CHAPS (Configuration Hardening Assessment PowerShell Script) Assignment Report

Prepared By- Ayush Mathur
Client: Microsoft windows

Executive Summary:

The CHAPS assessment was conducted on the systems belonging to Microsoft Windows Corporation to 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.

Introduction:

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 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. Examples of environments where this script is useful include Industrial Control System (ICS) environments where systems cannot be modified. These systems include Engineer / Operator workstations, Human Machine Interface (HMI) systems, and management servers that are deployed in production environments.

Assessment criteria:

How to use CHAPS -

- On the system open a CMD.exe window, preferably as an Administrator.
- Run the command - powershell.exe -exec bypass to being a PowerShell prompt
- Now run the Set-ExecutionPolicy Bypass -scope Process to allow scripts to execute.
- Now run the following command to execute the chaps.ps1 script.
- Now run the following command to execute the chaps-powersploit.ps1 script.
- Each script's outputs will be written to the user's Temp directory as defined by the $env:temp variable.

Windows Security Settings and Configurations and security patches

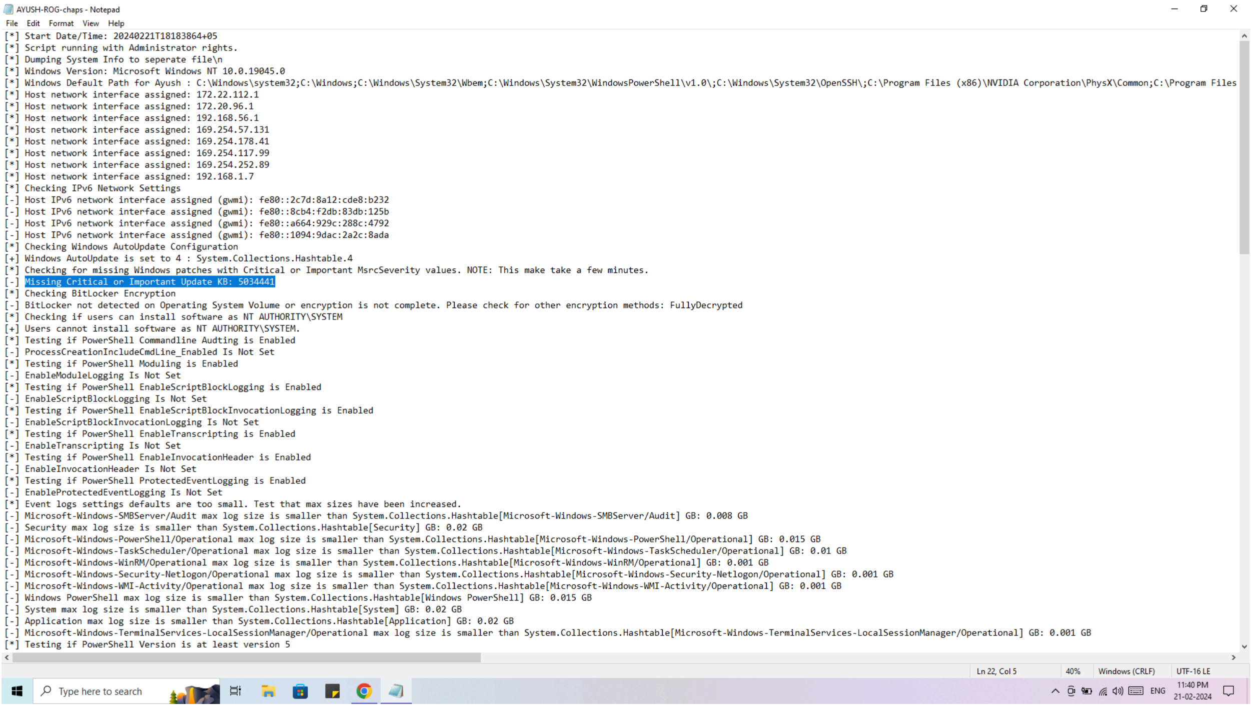
Some systems were missing critical security patches, leaving them vulnerable to known exploits.

- **Findings: Missing Critical or Important Update KB: 5034441**

This may allow attackers to bypass BitLocker encryption by using WinRE.

Recommandations:
Establish a robust patch management process to ensure timely installation of security updates and patches.

