PRACTICAL-9

AIM:

In computers, Foot printing is the process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment. Foot printing can reveal system vulnerabilities and improve the ease with which they can be exploited. Use the given approach to implement Footprinting: Gathering Target Information making use of following tools:

- Dmitry – Deepmagic
- UA Tester
- Whatweb

THEORY:

1. Dmitry - Deepmagic:

- DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line Application coded in C. DMitry has the ability to gather as much information as possible about a host.
- Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups, and more.
- The following is a list of the current features:

    - An Open Source Project.
    - Perform an Internet Number whois lookup.
    - Retrieve possible uptime data, system and server data.
    - Perform a SubDomain search on a target host.
    - Perform an E-Mail address search on a target host.
    - Perform a TCP Portscan on the host target.

- A Modular program allowing user specified modules

2. UA-Tester:

- This tool is designed to automatically check a given URL using a list of standard and non-standard User Agent strings provided by the user (1 per line).
- The results of these checks are then reported to the user for further manual analysis where required. Gathered data includes Response Codes, resulting URL in the case of a 30x response,
- MD5 and length of response body, and select Server headers.
- Results: When in non-verbose mode, only values that do not match the initial reference connection are reported to the user.
- If no results are shown for a specific user agent then all results match the initial reference connection.
- If you require a full output of all checks regardless of matches to the reference, please use the verbose setting.

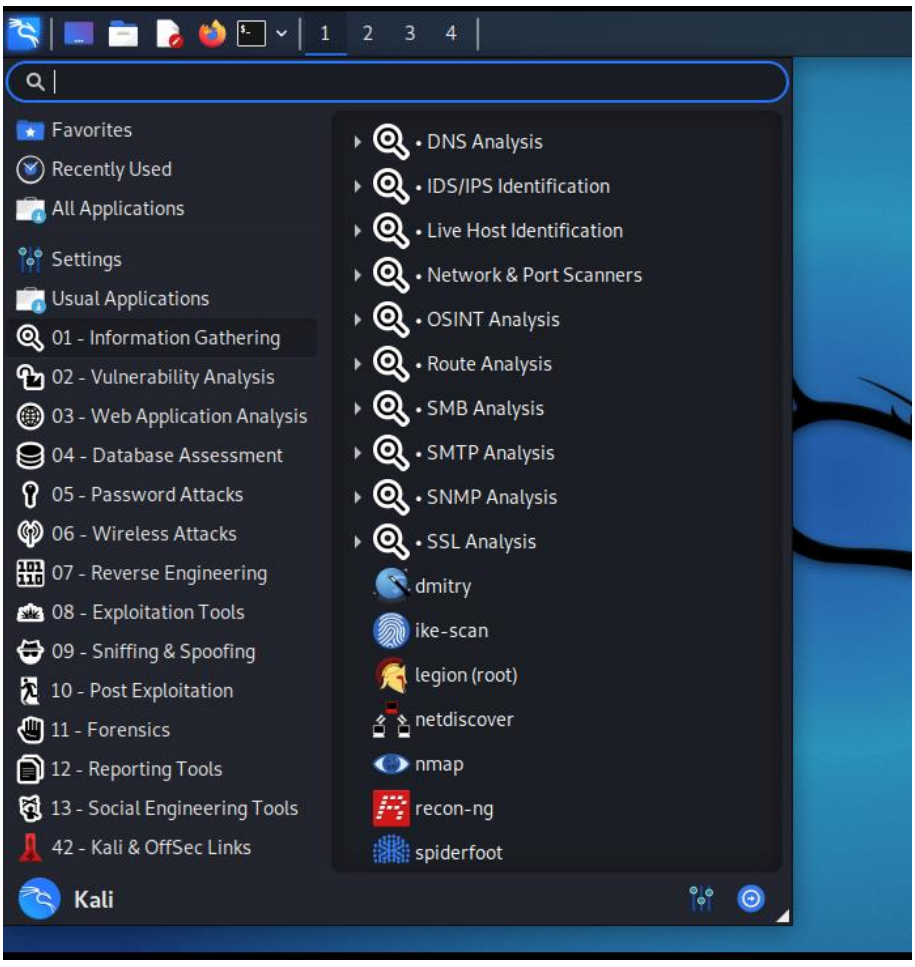
3. Whatweb:

