

Internship Final Report

Student Name: Ratnesh Raj Dwivedi

University: ITM University

Major: Computer Science

Internship Duration: April 10th, 2025 - May 3rd, 2025

Company: Hack Secure Domain: Cyber Security Mentor: Mr.Nishant Prajapati

Assistant Mentor: Mr. Aman Pandey

Coordinator: Mr. Shivam Kapoor

Objectives

My primary objectives for this internship were to:

- Develop a deep understanding of cybersecurity principles and practices.
- Gain hands-on experience in identifying, analyzing, and mitigating security threats.
- Enhance my skills in using cybersecurity tools and techniques in real-world scenarios.

Tasks and Responsibilities

During my internship, I was involved in the following key tasks:

- **Vulnerability Assessment:** Conducted a thorough scan of a target website to identify open ports and potential vulnerabilities.
- **Penetration Testing:** Performed brute-force attacks and directory enumeration on the website to uncover hidden directories and files.
- **Traffic Analysis:** Intercepted network traffic using Wireshark during a simulated login attempt, successfully capturing and analyzing transmitted credentials.
- **Decryption and Cryptanalysis:** Decrypted password-protected files using cryptographic tools and analyzed encoded hash values to recover plaintext passwords.
- **Reverse Engineering:** Used PE Explorer to analyze an executable file, identifying the entry point and other critical information.

- **Network Security:** Executed a de-authentication attack on a controlled network environment, capturing the handshake and subsequently cracking the Wi-Fi password using a custom wordlist.
- **Payload Creation:** Developed and deployed a Metasploit payload to establish a reverse shell connection on a virtual machine.

Beginner Level

TASK 1

Objective

Find all the ports that are open on the website <http://testphp.vulnweb.com/>

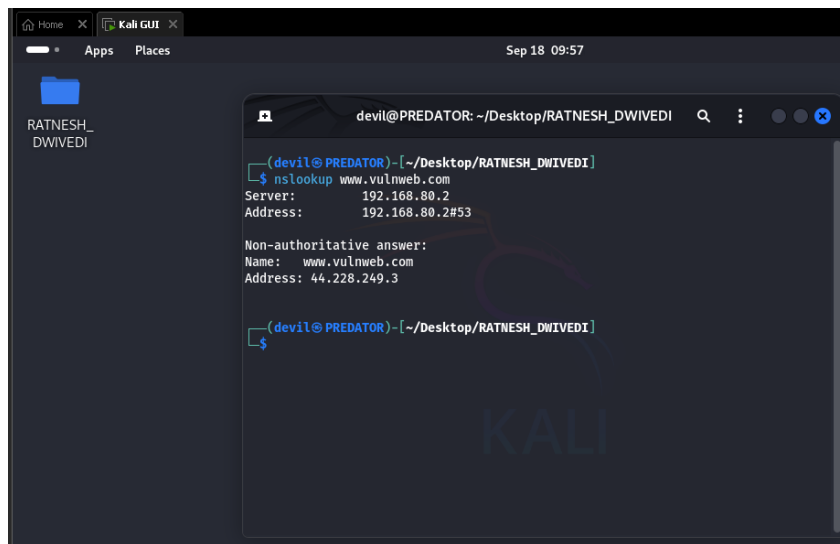
Introduction

The aim of this report is to conduct a port scan on the <http://testphp.vulnweb.com> website in order to identify open ports and the associated services. The research aims to enhance the website's security by providing insights into potential vulnerabilities