This update automatically applies Safe OS Dynamic Update (KB5034232) to the Windows Recovery Environment (WinRE) on a running PC to address a security vulnerability that could allow attackers to bypass BitLocker encryption by using WinRE.

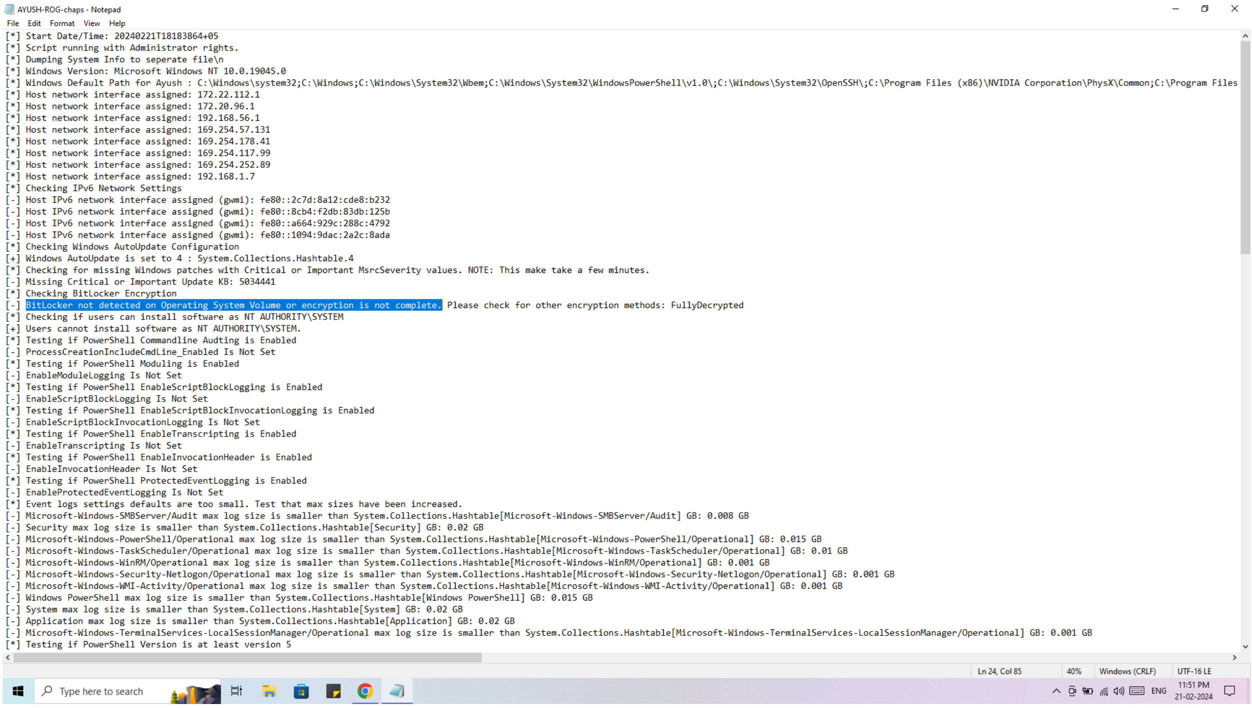


```
[*] Start Date/Time: 20240221T18183864+05
[*] Script running with Administrator rights.
[*] Dumping System Info to seperate file\n
[*] Windows Version: Microsoft Windows NT 10.0.19045.0
[*] Windows Default Path for Ayush : C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common;C:\Program Files
[*] Host network interface assigned: 172.22.112.1
[*] Host network interface assigned: 172.20.96.1
[*] Host network interface assigned: 192.168.56.1
[*] Host network interface assigned: 169.254.57.131
[*] Host network interface assigned: 169.254.178.41
[*] Host network interface assigned: 169.254.117.99
[*] Host network interface assigned: 169.254.252.89
[*] Host network interface assigned: 192.168.1.7
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi): fe80::2c7d:8a12:cde8:b232
[-] Host IPv6 network interface assigned (gwmi): fe80::8cb4:f2db:83db:125b
[-] Host IPv6 network interface assigned (gwmi): fe80::a664:929c:288c:4792
[-] Host IPv6 network interface assigned (gwmi): fe80::1094:9dac:2a2c:8ada
[*] 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.
[-] Missing Critical or Important Update KB: 5034441
[*] Checking BitLocker Encryption
[-] BitLocker not detected on Operating System Volume or encryption is not complete. Please check for other encryption methods: FullyDecrypted
[*] 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.
[-] Microsoft-Windows-SMBServer/Audit max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-SMBServer/Audit] GB: 0.008 GB
[-] Security max log size is smaller than System.Collections.Hashtable[Security] GB: 0.02 GB
[-] 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
```

