

PRACTICAL: 3

AIM:

Footprinting is the process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment. Footprinting can reveal system vulnerabilities and improve the ease with which they can be exploited. It is also known as reconnaissance. Study practical approach to implement Footprinting: Gathering Target Information making use of following tools:

Dmitry – Deepmagic

UA Tester

Whatweb

THEORY:

DMITRY: DMitry (Deepmagic Information Gathering Tool) is an open-source Linux CLI tool developed by James Greig. Coded in C. DMitry is a powerful information gathering tool that aims to gather as much information about a host that is possible. Features include subdomains search, email addresses, uptime information, system & server data, TCP port scan, whois info lookup, DMitry is a modular program that allows user-specified modules. DMitry is easy to use and removes the need to enter multiple commands. DMitry is preinstalled in Kali Linux, if you are using another distribution of Linux that does not come with DMitry preinstalled but you can install DMitry from the source. DMitry is part of a subset of information gathering tools included in Kali Linux. The purpose of these tools is to help attackers identify information about a target, to assist with locating potential attack vectors that may work on the system.

UA-Tester: UA-Tester is designed to automatically check a given URL using a list of standard and non-standard User Agent strings and provides us valuable information for how websites respond to certain browsers, bots or tools. This tool is written in Python by Chris John Riley. It also tries various options like setting cookie, redirection, URL-stability (whether the URL expires or not) and a lot more. Now I am not sure of how this might be used as a WAF-Tester. But I think, all these options & tests you perform resemble a Nmap scan.

WHATWEB: With WhatWeb you can get the details of any website, which plugin is being used, what is their version, which cms are being used here or which website is being used by the platform, which web framework should be used on the website, What security is being used here, the website's email address, account id, etc.

With the WhatWeb tool, you can also easily scan your local network whether any website or webserver is running there or not, this tool is made in Ruby language, which has more than 1800 plugins to manage the website. Uses that can extract a lot of useful information from a website.

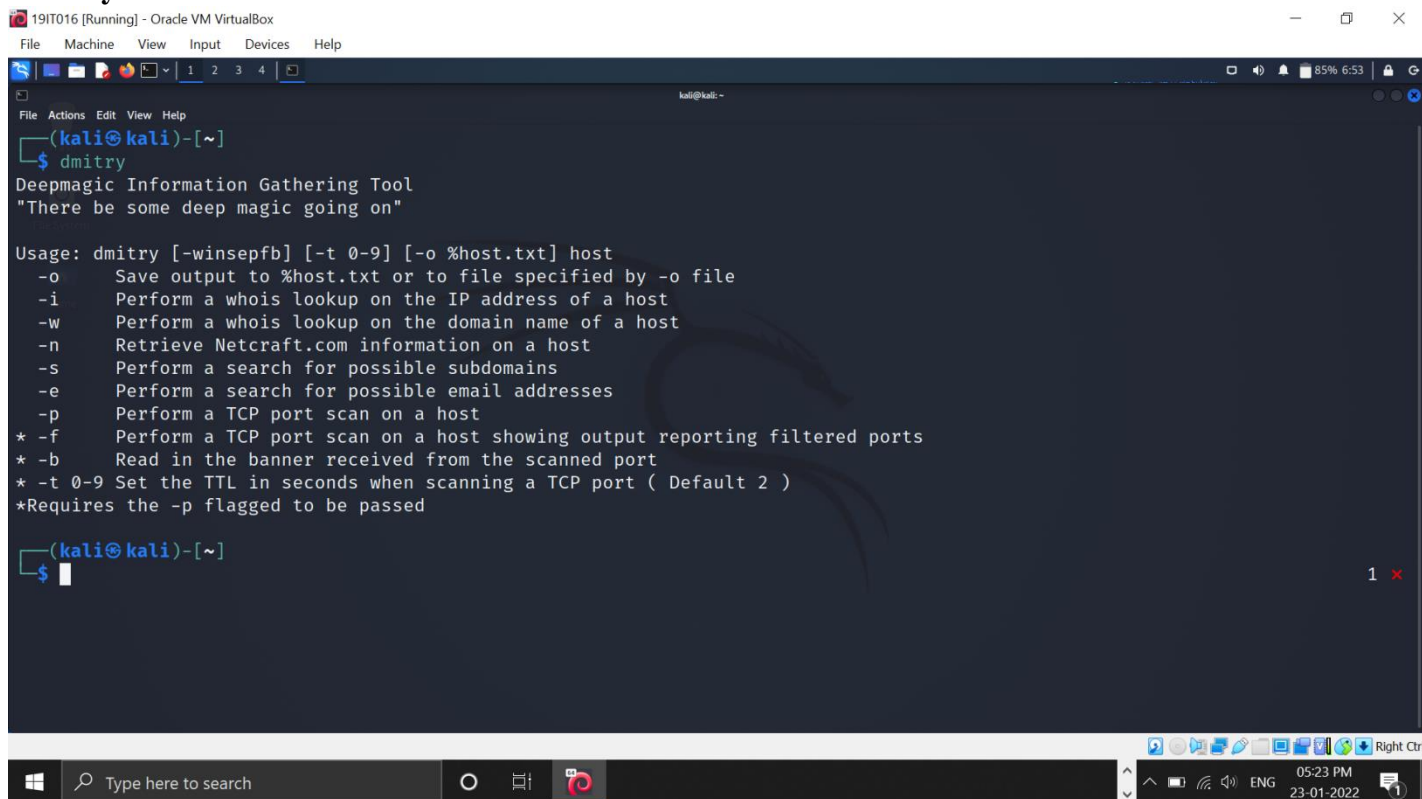
Most WhatWeb plugins are thorough and recognise a range of cues from subtle to obvious. For example, most WordPress websites can be identified by the meta HTML tag, e.g. ””, but a minority of WordPress websites remove this identifying tag but this does not thwart WhatWeb. The WordPress WhatWeb plugin has over 15 tests, which include checking the favicon, default installation files, login pages, and checking for “/wp-content/” within relative links.

