Experiment – 6

Name: Aniket Kumar **UID: 20BCS5306**

Semester: 5 **Section: 703/B**

Subject: Web and Mobile Security LAB **Subject Code: 20CSP-338**

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.

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 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

Check that D-tech tool is available on your system

3.:~$ cd D-tech and press Enter

4.:~/D-Tech$ ls

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

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

Step 6- [+] select any option from menu

>Enter 4 next

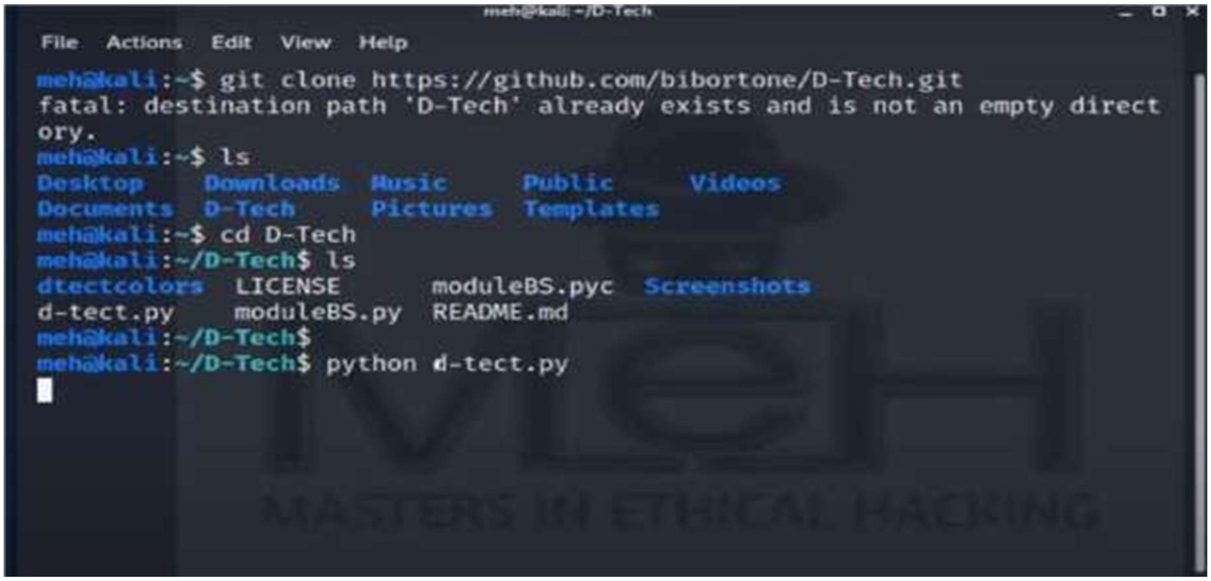
[+] enter domain

Demo.testfire.net

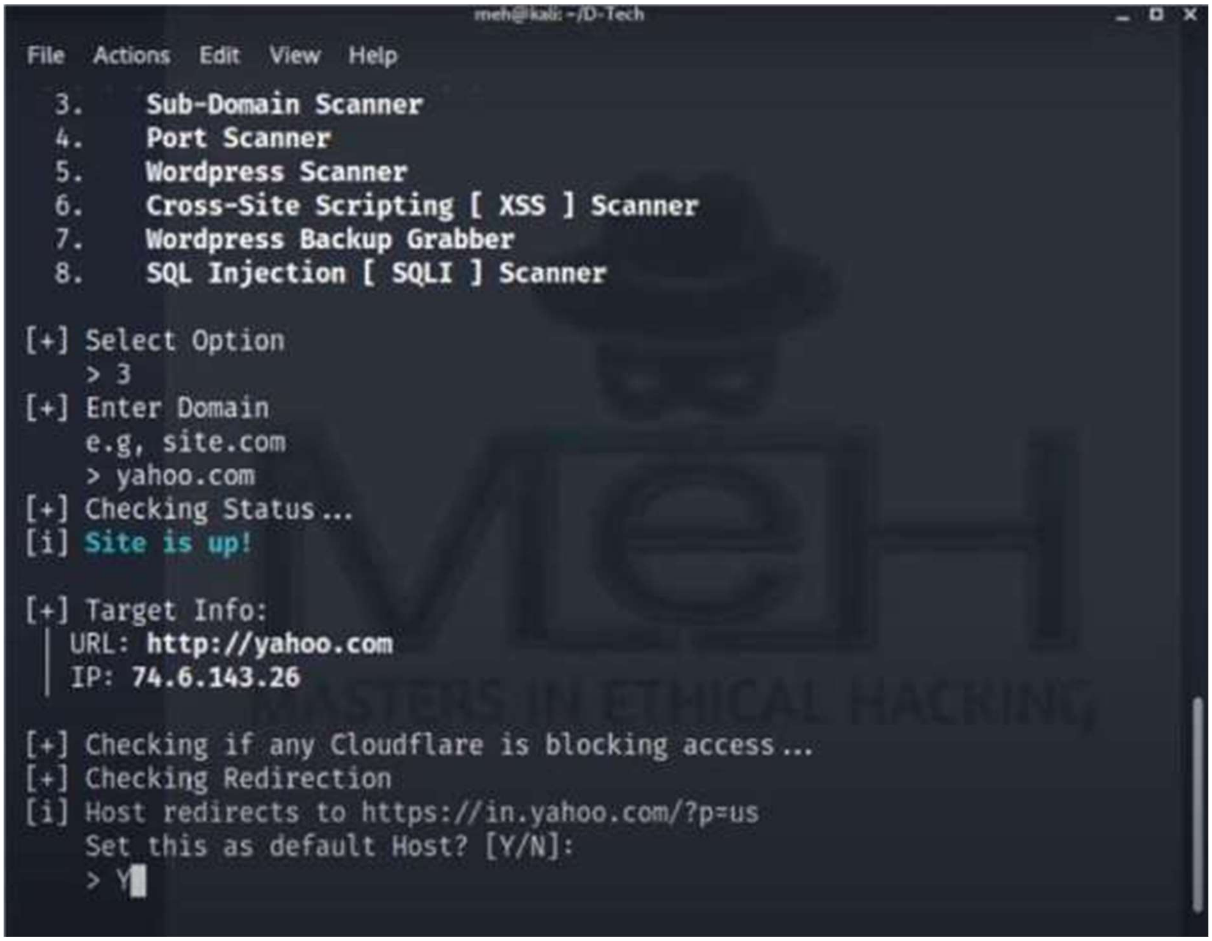
[+] checking Status…..