- **BitLocker not detected on Operating System Volume or encryption is not complete.**

Recommandations:

1. **Start Registry Editor, and navigate to the following subkey: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE**
2. **Delete the following entries:**
   - **OSPlatformValidation_BIOS**
   - **OSPlatformValidation_UEFI**
   - **PlatformValidation**
3. **Exit registry editor, and turn on BitLocker drive encryption again.**



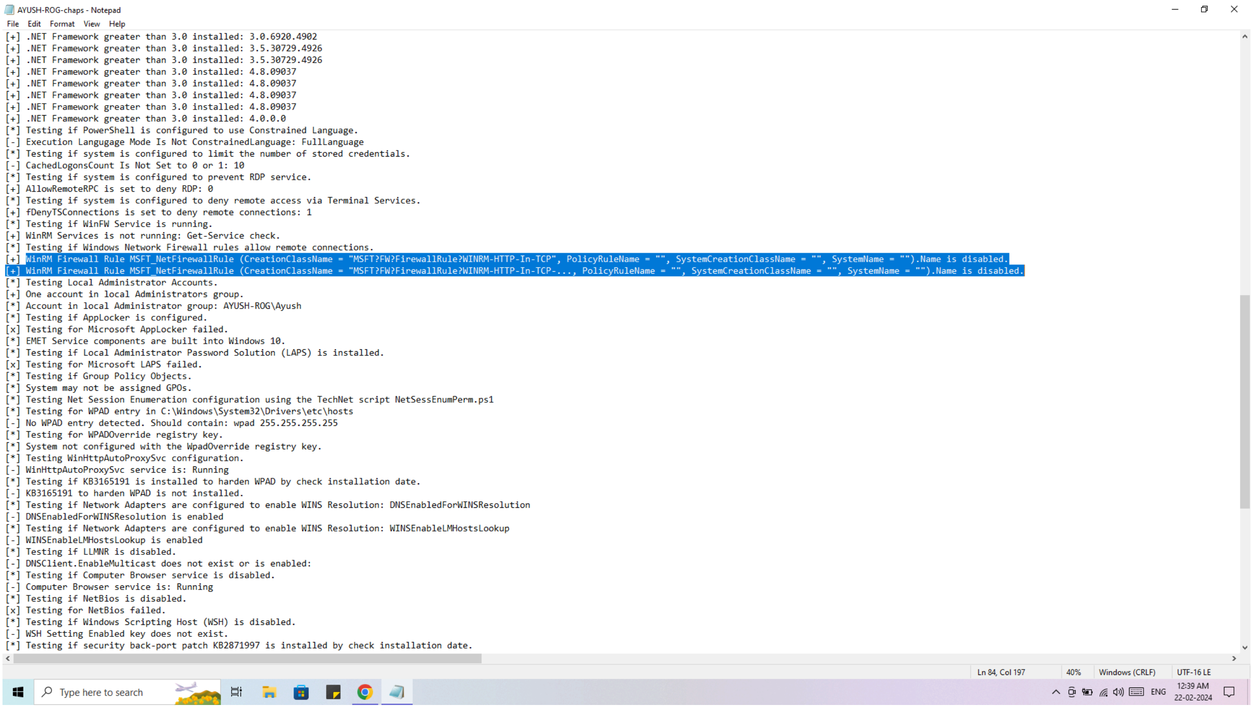
```
[*] Start Date/Time: 20240221T18183864+05
[*] Script running with Administrator rights.
[*] Dumping System Info to seperate file\n
[*] Windows Version: Microsoft Windows NT 10.0.19045.0
[*] Windows Default Path for Ayush : C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common;C:\Program Files
[*] Host network interface assigned: 172.22.112.1
[*] Host network interface assigned: 172.20.96.1
[*] Host network interface assigned: 192.168.56.1
[*] Host network interface assigned: 169.254.57.131
[*] Host network interface assigned: 169.254.178.41
[*] Host network interface assigned: 169.254.117.99
[*] Host network interface assigned: 169.254.252.89
[*] Host network interface assigned: 192.168.1.7
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi): fe80::2c7d:8a12:cde8:b232
[-] Host IPv6 network interface assigned (gwmi): fe80::8cb4:f2db:83db:125b
[-] Host IPv6 network interface assigned (gwmi): fe80::a664:929c:288c:4792
[-] Host IPv6 network interface assigned (gwmi): fe80::1094:9dac:2a2c:8ada
[*] 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.
[-] Missing Critical or Important Update KB: 5034441
[*] Checking BitLocker Encryption
[-] BitLocker not detected on Operating System Volume or encryption is not complete. Please check for other encryption methods: FullyDecrypted
[*] 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.
[-] Microsoft-Windows-SMBServer/Audit max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-SMBServer/Audit] GB: 0.008 GB
[-] Security max log size is smaller than System.Collections.Hashtable[Security] GB: 0.02 GB
[-] 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
```