- WhatWeb identifies websites.
- Its goal is to answer the question, “What is that Website?”.
- WhatWeb recognizes web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices. WhatWeb has over 1700 plugins, each to recognise something different.
- WhatWeb also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.
- WhatWeb can be stealthy and fast, or thorough but slow.
- WhatWeb supports an aggression level to control the trade off between speed and reliability.

- When you visit a website in your browser, the transaction includes many hints of what web technologies are powering that website.
- Sometimes a single webpage visit contains enough information to identify a website but when it does not, WhatWeb can interrogate the website further.
- The default level of aggression, called ‘stealthy’, is the fastest and requires only one HTTP request of a website.
- This is suitable for scanning public websites. More aggressive modes were developed for use in penetration tests.

Dmitry - Deepmagic:

- We can find Dmitry in Information Gathering section

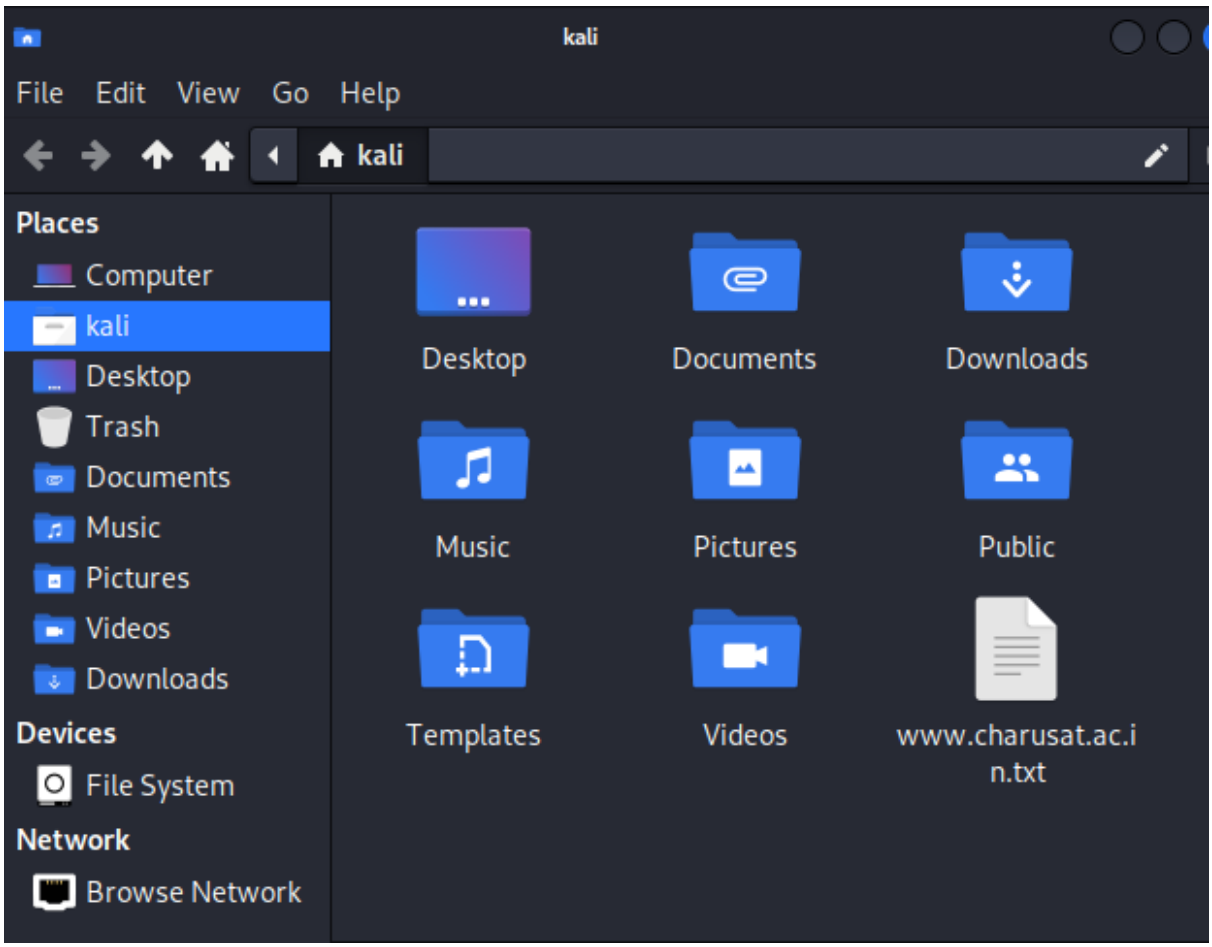


- Command: Dmitry -winsepo hackthissite.org
- We can use any website as target.

```
┌──(kali㉿kali)-[~]
└─$ dmitry -winsepo www.charusat.ac.in
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Writing output to 'www.charusat.ac.in.txt'

HostIP:185.151.30.139
HostName:www.charusat.ac.in

Gathered Inet-whois information for 185.151.30.139
---------------------------------------------------


inetnum:        185.151.30.0 - 185.151.30.255
netname:        CDN
descr:          Cloud Platform
country:        GB
admin-c:        HI825-RIPE
tech-c:         HI825-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-20i
created:        2018-09-19T13:27:19Z
last-modified:  2020-07-27T11:58:38Z
source:         RIPE

role:           Hosting Infrastructure
address:        Hawthorn House
admin-c:        AR36293-RIPE
nic-hdl:        HI825-RIPE
mnt-by:         MNT-20i
created:        2020-07-27T11:58:11Z
last-modified:  2020-07-27T11:59:21Z
source:         RIPE # Filtered

% Information related to '185.151.30.0/24AS48254'

route:          185.151.30.0/24
origin:         AS48254
mnt-by:         MNT-20i
created:        2018-09-20T12:52:20Z
last-modified:  2018-09-21T09:16:52Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.102.2 (BLAARKOP)
```