[] Not vulnerable

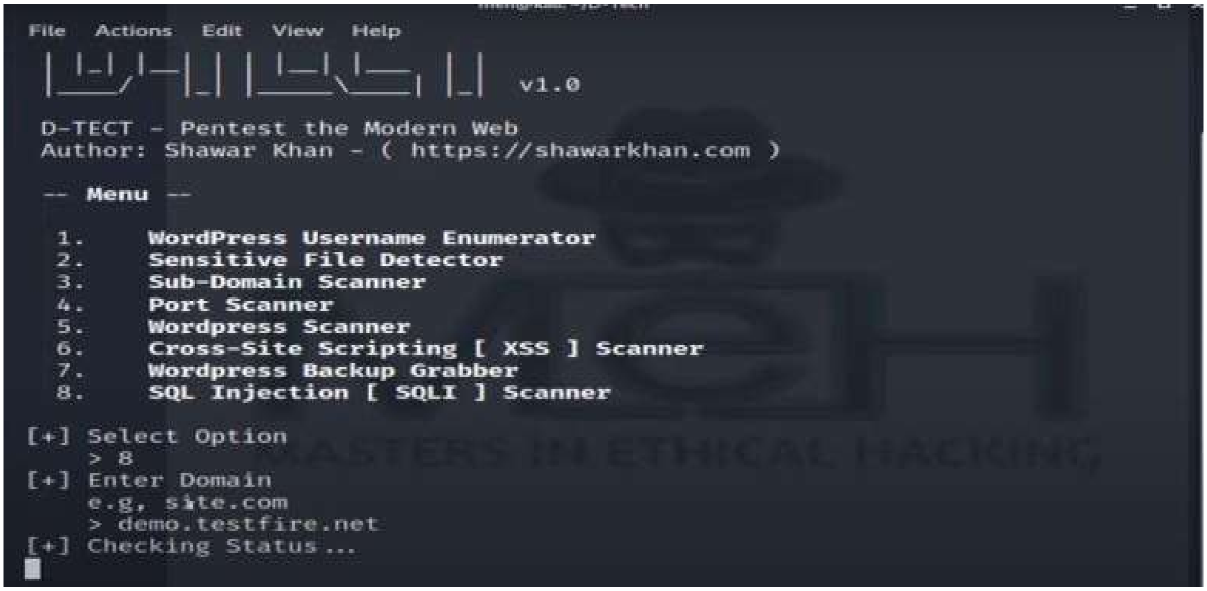
[+]exit or launch again?(e/a) **Output screenshot:**



