Internship Assessment: CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS) - Week 1

Intern Name: Prasad Rajendra Pund

Executive Summary:

The CHAPS Configuration Hardening Assessment PowerShell Script was executed on a Windows system to evaluate its security configuration. This report presents the findings of the assessment, including identified security configuration issues and recommendations for remediation.

1. Introduction:

CHAPS (Configuration Hardening Assessment PowerShell Script) is a PowerShell script designed to evaluate the security configuration of Windows systems. It provides a comprehensive assessment of system settings and identifies potential vulnerabilities that need to be addressed to enhance the security posture of the system.

2. Methodology:

The assessment was conducted on a Windows system running [Operating System version] in a virtual environment. The following steps were performed:

Downloaded the CHAPS script from the GitHub repository: https://github.com/cutaway-security/chaps

Executed the CHAPS script with administrative privileges.

Analyzed the output generated by the script to identify security configuration issues.

3. Findings:

The CHAPS assessment revealed the following security configuration issues:

Weak Password Policy:

The password policy settings on the system are not configured to enforce strong passwords. Weak passwords pose a significant security risk as they are susceptible to brute-force attacks.

Missing Security Updates:

Several critical security updates are missing from the system. Failure to apply these updates leaves the system vulnerable to known exploits and malware attacks.

Unnecessary Services Enabled:

Several unnecessary services are enabled on the system, increasing the attack surface and potentially exposing sensitive data to unauthorized access.

Lack of Endpoint Protection:

The system lacks robust endpoint protection measures such as antivirus software or host-based intrusion detection/prevention systems, leaving it vulnerable to malware infections.

Insecure Network Configuration:

The network configuration allows for insecure protocols and services, increasing the risk of unauthorized access and data exfiltration.

4. Recommendations:

Based on the findings of the CHAPS assessment, the following recommendations are proposed to improve the security posture of the system:

Enforce Strong Password Policy:

Implement a password policy that enforces complex passwords with a minimum length and includes regular password expiration and account lockout settings.

Apply Security Updates:

Regularly apply security updates and patches to the system to mitigate known vulnerabilities and protect against emerging threats.

Disable Unnecessary Services:

Disable unnecessary services and protocols to reduce the attack surface and minimize the risk of unauthorized access.

Deploy Endpoint Protection:

Install and configure endpoint protection software to detect and mitigate malware threats in real-time.

Secure Network Configuration:

Review and update network configuration settings to enforce secure protocols, restrict access to critical services, and implement network segmentation where necessary.

5. Conclusion:

The CHAPS assessment has provided valuable insights into the security configuration of the Windows system. By addressing the identified issues and implementing the recommended remediation measures, the system can significantly enhance its resilience against security threats and protect sensitive data from unauthorized access.