**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

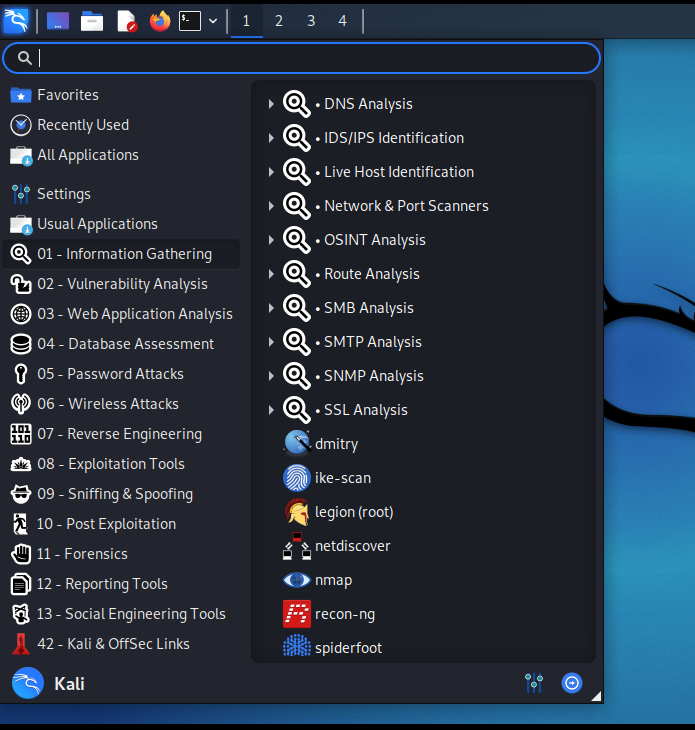
1. **UA-Tester:**

* 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.

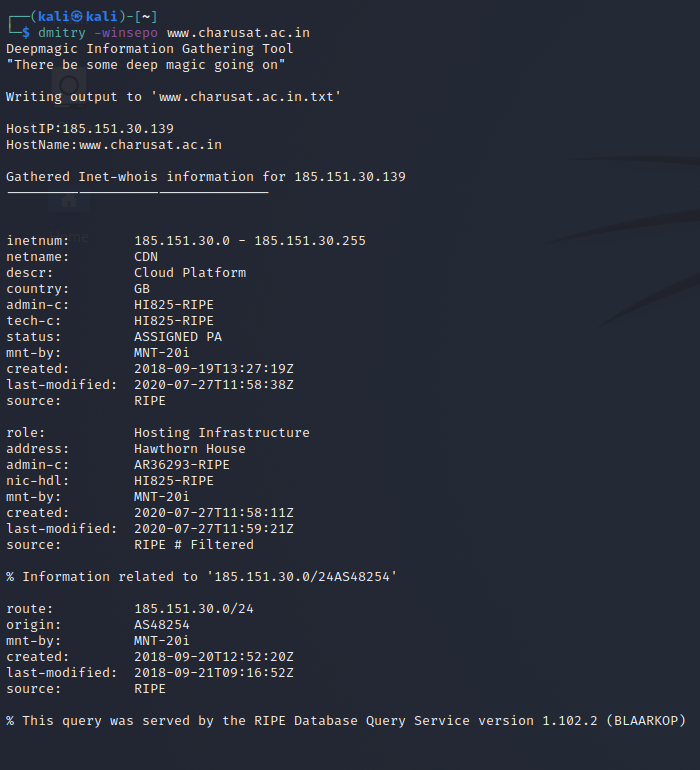
1. **Whatweb:**
   1. WhatWeb identifies websites.
   2. Its goal is to answer the question, “What is that Website?”.
   3. WhatWeb recognizes web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices. WhatWeb has over 1700 plugins, each to recognise something different.
   4. WhatWeb also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.
   5. WhatWeb can be stealthy and fast, or thorough but slow.
   6. WhatWeb supports an aggression level to control the trade off between speed and reliability.
   7. When you visit a website in your browser, the transaction includes many hints of what web technologies are powering that website.
   8. Sometimes a single webpage visit contains enough information to identify a website but when it does not, WhatWeb can interrogate the website further.
   9. The default level of aggression, called ‘stealthy’, is the fastest and requires only one HTTP request of a website.
   10. 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

