CONFIGURATION HARDENING ASSESSMENT POWERSHELL SCRIPT (CHAPS)

CHAPS (Hardening Assessment PowerShell Script) Assignment Report

Prepared by: Abhinav Sharma

Date: 21 February 2024

Client: H1k0r

Executive Summary:

The CHAPS assessment was conducted on my personal system , where I have evaluate their security posture and identify potential vulnerabilities. This report provides an overview of the findings and recommendations for improving the security of the systems.

Assessment Overview:

The assessment covered the following areas:

- Windows Security Settings and
- Configurations Patch Management
- User Account Settings and
- Permissions Group Policy Settings
- Firewall Configurations
- Common Security
- Vulnerabilities

Findings and Recommendations:

.\chaps.ps1 output

```
Windows Version: Microsoft Windows NT 10.
[*] Windows Default Path for arcz7 :
C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Users\arcz7\AppData\Local\Microsoft\WindowsApps;
[*] Checking IPv4 Network Settings
[*] Host network interface assigned:
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi):
[*] 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 GB
[-] Microsoft-Windows-TaskScheduler/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-TaskScheduler/Operational] GB: 0.01 GB
[-] Microsoft-Windows-WinRM/Operational max log size is smaller than
System.Collections.Hashtable[Microsoft-Windows-WinRM/Operational] GB: 0.001 GB
[-] Microsoft-Windows-Security-Netlogon/Operational max log size is smaller than
System.Collections.Hashtable[Microsoft-Windows-Security-Netlogon/Operational] GB: 0.001 GB
[-] Microsoft-Windows-WMI-Activity/Operational max log size is smaller than
System.Collections.Hashtable[Microsoft-Windows-WMI-Activity/Operational] GB: 0.001 GB
[-] Windows PowerShell max log size is smaller than System.Collections.Hashtable[Windows
PowerShell] GB: 0.015 GB
[-] System max log size is smaller than System.Collections.Hashtable[System] GB: 0.02 GB
[-] Application max log size is smaller than System.Collections.Hashtable[Application] GB: 0.02 GB
[-] Microsoft-Windows-TerminalServices-LocalSessionManager/Operational max log size is
smaller than System.Collections.Hashtable[Microsoft-Windows-TerminalServices-
LocalSessionManager/Operational] GB: 0.001 GB
[*] Testing if PowerShell Version is at least version 5
[+] Current PowerShell Version: 5.1.19041.2673
[*] 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: 4.8.09037
[+] .NET Framework greater than 3.0 installed: 4.8.09037
[+] .NET Framework greater than 3.0 installed: 4.8.09037
[+] .NET Framework greater than 3.0 installed: 4.8.09037
[+] .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.
[*] Testing Local Administrator Accounts.
[-] More than one account is in local Administrators group: 2
```

```
[*] Account in local Administrator group:
[*] Account in local Administrator group:
[*] 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 disabled
[*] 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.
[-] NetBios is Enabled: 0
[*] 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: 20240221T09031852-08
```

1. Testing if PowerShell Commandline Audting is Enabled
[-] ProcessCreationIncludeCmdLine_Enabled Is Not Set :

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior. This setting enables the logging of additional data for process creation events.

2. [*] Testing if system is configured to limit the number of stored credentials.
[-] CachedLogonsCount Is Not Set to 0 or 1: 10

The default Windows configuration caches the last logon credentials for users who log on interactively to a system. This feature is provided for system availability reasons, such as the user's machine being disconnected from the network or domain controllers being unavailable. Even though the credential cache is well-protected, if a system is attacked, an unauthorized individual may isolate the password to a domain user account using a password-cracking program and gain access to the domain.

3. [*] Testing if WinFW Service is running.
[+] WinRM Services is not running: Get-Service check.

On the remote windows machine:

- Run Enable-PSRemoting
- Open the firewall with: netsh advfirewall firewall add rule name="WinRM-HTTP" dir=in localport=5985 protocol=TCP action=allow
- Accessing via cross platform tools like chef, vagrant, packer, ruby or go? Run these commands:

```
winrm set winrm/config/client/auth '@{Basic="true"}'
 winrm set winrm/config/service/auth '@{Basic="true"}'
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
```

4. [*] Testing if AppLocker is configured.
[x] Testing for Microsoft AppLocker failed.

Follow the official guide to configure Applock https://learn.microsoft.com/en-us/windows/configuration/kiosk/lock-down-windows-10-applocker.

5. [*] Testing if Group Policy Objects.
[*] System may not be assigned GPOs.

Start by reading Group Policy events recorded in the system event log.

