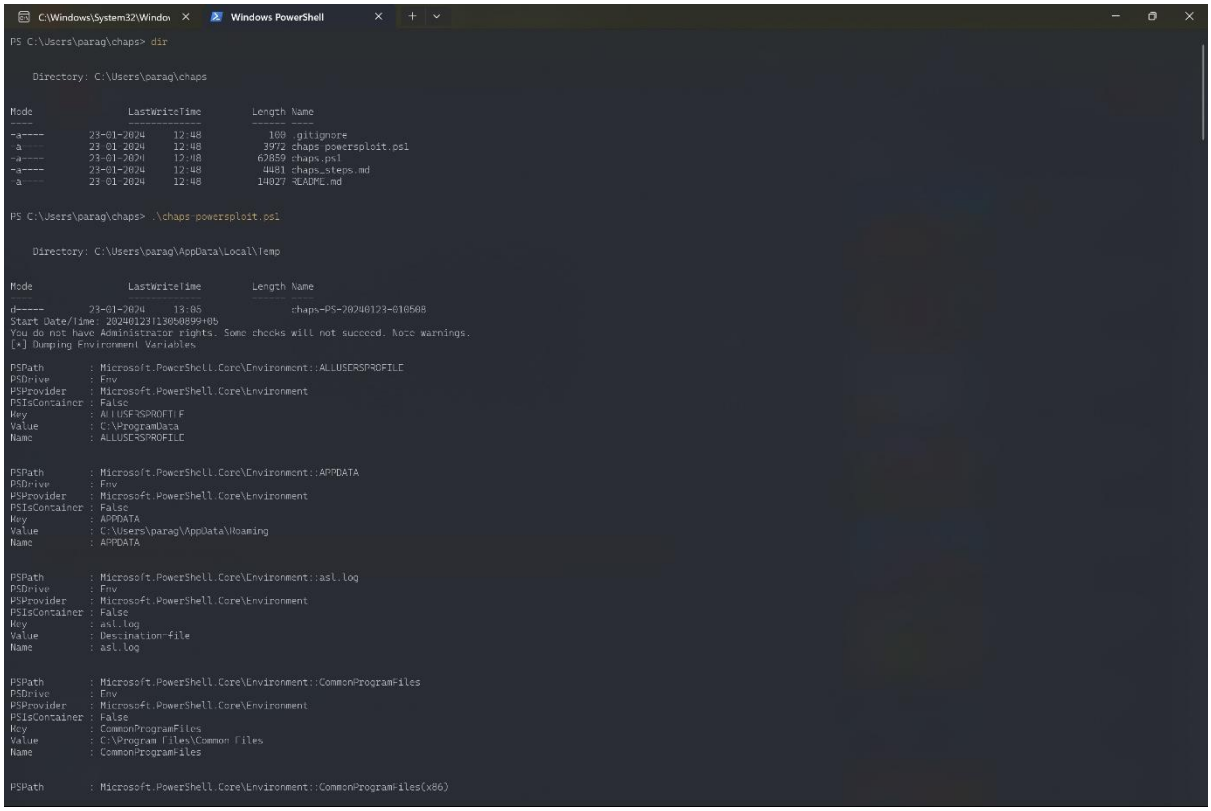
- Dir(For Lists Commands)
- Type This Command On Powershell
- \chaps.ps1(To Analys All Information Like:-OS Name, OS Version, OS Manufacture, Configuration Etc.)

```
PS C:\Users\parag\chaps> .\chaps.ps1


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


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        23-01-2024     12:52                chaps-20240123-125212
[*] Start Date/Time: 20240123T12521216+05
[-] You do not have Administrator rights. Some checks will not succeed. Note warnings.
[*] Dumping System Info to seperate file\n

Host Name:                 H4CK3R
OS Name:                   Microsoft Windows 11 Pro
OS Version:                10.0.22631 N/A Build 22631
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          paragbhangale.2023@outlook.com
Registered Organization:   HP
Product ID:                00330-80000-00000-AA768
Original Install Date:     05-11-2023, 07:45:25
System Boot Time:          21-01-2024, 20:07:33
System Manufacturer:       HP
System Model:              HP Spectre x360 2-in-1 Laptop 14-ef2xxx
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 186 Stepping 3 GenuineIntel ~1700 Mhz
BIOS Version:              Insyde F.04, 15-12-2023
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     32,461 MB
Available Physical Memory: 18,938 MB
Virtual Memory: Max Size:  37,325 MB
Virtual Memory: Available: 22,228 MB
Virtual Memory: In Use:    15,097 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\H4CK3R
Hotfix(s):                 6 Hotfix(s) Installed.
                           [01]: KB5033920
                           [02]: KB5012170
                           [03]: KB5027397
                           [04]: KB5032381
                           [05]: KB5034123
                           [06]: KB5032393
Network Card(s):           4 NIC(s) Installed.
                           [01]: Intel(R) Wi-Fi 6E AX211 160MHz
                                 Connection Name: Wi-Fi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.1.1
                                 IP address(es)
                                 [01]: 192.168.1.9
                                 [02]: fe80::6b61:25a1:7491:1b38
                                 [03]: 2401:4900:1c9b:91b4:d42e:c10:2afe:558
                                 [04]: 2401:4900:1c9b:91b4:bb23:dc1:a147:e9ce
                           [02]: Bluetooth Device (Personal Area Network)
```