Methodology

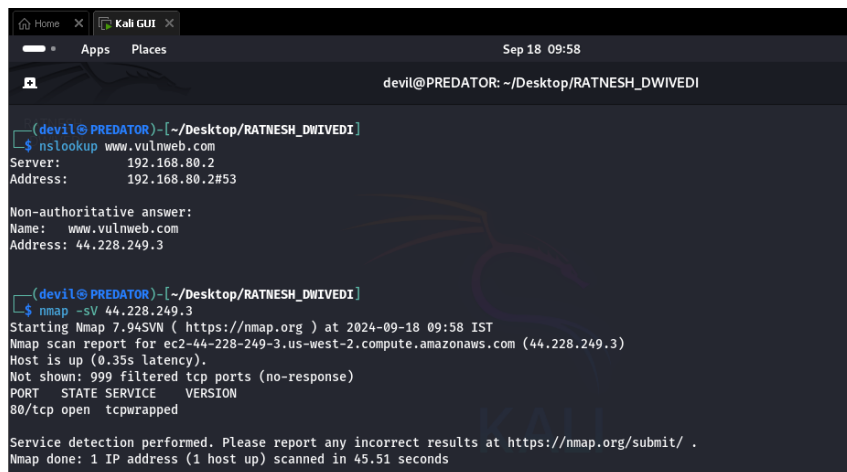
After obtaining the IP address of the website through a nslookup command, we proceeded to the next step: port scanning for open ports and vulnerabilities. For this purpose, we utilized the popular network scanning tool called 'Nmap'

IP Finding



Port Scanning

Command: `nmap 44.228.249.3 -sV`



Port scan results: Port 80(http) is Open.

Mitigation

Update Software Regularly: Keep your software up to date to patch any vulnerabilities that could be exploited.

Firewall Configuration: Configure your firewall to block access to unnecessary ports, limiting potential entry points for attackers.

Use Strong Passwords: Ensure that all accounts have strong, unique passwords to prevent unauthorized access.

Implement Network Segmentation: Divide your network into smaller segments to limit the spread of an attack if one part is compromised.

Disable Unused Services: Turn off any services or features that you don't need, reducing the number of potential vulnerabilities.

TASK 2

Objective

Brute force the website <http://testphp.vulnweb.com/> and find the directories that are present in the website.

Introduction

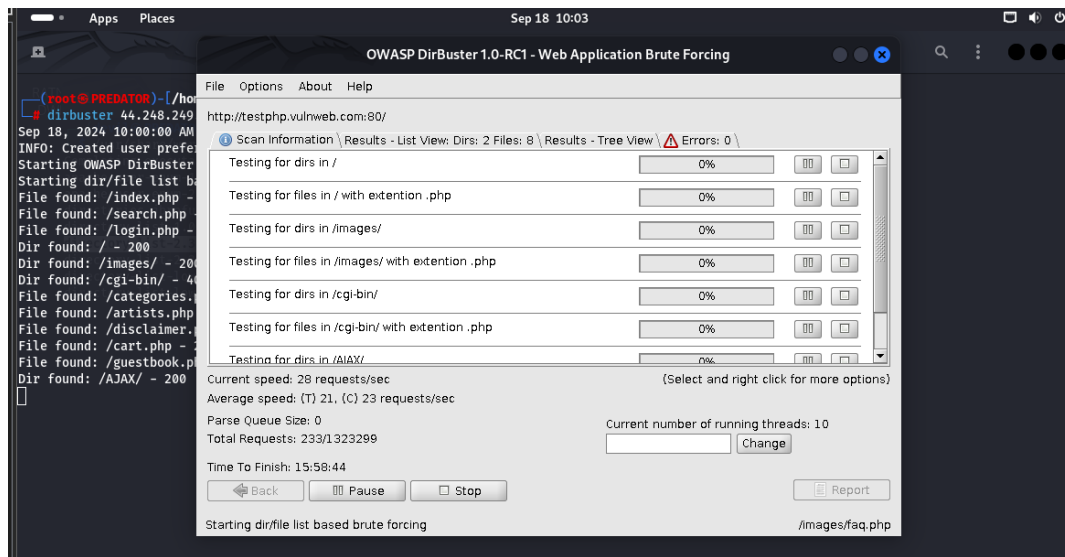
The report is about pretending to break into the login page of the website www.vulnweb.com using a tool called Burp Suite. The goal is to show how easy it can be for someone to get into a system when the login isn't very secure. This can provide some key insights and help us understanding the importance of a strong and robust security measures.

