Final Capstone Activity

# Objectives

For this Final Capstone Activity, you will conduct a complete penetration test starting with reconnaissance and then launching exploits against vulnerabilities that you have discovered. Finally, you will propose remediation for the exploits.

This assessment is in the form of a cybersecurity capture the flag exercise. You will use your ethical hacking skills to locate files that contain flag values. You will then report the flag values that you found as part of the assessment.

In this simulation of an ethical hacking engagement, you will use tools to exploit vulnerabilities that you discover in order to reach a goal. This can entail a trial-and-error approach that requires persistence and may include a degree of struggle. For your own skill development, working through this struggle can be productive. If you are completely stuck, you can access the answers and solutions at any time during this assessment.

* **Challenge 1** – Use SQL injection to find a flag file.
* **Challenge 2** – Use web server vulnerabilities to investigate directories and find a flag file.
* **Challenge 3** – Exploit open Samba shares to access a flag file.
* **Challenge 4** – Analyze a Wireshark capture file to find the location of a file containing flag information.

# Background / Scenario

You have been hired to conduct a penetration test for a customer. At the conclusion of the test, the customer has requested a complete report that includes any vulnerabilities discovered, successful exploits, and remediation steps to protect vulnerable systems. You have access to hosts on the 10.6.6.0/24 and 172.17.0.0/24 networks.

# Required Resources

* Kali VM customized for the Ethical Hacker course

# Instructions

## SQL Injection

**Total points: 25**

In this part, you must discover user account information on a server and crack the password of **Gordon Brown's** account. You will then locate the file that contains the Challenge 1 code and use **Gordon Brown's** account credentials to open the file at 172.17.0.2 to view its contents.

### Preliminary setup

* + - 1. Open a browser and go to the website at 10.6.6.100.

**Note:** If you have problems reaching the website, remove the https:// prefix from the IP address in the browser address field.

* + - 1. Login with the credentials **admin / password**.
      2. Set the DVWA security level to **low** and click **Submit**.

### Retrieve the user credentials for the Gordon Brown's account.

* + - 1. Identify the table that contains usernames and passwords.
      2. Locate a vulnerable input form that will allow you to inject SQL commands.
      3. Retrieve the username and the password hash for **Gordon Brown's** account.

### Crack Gordon Brown's account password.

Use any password hash cracking tool desired to crack Gordon Brown’s password

#### Question

What is the password of **Gordon Brown's** account?

Type your answers here.

abc123

### Locate and open the file with Challenge 1 code.

* + - 1. Log into **172.17.0.2** as **Gordon Brown**.
      2. Locate and open the flag file in the user's home directory.

#### Question

What is the name of the file with the code?

Type your answers here.

The filename is hkxisx.txt.

What is the message contained in the file? Enter the code that you find in the file.

Type your answers here.

Congratulations!

You found the flag for Challenge 1!

The code for this challenge is 4E9f12.

### Research and propose SQL attack remediation.

#### Question

What are five remediation methods for preventing SQL injection exploits?

Type your answers here.

Answers may vary but include:

1. using parameterized queries (prepared statements)

2. input checking

3. field validation

4. filtering user inputs

5. escaping user input

## Web Server Vulnerabilities

**Total points: 25**

In this part, you must find vulnerabilities on an HTTP server. Misconfiguration of a web server can allow for the listing of files contained in directories on the server. You can use any of the tools you learned in earlier labs to perform reconnaissance to find the vulnerable directories.

In this challenge, you will locate the flag file in a vulnerable directory on a web server.

### Preliminary setup

1. If not already, log into the server at 10.6.6.100 with the **admin / password** credentials.
2. Set the application security level to low.

### From the results of your reconnaissance, determine which directories are viewable using a web browser and URL manipulation.

Perform reconnaissance on the server to find directories where indexing was found.

#### Question

Which directories can be accessed through a web browser to list the files and subdirectories that they contain?

Type your answers here.

/config/ and /docs/

### View the files contained in each directory to find the file containing the flag.

Create a URL in the web browser to access the viewable subdirectories. Find the file with the code for Challenge 2 located in one of the subdirectories.