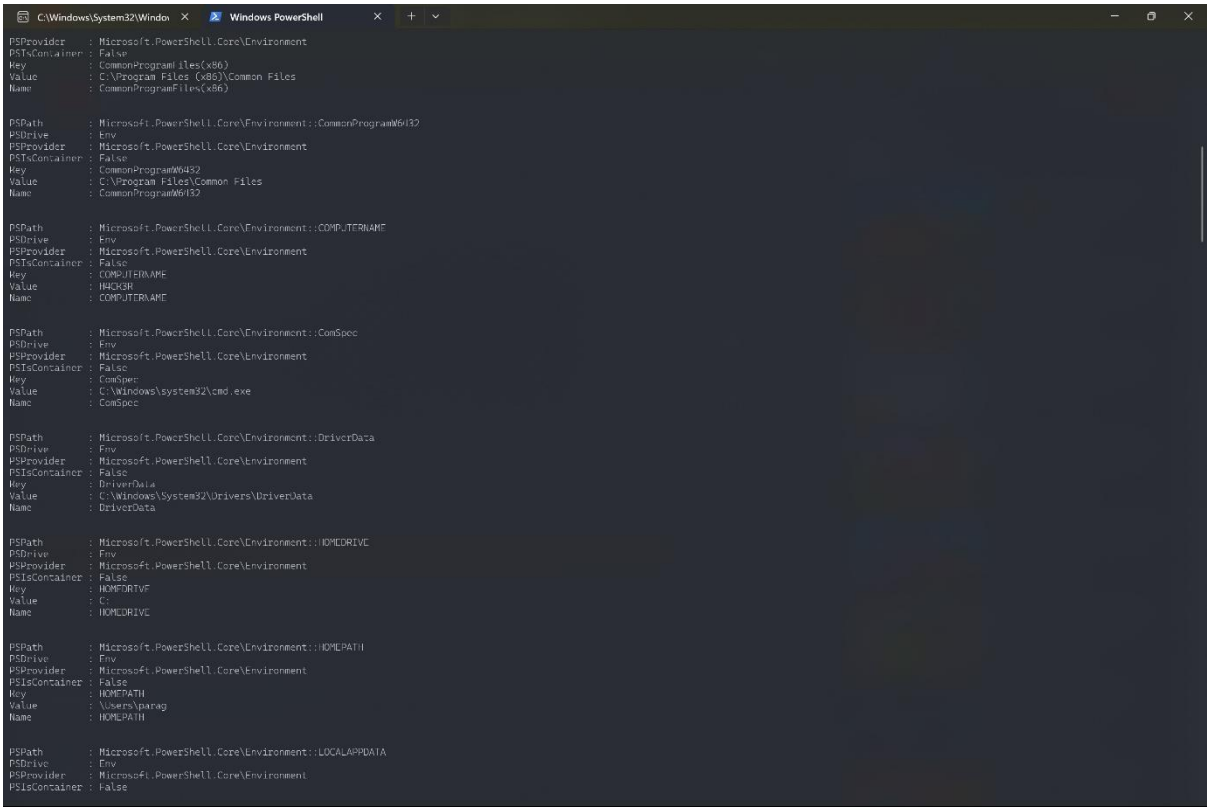
```
                                Connection Name: Bluetooth Network Connection
                                Status:          Media disconnected
                           [03]: VirtualBox Host-Only Ethernet Adapter
                                Connection Name: Ethernet 3
                                DHCP Enabled:    No
                                IP address(es)
                                [01]: 192.168.56.2
                                [02]: fe80::ebce:df21:7ea0:3beb
                           [04]: VirtualBox Host-Only Ethernet Adapter
                                Connection Name: Ethernet 2
                                DHCP Enabled:    No
                                IP address(es)
                                [01]: 192.168.56.1
                                [02]: fe80::e49d:ae6e:3ffc:1bb
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 parag : C:\Program Files\Common Files\Oracle\Java\javapath;C:\Program Files\Python312\Scripts\;C:\Program Files\Python312\;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C
:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Program Files\Git\cmd;C:\adb;C:\Program Files (x86)\Microsoft SQL Server\160\Tools\Binn\;C:\Program Files\Microsoft SQL Server\160\Too
ls\Binn\;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\;C:\Program Files\Microsoft SQL Server\160\DTS\Binn\;C:\Users\parag\AppData\Local\Microsoft\WindowsApps;;C:\Program Files\JetBrains
\PyCharm Community Edition 2023.2.5\bin;;C:\Program Files (x86)\Nmap
[*] Checking TPv4 Network Settings
[*] Host network interface assigned: 172.27.32.1
[*] Host network interface assigned: 192.168.56.1
[*] Host network interface assigned: 192.168.96.2
[*] Host network interface assigned: 169.254.213.52
[*] Host network interface assigned: 169.254.88.83
[*] Host network interface assigned: 169.254.183.235
[*] Host network interface assigned: 192.168.1.9
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi): fe80::6b61:25a1:7f91:1b38
[-] Host IPv6 network interface assigned (gwmi): 2401:4900:1c9b:91b4:d42e:c10:2af6:558
[-] Host IPv6 network interface assigned (gwmi): 2401:4900:1c9b:91b4:bb23:dc1:a147:e9ce
[-] Host IPv6 network interface assigned (gwmi): fe80::e6ce:df21:7ea0:3beb
[-] Host IPv6 network interface assigned (gwmi): fe80::e49d:ae6e:3ffc:1bb
[*] 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 Auditing is Enabled
[-] ProcessCreationIncludeCmdLine_Enabled Is Not Set
[*] Testing if PowerShell Modulog is Enabled
[-] EnableModuleLogging Is No. Se.
[*] 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 ProjectedFsLogging 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 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: 0.0
[*] 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 Language Mode is Not ConstrainedLanguage: FullLanguage
[*] Testing if system is configured to limit the number of stored credentials.
[-] CachedLogonsCount Is No. 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 WinHW 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:  HICK3R\Administrator
[*] Account in local Administrator group: HICK3R\parag
[*] Testing if AppLocker is configured.
[!] AppLocker not configured
[*] LMLI 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 2a5.2a5.255.255
[*] 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
```