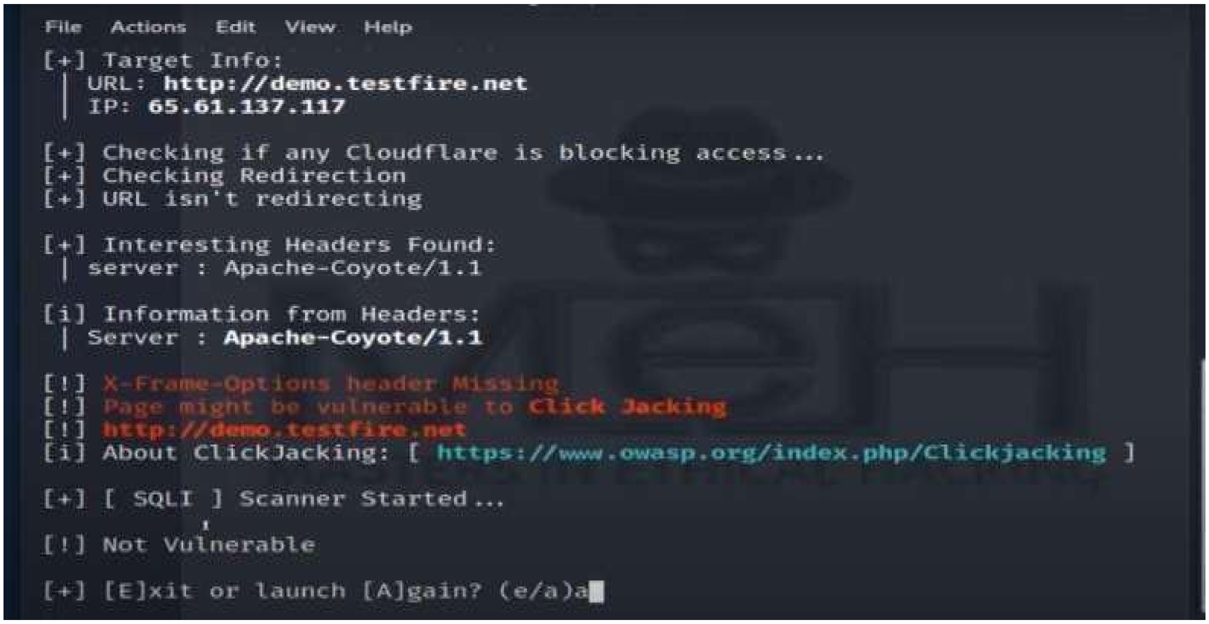
```
meh@kali:~$ git clone https://github.com/bibortone/D-Tech.git
fatal: destination path 'D-Tech' already exists and is not an empty direct
ory.
meh@kali:~$ ls
Desktop    Downloads  Music     Public     Videos
Documents  D-Tech     Pictures  Templates
meh@kali:~$ cd D-Tech
meh@kali:~/D-Tech$ ls
dtectcolors  LICENSE     moduleBS.pyc  Screenshots
d-tect.py    moduleBS.py  README.md
meh@kali:~/D-Tech$
meh@kali:~/D-Tech$ python d-tect.py
```



