Internship Assessment - Week 1

Configuration Hardening Assessment PowerShell Script (CHAPS)

Configuration Hardening Assessment PowerShell Script (CHAPS)

Introduction:

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

What is CHAPS?

CHAPS is a Power Shell script for checking system security settings where additional software and assessment tools, such as Microsoft Policy Analyzer, cannot be installed. The purpose of this script is to run it on a server or workstation to collect configuration information about that system. The information collected can then be used to provide recommendations (and references) to improve the security of the individual system and systemic issues within the organization's Windows environment.

Download link: https://github.com/cutaway-security/chaps

How to Run in windows?

Above the link using to download the CHAPS PowerShell script from the GitHub repository in Windows.

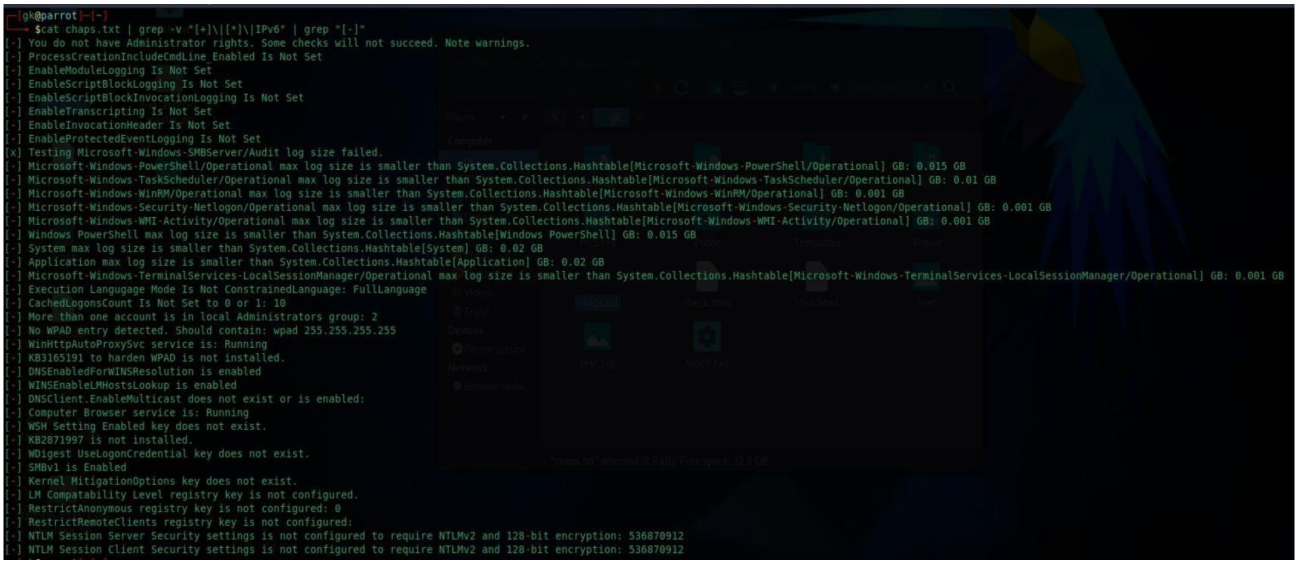
Using steps:

$ first open folder <**chaps-master**> then open <**cmd**>
$ **powershell.exe -exec bypass** - being a PowerShell prompt
$ **Set-ExecutionPolicy Bypass -scope Process** - allow scripts to execute
$ **./chaps.ps1** - run
$ **./chaps-powersploit.ps1** - run
$ output will be store in temp file
$ Search <Run> <%temp%> then you will be see temp folder its having two files.