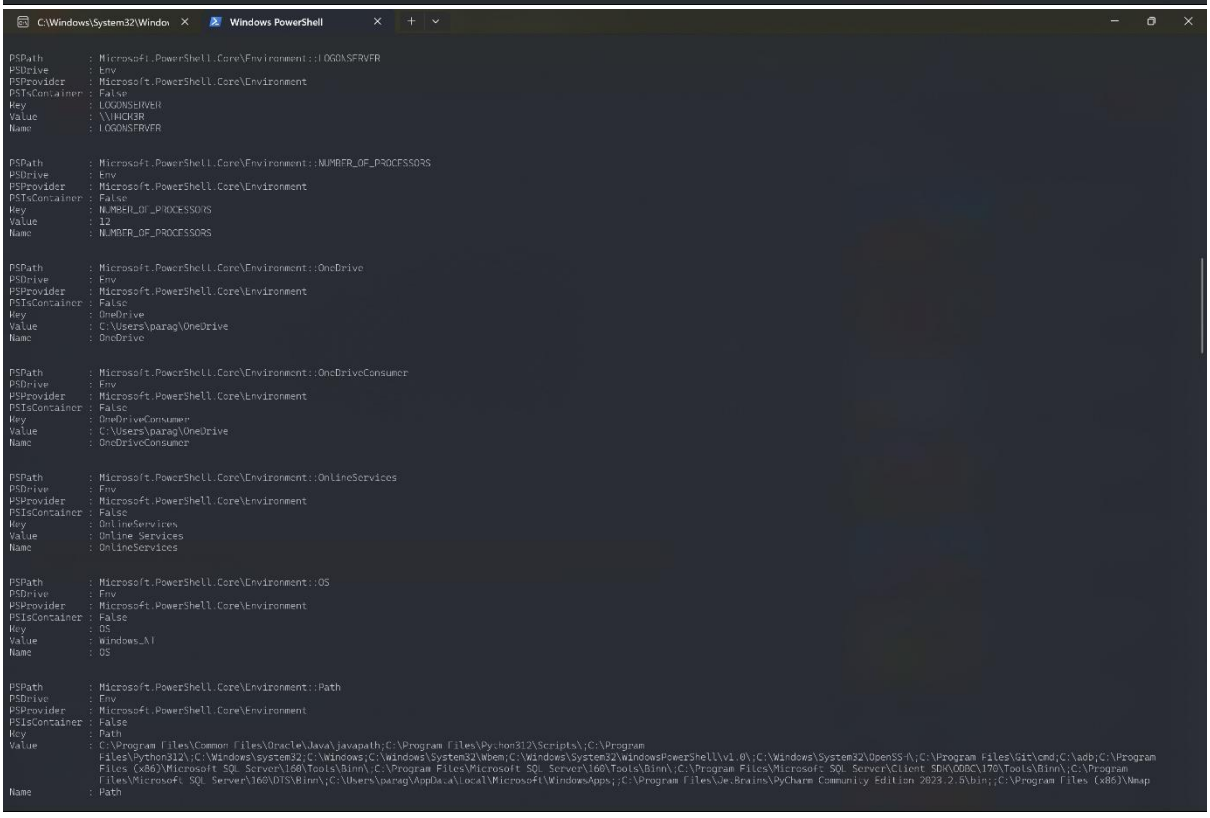
```
[+] LocalAccountTokenFilterPolicy Is Not Set
[*] Testing if PowerShell LocalAccountTokenFilterPolicy in Wow6432Node Policies is Disabled
[+] LocalAccountTokenFilterPolicy in Wow6432Node Is Not Set
[*] Testing if WDigest is disabled.
[-] WDigest UseLogonCredential key does not exist.
[*] Testing if SMBv1 is disabled.
[*] Testing if SMBv1 is disabled.
[-] SMBv1 is Enabled
[*] Testing if system is configured to audit SMBv1 activity.
[+] 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: 20240123T12533554+05
```



