CHAPS (Hardening Assessment PowerShell Script) Assignment Report

Prepared by: Anirban Banerjee

Date: 23.02.2024

Client: h1k0r

Executive Summary:

The CHAPS assessment was conducted on the systems belonging to h1k0r 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: Several systems were found to have weak password policies, including the absence of password complexity requirements.

Recommendations: Implement strong 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.

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

User Account Settings and Permissions:

Findings: Several user accounts had unnecessary administrative privileges, increasing the risk of unauthorized access.

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

Group Policy Settings:

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

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

Firewall Configurations:

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

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

Common Security Vulnerabilities:

Findings: Several 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 h1k0r's systems. By implementing the recommendations outlined in this report, h1k0r can reduce the risk of security breaches and protect sensitive data from unauthorized access.

Internship Assessment for h1k0r ceh Internships Week 1

Topic: CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS)

Assessment Answers:

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?

a. A report in CSV format that lists the security settings assessed and their status (enabled/disabled).

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?

a. It only assesses security settings related to configuration hardening and does not perform vulnerability scanning or penetration testing.

8. What are some ways to improve CHAPS?

a. Add support for assessing security settings on Linux and macOS machines.

9. What are some alternatives to CHAPS?

a. Microsoft Baseline Security Analyzer (MBSA)

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

In my opinion, CHAPS is extremely useful for assessing the configuration hardening of Windows machines. It provides an automated and systematic way to evaluate a system's security settings, making it easier to identify potential vulnerabilities and areas for improvement. By providing a detailed report of its findings, CHAPS enables IT

administrators to take informed actions to enhance their system's security posture. However, like any tool, it is most effective when used as part of a comprehensive security strategy that includes other measures such as regular software updates, user education, and robust access controls.