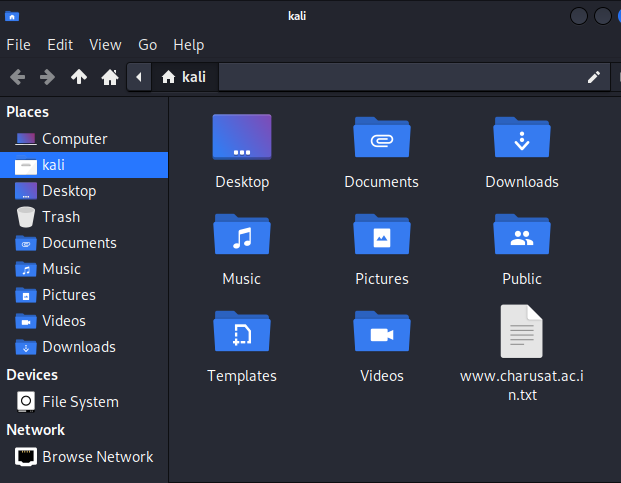


* Command: Dmitry -winsepo hackthissite.org
* We can use any website as target.



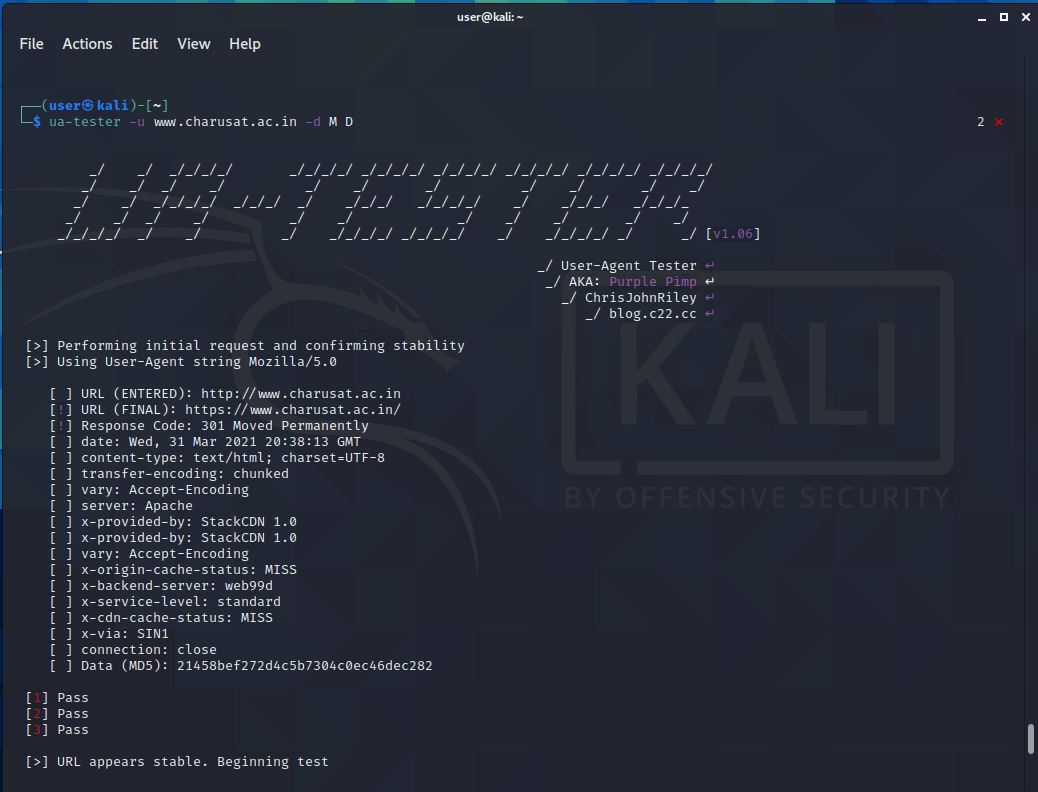


* The output is stored in “hackthissite.org.txt” file.