Methodology

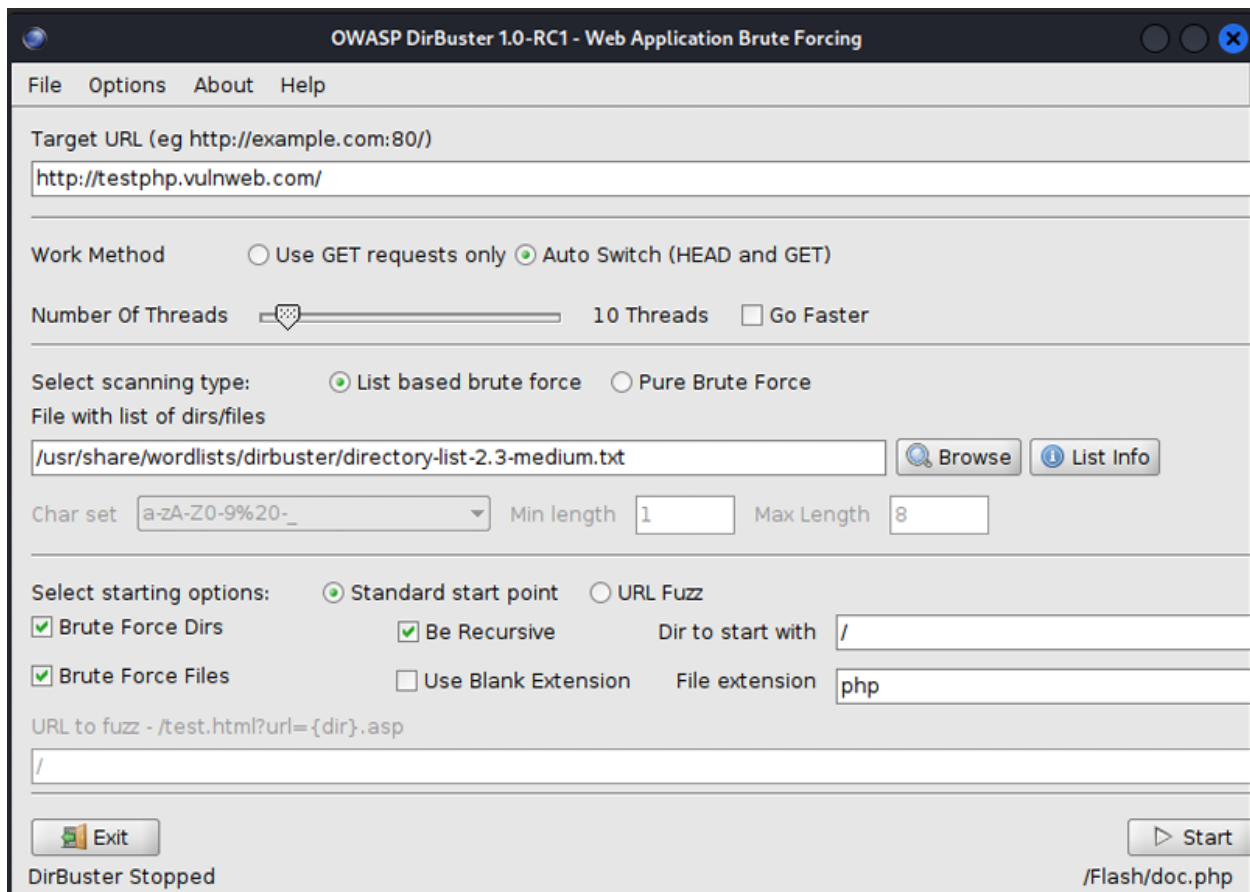
Here, I'm going to use the Dirbuster tool, which is a Java application designed to find hidden directories and files on web servers by brute-forcing their names. Dirbuster has 9 different lists that make it very good at discovering these hidden areas.

To use it, open your terminal and type "dirbuster". Then enter the target URL (<http://testphp.vulnweb.com>) as shown in the image below. Browse to `/usr/share/dirbuster/wordlists/` and select `directory-list-2-3-medium.txt` to start the brute force attack, the image also shows all the

Showing the running and the findings of dirbuster



Choosing a wordlist



Mitigation

Implement Strong Authentication: Use strong authentication mechanisms like multi-factor authentication (MFA) to restrict access to sensitive directories and files.