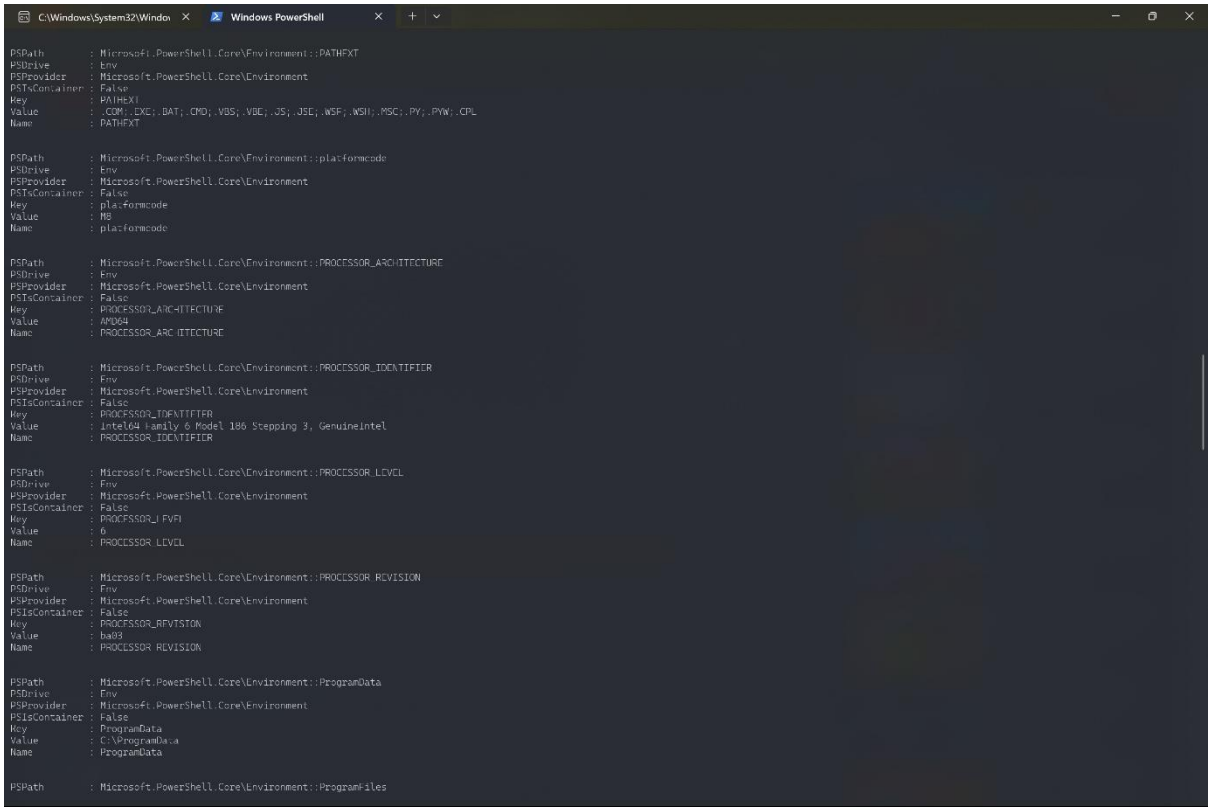
```
```

- 

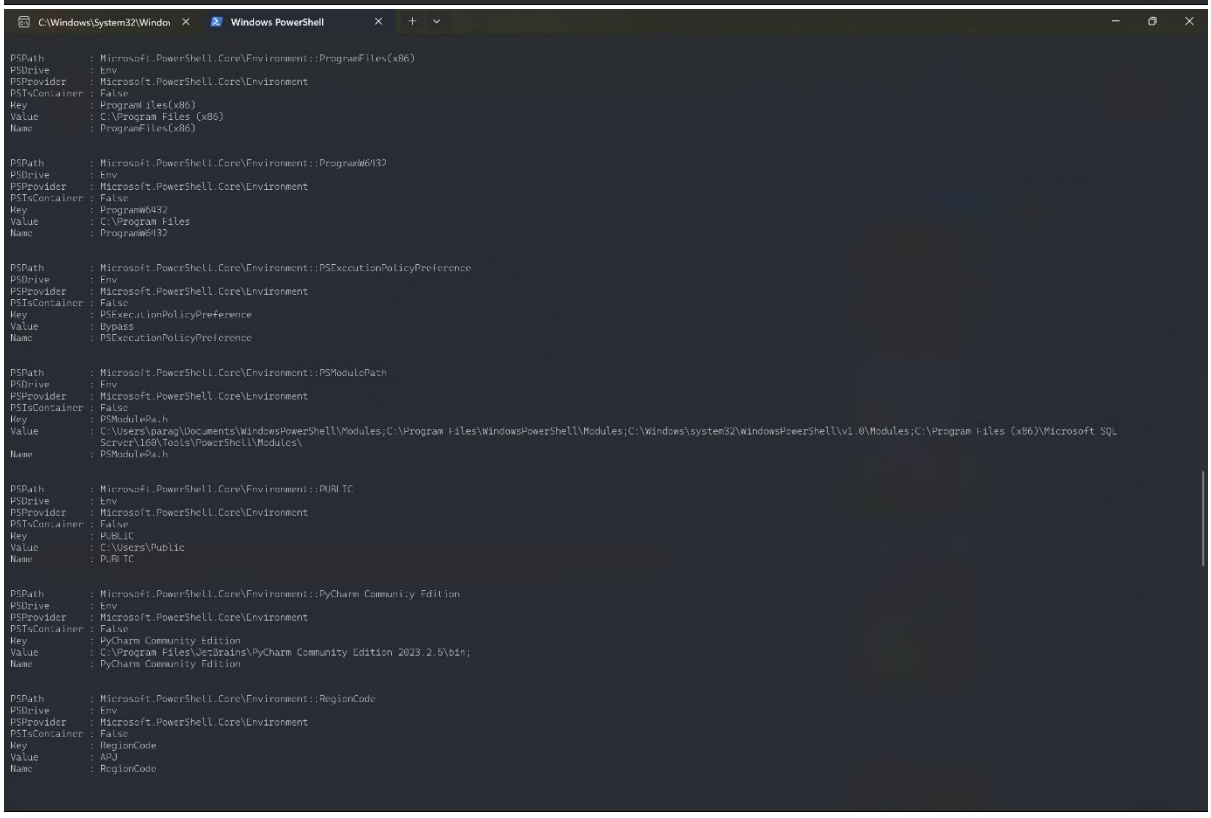

```
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : CommonProgramFiles(x86)
Value         : C:\Program Files (x86)\Common Files
Name          : CommonProgramFiles(x86)


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         : HACK3R
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::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\parag
Name          : HOMEPATH


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