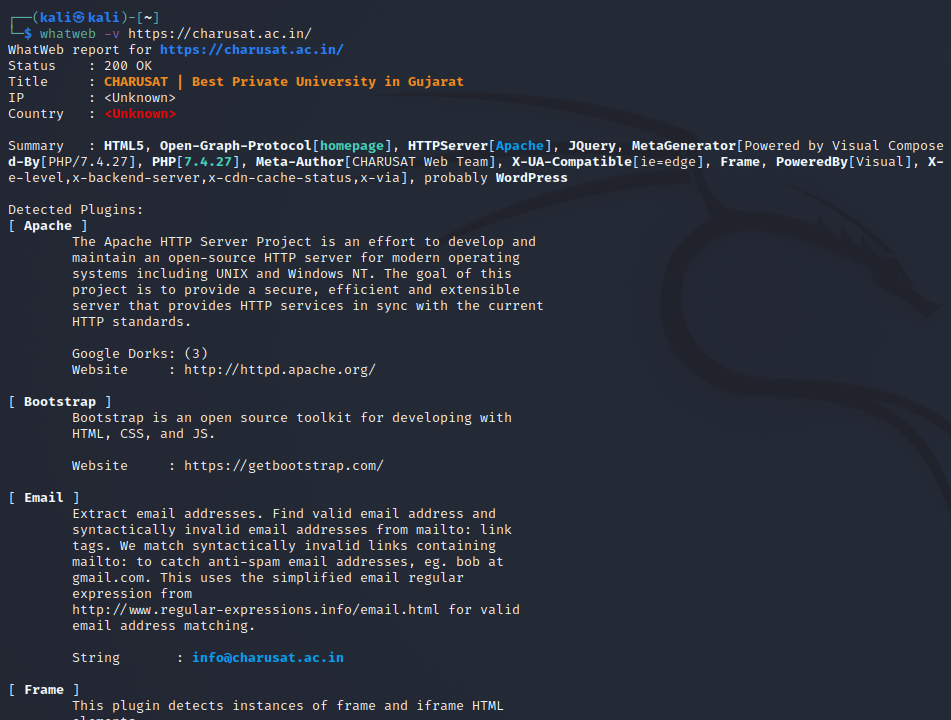
**UA Tester:**

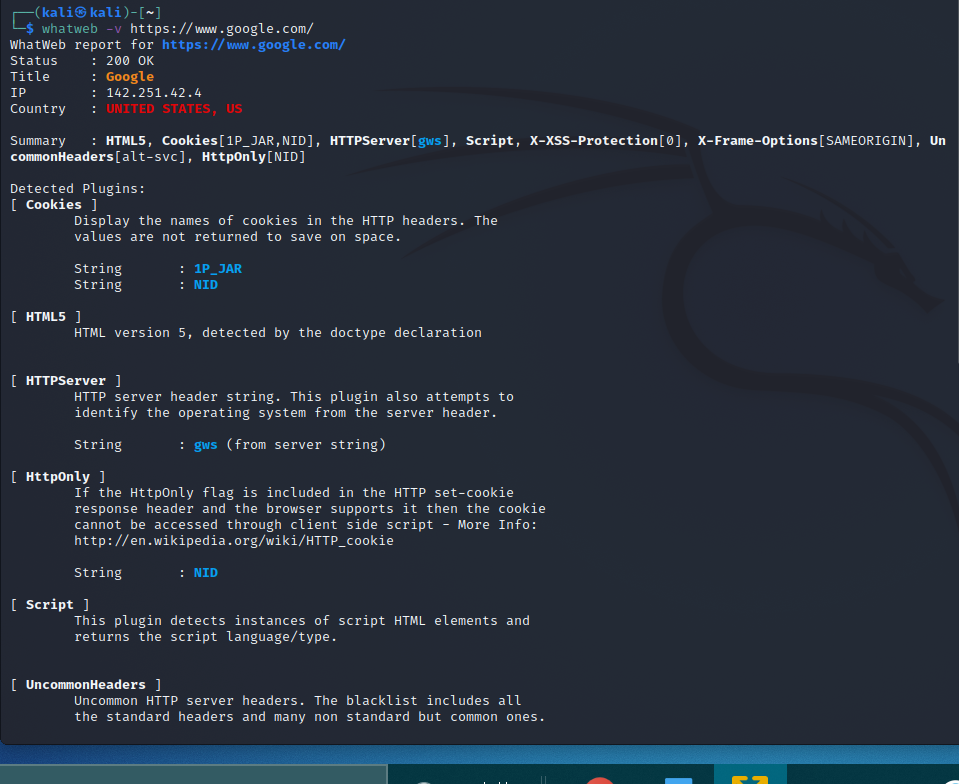
* We can use UA tester directly from terminal.
* Command: ua-tester -u [www.charusat.ac.in](http://www.charusat.ac.in) -d M D



**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.





**CONCLUSION:**

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