Those are output

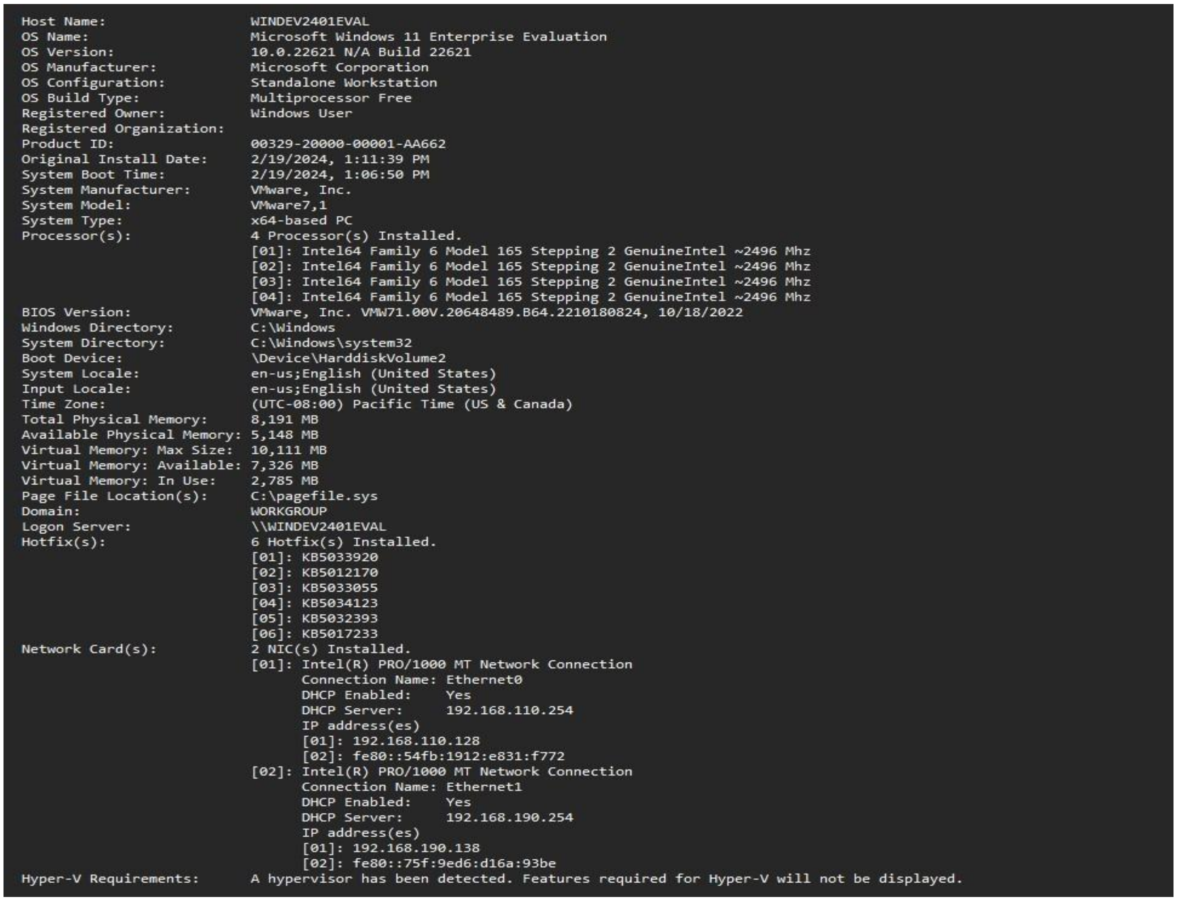
- chaps
- Sysinfo

Chaps output:



```
┌─[gk@parrot]─[~]
└──╼ $cat chaps.txt | grep -v "[+]\|[*]\|IPv6" | grep "[-]"
[-] You do not have Administrator rights. Some checks will not succeed. Note warnings.
[-] ProcessCreationIncludeCmdLine_Enabled Is Not Set
[-] EnableModuleLogging Is Not Set
[-] EnableScriptBlockLogging Is Not Set
[-] EnableScriptBlockInvocationLogging Is Not Set
[-] EnableTranscripting Is Not Set
[-] EnableInvocationHeader Is Not Set
[-] EnableProtectedEventLogging Is Not Set
[x] Testing Microsoft-Windows-SMBServer/Audit 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
[-] Execution Langugage Mode Is Not ConstrainedLanguage: FullLanguage
[-] CachedLogonsCount Is Not Set to 0 or 1: 10
[-] More than one account is in local Administrators group: 2
[-] No WPAD entry detected. Should contain: wpad 255.255.255.255
[-] WinHttpAutoProxySvc service is: Running
[-] KB3165191 to harden WPAD is not installed.
[-] DNSEnabledForWINSResolution is enabled
[-] WINSEnableLMHostsLookup is enabled
[-] DNSClient.EnableMulticast does not exist or is enabled:
[-] Computer Browser service is: Running
[-] WSH Setting Enabled key does not exist.
[-] KB2871997 is not installed.
[-] WDigest UseLogonCredential key does not exist.
[-] SMBv1 is Enabled
[-] Kernel MitigationOptions key does not exist.
[-] LM Compatability Level registry key is not configured.
[-] RestrictAnonymous registry key is not configured: 0
[-] RestrictRemoteClients registry key is not configured:
[-] NTLM Session Server Security settings is not configured to require NTLMv2 and 128-bit encryption: 536870912
[-] NTLM Session Client Security settings is not configured to require NTLMv2 and 128-bit encryption: 536870912
```

