Whatweb is the perfect name for this tool. Simply it answers the question, "What is that Website?" Whatweb can identify all sorts of information about a live website, like:

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

Whatweb offers both passive scanning and aggressive testing. Passive scanning just extracts data from HTTP headers simulating a normal visit. Aggressive options get deeper with recursion & various types of queries & identify all technologies just like a vulnerability scanner.

So a pentester can use this tool as both a recon tool & vulnerability scanner. There are various other features like proxy support, scan tuning, scanning a range of IPs, spidering etc.

Homepage: http://www.morningstarsecurity.com/research/whatweb

Options

```
Syntax: whatweb [options] <URLs>
```

Options is deprecated. Only major options or listed. Visit tool homepage for complete options

```
TARGET SELECTION:
<URLs>                  Enter URLs, filenames or nmap-format IP ranges.
--input-file=FILE, -i Identify URLs found in FILE, eg. -i /dev/stdin

TARGET MODIFICATION:
--url-prefix            Add a prefix to target URLs
--url-suffix            Add a suffix to target URLs
--url-pattern           Insert the targets into a URL. Requires --input-file,

AGGRESSION:
The aggression level controls the trade-off between speed/stealth and
reliability.
--aggression, -a=LEVEL Set the aggression level. Default: 1
Aggression levels are: 1,2,3 & 4

HTTP OPTIONS:
--user-agent, -U=AGENT Identify as AGENT instead of WhatWeb/0.4.8-dev.
--follow-redirect=WHEN Control when to follow redirects.Default: always
--max-redirects=NUM   Maximum number of contiguous redirects. Default: 10

AUTHENTICATION:
--user, -u=<user:password> HTTP basic authentication
Add session cookies with --header, e.g. --header "Cookie: SESSID=1a2b3c;"

PROXY:
--proxy                 <hostname[:port]> Set proxy hostname and port
Default: 8080
--proxy-user            <username:password> Set proxy user and password
```

```
PLUGINS:
--list-plugins, -l    List all plugins

OUTPUT:
--verbose, -v         Verbose output includes plugin descriptions. Use
twice for debugging.
--colour,--color=WHEN control whether colour is used. WHEN='always',
'never' or 'auto'
--quiet, -q           Do not display brief logging to STDOUT
--no-errors           Suppress error messages

LOGGING:
--log-brief=FILE      Log brief, one-line output
--log-verbose=FILE    Log verbose output
--log-xml=FILE        Log XML format

PERFORMANCE & STABILITY:
--max-threads, -t     Number of simultaneous threads. Default: 25.
--open-timeout        Time in seconds. Default: 15
--read-timeout        Time in seconds. Default: 30
--wait=SECONDS        Wait SECONDS between connections

HELP & MISCELLANEOUS:
--help, -h            This help
--debug               Raise errors in plugins
--version             Display version information. (WhatWeb 0.4.8-dev)
```

Lab 1: Perform Simple enumeration of websites over the internet.

In this lab, we will perform simple enumeration of websites. The result of this is we can get to know the technologies used in the website & webserver.