#### Questions

In which two subdirectories can you look for the file?

Type your answers here.

/config/ and /docs/

What is the filename with the Challenge 2 code?

Type your answers here.

user\_form.html

Which subdirectory held the file?

Type your answers here.

/docs

What is the message contained in the flag file? Enter the code that you find in the file.

Type your answers here.

Great work!

You found the flag file for Challenge 2!

The code for tis flag is 18xf9-4z

### Research and propose directory listing exploit remediation.

#### Question:

What are two remediation methods for preventing directory listing exploits?

Type your answers here.

Answers may vary but include: Configure your web server to prevent directory listings for all paths beneath the web root. Place into each directory a default file (such as index.htm) that the web server will display instead of returning a directory listing.

## Exploit open SMB Server Shares

**Total points: 25**

In this part, you want to discover if there are any unsecured shared directories located on an SMB server in the 10.6.6.0/24 network. You can use any of the tools you learned in earlier labs to find the drive shares available on the servers.

### Scan for potential targets running SMB.

Use scanning tools to scan the 10.6.6.0/24 LAN for potential targets for SMB enumeration.

#### Question

Which host on the 10.6.6.0/24 network has open ports indicating it is likely running SMB services?

Type your answers here.

10.6.6.23 because ports 139 and 445 are open.

### Determine which SMB directories are shared and can be accessed by anonymous users.

Use a tool to scan the device that is running SMB and locate the shares that can be accessed by anonymous users.

#### Question

What shares are listed on the SMB server? Which ones are accessible without a valid user login?

Type your answers here.

homes, workfiles, print$. workfiles and print$ are accessible by anonymous users.

### Investigate each shared directory to find the file.

Use the SMB-native client to access the drive shares on the SMB server. Use the dir, ls, cd, and other commands to find subdirectories and files.

Locate the file with the Challenge 3 code. Download the file and open it locally.

#### Questions

In which share is the file found?

Type your answers here.

print$

What is the name of the file with Challenge 3 code?

Type your answers here.

OTHER/taxes.txt

Enter the code for Challenge 3 below.

Type your answers here.

A9!15wa2

### Research and propose SMB attack remediation.

#### Question

What are two remediation methods for preventing SMB servers from being accessed?

Type your answers here.

Answers may vary but include: Keeping the SMB server OSs up-to-date and patched, use strong authentication, restrict access, enable SMB signing, firewall SMB/Microsoft ports to internal hosts only. Do not allow anonymous login to SMB shares.

## Analyze a PCAP File to Find Information.

**Total Points**: **25**

As part of your reconnaissance effort, your team captured traffic using Wireshark. The capture file, **SA.pcap,** is located in the **OTHER** subdirectory within the **kali** user home directory.

### Find and analyze the SA.pcap file.

Analyze the content of the PCAP file to determine the IP address of the target computer and the URL location of the file with the Challenge 4 code.

#### Question

What is the IP address of the target computer?

Type your answers here.

10.6.6.14

What directories on the target are revealed in the PCAP?

Type your answers here.

Answers may vary. The directories can include: /data, /styles, /passwords, /icons.txt.

### Use a web browser to display the contents of the directories on the target computer.

Use a web browser to investigate the URLs listed in the Wireshark output. Find the file with the code for Challenge 4.

#### Questions

What is the URL of the file?

Type your answers here.

http://10.6.6.14/data/accounts.xml

What is the content of the file?

Type your answers here.

Usernames, accounts and passwords

What is the code for Challenge 4?

Type your answers here.

zz90014x

### Research and propose remediation that would prevent file content from being transmitted in clear text.

Further examine the capture file. The contents of the files are transmitted in clear text and can be viewed in Wireshark.

#### Question

What are two remediation methods that can prevent unauthorized persons from viewing the content of the files?

Type your answers here.

Encrypt files, use a VPN or SSL to send files, don’t store account or other sensitive information in web-accessible locations.

Congratulations! You have completed the skills assessment.