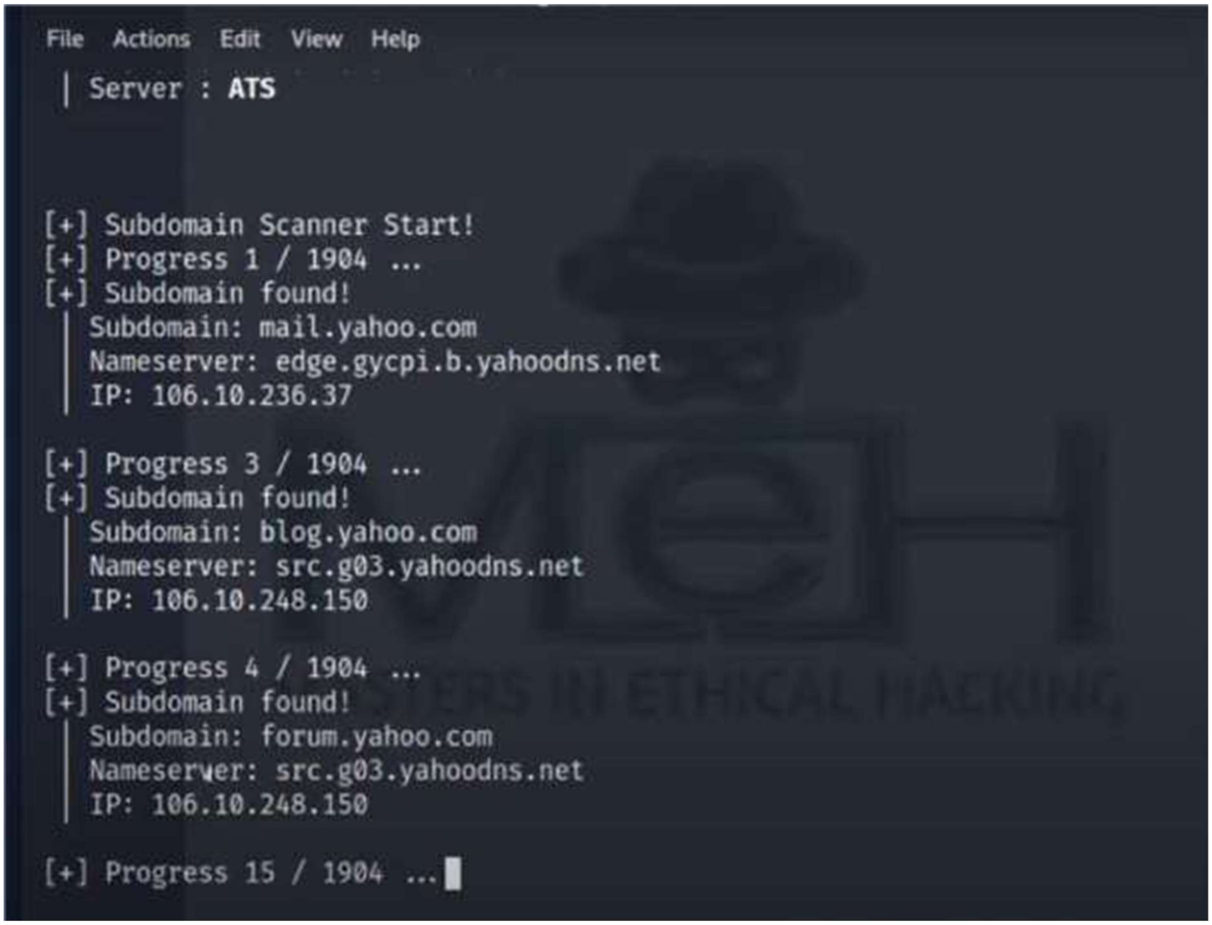
```
  3.    Sub-Domain Scanner
  4.    Port Scanner
  5.    Wordpress Scanner
  6.    Cross-Site Scripting [ XSS ] Scanner
  7.    Wordpress Backup Grabber
  8.    SQL Injection [ SQLI ] Scanner

[+] Select Option
    > 3
[+] Enter Domain
    e.g, site.com
    > yahoo.com
[+] Checking Status ...
[i] Site is up!

[+] Target Info:
  | URL: http://yahoo.com
  | IP: 74.6.143.26

[+] Checking if any Cloudflare is blocking access...
[+] Checking Redirection
[i] Host redirects to https://in.yahoo.com/?p=us
    Set this as default Host? [Y/N]:
    > Y
```



```
                                                 v1.0

 D-TECT - Pentest the Modern Web
 Author: Shawar Khan - ( https://shawarkhan.com )

 -- Menu --

  1.    WordPress Username Enumerator
  2.    Sensitive File Detector
  3.    Sub-Domain Scanner
  4.    Port Scanner
  5.    Wordpress Scanner
  6.    Cross-Site Scripting [ XSS ] Scanner
  7.    Wordpress Backup Grabber
  8.    SQL Injection [ SQLI ] Scanner

[+] Select Option
    > 8
[+] Enter Domain
    e.g, site.com
    > demo.testfire.net
[+] Checking Status ...
```



```
[+] Target Info:
 | URL: http://demo.testfire.net
 | IP: 65.61.137.117

[+] Checking if any Cloudflare is blocking access ...
[+] Checking Redirection
[+] URL isn't redirecting

[+] Interesting Headers Found:
 | server : Apache-Coyote/1.1

[i] Information from Headers:
 | Server : Apache-Coyote/1.1

[!] X-Frame-Options header Missing
[!] Page might be vulnerable to Click Jacking
[!] http://demo.testfire.net
[i] About ClickJacking: [ https://www.owasp.org/index.php/Clickjacking ]

[+] [ SQLI ] Scanner Started...

[!] Not Vulnerable

[+] [E]xit or launch [A]gain? (e/a)a
```



```
 | Server : ATS



[+] Subdomain Scanner Start!
[+] Progress 1 / 1904 ...
[+] Subdomain found!
 | Subdomain: mail.yahoo.com
 | Nameserver: edge.gycpi.b.yahoodns.net
 | IP: 106.10.236.37

[+] Progress 3 / 1904 ...
[+] Subdomain found!
 | Subdomain: blog.yahoo.com
 | Nameserver: src.g03.yahoodns.net
 | IP: 106.10.248.150

[+] Progress 4 / 1904 ...
[+] Subdomain found!
 | Subdomain: forum.yahoo.com
 | Nameserver: src.g03.yahoodns.net
 | IP: 106.10.248.150

[+] Progress 15 / 1904 ...
```

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.