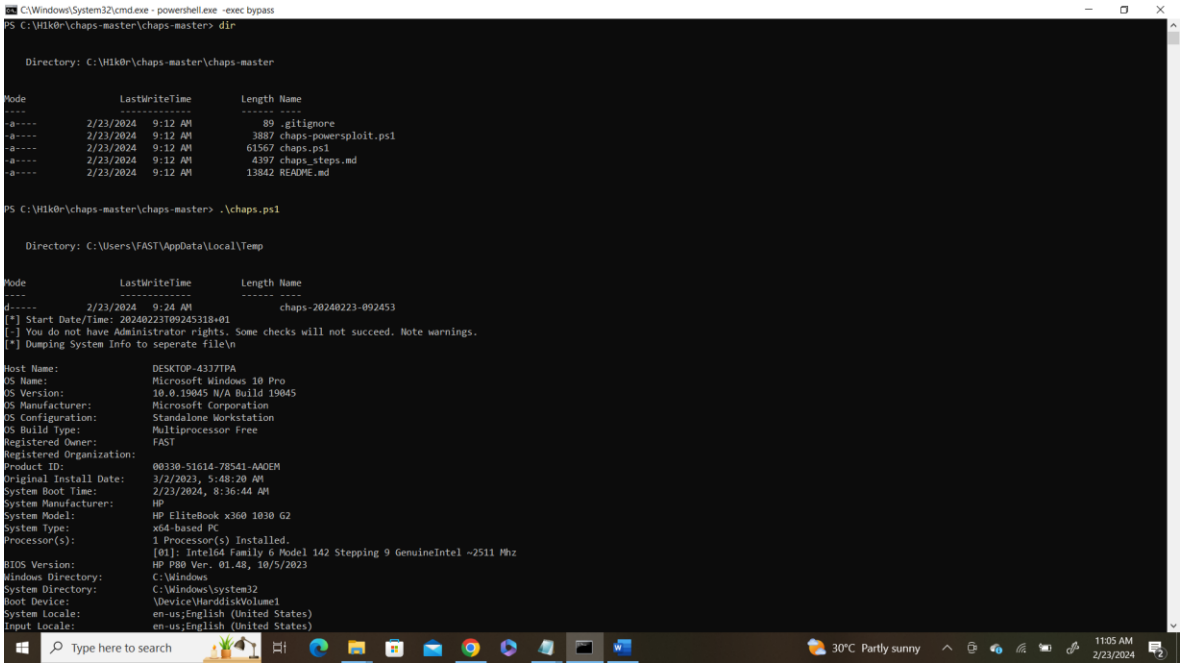
CHAPS (Hardening Assessment PowerShell Script) Assignment Report

Prepared by: [DAFE FRANK]



Date: [22/02/2024]

Client: FRANKIE'S TECHSTERS

Executive Summary:

The CHAPS assessment was conducted on the systems belonging to Frankie's Techsters to evaluatetheir 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:

The CHAPS Configuration Hardening Assessment PowerShell Script covered a wide range of areas related to Windows security configurations and settings. Here are the main areas that were assessed:

1. **Administrator Rights:**
   - Check if the script has elevated privileges for accurate assessments.

2. **Windows Version:**
   - Information about the installed Windows version.

3. **AutoUpdate Configuration:**
   - Windows AutoUpdate settings.

4. **Missing Windows Patches:**
   - Identification of missing critical or important updates.

5. **BitLocker Encryption:**
   - Detection of BitLocker encryption on the system.

6. **PowerShell Logging and Auditing:**
   - Testing various PowerShell logging and auditing settings.

7. **Event Log Sizes:**
   - Checking and recommending appropriate sizes for different event logs.

8. **PowerShell and .NET Framework Versions:**
   - Verification of PowerShell and .NET Framework versions.

9. **Cached Logons Count:**
   - Assessment of cached logons count.

10. **RDP and Remote Access:**
    - Configuration related to Remote Desktop Protocol (RDP) and remote access via Terminal Services.

11. **Local Administrator Accounts:**
    - Detection of local administrator accounts and recommendations.

12. **AppLocker and LAPS:**
    - Checking for the configuration of AppLocker and Local Administrator Password Solution

(LAPS).