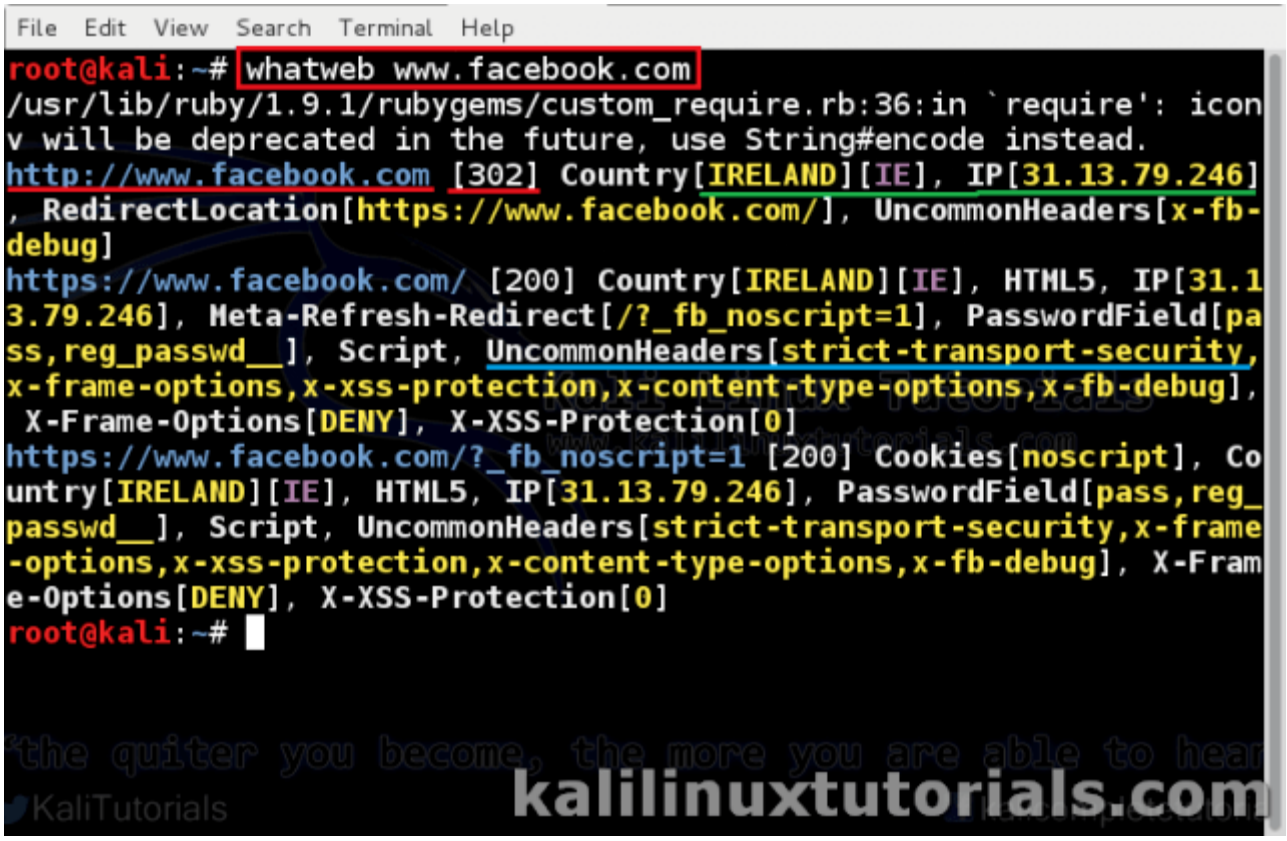
Note: Please don't use this against government or military websites without prior permission. The author of this article or tool itself are not responsible for any consequences if misused.

Scenario:

Attacker: Kali Linux VM

Target: www.facebook.com

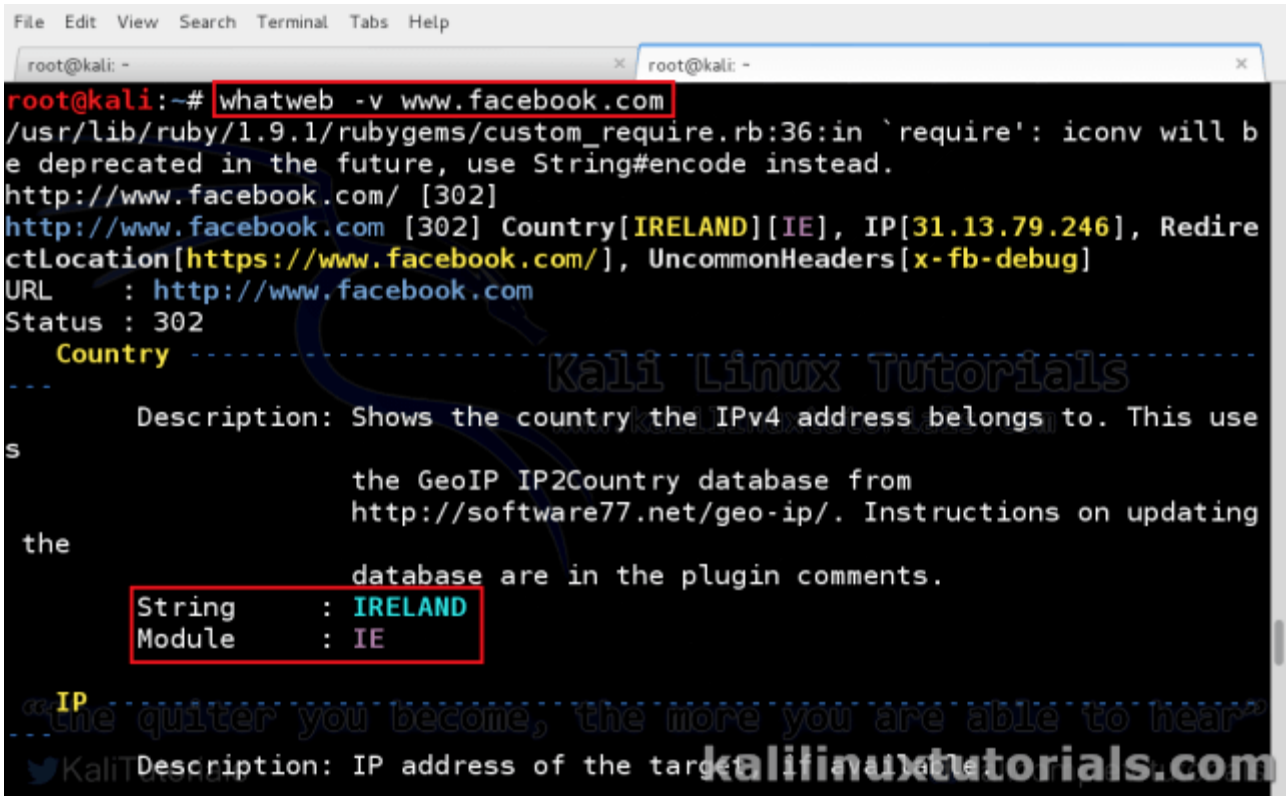
```
Command: whatweb www.facebook.com
```



