DEPARTMENT OF
COMPUTER SCIENCE & ENGINEERING
Discover. Learn. Empower.

Experiment: 2.2

Student Name: Yash Kumar
UID: 20BCS9256
Branch: BE-CSE
Section/Group: 616 'B'
Semester: 5th
Subject Name: WMS Lab
Subject Code: 21CSP-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. 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. **DTECT** 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:

1. Go to Google and search central ops.net.
2. There you can a Info about DNS Records, Network and vice versa.
3. If you want info about domain registrar, registration time and other info.
4. Then u will get at https://whois.domaintools.com/ Using tools:

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

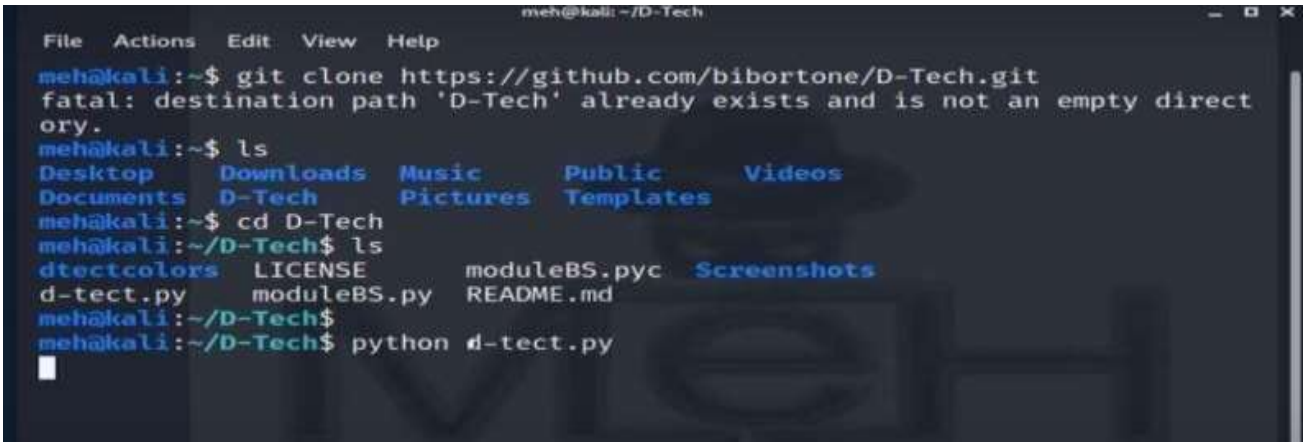
Demo.testfire.net

[+] checking Status…..

[] Not vulnerable

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

Output screenshot:


meh@kali: ~/D-Tech
File Actions Edit View Help
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

DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup

Home > Whois Lookup > Amazon.com

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)

Domain Status	Registered And Active Website
IP History	479 changes on 479 unique IP addresses over 16 years
Registrar History	2 registrars with 1 drop
Hosting History	4 changes on 4 unique name servers over 18 years

— Website

Website Title	None given.
Server Type	Server
Response Code	200
Terms	360 (Unique: 217, Linked: 178)
Images	23 (Alt tags missing: 3)
Links	68 (Internal: 66, Outbound: 0)

Network Whois record

Queried **whois.arin.net** with "**n 52.95.116.115**"...

```
NetRange:       52.84.0.0 - 52.95.255.255
CIDR:           52.84.0.0/14, 52.88.0.0/13
NetName:        AT-88-Z
NetHandle:      NET-52-84-0-0-1
Parent:         NET52 (NET-52-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS16509, AS14618
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        1991-12-19
Updated:        2022-03-21
Ref:            https://rdap.arin.net/registry/ip/52.84.0.0


OrgName:        Amazon Technologies Inc.
OrgId:          AT-88-Z
Address:        410 Terry Ave N.
City:           Seattle
StateProv:      WA
PostalCode:     98109
Country:        US
RegDate:        2011-12-08
Updated:        2022-09-30
Comment:        All abuse reports MUST include:
Comment:        * src IP
Comment:        * dest IP (your IP)
Comment:        * dest port
Comment:        * Accurate date/timestamp and timezone of activity
```

DNS records

DNS query for **115.116.95.52.in-addr.arpa** returned an error from the server: **NameError**

name	class	type	data	time to live
amazon.in	IN	HINFO	CPU: RFC8482 OS:	3600s (01:00:00)

Traceroute

Tracing route to **amazon.in [52.95.116.115]**...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	1	0	0	169.254.158.58	
2	6	1	0	169.48.118.158	ae103.ppr02.dal13.networklayer.com
3	0	0	0	169.48.118.138	8a.76.30a9.ip4.static.sl-reverse.com
4	2	2	2	169.45.18.42	ae17.cbs02.dr01.dal04.networklayer.com
5	25	25	26	169.45.18.5	ae2.cbs01.eq01.chi01.networklayer.com
6	44	*	44	50.97.17.49	ae0.cbs02.tl01.nyc01.networklayer.com
7	117	114	*	169.45.19.47	ae1.cbs01.tg01.lon01.networklayer.com
8	113	113	113	169.45.18.13	d.12.2da9.ip4.static.sl-reverse.com
9	112	112	112	195.66.237.175	

Whois Record (last updated on 2022-10-13)

```
Domain Name: amazon.com
Registry Domain ID: 281209_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-08-26T19:19:56+0000
Creation Date: 1994-11-01T05:00:00+0000
Registrar Registration Expiration Date: 2024-10-30T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Hostmaster, Amazon Legal Dept.
Registrant Organization: Amazon Technologies, Inc.
Registrant Street: P.O. Box 8102
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89507
Registrant Country: US
Registrant Phone: +1.2062664064
Registrant Phone Ext:
Registrant Fax: +1.2062667010
Registrant Fax Ext:
Registrant Email: hostmaster@amazon.com
Registry Admin ID:
Admin Name: Hostmaster, Amazon Legal Dept.
Admin Organization: Amazon Technologies, Inc.
Admin Street: P.O. Box 8102
```

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 endusers.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.

Reference:

https://github.com/bibortone/D-Tech.git

https://www.youtube.com/watch?v=mThB2BrlGCg

https://www.hackingarticles.in/beginner-guide-website-footprinting/

.