CST-321 Activity 7 Guide

Contents

Basic System Security

Overview

In this activity, students will work study security from IT, code, and administrative perspectives.

Execution

Execute this assignment according to the following guidelines:

1. Reading the following articles and answer the questions:
    a. Read the following article on inside security from CNET:
        i. The Biggest Cyberthreat to Companies Could Come from the Inside
        ii. How would user administration and access controls help solve this problem?
    b. Read the article on buffer overflows from OWASP:
        i. Buffer Overflow
        ii. What are some techniques and approaches to prevent buffer overflows?
    c. Read the documentation on Ubuntu Desktop User Administration:
        i. Go to the Ubuntu Desktop documentation home page.
        ii. Click on the User & System Settings link.
        iii. Click on the User Accounts link.
        iv. Review each of the sections in the documentation to understand how to add a new user, delete a user, change the password of a user, and control who has administrative privileges.

Applying Basic Security

Overview

In this activity, students will study security in log files and then how to harden a Linux Server.

Execution

Execute this assignment according to the following guidelines:

1. Reading the following tutorials:
    a. "Beginning Grep for Linux SysAdmins," from LiNux, for system administrators.
    b. "Linux Log Files Location And How Do I View Logs Files on Linux?" from nixCraft
    c. "Logging Cheat Sheet," from OWASP
    d. Reference the documentation on Ubuntu Desktop User Administration:
        i. Go to the Ubuntu Desktop documentation home page.
        ii. Click on the User & System Settings link.
        iii. Click on the User Accounts link.
        iv. Review each of the sections in the documentation to understand how to add a new user, delete a user, change the password of a user, and control who has administrative privileges.
2. Per guidance from your instructor, run the following commands in a Terminal:
    a. Create a new User with a password of your choosing in the default Group.
    b. Validate the new User by logging off and logging into the new Users account.
    c. Validate the new User's home directory.
    d. Validate the new User's groups (use the groups command).
    e. Log off and log back into your account.
    f. Add the new User to a Group 'TestMe' and validate (use the –force-badname option).
    g. Log off and log back into your account.
    h. Delete the new User and validate.
    i. Delete the new User's home directory and validate.
    j. Take a screenshot of the Terminal and Console window output.
    k. Write a theory of operation explaining how the commands worked.
3. Per guidance from your instructor, write a bash script to support the following capabilities:
    a. Write a bash script using GREP to detect the following scenario: Display all Users who have logged in during non-office hours (8:00AM to 5:00PM).
    b. Take a screenshot of the Terminal and Console window output.
    c. Write a theory of operation explaining how the script worked.
4. Research how you would approach hardening a Linux server.
    a. What are some areas and services that possibly need to be hardened?
    b. What configuration files would possibly need to be hardened?
    c. What Linux commands would you need to know to do this job?
    d. What other possible tools would you need to do this job?
    e. What additional training or resources would you need to do this job?

Working with OpenSSL

Overview

In this activity, students will work with the OpenSSL system in Linux.

Execution

Execute this assignment according to the following guidelines:

1. Reading the following tutorials on OpenSSL from madboa.com:
    a. Go to https://www.madboa.com/geek/openssl/.
    b. Read the following tutorials:
        i. Encryption/Decryption, Digests, and Password hashes
2. Per guidance from your instructor, run the following commands in a Terminal:
    a. Check the version of OpenSSL by running: openssl version.
    b. Create a text file named *test.txt* with any text as its contents.
    c. Encrypt this file using AES: openssl enc -aes-256-cbc -salt -in test.txt -out test.enc
    d. Encrypt this file using AES and Base64 Encode: Same as above but add –a option and use the output enc file as the input into the decrypt.
        i. Why you would Base64 encode a file?
    e. Decrypt both of the files (use the tutorial as guidance).
    f. Take a screenshot of the Terminal and Console window output.
    g. Write a theory of operation explaining how the commands worked.
    h. Create a Password by running: openssl passwd [Your Text Here].
    i. Take a screenshot of the Terminal and Console window output.
    j. Write a theory of operation explaining how the commands worked.
    k. Download an image file from the internet:
        i. The examples below are shown using pic1.png but you should substitute the name of the image file with your own filename.
    l. Create a MD5 Hash on the image file by running: openssl dgst -md5 pic1.png
    m. Create a MD5 Hash on the image file by running: md5sum pic1.png
        i. What is steganography?
        ii. How could an MD5 hash be used to prevent steganography?
    n. Take a screenshot of the Terminal and Console window output.

Working with Network Utilities

Overview

In this activity, students will work with the network utilities in Linux.

Execution

Execute this assignment according to the following guidelines:

1. Reading the following tutorials on networking:
    a. For *netstat* go to: http://www.binarytides.com/linux-netstat-command-examples/.

        i. Complete the hands-on tutorials 1 thru 9.
    b. For ifconfig, read http://www.tecmint.com/ifconfig-command-examples/.
        i. Complete the hands-on tutorials 1 thru 5 and 10.
2. Per guidance from your instructor, run the following commands in a Terminal:
    a. Install netstat network utility: sudo apt install net-tools
    b. Find your hostname of your computer by running: hostname
    c. List all network interfaces by running: ifconfig -a
    d. List all open connections by running: netstat -a
    e. List only TCP or UDP connections by running: netstat -at
    f. Check listening connections by running: netstat -tnl
    g. Get Connections with process name/pid and user id by running: sudo netstat -ltpe
    h. Print network interfaces by running: netstat -i
    i. Take a screenshot of the Terminal and Console window output.
    j. For each command write a theory of operation explain how the commands worked and what purpose they would have for securing or administrating a Linux system.

Ethical Hacking

Overview

In this activity, students will study security from an ethical hacking perspective.

Execution

Execute this assignment according to the following guidelines:

1. Reading the following articles and answer the questions:
    a. Read the tutorial "Ethical Hacking - Overview," from Tutorials Point.
    Pick some of the tutorials that are related to IT and software development.
        i. What are some types of hacking?
        ii. What tools are available?
        iii. What are some different attacks?
        iv. What other possible tools would you need to do this job?
        v. What additional training or resources would you need to do this job??
    b. Read the article "Trusted Computing Base," from Wikipedia.
        i. What is the trusted computing base?
        ii. Why is this important?

Research Questions

For traditional ground students, answer the following questions in a Microsoft Word document:

a. Research and analyze the various single-factor authentication schemes from Chapter 9 of your book. Identify 6 different authentication schemes that could be used to

access an operating system or application. In a table and write-up of at least 200 words, document your findings.

b. Research and analyze the various multi-factor authentication schemes that are in use today. Identify 3 different multi-factor authentication schemes that could be used to access an operating system or application. In a table and write-up of at least 200 words, document your findings.

Submission

1. In a Microsoft Word document, complete the following for the activity report:
    a. Cover sheet with your name, the name of this assignment, and the date.
    b. Section with a title that contains all theory of operation write-ups, answers to questions asked in the activity, and any screenshots taken during the activity.
    c. Section with a title that contains the answers to the Research Questions (traditional ground students only).

Submit the activity report to the digital classroom.

Appendix A – Sample Programs

The following can be used as guidance to program the C programs in the activity.

None available at present.