Firewall Configuration

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

Findings: 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.



```
[+] .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.
[+] 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.
[+] One account in local Administrators group.
[*] Account in local Administrator group: AYUSH-ROG\Ayush
[*] Testing if AppLocker is configured.
[x] Testing for Microsoft AppLocker failed.
[*] EMET Service components are built into Windows 10.
[*] Testing if Local Administrator Password Solution (LAPS) is installed.
[x] Testing for Microsoft LAPS failed.
[*] Testing if Group Policy Objects.
[*] System may not be assigned GPOs.
[*] Testing Net Session Enumeration configuration using the TechNet script NetSessEnumPerm.ps1
[*] Testing for WPAD entry in C:\Windows\System32\Drivers\etc\hosts
[-] No WPAD entry detected. Should contain: wpad 255.255.255.255
[*] Testing for WPADOverride registry key.
[*] System not configured with the WpadOverride registry key.
[*] Testing WinHttpAutoProxySvc configuration.
[-] WinHttpAutoProxySvc service is: Running
[*] Testing if KB3165191 is installed to harden WPAD by check installation date.
[-] KB3165191 to harden WPAD is not installed.
[*] Testing if Network Adapters are configured to enable WINS Resolution: DNSEnabledForWINSResolution
[-] DNSEnabledForWINSResolution is enabled
[*] Testing if Network Adapters are configured to enable WINS Resolution: WINSEnableLMHostsLookup
[-] WINSEnableLMHostsLookup is enabled
[*] Testing if LLMNR is disabled.
[-] DNSClient.EnableMulticast does not exist or is enabled:
[*] Testing if Computer Browser service is disabled.
[-] Computer Browser service is: Running
[*] Testing if NetBios is disabled.
[x] Testing for NetBios failed.
[*] Testing if Windows Scripting Host (WSH) is disabled.
[-] WSH Setting Enabled key does not exist.
[*] Testing if security back-port patch KB2871997 is installed by check installation date.
```

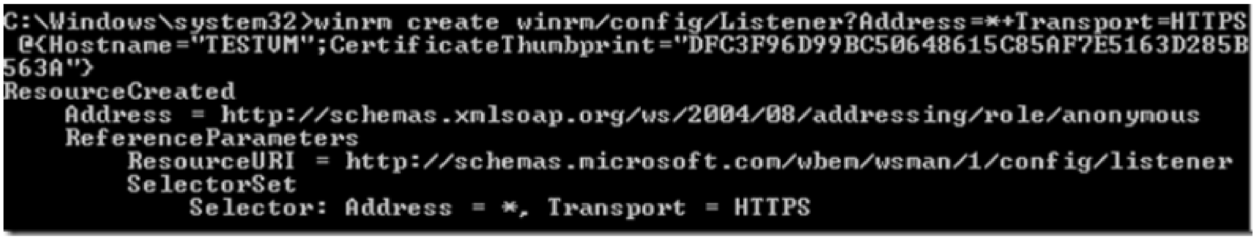
Recommandations: : Tighten firewall configurations to restrict traffic to necessary ports and protocols.

By default, WinRM over HTTP is configured to be listed on 5985. We need to enable it on 5986 and bind the certificate.