- 


```
PSPath        : Microsoft.PowerShell.Core\Environment::LOGONSERVER
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : LOGONSERVER
Value         : \\HACK3R
Name          : LOGONSERVER


PSPath        : Microsoft.PowerShell.Core\Environment::NUMBER_OF_PROCESSORS
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : NUMBER_OF_PROCESSORS
Value         : 12
Name          : NUMBER_OF_PROCESSORS


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


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


PSPath        : Microsoft.PowerShell.Core\Environment::OnlineServices
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : OnlineServices
Value         : Online Services
Name          : OnlineServices


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
Key           : Path
Value         : C:\Program Files\Common Files\Oracle\Java\javapath;C:\Program Files\Python312\Scripts\;C:\Program
                Files\Python312\;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Program Files\Git\cmd;C:\adb;C:\Program
                Files (x86)\Microsoft SQL Server\160\Tools\Binn\;C:\Program Files\Microsoft SQL Server\160\Tools\Binn\;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\;C:\Program
                Files\Microsoft SQL Server\160\DTS\Binn\;C:\Users\parag\AppData\Local\Microsoft\WindowsApps;;C:\Program Files\JetBrains\PyCharm Community Edition 2023.2.5\bin;;C:\Program Files (x86)\Nmap
Name          : Path
```

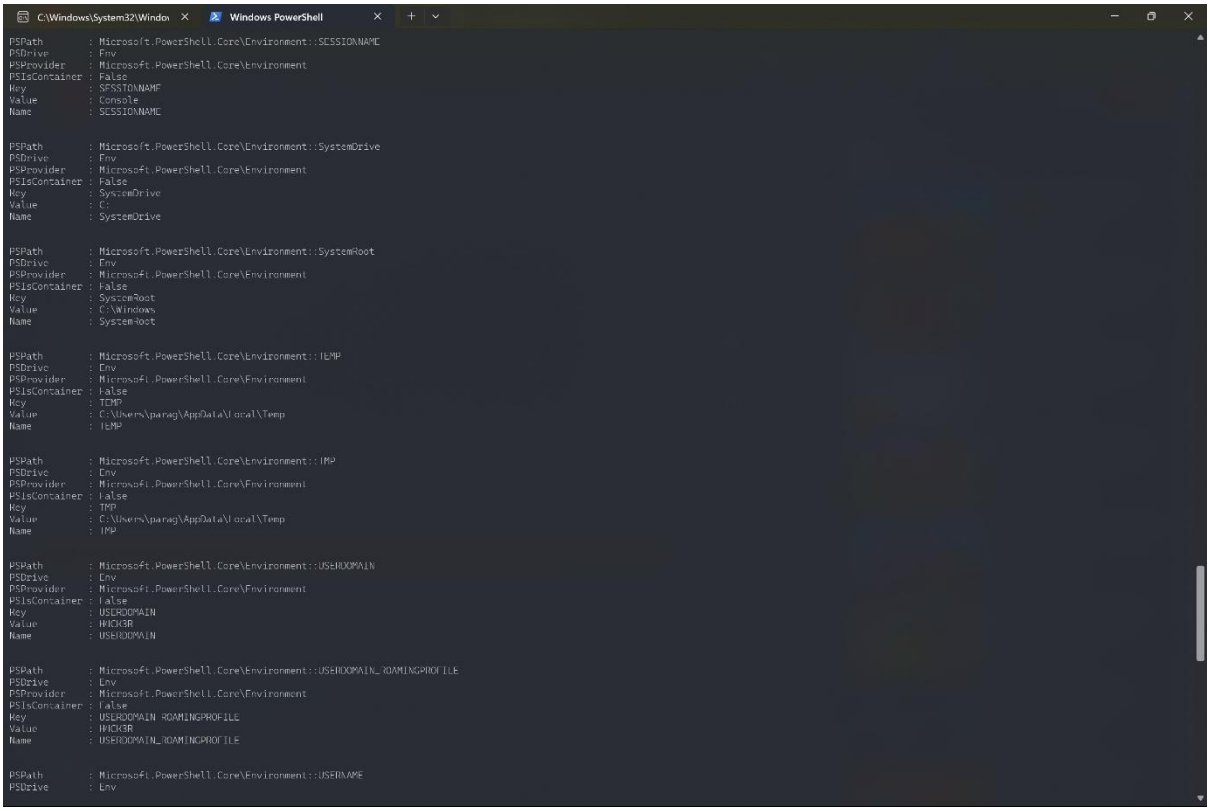
- 