CODE:**Dmitry:**

```
dmitry -winsepo 19IT016_dmitry.txt flipkart.com
```

UA-Tester:**Whatweb:**

```
Whatweb -v amazon.com
```

OUTPUT:**Dmitry:**A screenshot of a Kali Linux terminal window titled "19IT016 [Running] - Oracle VM VirtualBox". The terminal shows the command "dmitry" being entered, which outputs "Deepmagic Information Gathering Tool" and "There be some deep magic going on". Below this, the usage instructions for dmitry are displayed, including options for saving output, performing whois lookups, retrieving Netcraft.com information, searching for subdomains and email addresses, and performing TCP port scans. The terminal prompt "(kali@kali)-[~]" is visible at the bottom of the terminal window.

```
19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
(kali@kali)-[~]
$ dmitry
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepf] [-t 0-9] [-o %host.txt] host
-o Save output to %host.txt or to file specified by -o file
-i Perform a whois lookup on the IP address of a host
-w Perform a whois lookup on the domain name of a host
-n Retrieve Netcraft.com information on a host
-s Perform a search for possible subdomains
-e Perform a search for possible email addresses
-p Perform a TCP port scan on a host
* -f Perform a TCP port scan on a host showing output reporting filtered ports
* -b Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
* Requires the -p flagged to be passed

(kali@kali)-[~]
$
```

Open dmitry console in your kali os. Here we can see bunch of use cases of dmitry.

```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

(kali@kali)~$ dmitry -winsepo 19IT016_dmitry.txt flipkart.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Writing output to '19IT016_dmitry.txt'

HostIP:163.53.78.110
HostName:flipkart.com

Gathered Inet-whois information for 163.53.78.110

inetnum:      163.35.0.0 - 163.61.255.255
netname:      NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:        IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks:      For registration information,
remarks:      you can consult the following sources:
remarks:
remarks:      IANA
remarks:      http://www.iana.org/assignments/ipv4-address-space
remarks:      http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:      http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:      AFRINIC (Africa)
remarks:      http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:      APNIC (Asia Pacific)
remarks:      http://www.apnic.net/ whois.apnic.net
remarks:
remarks:      ARIN (Northern America)
remarks:      http://www.arin.net/ whois.arin.net
remarks:
remarks:      LACNIC (Latin America and the Caribbean)
remarks:      http://www.lacnic.net/ whois.lacnic.net
remarks:

```

We are going to fetch some information of bWAPP website and will store that information in 19IT016_dmitry.txt file.

This is the file generated by dmitry command and we have stored all of the information in this file.