Hide Sensitive Files: Ensure that sensitive files and directories are not publicly accessible or are stored in locations that are difficult to guess.

Use a Web Application Firewall (WAF): Deploy a WAF to detect and block suspicious activities, including brute force attacks.

Regularly Update Software: Keep your web server and applications up to date with the latest security patches to prevent exploitation of known vulnerabilities.

Configure Proper Permissions: Set proper file and directory permissions to limit access to only authorized users.

TASK 3

Objective

Make a login in the website <http://testphp.vulnweb.com/> and intercept the network traffic using Wireshark and find the credentials that were transferred through the network.

Introduction

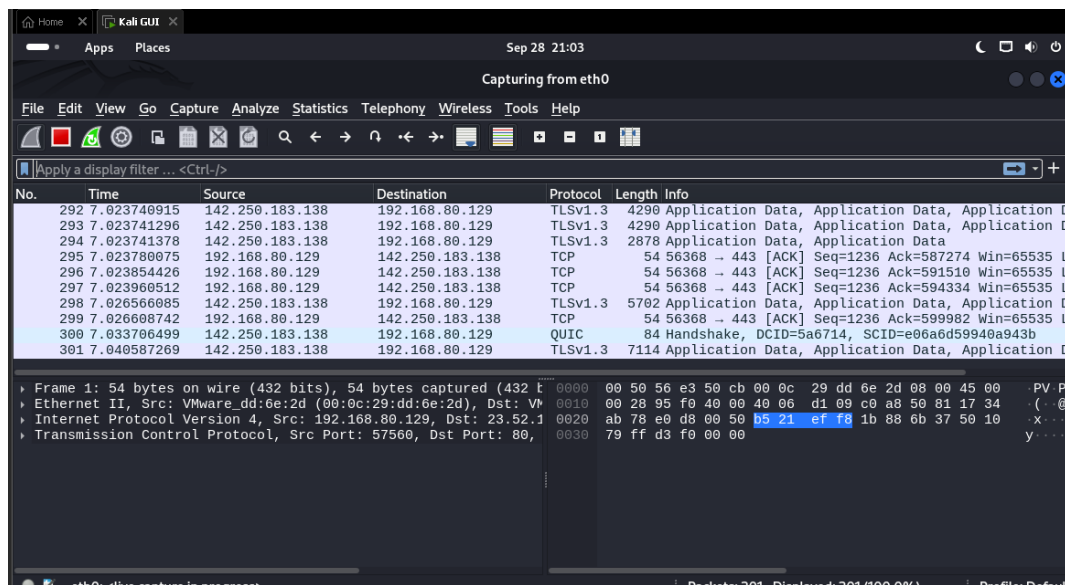
This report explains how to use Wireshark to capture network traffic on the website <http://testphp.vulnweb.com> and find login credentials. The goal is to show why it's important to protect sensitive information sent over the internet and to suggest ways to improve cybersecurity measures.

Methodology

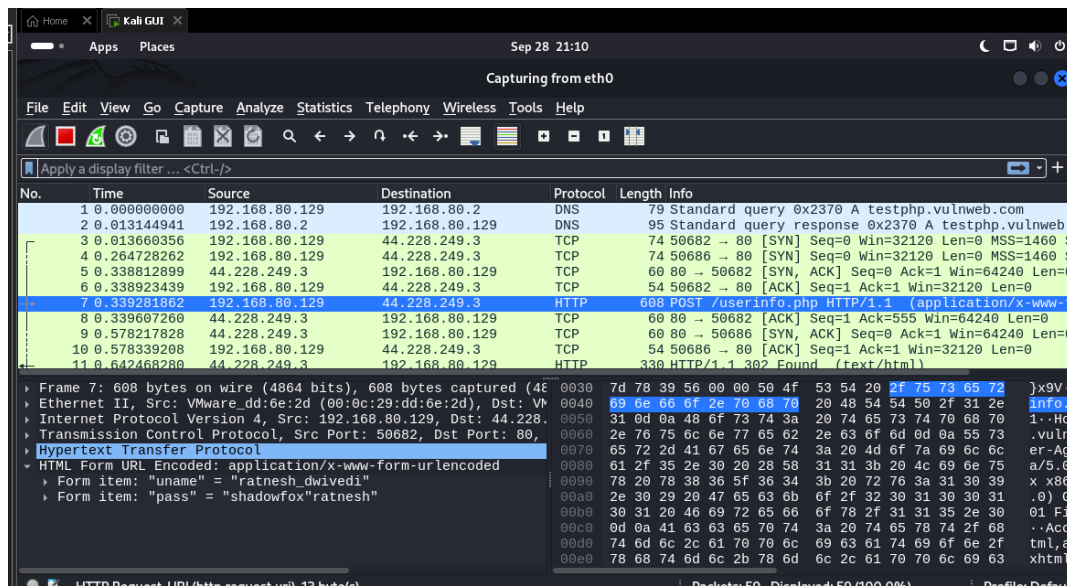
Open Wireshark and select the eth0 interface to start capturing network traffic. Then, go to the website <http://testphp.vulnweb.com/> using the Firefox browser and enter the login credentials.

