Internship Final Report

Student Name: Lalit Prajapati
University: South indian association college
Major: Begginer
Internship Duration: October 1st, 2024 - October 31st, 2024
Company: ShadowFox
Domain: Cyber Security
Mentor: Mr. Surendharan
Assistant Mentor: Mr. Pranshu
Coordinator: Mr. Aakash

Objectives

The main objective of this task is to practice and understand basic ethical hacking techniques using a safe and intentionally vulnerable website, http://testphp.vulnweb.com/**. This task helps beginners learn how to:**

- **Discover open network ports on a server**
- **Find hidden directories using brute force**
- **Capture and analyze unencrypted login data using network sniffing tools like Wireshark**

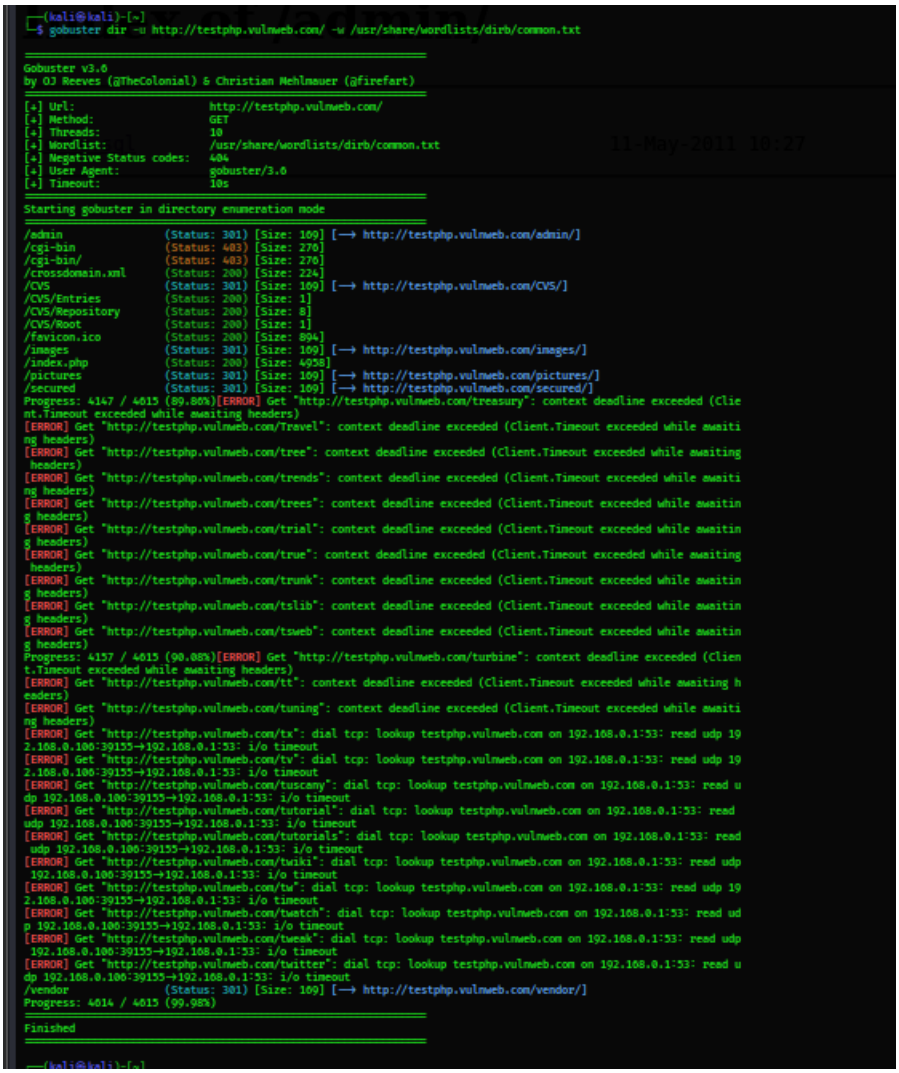
Tasks and Responsibilities

1. **Port Scanning**
   Use the nmap tool to scan and identify all open ports on the target web server. This helps to understand what services are running and which ports might be vulnerable.