These are some information related to bWAPP website route, source, creation date and origin.

```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

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

Gathered Inic-whois information for flipkart.com

Domain Name: FLIPKART.COM
Registry Domain ID: 1009529768_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-05-13T12:46:17Z
Creation Date: 2007-06-03T19:32:20Z
Registry Expiry Date: 2025-06-03T19:32:20Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: SDNS14.ULTRADNS.BIZ
Name Server: SDNS14.ULTRADNS.COM
Name Server: SDNS14.ULTRADNS.NET
Name Server: SDNS14.ULTRADNS.ORG
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-01-23T07:32:45Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois

```

In these image there are information of domain name, id, website updation date, registrar's url, name and many more things.

```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.

Gathered Netcraft information for flipkart.com

Retrieving Netcraft.com information for flipkart.com
  
```

These are some terms and conditions related to website.

```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
Gathered Netcraft information for flipkart.com

Retrieving Netcraft.com information for flipkart.com
Netcraft.com Information gathered

Gathered Subdomain information for flipkart.com

Searching Google.com:80 ...
HostName:www.flipkart.com
HostIP:163.53.78.110
HostName:seller.flipkart.com
HostIP:163.53.78.21
HostName:m.flipkart.com
HostIP:163.53.78.110
HostName:stories.flipkart.com
HostIP:192.124.249.115
HostName:affiliate.flipkart.com
HostIP:163.53.78.102
Searching Altavista.com:80...
Found 5 possible subdomain(s) for host flipkart.com, Searched 0 pages containing 0 results

Gathered E-Mail information for flipkart.com

Searching Google.com:80 ...
krishna.ku@flipkart.com
Searching Altavista.com:80...
Found 1 E-Mail(s) for host flipkart.com, Searched 0 pages containing 0 results

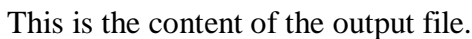
Gathered TCP Port information for 163.53.78.110

Port      State
80/tcp    open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed
Error: Unable to close file stream writing to 19IT016_dmitry.txt

(kali@kali)-[~]
$
  
```

In this image we can see port information and email information of the website.



Open whatweb console. Here we can see some information about whatweb and it's uses.

```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali:~$ whatweb -v amazon.com
WhatWeb report for http://amazon.com
Status : 301 Moved Permanently
Title : 301 Moved Permanently
IP : 205.251.242.103
Country : UNITED STATES, US

Summary : RedirectLocation[https://amazon.com/], HTTPServer[Server]

Detected Plugins:
[ HTTPServer ]
  HTTP server header string. This plugin also attempts to
  identify the operating system from the server header.

  String : Server (from server string)

[ RedirectLocation ]
  HTTP Server string location. used with http-status 301 and
  302

  String : https://amazon.com/ (from location)

HTTP Headers:
  HTTP/1.1 301 Moved Permanently
  Server: Server
  Date: Sun, 23 Jan 2022 12:18:47 GMT
  Content-Type: text/html
  Content-Length: 179
  Connection: keep-alive
  Location: https://amazon.com/
  