13. **Group Policy Objects (GPOs):**
    - Determining if the system is assigned Group Policy Objects.

14. **Network Configuration:**
    - Assessment of IPv4 and IPv6 network settings.

15. **WPAD and Proxy Settings:**
    - Detection of Web Proxy Auto-Discovery (WPAD) settings.

16. **Firewall Settings:**
    - Evaluation of Windows Firewall rules.

17. **Various Security Configurations:**
    - Checks related to WinRM, NetBios, SMBv1, Windows Scripting Host, and more.

18. **Security Back-Port Patch KB2871997:**
    - Verification of the installation status of a specific security back-port patch.

19. **SMBv1 and Auditing:**
    - Assessment of SMBv1 settings and auditing.

20. **Credential Guard and Device Guard:**
    - Verification of the presence of Credential Guard and Device Guard.

21. **NTLM and Anonymous Enumeration:**
    - Testing settings related to NTLM and anonymous enumeration.

22. **Audit Logon Settings:**
    - Testing audit settings for logon activities.

These areas cover a broad spectrum of Windows security configurations and are essential for maintaining a secure system. Reviewing and addressing the recommendations in each of these areas can help enhance the overall security posture of the Windows environment.

Findings and Recommendations:

Based on the output of the CHAPS Configuration Hardening Assessment PowerShell Script, here are the findings and corresponding recommendations:

1. **Administrator Rights:**
   - **Finding:** The script does not have Administrator rights, leading to some checks not succeeding.

- **Recommendation:** Run the script with elevated privileges to ensure accurate assessments.

2. **AutoUpdate Configuration:**
   - **Finding:** Windows AutoUpdate is set to value "4".
   - **Recommendation:** Validate if this configuration aligns with the organization's update policy.

3. **Missing Windows Patches:**
   - **Finding:** The system is missing the critical or important update KB5034441.
   - **Recommendation:** Install the missing update to address potential vulnerabilities.

4. **BitLocker Encryption:**
   - **Finding:** BitLocker is not detected.
   - **Recommendation:** Consider implementing BitLocker or an equivalent encryption method for data protection.

5. **PowerShell Logging and Auditing:**
   - Various settings related to PowerShell logging are not configured.
   - **Recommendation:** Enable PowerShell logging and auditing to enhance security monitoring.

6. **Event Log Sizes:**
   - Several event logs have default or insufficient sizes.
   - **Recommendation:** Adjust event log sizes based on best practices to retain sufficient log data.

7. **PowerShell and .NET Framework Versions:**
   - **Finding:** PowerShell version is 5.1, and .NET Framework 4.8 is installed.
   - **Recommendation:** Keep PowerShell and .NET Framework up to date for security enhancements.

8. **Cached Logons Count:**
   - **Finding:** CachedLogonsCount is set to 10.
   - **Recommendation:** Set CachedLogonsCount to 0 or 1 for improved security.

9. **RDP and Remote Access:**
   - **Finding:** AllowRemoteRPC is set to deny RDP, and fDenyTSConnections is set to deny remote connections.
   - **Recommendation:** Verify if these settings align with security policies. Adjust as needed.

10. **Local Administrator Accounts:**
   - **Finding:** More than one account is in the local Administrators group.
   - **Recommendation:** Review and manage local administrator accounts to minimize security risks.

11. **AppLocker and LAPS:**
   - **Finding:** AppLocker is not configured, and Microsoft LAPS is not installed.
   - **Recommendation:** Consider implementing AppLocker and evaluate Microsoft LAPS for enhanced security.

12. **Group Policy Objects (GPOs):**
   - **Finding:** The system may not be assigned GPOs.
   - **Recommendation:** Verify and assign appropriate Group Policy Objects for consistent security settings.

13. **Network Configuration:**
   - **Finding:** Multiple network interfaces are assigned IP addresses.
   - **Recommendation:** Review and validate network configurations for correctness and security.

14. **WPAD and Proxy Settings:**
   - **Finding:** No WPAD entry detected.
   - **Recommendation:** Monitor and configure Web Proxy Auto-Discovery (WPAD) if necessary.

