Experiment 6 (Penetration Testing and Foot Printing)

Student Name: Lipakshi | **UID:** 20BCS5082

Branch: BE CSE | **Section/Group:** 607 / B

Semester: 5th | **Date of performance:** 03.11.22

Subject: Web and Mobile Security Lab | **Subject Code:** 20CSP_338

Aim/Overview of the Practical:

Perform Penetration testing on a web application to gather information about the system (Foot printing).

Task to be done / Which logistics used:

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 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.

Steps for experiment/practical/Code:

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

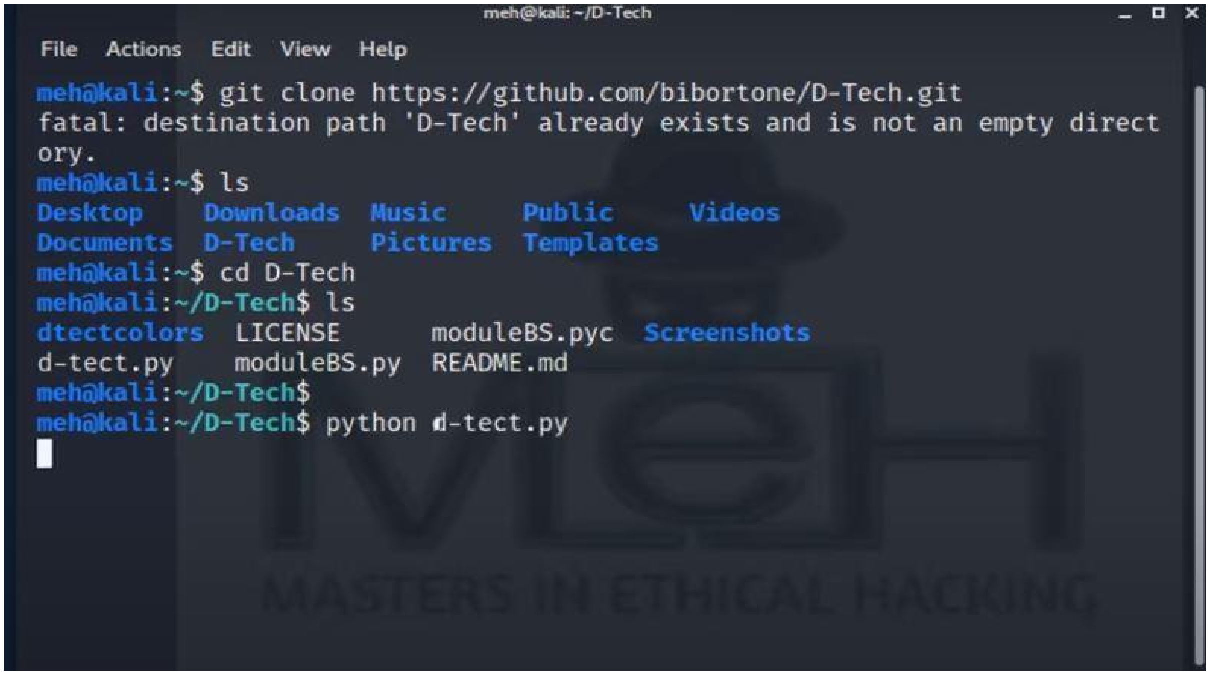
Demo.testfire.net

[+] checking Status…..

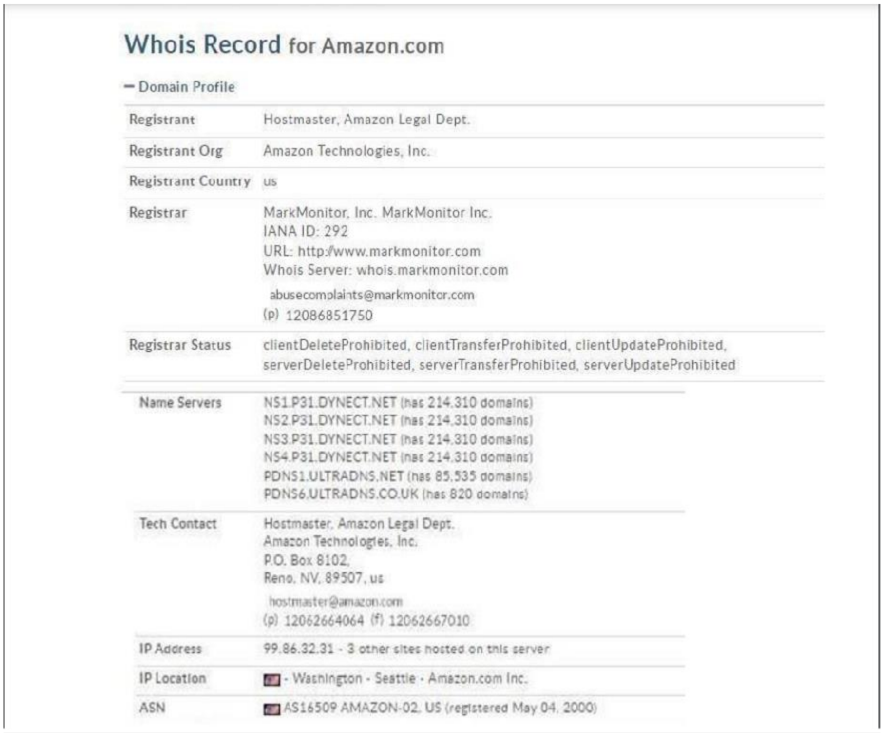
[] Not vulnerable

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

Result/Output/Writing Summary:



```
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
```



Whois Record for Amazon.com

— Domain Profile

Registrant	Hostmaster, Amazon Legal Dept.
Registrant Org	Amazon Technologies, Inc.
Registrant Country	us
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http:/www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12086851750
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Name Servers	NS1.P31.DYNECT.NET (has 214.310 domains) NS2.P31.DYNECT.NET (has 214.310 domains) NS3.P31.DYNECT.NET (has 214.310 domains) NS4.P31.DYNECT.NET (has 214.310 domains) PDNS1.ULTRADNS.NET (has 85.535 domains) PDNS6.ULTRADNS.CO.UK (has 820 domains)
Tech Contact	Hostmaster, Amazon Legal Dept. Amazon Technologies, Inc. P.O. Box 8102, Reno, NV, 89507, us hostmaster@amazon.com (p) 12062664064 (f) 12062667010
IP Address	99.86.32.31 - 3 other sites hosted on this server
IP Location	🇺🇸 - Washington - Seattle - Amazon.com Inc.
ASN	🇺🇸 AS16509 AMAZON-02, US (registered May 04, 2000)

Learning outcomes (What I have learnt):

a. Collect and log all vulnerabilities in the system. Don't ignore any scenario considering that it won't be executed by the end-users.

b. How to perform Penetration Testing effectively.