Sysinfo file output:



```
Host Name:                 WINDEV2401EVAL
OS Name:                   Microsoft Windows 11 Enterprise Evaluation
OS Version:                10.0.22621 N/A Build 22621
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00329-20000-00001-AA662
Original Install Date:     2/19/2024, 1:11:39 PM
System Boot Time:          2/19/2024, 1:06:50 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              4 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 165 Stepping 2 GenuineIntel ~2496 Mhz
                           [02]: Intel64 Family 6 Model 165 Stepping 2 GenuineIntel ~2496 Mhz
                           [03]: Intel64 Family 6 Model 165 Stepping 2 GenuineIntel ~2496 Mhz
                           [04]: Intel64 Family 6 Model 165 Stepping 2 GenuineIntel ~2496 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.20648489.B64.2210180824, 10/18/2022
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     8,191 MB
Available Physical Memory: 5,148 MB
Virtual Memory: Max Size:  10,111 MB
Virtual Memory: Available: 7,326 MB
Virtual Memory: In Use:    2,785 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\WINDEV2401EVAL
Hotfix(s):                 6 Hotfix(s) Installed.
                           [01]: KB5033920
                           [02]: KB5012170
                           [03]: KB5033055
                           [04]: KB5034123
                           [05]: KB5032393
                           [06]: KB5017233
Network Card(s):           2 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.110.254
                                 IP address(es)
                                 [01]: 192.168.110.128
                                 [02]: fe80::54fb:1912:e831:f772
                           [02]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Ethernet1
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.190.254
                                 IP address(es)
                                 [01]: 192.168.190.138
                                 [02]: fe80::75f:9ed6:d16a:93be
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

Report of Chaps:

```
 [-] You do not have Administrator rights. Some checks will not succeed. Note warnings.
 [-] ProcessCreationIncludeCmdLine_Enabled Is Not Set
 [-] EnableModuleLogging Is Not Set
 [-] EnableScriptBlockLogging Is Not Set
 [-] EnableScriptBlockInvocationLogging Is Not Set
 [-] EnableTranscripting Is Not Set
 [-] EnableInvocationHeader Is Not Set
 [-] EnableProtectedEventLogging Is Not Set
 [x] Testing Microsoft-Windows-SMBServer/Audit 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
 [-] Execution Langugage Mode Is Not ConstrainedLanguage: FullLanguage
 [-] CachedLogonsCount Is Not Set to 0 or 1: 10
 [-] More than one account is in local Administrators group: 2
 [-] No WPAD entry detected. Should contain: wpad 255.255.255.255
 [-] WinHttpAutoProxySvc service is: Running
 [-] KB3165191 to harden WPAD is not installed.
 [-] DNSEnabledForWINSResolution is enabled
 [-] WINSEnableLMHostsLookup is enabled
 [-] DNSClient.EnableMulticast does not exist or is enabled:
 [-] Computer Browser service is: Running
 [-] WSH Setting Enabled key does not exist.
 [-] KB2871997 is not installed.
 [-] WDigest UseLogonCredential key does not exist.
 [-] SMBv1 is Enabled
 [-] Kernel MitigationOptions key does not exist.
 [-] LM Compatability Level registry key is not configured.
 [-] RestrictAnonymous registry key is not configured: 0
 [-] RestrictRemoteClients registry key is not configured:
```

[-] NTLM Session Server Security settings is not configured to require NTLMv2 and 128-bit encryption: 536870912
[-] NTLM Session Client Security settings is not configured to require NTLMv2 and 128-bit encryption: 536870912

Recommendations for remediation :

- Implement strong password policies, including minimum password length, complexity requirements, and regular password expiration.
- Establish a robust patch management process to ensure timely installation of security updates and patches.
- Review and adjust user permissions to adhere to the principle of least Privilege
- Standardize policy settings and ensure consistent enforcement across the environment
- Apply relevant security patches and implement measures to mitigate known vulnerabilities.

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.

2. What is the purpose of CHAPS?
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?
a. Password policy settings, local security policy settings, and user rights assignments.

4. How does CHAPS assess the security settings of Windows machines?
a. By querying the Windows registry and security policy settings.

5. What is the output of CHAPS?
b. A log file that lists all the files scanned and their status (infected/clean).

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.

7. What are some limitations of CHAPS?
d. It may generate false positives or false negatives, depending on the system configuration.

8. What are some ways to improve CHAPS?
c. Improve the accuracy of the assessments to minimize false positives and false negatives.