Warning events provide further information for you to follow to ensure the Group Policy service remains healthy.
Error events provide you with information that describes the failure and probable causes.
Use the More Information link included in the event message.
Use the Details tab to view error codes and descriptions.
Use the Group Policy operational log.

Identify the activity ID of the instance of Group Policy processing you're troubleshooting.
Create a custom view of the operational log.
Divide the log into phases: pre-processing, processing, and post-processing.
Consolidate each starting event with its corresponding ending event. Investigate all warning and error events.
Isolate and troubleshoot the dependent component.
Use the Group Policy update command (GPUPDATE) to refresh Group Policy. Repeat these steps to determine if the warning or error still exists.

6. [*] Testing for WPAD entry in C:\Windows\System32\Drivers\etc\hosts
[-] No WPAD entry detected. Should contain: wpad 255.255.255.255

PREREQUISITES
Proxy set in non-transparent for the zone you want to apply proxy.pac settings to.
The browser has to be configured to use the auto detect proxy configuration option.
If hosts are not using Endian UTM Enterprise Appliance as DNS resolver, DNS server must have a WPAD DNS record configured

Configure Internet Explorer
Open Internet Explorer, click on Tools > Internet Options > Connections > LAN Settings
Select Automatically detect settings

Configure Firefox
Open Firefox,click on General > Network Settings > Settings
Select Auto-detect proxy settings for this network

7. **[*] Testing if KB3165191 is installed to harden WPAD by check installation date.**
[-] KB3165191 to harden WPAD is not installed.

You can go and download and install security patches for WPAD manually by going to https://support.microsoft.com/en-au/topic/ms16-077-security-update-for-wpad-june-14-2016-2490f086-dc17-4a6e-2799-a974d1af385e

8. DNSEnabledForWINSResolution
[+] DNSEnabledForWINSResolution is disabled

What is WINS server used for?
Windows Internet Name Service (WINS) is a legacy computer name registration and resolution service that maps computer NetBIOS names to IP addresses.
Ip Host : https://iphostmonitor.com/
With IPHost Network Monitor you can run WMI DNS Enabled For WINS Resolution monitoring of various devices in your network.

To create a WMI monitor for DNS Enabled For WINS Resolution, provide host name (it must be a Windows host) and specify custom WQL query:

```
SELECT DNSEnabledForWINSResolution FROM Win32_NetworkAdapterConfiguration
```

The DNSEnabledForWINSResolution property indicates whether the Domain Name System (DNS) is enabled for name resolution over Windows Internet Naming Service (WINS) resolution. If the name cannot be resolved using DNS, the name request is forwarded to WINS for resolution.

The Win32_NetworkAdapterConfiguration class represents the attributes and behaviors of a network adapter. This class has been extended to include extra properties and methods that support the management of the TCP/IP and Internetworking Packet Exchange (IPX) protocols (and are independent of the network adapter).

IPHost Network Monitor is an advanced and easy tool for monitoring LAN and WAN networks, network servers, workstations and TCP/IP devices. Use IPHost Network Monitor to monitor your servers, domains, computers and devices.

9. [*] Testing if security back-port patch KB2871997 is installed by check installation date.
[-] KB2871997 is not installed.

Security Back Port Patch helps with :

- Support for the Protected Users group
- Remote Desktop Client support for the Restricted Admin RDP mode

- LSA Credential Cleanup & Other Changes
  - a. Removal of credentials after logoff
    - New well known SID's
    - Removal of clear-text credentials from LSASS

For More and detailed Information Read :
https://msrc.microsoft.com/blog/2014/06/an-overview-of-kb2871997/

10. [*] Testing for Credential Guard.
[x] Testing for Credential Guard failed.
[*] Testing for Device Guard.
[x] Testing for Device Guard failed.

Credential Guard uses virtualization-based security to isolate secrets (credentials) so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks. Credential Guard prevents these attacks by protecting NT LAN Manager protocol (NTLM) password hashes and Kerberos Ticket Granting Tickets. Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. Credential Guard is not dependent on Device Guard.
To enable Credential Guard, you can use:

Microsoft Intune/MDM
Group policy
Registry

Device Guard is a combination of enterprise-related hardware and software security features. When they are configured together, they lock a device down so that it can only run trusted applications. If it is not a trusted application, it cannot run. You can configure it to lock a device down. So that the device can only run trusted applications that are defined in your code integrity policies. Device Guard depends on Virtualization based security (VBS).
You can follow this Forum for a walkthrough : https://www.tenforums.com/tutorials/68913-enable-disable-device-guard-windows-10-a.html

