CHAPS (Hardening Assessment PowerShell Script) Assignment Report

Prepared by: [Odoyi Faith Chizubem]
Date: [22/02/24]
Client: Odoyi Chizubem PC

Executive Summary:

The CHAPS assessment was conducted on the systems belonging to Odoyi Faith 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.

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:

Windows Security Settings and Configurations:

Findings: No systems were found to have weak password policies, including the absence of password complexity requirements.

Recommendations: Implement more stronger 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.
As shown below

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

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

User Account Settings and Permissions:

Findings: only two accounts had administrative privileges, which does not increase the risk of unauthorized access.

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

Group Policy Settings:

Findings: There was no assigned group policy

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

Firewall Configurations:

Findings: Firewall rules does not allow for remote connection.

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

Common Security Vulnerabilities:

[*] Testing Lanman Authentication for LM Compatability Level registry key.
[-] LM Compatability Level registry key is not configured.

Findings: no systems were found to be vulnerable to common exploits, such as EternalBlue and MS17-010.

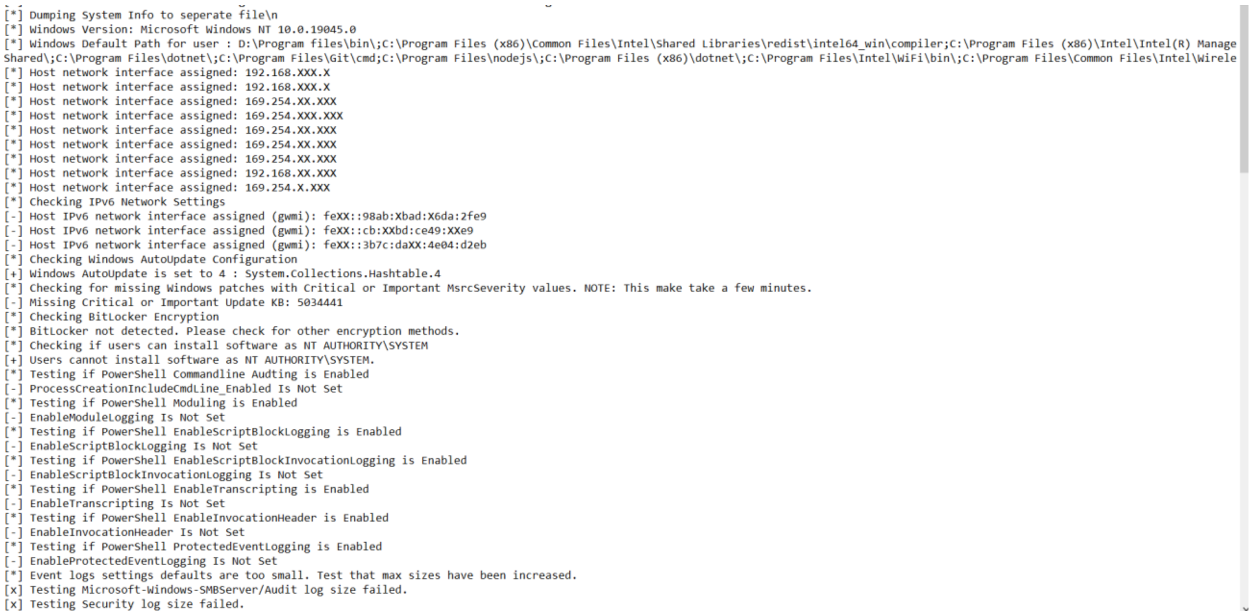
Recommendations: Apply relevant security patches and implement measures to mitigate known vulnerabilities.

Conclusion:

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

This concludes the CHAPS Hardening Assessment Report for Odoyi Faith PC.

Scan Results



```
[*] Dumping System Info to seperate file\n
[*] Windows Version: Microsoft Windows NT 10.0.19045.0
[*] Windows Default Path for user : D:\Program files\bin\;C:\Program Files (x86)\Common Files\Intel\Shared Libraries\redist\intel64_win\compiler;C:\Program Files (x86)\Intel\Intel(R) Manage
Shared\;C:\Program Files\dotnet\;C:\Program Files\Git\cmd;C:\Program Files\nodejs\;C:\Program Files (x86)\dotnet\;C:\Program Files\Intel\WiFi\bin\;C:\Program Files\Common Files\Intel\Wirele
[*] Host network interface assigned: 192.168.XXX.X
[*] Host network interface assigned: 192.168.XXX.X
[*] Host network interface assigned: 169.254.XX.XXX
[*] Host network interface assigned: 169.254.XXX.XXX
[*] Host network interface assigned: 169.254.XX.XXX
[*] Host network interface assigned: 169.254.XX.XXX
[*] Host network interface assigned: 169.254.XX.XXX
[*] Host network interface assigned: 192.168.XX.XXX
[*] Host network interface assigned: 169.254.X.XXX
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi): feXX::98ab:Xbad:X6da:2fe9
[-] Host IPv6 network interface assigned (gwmi): feXX::cb:XXbd:ce49:XXe9
[-] Host IPv6 network interface assigned (gwmi): feXX::3b7c:daXX:4e04:d2eb
[*] 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. 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.
```