1. **pen a command prompt window as Administrator (not PowerShell)**
2. **Run the following command, pasting your new certificate's thumbprint into the command (all on one line):**

winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<your_server_dns_name_or_whatever_you_like>"; CertificateThumbprint="<certificate_thumbprint_from powershell>"}

You should get the following returned:



```
C:\Windows\system32>winrm create winrm/config/Listener?Address=*+Transport=HTTPS
 @{Hostname="TESTVM";CertificateThumbprint="DFC3F96D99BC50648615C85AF7E5163D285B
563A"}
ResourceCreated
    Address = http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
    ReferenceParameters
        ResourceURI = http://schemas.microsoft.com/wbem/wsman/1/config/listener
        SelectorSet
            Selector: Address = *, Transport = HTTPS
```

Common Security Vulnerabilities:

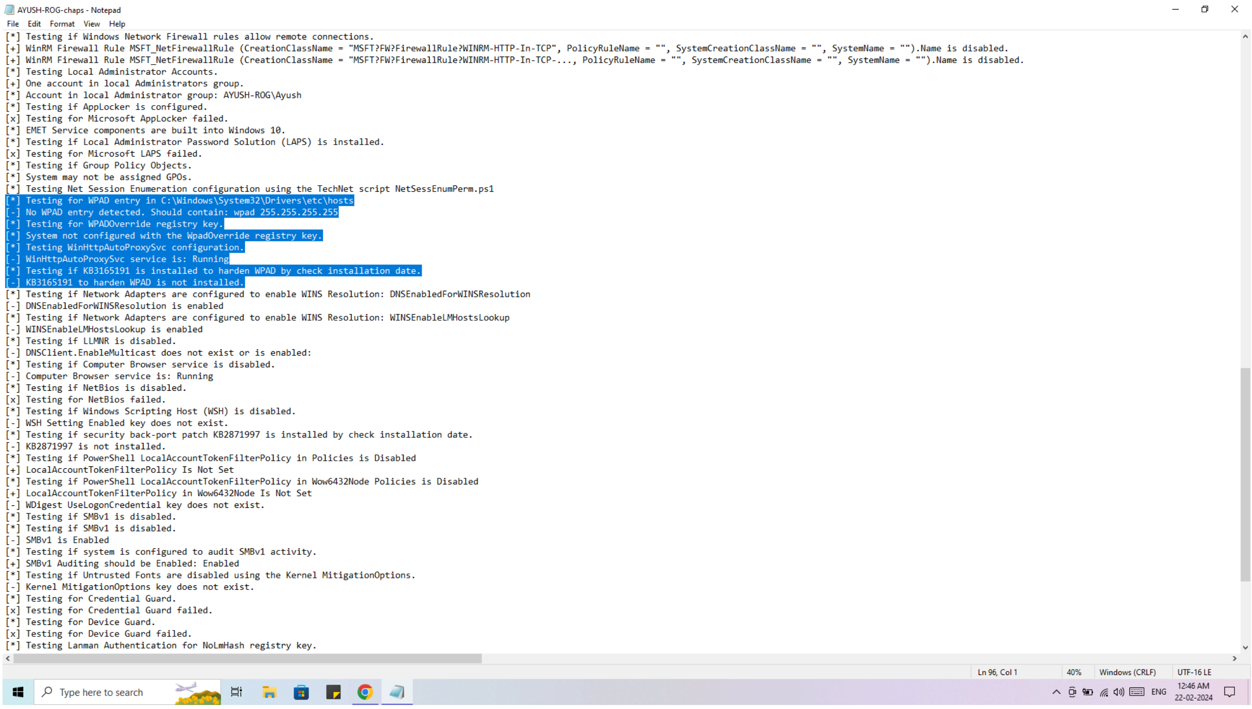
Several systems were found to be vulnerable to common exploits

No WPAD entry detected. Should contain: wpad 255.255.255.255

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow elevation of privilege if the Web Proxy Auto Discovery (WPAD) protocol falls back to a vulnerable proxy discovery process on a target system.

KB3165191 to harden WPAD is not installed.