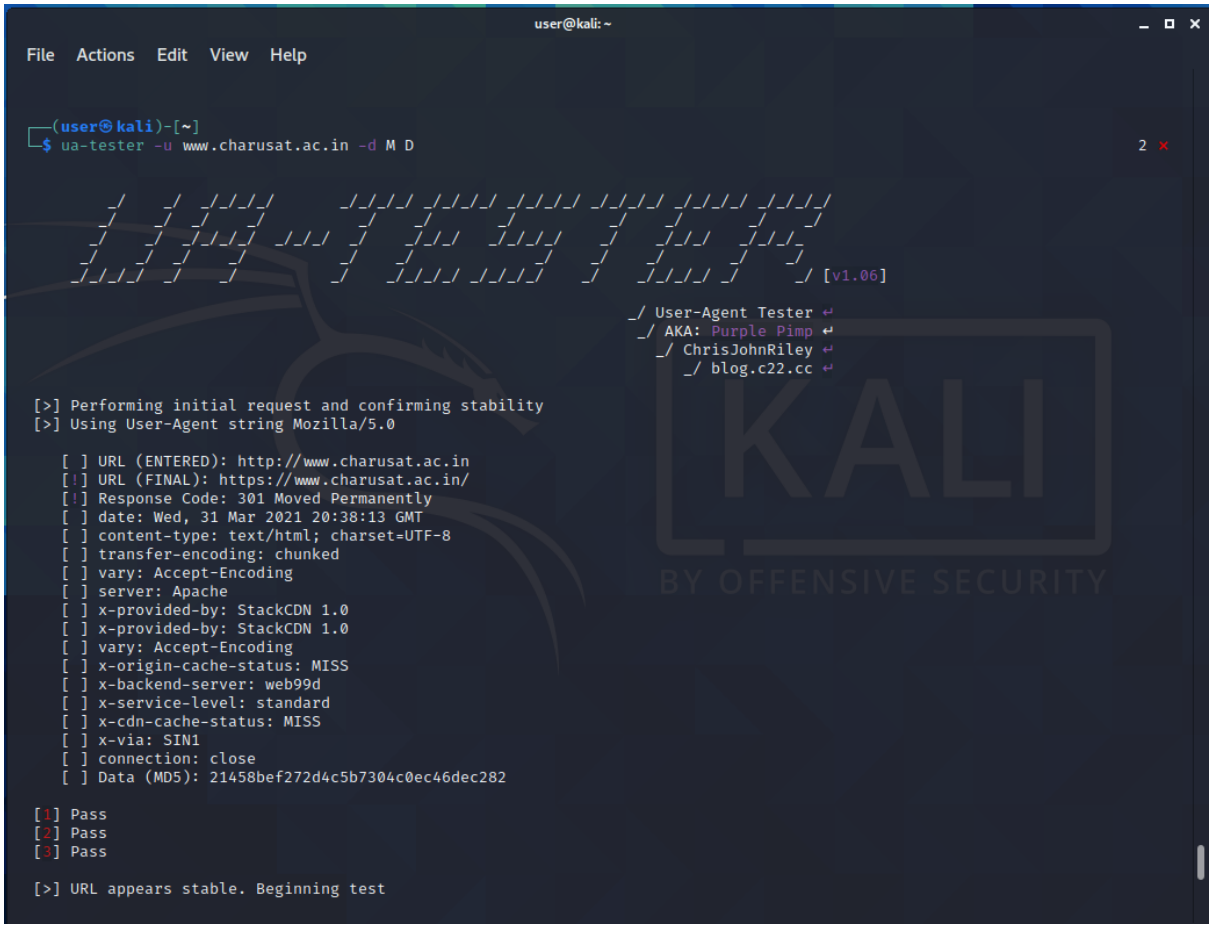
```
Domain Name: charusat.ac.in
Registry Domain ID: D3646415-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2019-08-21T09:39:44Z
Creation Date: 2009-06-03T05:11:55Z
Registry Expiry Date: 2028-06-03T05:11:55Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Charotar University of Science and Technology
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Gujarat
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
```

- The output is stored in “hackthissite.org.txt” file.



UA Tester:

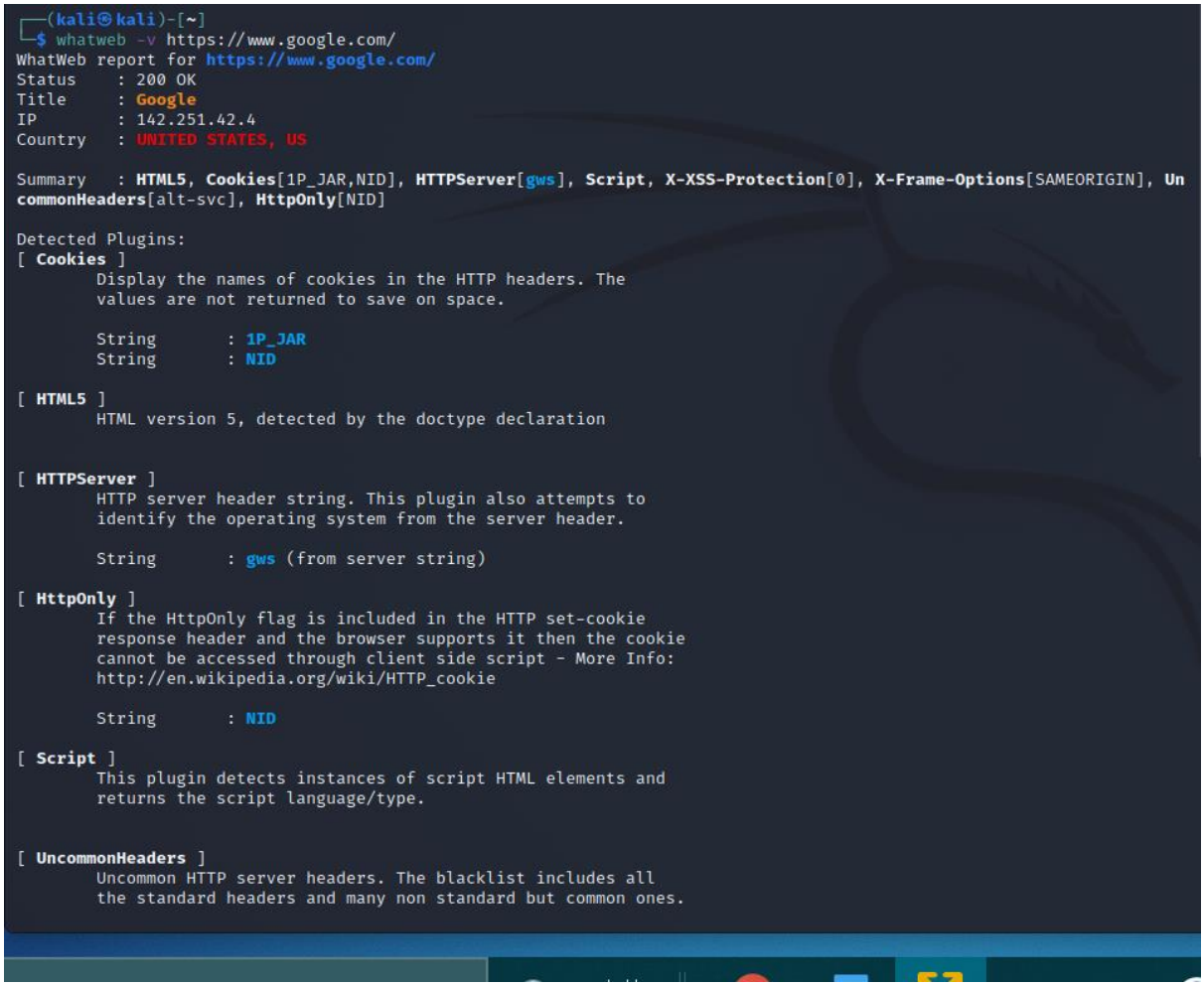
- We can use UA tester directly from terminal.
- Command: ua-tester -u www.charusat.ac.in -d M D



Whatweb:

- We can also use Whatweb directly from terminal.
- Command: whatweb -v https://charusat.ac.in/
- We can use any website we want as target.

```
┌──(kali㉿kali)-[~]
└─$ whatweb -v https://charusat.ac.in/
WhatWeb report for https://charusat.ac.in/
Status    : 200 OK
Title     : CHARUSAT | Best Private University in Gujarat
IP        : <Unknown>
Country   : <Unknown>

Summary   : HTML5, Open-Graph-Protocol[homepage], HTTPServer[Apache], JQuery, MetaGenerator[Powered by Visual Compose
d-By[PHP/7.4.27], PHP[7.4.27], Meta-Author[CHARUSAT Web Team], X-UA-Compatible[ie=edge], Frame, PoweredBy[Visual], X-
e-level,x-backend-server,x-cdn-cache-status,x-via], probably WordPress

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ Bootstrap ]
        Bootstrap is an open source toolkit for developing with
        HTML, CSS, and JS.

        Website     : https://getbootstrap.com/

[ Email ]
        Extract email addresses. Find valid email address and
        syntactically invalid email addresses from mailto: link
        tags. We match syntactically invalid links containing
        mailto: to catch anti-spam email addresses, eg. bob at
        gmail.com. This uses the simplified email regular
        expression from
        http://www.regular-expressions.info/email.html for valid
        email address matching.

        String      : info@charusat.ac.in

[ Frame ]
        This plugin detects instances of frame and iframe HTML
```



CONCLUSION:

- In this practical, we learned tools like Dmitry, UA-tester and Whatweb for information gathering.