```
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;.PY;.PYW;.CPL
Name          : PATHEXT


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


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 186 Stepping 3, 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         : ba03
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
```

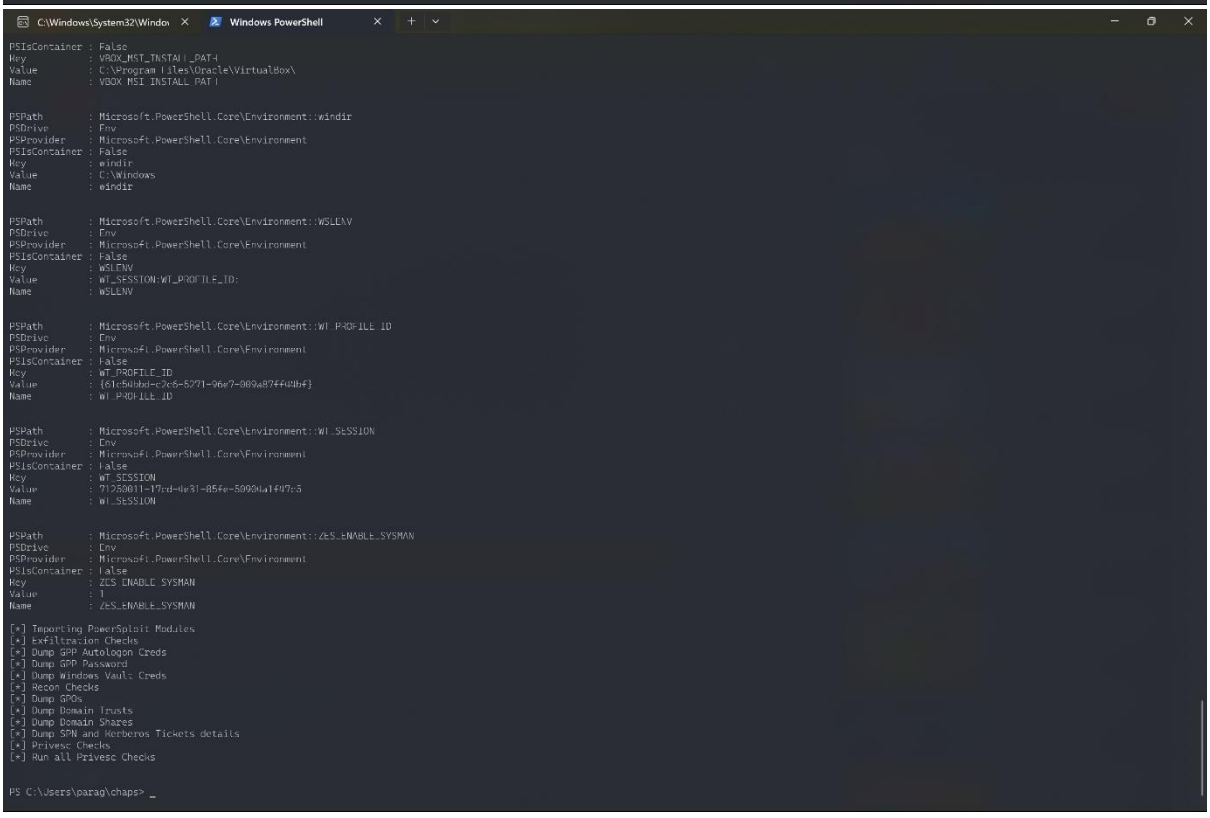
- 


