xTeam: Industrial Control Systems Security

NAME : DHILIPAN KUMAR P

Internship Assessment: week 1

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.

https://github.com/cutaway-security/chaps

Assignment

Title: Internship Assessment on CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS)

Objective:

The objective of this internship assessment is to evaluate the intern's understanding and proficiency in CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS) and its use in assessing the security configuration of Windows operating systems.

Task:

As an intern, your task for the first week of h1k0r ceh Internship is to perform a CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS) on a Windows system, analyze the results, and provide a report summarizing the findings.

Steps:

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

- Run the script on a Windows system, either physical or virtual, with administrator privileges.
    - Analyze the output of the script and identify the security configuration issues that need to be addressed.
- Provide a report summarizing the findings, including a brief explanation of the issues and recommendations for remediation.

DHILIPAN KUMAR P

- Submit the report to your internship supervisor for review and feedback.

Assessment criteria:

- Demonstration of understanding and proficiency in CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS).
- Accuracy and completeness of the security configuration issues identified.
- Clarity and conciseness of the report, including the recommendations for remediation.
- Ability to follow instructions and meet deadlines.
- Professionalism and communication skills in submitting the report and responding to feedback.

Submission instructions:

- The report should be submitted in a PDF format via email to your internship supervisor by the end of the first week of the internship.
- The subject line of the email should include "Internship Assessment: CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS) - Week 1".
- The body of the email should include your name and contact information.

Note:

The assessment is designed to evaluate your understanding and proficiency in CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS) and its use in assessing the security configuration of Windows operating systems. You are expected to complete the task independently and provide original work. Any form of plagiarism will not be tolerated and may result in disciplinary action. If you have any questions or concerns, please feel free to contact your internship supervisor.

DHILIPAN KUMAR P

Internship Assessment for h1k0r ceh Internships Week 1

Topic: CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS)

Instructions:

Read and understand the purpose of CHAPS Configuration Hardening Assessment PowerShell Script (CHAPS).

Read and understand the PowerShell script provided.

Answer the following questions based on your understanding of CHAPS and the PowerShell script.

Assessment Questions:

1. 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.

ANS : A

2. 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

ANS : A

3. 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.

ANS : A

4. How does CHAPS assess the security settings of Windows machines?

DHILIPANKUMAR P

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.

ANS : A

5. What is the output of CHAPS?
    a. A report in CSV format that lists the security settings assessed and their status (enabled/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.

ANS : B

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.
    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.

ANS : A

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.
    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.

ANS : A

8. 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.

ANS : A

DHILIPKUMAR P

9. What are some alternatives to CHAPS?

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

ANS : C

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

    IT's Information Gathering Tools

DHILIPAN KUMAR P