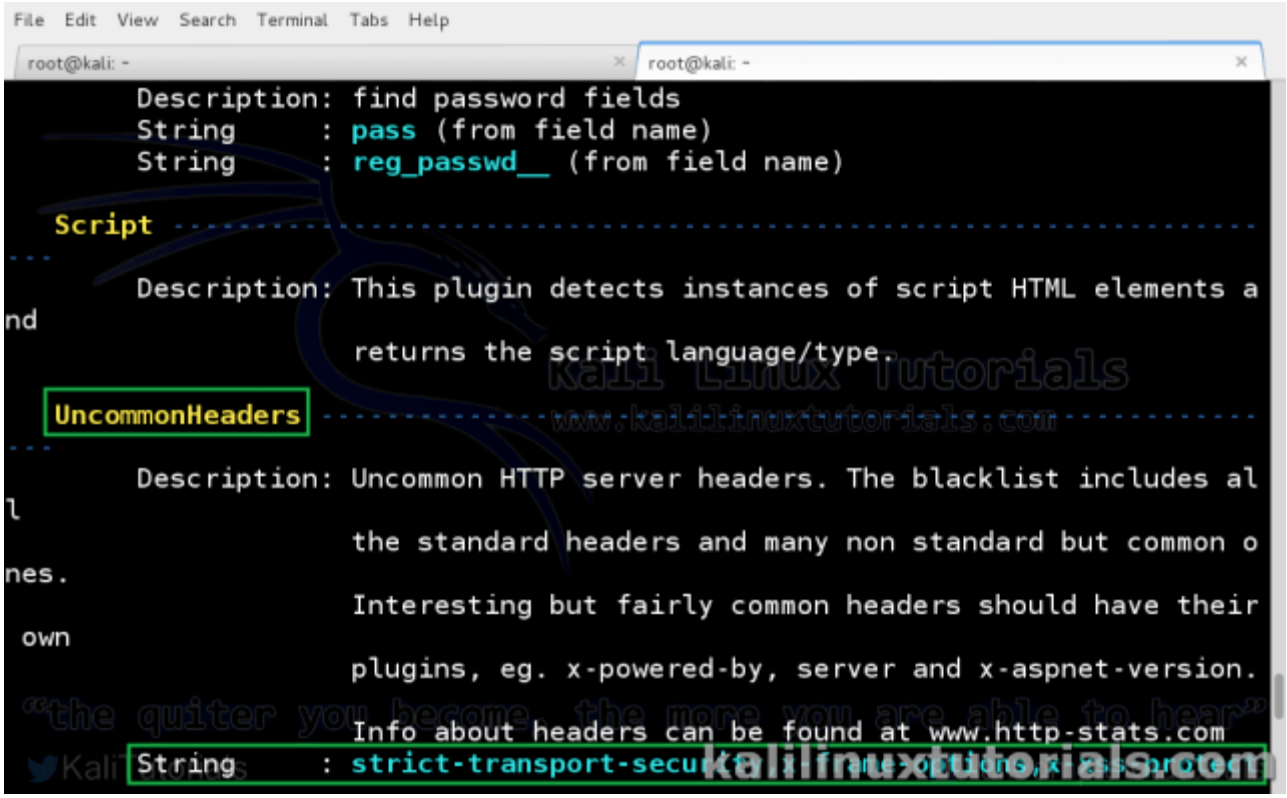
Basic Details

To give a more verbose Output

`Command: whatweb -v www.facebook.com`



Displaying Details about modules



Displaying Details about modules

Practically, how we can use this information for Vulnerability Analysis is that sometimes you may get that the webserver is an outdated version of Apache or IIS. Or sometimes, the website is running an old WordPress version vulnerable to many issues. Like that, you