```

we can see the ip address,status and country of the website.And also we can see more information related to plugins and technologies used in the website.

```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali:~$ whatweb https://www.amazon.com/
WhatWeb report for https://www.amazon.com/
Status : 200 OK
Title : Amazon.com. Spend less. Smile more.
IP : 49.44.165.41
Country : INDIA, IN

Summary : Object, Content-Language[en-US], HttpOnly[sp-cdn], HTML5, Frame, UncommonHeaders[x-amz-rid,accept-ch-lifetime,x-content-type-options,accept-ch,pe
atus], X-UA-Compatible[IE=edge], Script[a-state,application/json,text/javascript,text/x-lazy-loaded-content], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1
ransport-Security[max-age=474747; includeSubDomains; preload], Open-Graph-Protocol[164734381262], Cookies[i18n-prefs,session-id,session-id-time,skin,sp-cdn]

Detected Plugins:
[ Content-Language ]
  Detect the content-language setting from the HTTP header.

  String : en-US

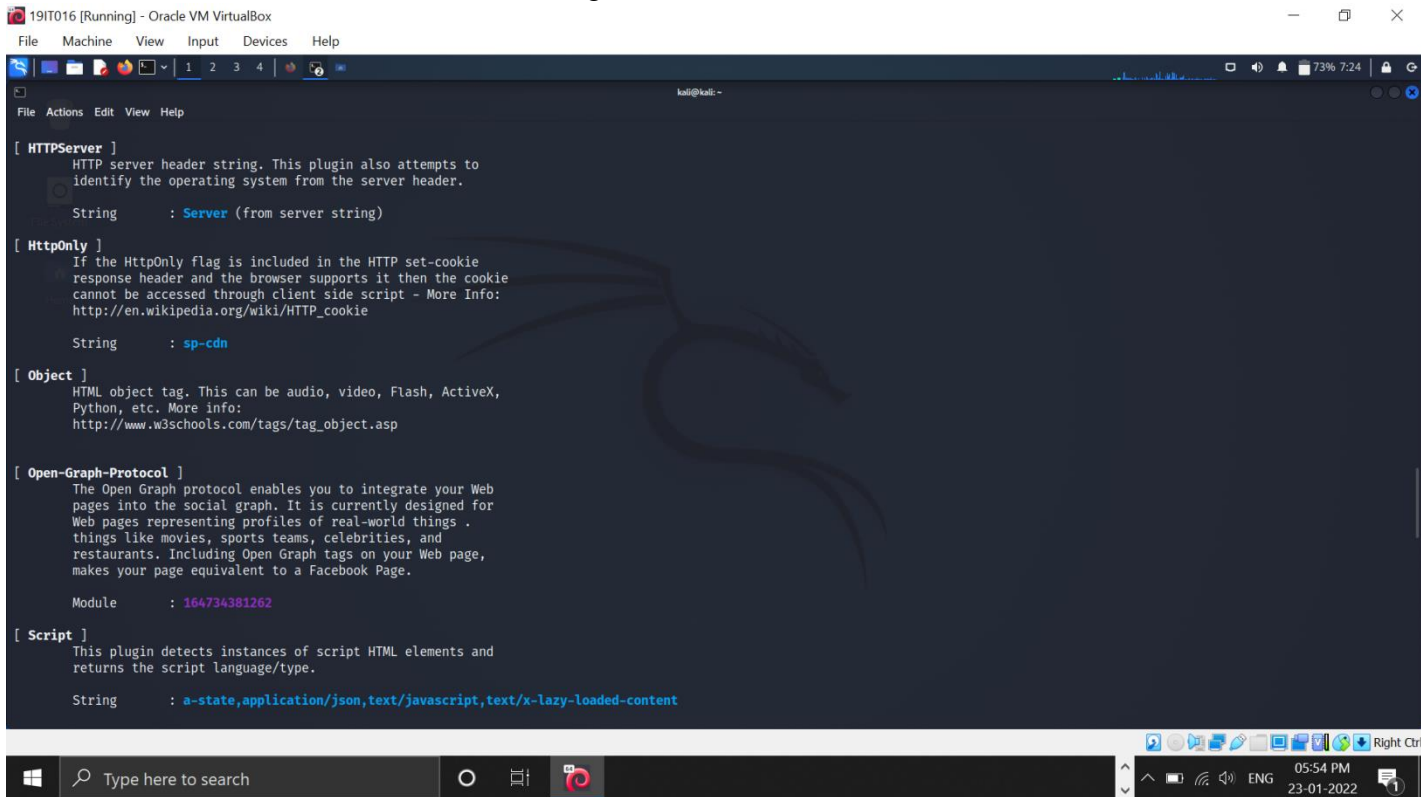
[ Cookies ]
  Display the names of cookies in the HTTP headers. The
  values are not returned to save on space.

  String : session-id
  String : session-id-time
  String : i18n-prefs
  String : sp-cdn
  String : skin

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

[ HTML5 ]
  HTML version 5, detected by the doctype declaration
  