The vulnerabilities could allow elevation of privilege if the Web Proxy Auto Discovery (WPAD) protocol falls back to a vulnerable proxy discovery process on a target system.



```
[*] 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.
[+] One account in local Administrators group.
[*] Account in local Administrator group: AYUSH-ROG\Ayush
[*] Testing if AppLocker is configured.
[x] Testing for Microsoft AppLocker failed.
[*] EMET Service components are built into Windows 10.
[*] Testing if Local Administrator Password Solution (LAPS) is installed.
[x] Testing for Microsoft LAPS failed.
[*] Testing if Group Policy Objects.
[*] System may not be assigned GPOs.
[*] Testing Net Session Enumeration configuration using the TechNet script NetSessEnumPerm.ps1
[*] Testing for WPAD entry in C:\Windows\System32\Drivers\etc\hosts
[-] No WPAD entry detected. Should contain: wpad 255.255.255.255
[*] Testing for WPADOverride registry key.
[*] System not configured with the WpadOverride registry key.
[*] Testing WinHttpAutoProxySvc configuration.
[-] WinHttpAutoProxySvc service is: Running
[*] Testing if KB3165191 is installed to harden WPAD by check installation date.
[-] KB3165191 to harden WPAD is not installed.
[*] Testing if Network Adapters are configured to enable WINS Resolution: DNSEnabledForWINSResolution
[-] DNSEnabledForWINSResolution is enabled
[*] Testing if Network Adapters are configured to enable WINS Resolution: WINSEnableLMHostsLookup
[-] WINSEnableLMHostsLookup is enabled
[*] Testing if LLMNR is disabled.
[-] DNSClient.EnableMulticast does not exist or is enabled:
[*] Testing if Computer Browser service is disabled.
[-] Computer Browser service is: Running
[*] Testing if NetBios is disabled.
[x] Testing for NetBios failed.
[*] Testing if Windows Scripting Host (WSH) is disabled.
[-] WSH Setting Enabled key does not exist.
[*] Testing if security back-port patch KB2871997 is installed by check installation date.
[-] KB2871997 is not installed.
[*] Testing if PowerShell LocalAccountTokenFilterPolicy in Policies is Disabled
[+] LocalAccountTokenFilterPolicy Is Not Set
[*] Testing if PowerShell LocalAccountTokenFilterPolicy in Wow6432Node Policies is Disabled
[+] LocalAccountTokenFilterPolicy in Wow6432Node Is Not Set
[-] 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.
```

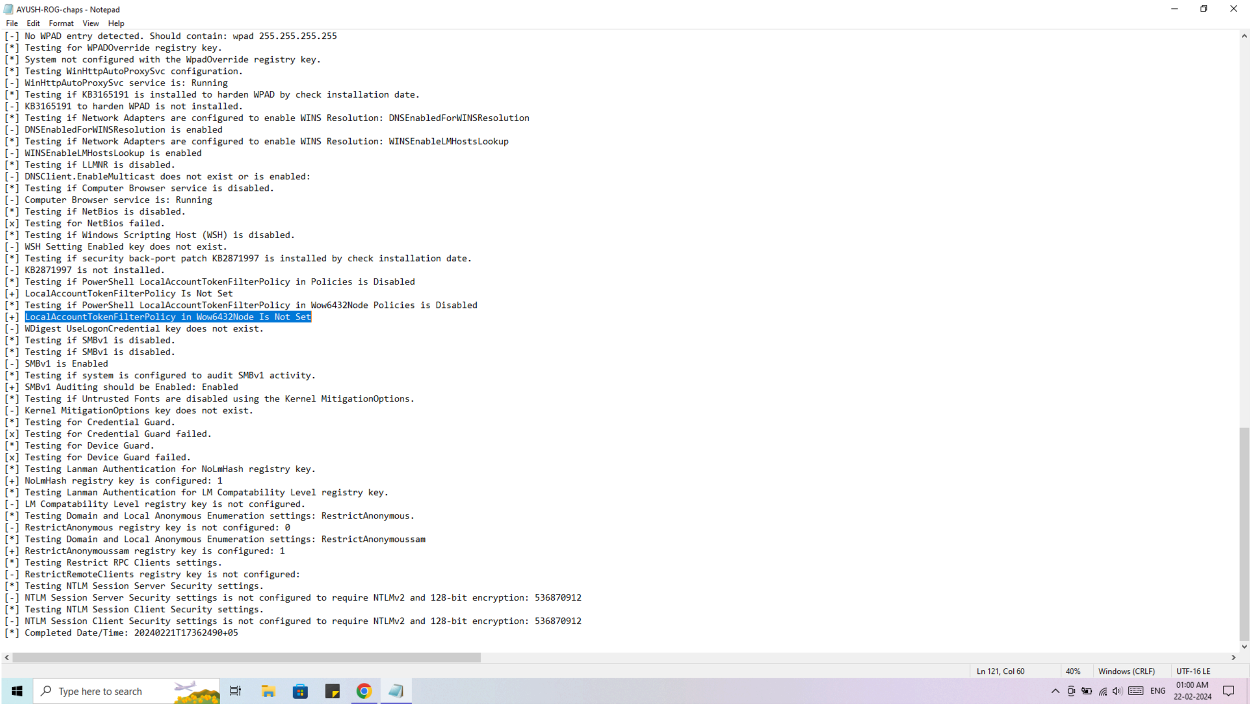
Recommendations: Apply relevant security patches and implement measures to mitigate known vulnerabilities

