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.

Instructions

Challenge 1: 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.

Step 1: Preliminary setup

a. 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.

b. Login with the credentials **admin / password**.
c. Set the DVWA security level to **low** and click **Submit**.

Step 2: Retrieve the user credentials for the Gordon Brown's account.

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

Step 3: Crack Gordon Brown's account password.

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

What is the password of Gordon Brown's account?

Answer Area

<!----><!---->

Step 4: Locate and open the file with Challenge 1 code.

a. Log into **172.17.0.2** as **Gordon Brown**.
b. Locate and open the flag file in the user's home directory.
What is the name of the file with the code?

Answer Area

<!----><!---->

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

Answer Area

<!----><!---->

Step 5: Research and propose SQL attack remediation.

What are five remediation methods for preventing SQL injection exploits?

Answer Area

<!----><!---->

Challenge 2: 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.

Step 1: Preliminary setup

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

Step 2: 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.

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

Answer Area

<!----><!---->

Step 3: 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.

In which two subdirectories can you look for the file?

Answer Area

<!----><!---->

What is the filename with the Challenge 2 code?

Answer Area

<!----><!---->

Which subdirectory held the file?

Answer Area

<!----><!---->

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

Answer Area

<!----><!---->

Step 4: Research and propose directory listing exploit remediation.

What are two remediation methods for preventing directory listing exploits?

Answer Area

<!----><!---->

Challenge 3: 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.

Step 1: Scan for potential targets running SMB.

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

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

Answer Area

<!----><!---->

Step 2: 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.

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

Answer Area

<!----><!---->

Step 3: 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.

In which share is the file found?

Answer Area

<!----><!---->

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

Answer Area

<!----><!---->

Enter the code for Challenge 3 below.

Answer Area

<!----><!---->

Step 4: Research and propose SMB attack remediation.

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

Answer Area

<!----><!---->

Challenge 4: 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.

Step 1: 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.

What is the IP address of the target computer?

Answer Area

<!----><!---->

What directories on the target are revealed in the PCAP?

Answer Area

<!----><!---->

Step 2: 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.

What is the URL of the file?

Answer Area

<!----><!---->

What is the content of the file?

Answer Area

<!----><!---->

What is the code for Challenge 4?

Answer Area

<!----><!---->

Step 3: Research and propose remediation that would prevent file content from being transmitted in clear text.

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

Answer Area

<!----><!---->

Congratulations! You have completed the skills assessment.

Answer Key