```

Here are some more information of technologies this website had used.



```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali:~$

[ HTTPServer ]
  HTTP server header string. This plugin also attempts to
  identify the operating system from the server header.
  String      : Server (from server string)

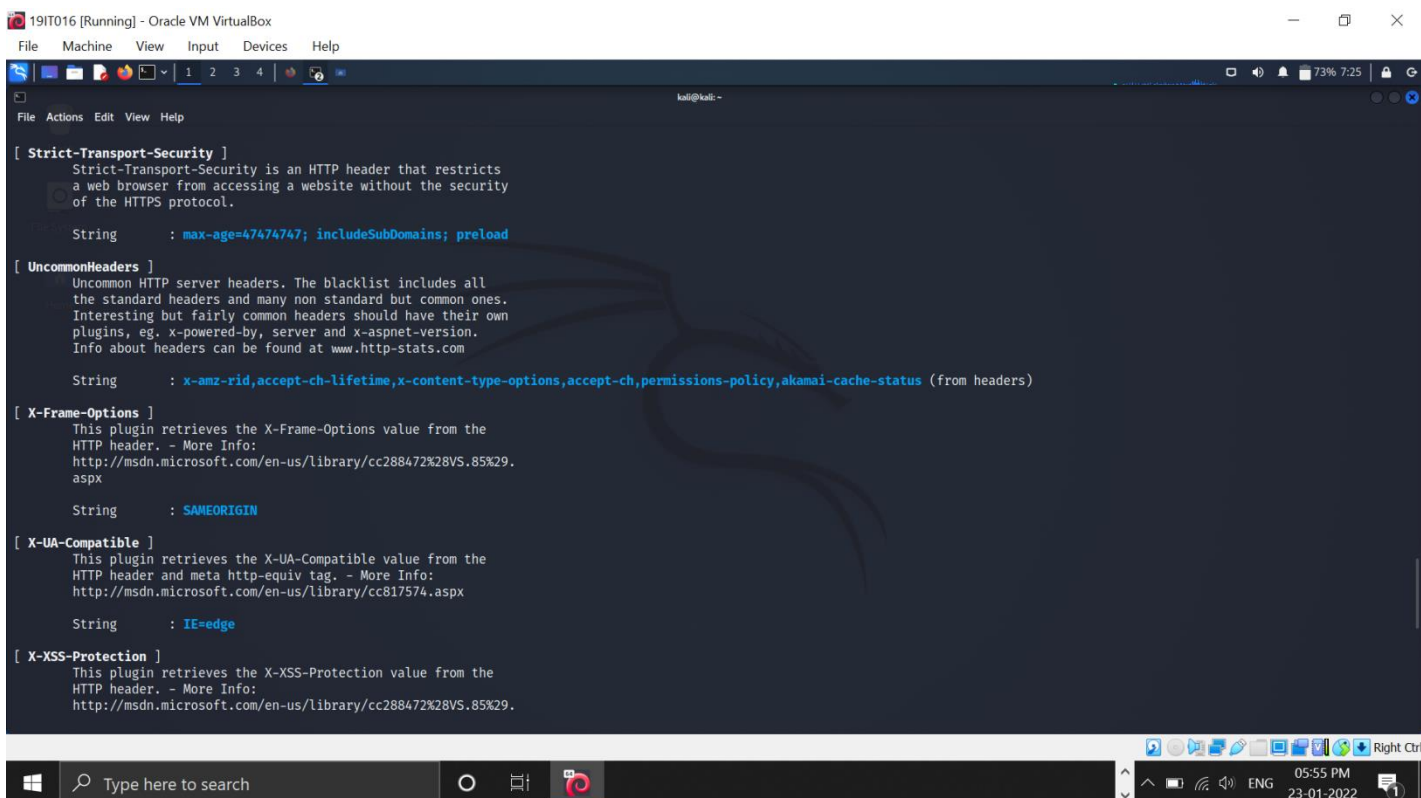
[ HttpOnly ]
  If the HttpOnly flag is included in the HTTP set-cookie
  response header and the browser supports it then the cookie
  cannot be accessed through client side script - More Info:
  http://en.wikipedia.org/wiki/HTTP_cookie
  String      : sp-cdn

[ Object ]
  HTML object tag. This can be audio, video, Flash, ActiveX,
  Python, etc. More info:
  http://www.w3schools.com/tags/tag_object.asp

[ Open-Graph-Protocol ]
  The Open Graph protocol enables you to integrate your Web
  pages into the social graph. It is currently designed for
  Web pages representing profiles of real-world things .
  things like movies, sports teams, celebrities, and
  restaurants. Including Open Graph tags on your Web page,
  makes your page equivalent to a Facebook Page.
  Module      : 164734381262

[ Script ]
  This plugin detects instances of script HTML elements and
  returns the script language/type.
  String      : a-state,application/json,text/javascript,text/x-lazy-loaded-content
  