```
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)


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::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\parag\Documents\WindowsPowerShell\Modules;C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules;C:\Program Files (x86)\Microsoft SQL
                Server\160\Tools\PowerShell\Modules\
Name          : PSModulePath


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 2023.2.5\bin;
Name          : PyCharm Community Edition


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

-

- 


```
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
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\parag\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\parag\AppData\Local\Temp
Name          : TMP


PSPath        : Microsoft.PowerShell.Core\Environment::USERDOMAIN
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : USERDOMAIN
Value         : HACK3R
Name          : USERDOMAIN


PSPath        : Microsoft.PowerShell.Core\Environment::USERDOMAIN_ROAMINGPROFILE
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : USERDOMAIN_ROAMINGPROFILE
Value         : HACK3R
Name          : USERDOMAIN_ROAMINGPROFILE


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

- 


```
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::WSLENV
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : WSLENV
Value         : WT_SESSION:WT_PROFILE_ID:
Name          : WSLENV


PSPath        : Microsoft.PowerShell.Core\Environment::WT_PROFILE_ID
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : WT_PROFILE_ID
Value         : {61c50bbd-c2c6-5271-96e7-009a87ff44bf}
Name          : WT_PROFILE_ID


PSPath        : Microsoft.PowerShell.Core\Environment::WT_SESSION
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : WT_SESSION
Value         : 71250011-17cd-4e31-85fe-5990a1f47c5
Name          : WT_SESSION


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\parag\chaps> _
```

Internship Assessment for h1k0r ceh Internships Week 1

Topic: CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS)

Instructions:

Read and understand the purpose of CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS).

Read and understand the PowerShell script provided.

Answer the following questions based on your understanding of CHAPS and the PowerShell script.

Assessment Questions:

1.What is CHAPS?

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

b. An antivirus software for Windows machines.

c. A tool for encrypting files on Windows machines.

d. A remote desktop access software for Windows machines.

2.What is the purpose of CHAPS?

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

b. To perform system backups on Windows machines.

c. To scan for and remove malware on Windows machines.

d. To remotely access and control Windows machines.

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

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

b. Internet connectivity settings, system update settings, and firewall settings.

c. Installed software settings, system configuration settings, and network share settings.

d. Disk encryption settings, user account settings, and virtual machine settings.

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

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

b. By running a full system scan for viruses and malware.

c. By checking the status of installed software and applications.

d. By analyzing network traffic and firewall logs.

5.What is the output of CHAPS?

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

b. A log file that lists all the files scanned and their status (infected/clean).

c. A list of installed software and their versions.

d. A list of all network devices connected to the Windows machine.

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

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

b. It can be used to remotely access and control Windows machines, making it easier for IT administrators to manage their systems.

c. It can help monitor and track the software usage on Windows machines.

d. It can be used to scan for and remove malware on Windows machines.

7.What are some limitations of CHAPS?

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

b. It can only be run on Windows machines running PowerShell version 5.1 or later.

c. It requires administrative privileges to run.

d. It may generate false positives or false negatives, depending on the system configuration.

8.What are some ways to improve CHAPS?

a. Add support for assessing security settings on Linux and macOS machines.

b. Add support for vulnerability scanning and penetration testing.

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

d. Provide an automated way to remediate security vulnerabilities found during the assessment.

9.What are some alternatives to CHAPS?

a. Microsoft Baseline Security Analyzer (MBSA)

b. Nessus Vulnerability Scanner

c. Open VAS

d. Qualys Guard Vulnerability Management