15. **Firewall Settings:**
   - **Finding:** Access is denied when checking firewall rules.
   - **Recommendation:** Resolve permission issues to ensure accurate firewall rule assessments.

16. **Various Security Configurations:**
   - Assessments related to WinRM, NetBios, SMBv1, Windows Scripting Host, and more.
   - **Recommendation:** Review and adjust configurations based on security best practices.

17. **Security Back-Port Patch KB2871997:**
   - **Finding:** KB2871997 is not installed.
   - **Recommendation:** Consider installing the security back-port patch for additional protection.

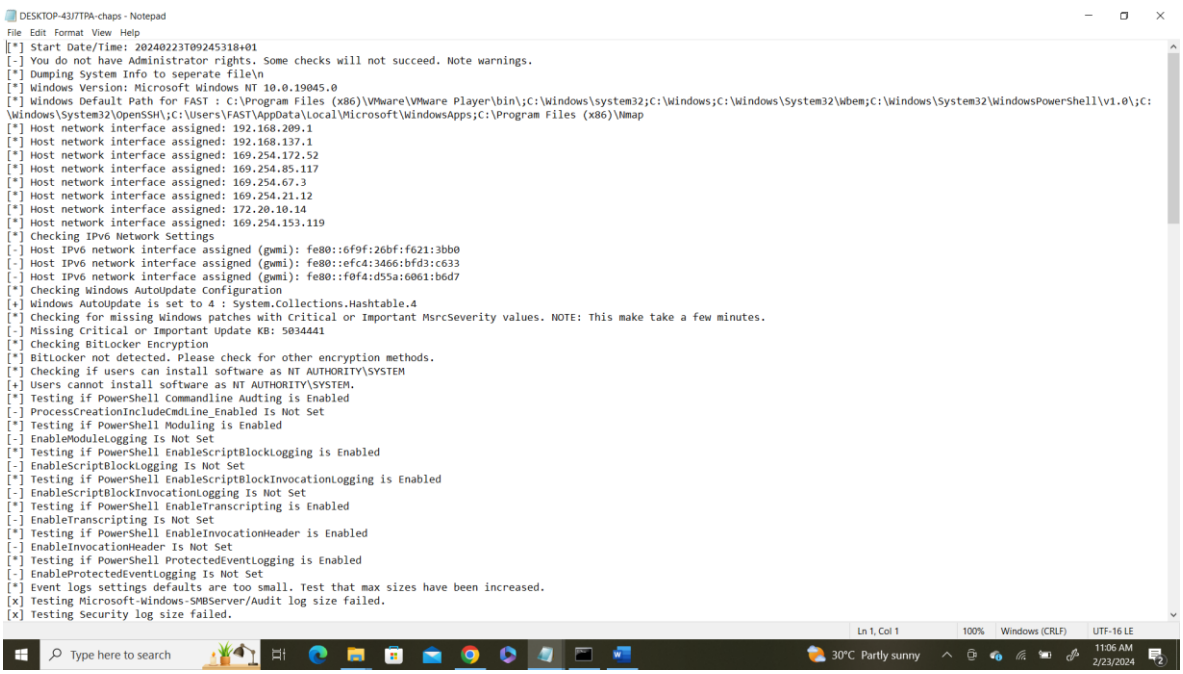
18. **SMBv1 and Auditing:**

- **Finding:** SMBv1 is enabled; SMBv1 Auditing should be enabled.
- **Recommendation:** Consider disabling SMBv1 and enabling auditing for enhanced security.

19. **Credential Guard and Device Guard:**
- **Finding:** Credential Guard and Device Guard are not detected.
- **Recommendation:** Evaluate and implement Credential Guard and Device Guard for advanced threat protection.

20. **NTLM and Anonymous Enumeration:**
- Assessments related to NTLM, anonymous enumeration, and audit logon settings.
- **Recommendation:** Configure settings to align with security best practices.

These findings and recommendations provide a comprehensive overview of potential security improvements for the Windows environment. It's crucial to assess each recommendation in the context of organizational policies and security requirements. Addressing these recommendations can contribute to a more robust and secure system configuration.



Conclusion:

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

This concludes the CHAPS Hardening Assessment Report for Frankie's Techsters.