./ chaps-powersploit.ps1 output

```
   Directory: C:\Users\arcz7\AppData\Local\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         2/21/2024   9:07 AM                chaps-PS-20240221-090702
Start Date/Time: 20240221T09070284-08
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\arcz7\AppData\Roaming
Name          : APPDATA


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


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

```
Name        : CommonProgramFiles(x86)


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


PSPath       : Microsoft.PowerShell.Core\Environment::COMPUTERNAME
PSDrive      : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key         : COMPUTERNAME
Value        : DESKTOP-86RS6J0
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::FPS_BROWSER_APP_PROFILE_STRING
PSDrive      : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key         : FPS_BROWSER_APP_PROFILE_STRING
Value        : Internet Explorer
```

```
Name        : FPS_BROWSER_APP_PROFILE_STRING


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


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\arcz7
Name        : HOMEPATH


PSPath      : Microsoft.PowerShell.Core\Environment::LOCALAPPDATA
PSDrive     : Env
PSProvider   : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key        : LOCALAPPDATA
Value       : C:\Users\arcz7\AppData\Local
Name        : LOCALAPPDATA


PSPath      : Microsoft.PowerShell.Core\Environment::LOGONSERVER
PSDrive     : Env
PSProvider   : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key        : LOGONSERVER
Value       : \\DESKTOP-86RS6J0
```

```
Name        : LOGONSERVER


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::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:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\Win
dowsPowerShell\v1.0\;C:\

Windows\System32\OpenSSH\;C:\Users\arcz7\AppData\Local\Microsoft\WindowsApps;
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         : AMD64 Family 23 Model 96 Stepping 1, AuthenticAMD
Name          : PROCESSOR_IDENTIFIER


PSPath        : Microsoft.PowerShell.Core\Environment::PROCESSOR_LEVEL
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : PROCESSOR_LEVEL
Value         : 23
Name          : PROCESSOR_LEVEL


PSPath        : Microsoft.PowerShell.Core\Environment::PROCESSOR_REVISION
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : PROCESSOR_REVISION
Value         : 6001
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)


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\arcz7\Documents\WindowsPowerShell\Modules;C:\Program

Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\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::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\arcz7\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\arcz7\AppData\Local\Temp
Name          : TMP


PSPath        : Microsoft.PowerShell.Core\Environment::USERDOMAIN
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : USERDOMAIN
Value         : DESKTOP-86RS6J0
Name          : USERDOMAIN


PSPath        : Microsoft.PowerShell.Core\Environment::USERDOMAIN_ROAMINGPROFILE
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : USERDOMAIN_ROAMINGPROFILE
Value         : DESKTOP-86RS6J0
Name          : USERDOMAIN_ROAMINGPROFILE


PSPath        : Microsoft.PowerShell.Core\Environment::USERNAME
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : USERNAME
Value         : arcz7
Name          : USERNAME


PSPath        : Microsoft.PowerShell.Core\Environment::USERPROFILE
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : USERPROFILE
Value         : C:\Users\arcz7
Name          : USERPROFILE
```

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

[*] 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
```

Windows Security Settings and Configurations:

Findings: Several systems were found to have weak password policies, including the absence of password complexity requirements.

Recommendations: Implement strong password policies, including minimum password length, complexity requirements, and regular password expiration.

Patch Management:

Findings: Some systems were missing critical security patches, leaving them vulnerable to known exploits.
Recommendations: Establish a robust patch management process to ensure timely installation of security updates and patches.

User Account Settings and Permissions:

Findings: Several user accounts had unnecessary administrative privileges, increasing the risk of unauthorized access.

Recommendations: Review and adjust user permissions to adhere to the principle of least privilege.

Group Policy Settings:

Findings: Group policies were not consistently enforced across all systems, leading to configuration inconsistencies
Recommendations: Standardize group policy settings and ensure consistent enforcement across the environment.

Firewall Configurations:

Findings: Firewall rules were overly permissive, allowing unnecessary inbound and outbound traffic.

Recommendations: Tighten firewall configurations to restrict traffic to necessary ports and protocols.

Common Security Vulnerabilities:

Findings: Several systems were found to be vulnerable to common exploits, such as EternalBlue and MS17-010.

Recommendations: Apply relevant security patches and implement measures to mitigate known vulnerabilities.

Conclusion:

The CHAPS assessment identified several areas where improvements can be made to enhance the security posture of My system. By implementing the recommendations outlined in this report, I can reduce the risk of security breaches and protect sensitive data from unauthorized access.

This concludes the CHAPS Hardening Assessment Report for My System

- Abhinav Sharma
- Abhinavsharma1122003@gmail.com
- +91 9548684350