Switch back to Wireshark to analyse the captured network traffic. Pay attention to the source and destination IP addresses, the protocols used, and any information transmitted during the login process.

Opening wireshark and selecting eth0 to start capturing packets.



Putting a filter for http packets to find out the credentials.



The used credentials are shown in plain text in wireshark

Username: - ratnesh_dwivedi

Password: - shadowfox"ratnesh

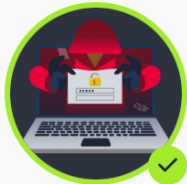
Mitigation

- **Use HTTPS:** Make sure the website uses HTTPS instead of HTTP. HTTPS encrypts the data, making it harder for others to see your credentials.
- **Install Security Certificates:** Use SSL/TLS certificates to encrypt data between the user's browser and the web server.
- **Avoid Public Wi-Fi:** Don't log in to important accounts over public Wi-Fi, as these networks are less secure.
- **Use Strong Passwords:** Create strong, unique passwords for each of your accounts to reduce the risk if your credentials are intercepted.
- **Enable Multi-Factor Authentication (MFA):** Use MFA to add an extra layer of security, making it harder for attackers to access your account even if they get your password.

CTF

THM Profile :- <https://tryhackme.com/p/ratneshd202>

1.Red Team Fundamentals (THM)



Woop woopl Your answer is correct

Congratulations on completing Red Team Fundamentals!!! 🎉

Points earned 🎯 88	Completed tasks 📋 7	Room type 👤 Walkthrough	Difficulty 📶 Easy	Streak 🔥 1
-----------------------	------------------------	----------------------------	----------------------	---------------

🗉 Leave Feedback

Next

2.Pickle Rick(THM)

```
root@ip-10-10-205-232:/dev/shm# cd
root@ip-10-10-205-232:~# ls
3rd.txt  snap
root@ip-10-10-205-232:~# cat 3rd.txt
3rd ingredients: fleeb juice
root@ip-10-10-205-232:~# ls
3rd.txt  snap
root@ip-10-10-205-232:~# cd /home
root@ip-10-10-205-232:/home# ls
rick  ubuntu
root@ip-10-10-205-232:/home# cd rick/
root@ip-10-10-205-232:/home/rick# ls
second ingredients
root@ip-10-10-205-232:/home/rick# cat *
1 jerry tear
root@ip-10-10-205-232:/home/rick#
```

1. Mr. Meesek hair
2. 1 jerry tear
3. Fleeb juice

ETHICAL HACKING PROJECT

1. Password Strength Checker Create a Python program to evaluate password strength based on length, uppercase/lowercase letters, numbers, and special characters. Provide feedback like "Weak," "Moderate," or "Strong."

Working Process:

1. User types a password in the input box.
2. The program checks:
 - a. **Length** of the password.
 - b. **Complexity** (uppercase, lowercase, digit, special character).

- c. **Uniqueness** (avoids common passwords).
3. It calculates a score and determines the **strength level**.
4. It shows color-coded feedback and improvement **suggestions** in real-time.