```

Here we can see which version of jquery is used. Which script is used.



```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali:~$

[ Strict-Transport-Security ]
  Strict-Transport-Security is an HTTP header that restricts
  a web browser from accessing a website without the security
  of the HTTPS protocol.
  String      : max-age=47474747; includeSubDomains; preload

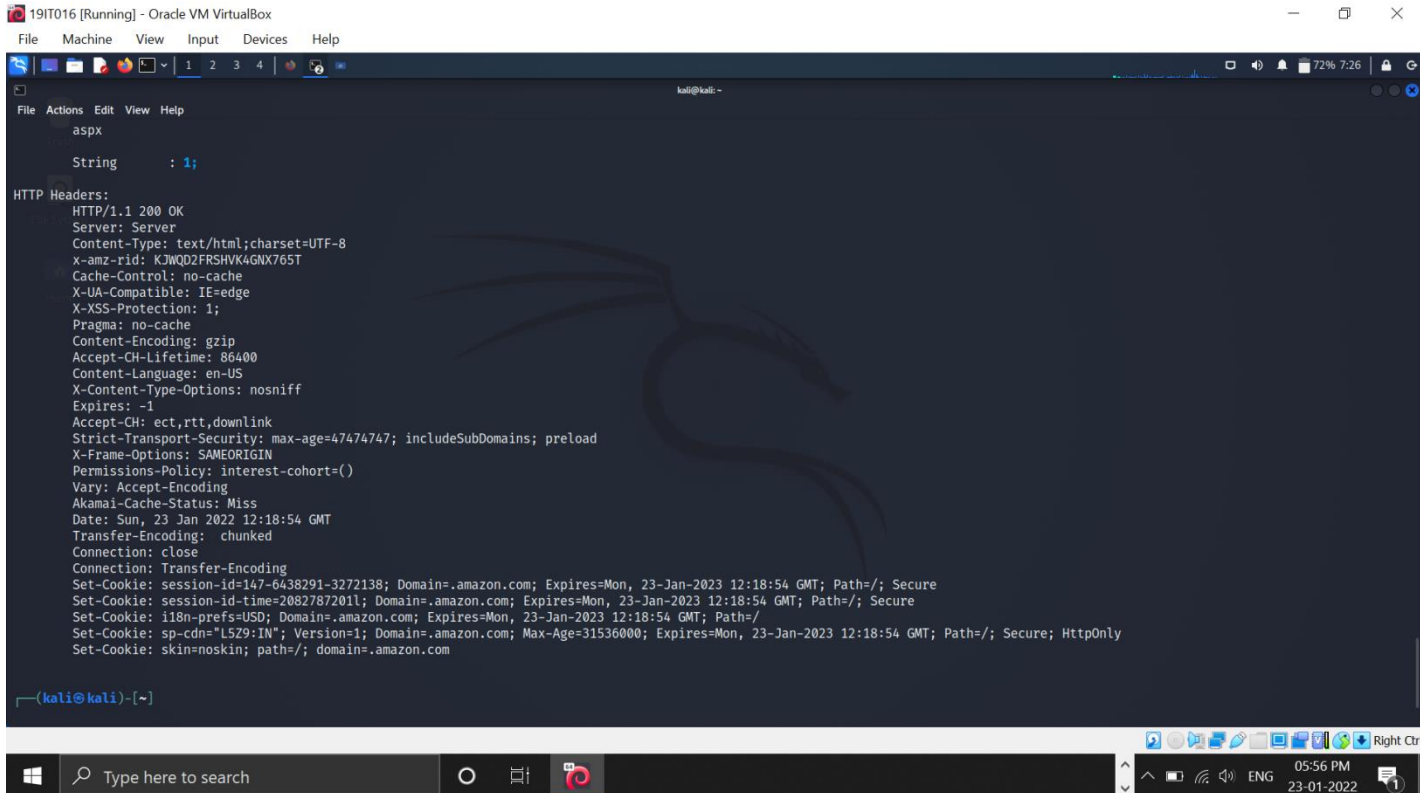
[ UncommonHeaders ]
  Uncommon HTTP server headers. The blacklist includes all
  the standard headers and many non standard but common ones.
  Interesting but fairly common headers should have their own
  plugins, eg. x-powered-by, server and x-aspnet-version.
  Info about headers can be found at www.http-stats.com
  String      : x-amz-rid,accept-ch-lifetime,x-content-type-options,accept-ch,permissions-policy,akamai-cache-status (from headers)

[ X-Frame-Options ]
  This plugin retrieves the X-Frame-Options value from the
  HTTP header. - More Info:
  http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.aspx
  String      : SAMEORIGIN

[ X-UA-Compatible ]
  This plugin retrieves the X-UA-Compatible value from the
  HTTP header and meta http-equiv tag. - More Info:
  http://msdn.microsoft.com/en-us/library/cc817574.aspx
  String      : IE=edge

[ X-XSS-Protection ]
  This plugin retrieves the X-XSS-Protection value from the
  HTTP header. - More Info:
  http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.aspx
  