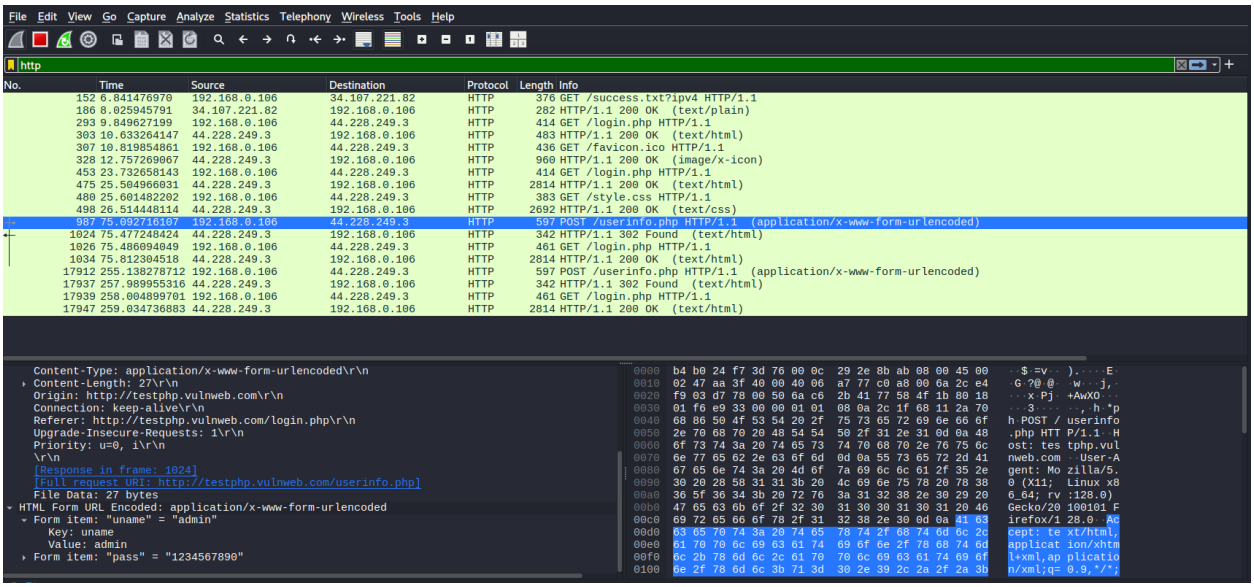
```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn testphp.vulnweb.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 08:47 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.33s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 27.67 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -T5 testphp.vulnweb.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 09:01 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.27s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0
|_http-title: Home of Acunetix Art
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 4.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:4.15
Aggressive OS guesses: Linux 4.15 (91%), Linux 4.19 - 5.15 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   17.21 ms  192.168.0.1
2   ...
3   35.11 ms  103.228.155.165
4   16.43 ms  59.163.29.81.static.vsnl.net.in (59.163.29.81)
5   300.73 ms 172.31.244.45
6   ... 12
13  256.72 ms if-ae-0-2.tcore1.sv1-santaclara.as6453.net (63.243.251.1)
14  295.53 ms if-ae-20-2.tcore1.00s-seattle.as6453.net (64.86.123.94)
15  296.08 ms ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.34 seconds
```

2. **Directory Brute Forcing**
   Use tools like gobuster or dirb to find hidden directories and pages on the website by trying many possible URLs. This is useful to find admin panels, login pages, upload portals, and other useful resources.



3. **Intercepting Login Traffic**
   Log into the website using test credentials and capture the network traffic using Wireshark. Analyze the data to check whether the credentials are visible and how they are sent to the server.



Learning Outcomes

By completing this task, I learned:

- How to use **Nmap** for port scanning and understand how servers expose certain services.
- How to use **gobuster** or **dirb** for discovering hidden directories on a website.
- How login forms work and how **HTTP requests** can leak sensitive information if not encrypted.
- How to use **Wireshark** to capture and analyze network traffic.
- The importance of **HTTPS** in protecting login credentials from being stolen.

Challenges and Solutions

1. **Challenge:** Network scanning might be blocked by some internet providers or firewalls.
   Solution: I ensured I was using a safe and legal target website (provided by Acunetix) and ran the scan on my own system or using a VPN if needed.
2. **Challenge:** Gobuster requires a good wordlist to find valid directories.
   Solution: I used the built-in wordlist from Kali Linux located at /usr/share/wordlists/dirb/common.txt to increase chances of success.
3. **Challenge:** Wireshark captures a lot of data and can be confusing.
   Solution: I used filters like http and looked for **POST** requests to make the analysis easier.

Conclusion

This beginner-level ethical hacking task helped me understand the basic concepts of penetration testing in a practical and legal environment. I was able to identify open ports, find hidden directories, and capture sensitive data being sent over an insecure connection. It taught me the importance of securing web applications and how hackers can exploit basic vulnerabilities. This hands-on experience is a strong foundation for advancing in cybersecurity.

Acknowledgments

I would like to thank:

- **Acunetix** for providing the vulnerable web application (http://testphp.vulnweb.com/) for practice.
- The creators of open-source tools like **Nmap**, **Gobuster**, and **Wireshark**, which are essential for cybersecurity learning.
- My instructor/mentor for guiding me through the ethical hacking process and ensuring I used these tools responsibly and legally.