Key Functions:

- **check_password_strength()**: Core logic that evaluates the password and returns its strength level and tips.
- **on_password_change()**: Updates the strength and suggestions as the user types.
- **on_submit()**: Displays a popup with the final password strength.

Github Link :-

[https://github.com/ratnesh1dwivedi/Projects/blob/main/Password Strength Checker.py](https://github.com/ratnesh1dwivedi/Projects/blob/main/Password%20Strength%20Checker.py)

2. Basic Port Scanner Write a Python script to scan open ports on a given IP address and port range. Handle invalid inputs and display open ports.

Working Process:

1. User inputs a **target IP address** and **port range**.
2. The tool **validates the IP and ports**.
3. It attempts to **connect to each port** using a TCP socket.
4. If a connection is successful, the port is marked as **open**.
5. Displays all **open ports** and **scan time**.

Key Functions:

- **is_valid_ip()** – Verifies IP address format.
- **scan_ports()** – Scans ports and returns the list of open ones.
- **main()** – Handles input, calls functions, and displays results.

GitHub Link:-

<https://github.com/ratnesh1dwivedi/Projects/blob/main/Port%20Scanner.py>

3. File Encryption/Decryption Tool Create a Python program to encrypt and decrypt text files using a secret key with the cryptography library. Include options to save the output as a new file.

Working Process (Overview):

1. **User loads an image** into the GUI.
2. A **password-based encryption key** is generated or loaded.
3. User selects encryption method: **Scramble** or **AES**.
4. Image is encrypted or decrypted using the selected method.
5. User can **save** the processed image.

Key Functions:

- **load_image()** – Loads and converts the image to a format suitable for processing.
- **generate_key() / load_key()** – Creates or imports a secure key using PBKDF2 (password-based key derivation).
- **encrypt_image() / decrypt_image()** – Handles encryption and decryption via:
 - **scramble**: pixel shuffling using pseudo-random seed.
 - **aes**: AES block cipher in ECB mode.
- **save_image()** – Saves the processed (encrypted/decrypted) image.
- **GUI (Tkinter)** – Allows users to interact with the tool via buttons, options, and visual feedback.

Github Link:- https://github.com/ratnesh1dwivedi/Projects/blob/main/Image_Encrypt.py

Learning Outcomes

- **Technical Proficiency:** I gained practical experience in various cybersecurity tools and techniques, including vulnerability scanning, penetration testing, and cryptographic analysis.
- **Understanding of Cybersecurity Lifecycle:** I developed a comprehensive understanding of the steps involved in securing systems, from initial vulnerability assessment to implementing mitigations.
- **Problem-Solving Skills:** Tackling complex security challenges enhanced my analytical thinking and my ability to devise effective solutions under pressure.
- **Professional Development:** My experience improved my ability to work in a team, communicate technical information clearly, and manage time efficiently in a fast-paced environment.

Challenges and Solutions

- **Adapting to Complex Tools:** Initially, mastering advanced cybersecurity tools like Metasploit and Wireshark was challenging. I overcame this by dedicating time to study tutorials and practicing in a simulated environment, which significantly improved my proficiency.
- **Handling Advanced Security Scenarios:** The complexity of real-world security threats required a deep understanding of underlying principles. I tackled this by engaging in continuous learning and seeking guidance from my coordinator and team members.

Conclusion

My internship at Hack Secure was an enriching experience that significantly expanded my knowledge and skills in cybersecurity. The practical exposure to real-world security challenges and the application of advanced tools have solidified my interest in pursuing a career in cybersecurity. This experience has been instrumental in preparing me for the complexities of the cybersecurity field.

Acknowledgments

I express my sincere gratitude to Hack Secure, especially my mentor, Mr. Aman Pandey, and assistant mentor Mr. Prabhat Raj, for their guidance and support throughout my internship. I also thank ITM University for providing this internship opportunity, which has been crucial in my personal and professional development.

This report encapsulates the essence of my internship experience, highlighting the integration of academic knowledge with practical skills in a professional setting. It reflects my journey of learning, growth, and development in the field of cybersecurity.