```

Here we can see what is strict-transport-security what is max string strength an all.



```
19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: -
File Actions Edit View Help
aspx
String      : 1;
HTTP Headers:
HTTP/1.1 200 OK
Server: Server
Content-Type: text/html; charset=UTF-8
x-amz-rid: KJWQD2FRSHVK4GNX765T
Cache-Control: no-cache
X-UA-Compatible: IE=edge
X-XSS-Protection: 1;
Pragma: no-cache
Content-Encoding: gzip
Accept-CH-Lifetime: 86400
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: -1
Accept-CH: ect,rtt,downlink
Strict-Transport-Security: max-age=47474747; includeSubDomains; preload
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Vary: Accept-Encoding
Akamai-Cache-Status: Miss
Date: Sun, 23 Jan 2022 12:18:54 GMT
Transfer-Encoding: chunked
Connection: close
Connection: Transfer-Encoding
Set-Cookie: session-id=147-6438291-3272138; Domain=.amazon.com; Expires=Mon, 23-Jan-2023 12:18:54 GMT; Path=/; Secure
Set-Cookie: session-id-time=20827872011; Domain=.amazon.com; Expires=Mon, 23-Jan-2023 12:18:54 GMT; Path=/; Secure
Set-Cookie: i18n-prefs=USD; Domain=.amazon.com; Expires=Mon, 23-Jan-2023 12:18:54 GMT; Path=/
Set-Cookie: sp-cdn="L5Z9:IN"; Version=1; Domain=.amazon.com; Max-Age=31536000; Expires=Mon, 23-Jan-2023 12:18:54 GMT; Path=/; Secure; HttpOnly
Set-Cookie: skin=noskin; path=/; domain=.amazon.com

(kali@kali)-[~]
```

Some more information related to website technologies and plugins.

LATEST APPLICATIONS:

With the use of Dmitry you can:

- Perform an Internet Number whois lookup.
- Retrieve possible uptime data, system and server data.
- Perform an E-Mail address search on a target host.

UA-tester is used 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.

UA-tester is also used for:

- Initial version.
- Improved redirect handling.
- Released for limited Alpha testing
- Changed handling of default UA strings (no need for -d), added verbose output, single mode - s, handler for URL without HTTP://
- Added Android default UA string, altered -h to reflect changes to usage
- Expanded on user feedback to avoid confusion of results, added feedback to clarify results, expanded default user agent strings (categorized)

WhatWeb recognises web technologies including content management systems (CMS).

WhatWeb has over 1800 plugins, each to recognise something different.

WhatWeb identifies:

- Platform
- CMS platform
- Type of Script
- Google Analytics
- Webserver Platform
- IP address, Country
- Plugins & their libraries used
- Server Headers, Cookies and a lot more

LEARNING OUTCOME:

In this practical we have learned three useful kali linux tool which are used by many penetration testers and hackers for information gathering. First we have seen the what are the uses of dmitry, ua-tester and whatweb tool and then we used these tools on our kali os to gain practical knowledge. We learned that dmitry is used for information gathering, ua-tester is used for checking whether a website provides different pages for different user agents like for mobile, desktop bots etc. And whatweb is used to check which technologies website has used for creation of website.

REFERENCES:

1. Dmitry : https://www.youtube.com/watch?v=_zd3goGLM7Q
 2. UA Tester : <https://www.youtube.com/watch?v=WsTupi32ZYE>
- WhatWeb : <https://www.youtube.com/watch?v=Fx9sIgxcNwU>