**EXPERIMENT-6**

**Student’s Name: UID: 20BCS**

**Section/Group: 707\_WM\_B Subject Code: 20CSP-338**

**Subject Name: WMS Lab Date of performance:21/10/2022**

**Branch: BE CSE Semester:5th**

**Aim:**Perform Penetration testing on a web application to gather Information about the system (Foot Printing).

**Objective:**To perform penetration testing and foot printing on any Web Application

**Software/Hardware Requirements:**Kali Linux, D-tech tools or any pen Testing tools and any platform using Python 2.7

Tools to be used:

1. D-Tech

2. NMAP

3. Metasploit

4. Wire Shark

**Introduction:**Web application penetration testing is the practice of simulating attacks on a system in an attempt to gain access to sensitive data, with the purpose of determining whether a system is secure. These attacks are performed either internally or externally on a system, and they help provide information about the target system, identify vulnerabilities within them, and uncover exploits that could actually compromise the system. It is an essential health check of a system that informs testers whether remediation and security measures are needed.



Foot printing of any web side

Whos is Details

Software used and version

OS Details

Sub Domains

File Name and File Path

Scripting Platform & CMS Details

Contact Details

**Description**:

* **D-TECT** is an All-In-One Tool for Penetration Testing. This is specially programmed for Penetration Testers and Security Researchers to make their job easier, instead of launching different tools for performing different task.
* **D-TECT** provides multiple features and detection features which gather target information and finds different flaws in it.

**Features:**

* Sub-domain Scanning
* Port Scanning
* Wordpress Scanning
* Wordpress Username Enumeration
* Wordpress Backup Grabbing
* Sensitive File Detection
* Same-Site Scripting Scanning
* Click Jacking Detection
* Powerful XSS vulnerability scanning
* SQL Injection vulnerability scanning
* User-Friendly UI

**Steps/Method/Coding:**

1. Install kali Linux virtual machine and D-tech tools Open Terminal.
2. :~$ git clone <https://github.com/bibortone/D-Tech.git>

:~$ ls

1. Check that D-tech tool is available on your system
2. :~$ cd D-tech and press Enter

:~/D-Tech$ ls

:~/D-Tech$ python d-tech.py(run the tools)

1. Get menu after run the tools

1. Word press username enumerator

2. Sensitive file detector

3. Cross-Site Scripting [ XSS ] Scanner:

4. SQL Injection [ SQLI ] Scanner:

5. Sub-domain Scanner:

6. Same Site Scripting detection:

7. Port scanner

8. Word press scanner

6. [+] select any option from menu

>Enter 4 next

[+] enter domain

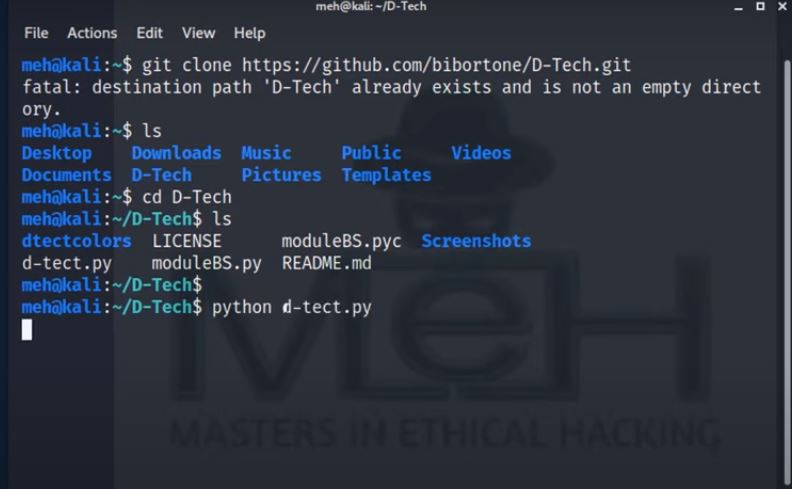
Demo.testfire.net

[+] checking Status…..

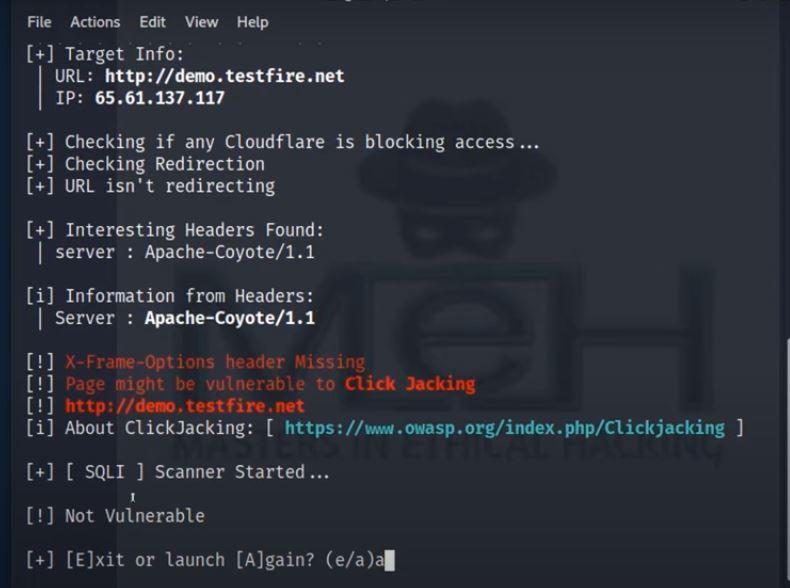
[] Not vulnerable

[+]exit or launch again?(e/a)

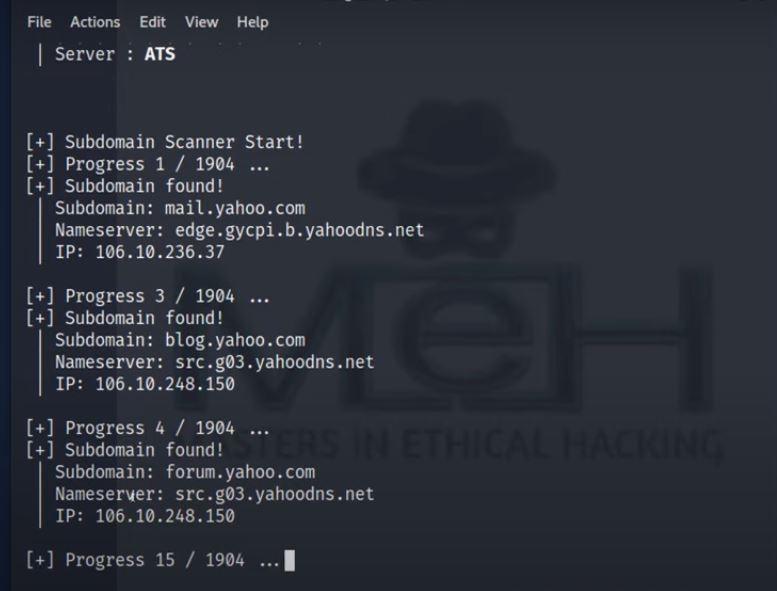
**Output screenshot:**

****

****

****

****

****

**Learning Outcomes:**

Finally, as a penetration tester, you should collect and log all vulnerabilities in the system. Don’t ignore any scenario considering that it won’t be executed by the end-users.If you are a penetration tester, please help our readers with your experience, tips, and sample test cases on how to perform Penetration Testing effectively.