Group Policy Settings

Findings: Group policies were not consistently enforced across all systems, leading to configuration inconsistencies.

LocalAccountTokenFilterPolicy in Wow6432Node Is Not Set

The Wow6432 registry entry indicates that you're running a 64-bit version of Windows. The OS uses this key to present a separate view of HKEY_LOCAL_MACHINE\SOFTWARE for 32-bit applications that run on a 64-bit version of Windows. When a 32-bit application queries a value under the HKEY_LOCAL_MACHINE\SOFTWARE\<company>\<product> subkey, the application reads from the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\<company>\<product> subkey



```
[-] No WPAD entry detected. Should contain: wpad 255.255.255.255
[*] Testing for WPADOverride registry key.
[*] System not configured with the WpadOverride registry key.
[*] Testing WinHttpAutoProxySvc configuration.
[-] WinHttpAutoProxySvc service is: Running
[*] Testing if KB3165191 is installed to harden WPAD by check installation date.
[-] KB3165191 to harden WPAD is not installed.
[*] Testing if Network Adapters are configured to enable WINS Resolution: DNSEnabledForWINSResolution
[-] DNSEnabledForWINSResolution is enabled
[*] Testing if Network Adapters are configured to enable WINS Resolution: WINSEnableLMHostsLookup
[-] WINSEnableLMHostsLookup is enabled
[*] Testing if LLMNR is disabled.
[-] DNSClient.EnableMulticast does not exist or is enabled:
[*] Testing if Computer Browser service is disabled.
[-] Computer Browser service is: Running
[*] Testing if NetBios is disabled.
[x] Testing for NetBios failed.
[*] Testing if Windows Scripting Host (WSH) is disabled.
[-] WSH Setting Enabled key does not exist.
[*] Testing if security back-port patch KB2871997 is installed by check installation date.
[-] KB2871997 is not installed.
[*] Testing if PowerShell LocalAccountTokenFilterPolicy in Policies is Disabled
[+] LocalAccountTokenFilterPolicy Is Not Set
[*] Testing if PowerShell LocalAccountTokenFilterPolicy in Wow6432Node Policies is Disabled
[+] LocalAccountTokenFilterPolicy in Wow6432Node Is Not Set
[-] 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: 20240221T17362490+05
```

Recommendations: Standardize group policy settings and ensure consistent enforcement across the environment.

Conclusion:

The CHAPS assessment identified several areas where improvements can be made to enhance the security posture of Microsoft Windows Corporation's systems. By implementing the recommendations outlined in this report, Microsoft Corporation can reduce the risk of security breaches and protect sensitive data from unauthorized access. This concludes the CHAPS Hardening Assessment Report for Windows Corporation.

Assessment Questions

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.**

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.**

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.**

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.**

What is the output of CHAPS?

a. enaA report in CSV format that lists the security settings assessed and their status (bled/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.

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.

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.

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.

What are some alternatives to CHAPS?

a. **Microsoft Baseline Security Analyzer (MBSA)**
b. **Nessus Vulnerability Scanner**
c. **OpenVAS**
d. **Qualysguard Vulnerability Management**

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

It is useful for a PowerShell script for checking system security settings where additional software and assessment tools, such as Microsoft Policy Analyzer, cannot be installed. The purpose of this script is to run it on a server or workstation to collect configuration information about that system. The script does not make modifications to the system other than saving a file of the detected settings. This is particularly valuable for systems, such as master and support servers, in Industrial Control Systems (ICS) environments.