can find out the vulns & exploits for different versions of technologies used in the website.

Lab 2: Perform Enumeration of a range of websites

whatweb allows you to test for a range of IP addresses. In this lab, we test a range of IPs on a local network. This can be useful while doing Pentests inside a production network or sometimes like finding out a list of Web-UIs or cpanels on a range of IPs.

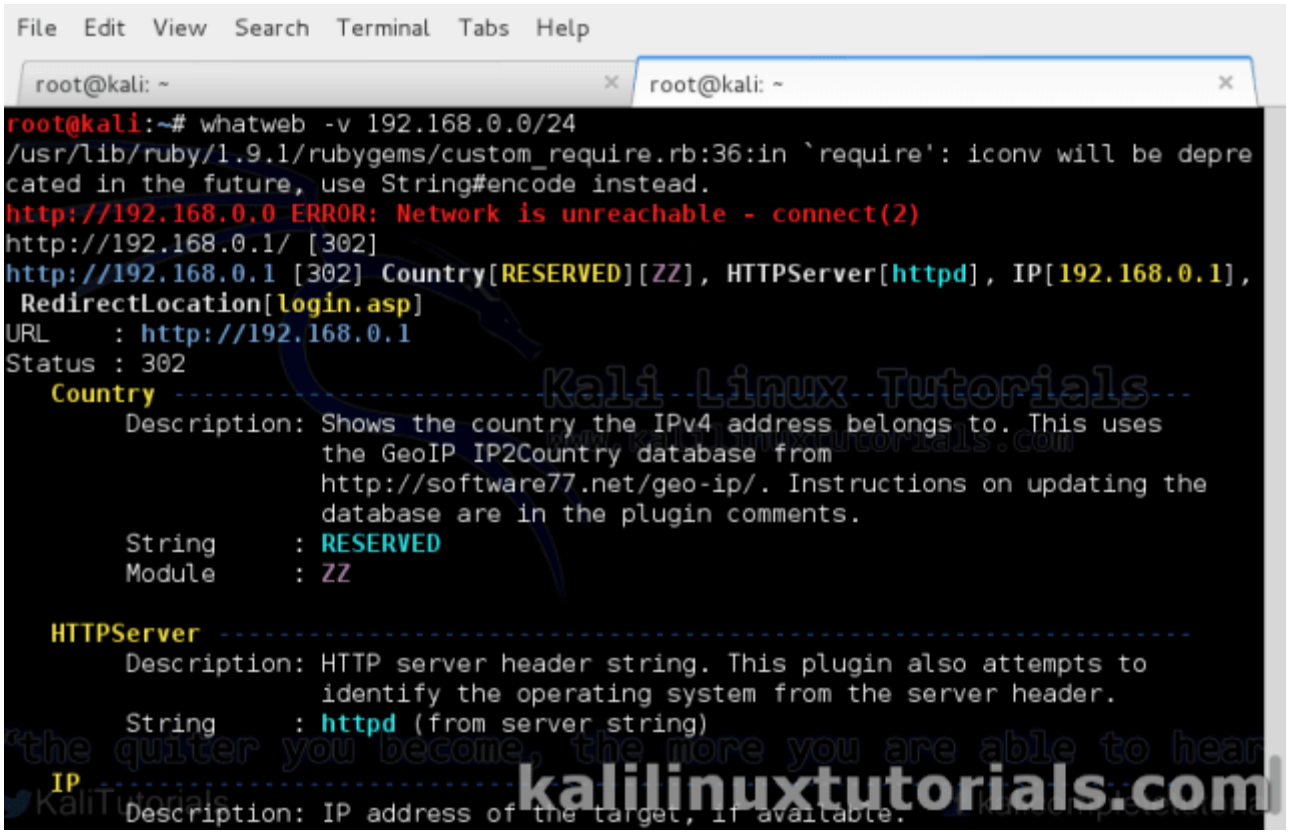
Scenario:

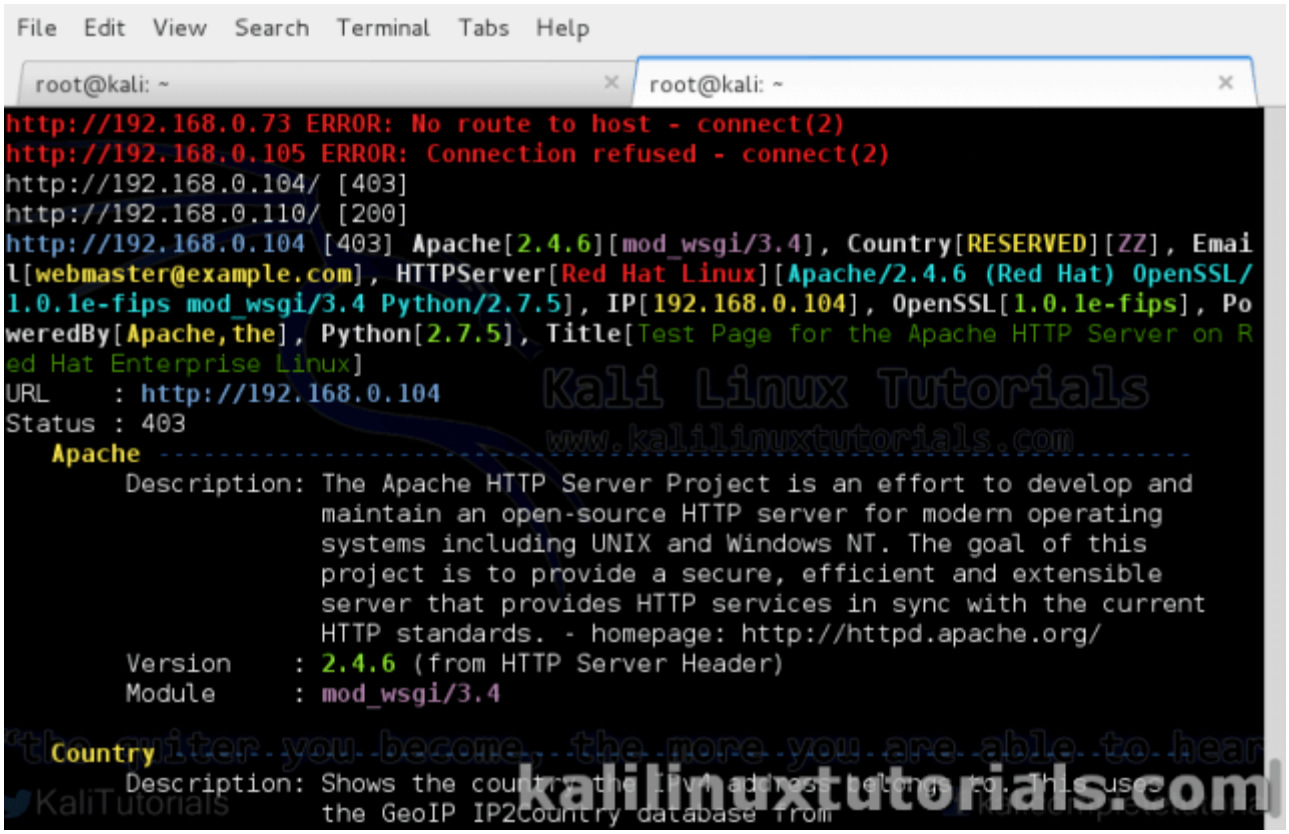
Internal Network : 192.168.0.0/24

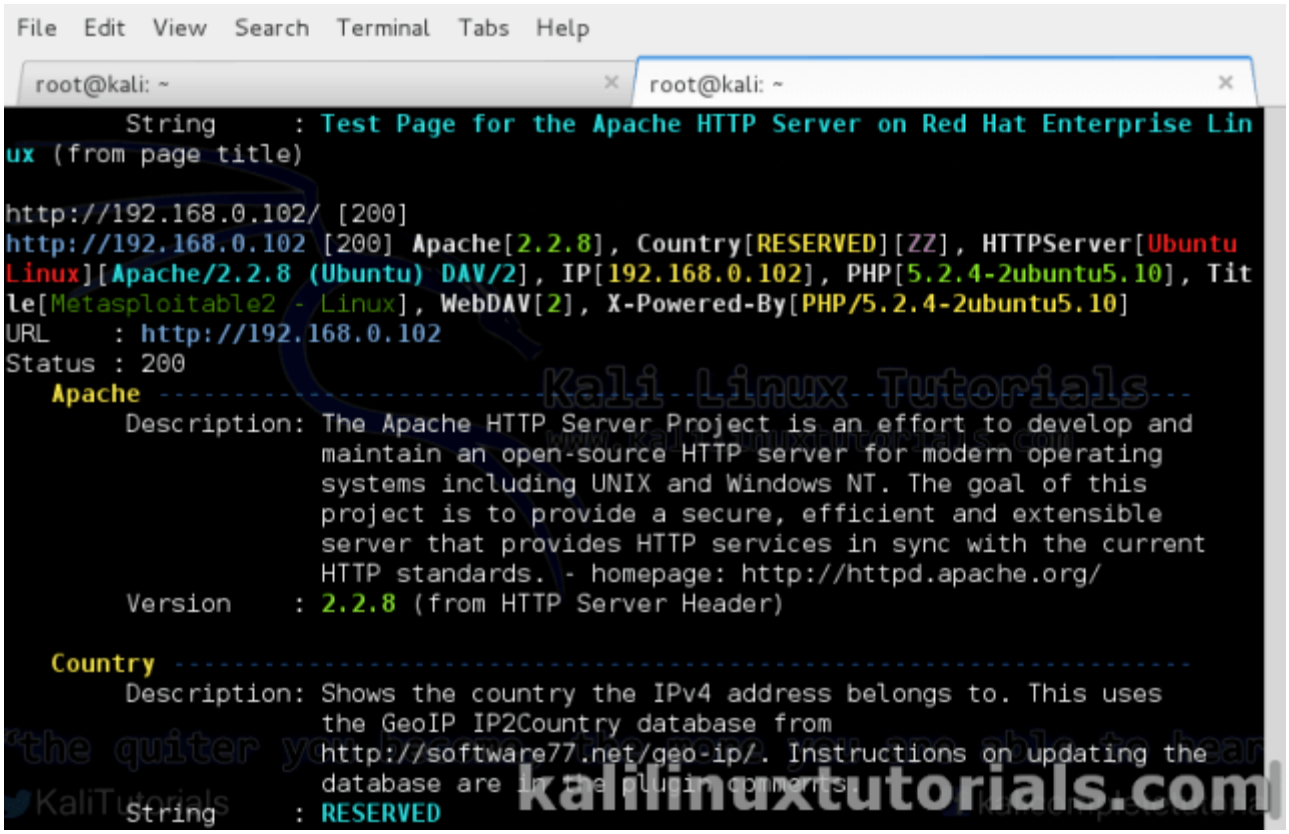
Attacker: Kali Linux

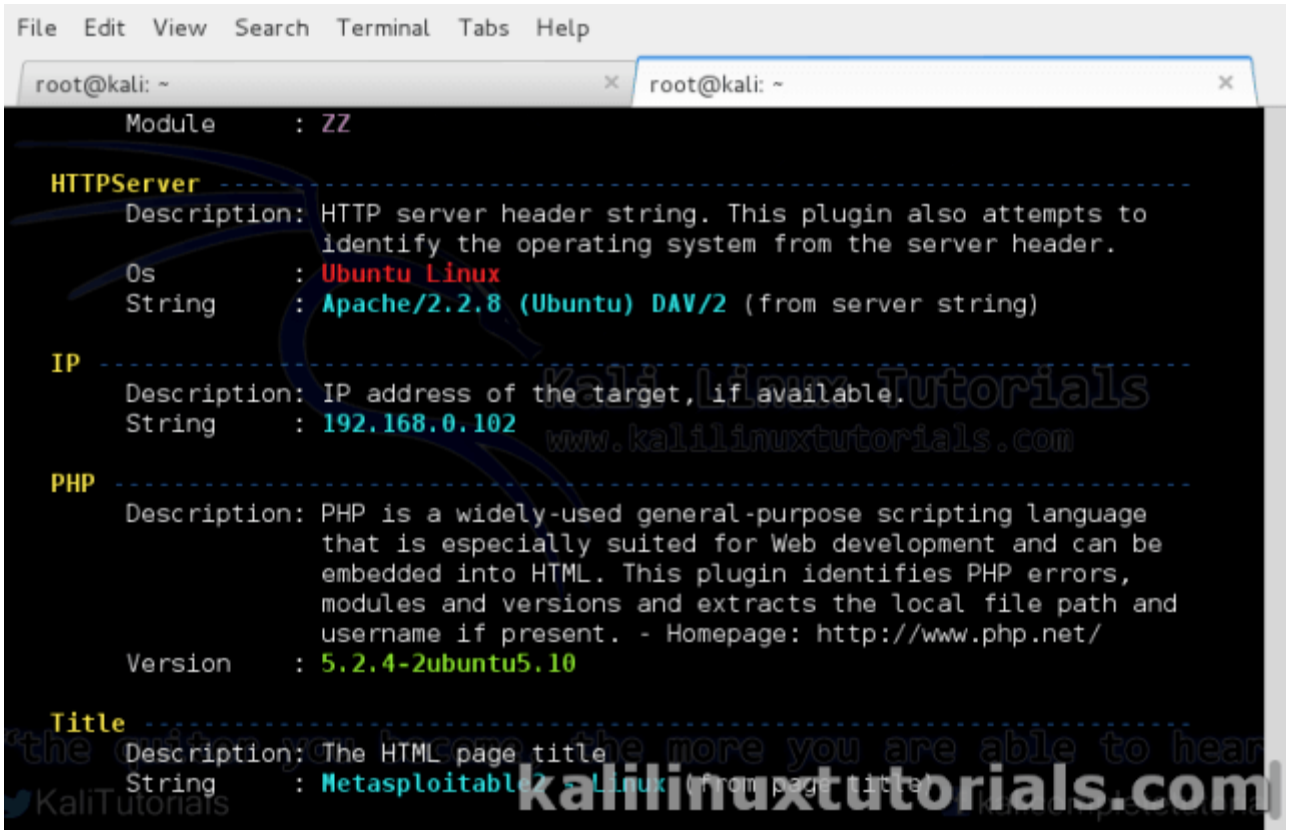
```
command: whatweb -v 192.168.0.1/24
```

Interestingly, the verbose output gives out coloured strings on interesting information. Take look at all those colours in the images below & identify all modules.


File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
root@kali:~# whatweb -v 192.168.0.0/24
/usr/lib/ruby/1.9.1/rubygems/custom_require.rb:36:in `require': iconv will be deprecated in the future, use String#encode instead.
http://192.168.0.0 ERROR: Network is unreachable - connect(2)
http://192.168.0.1/ [302]
http://192.168.0.1 [302] Country[RESERVED][ZZ], HTTPServer[httpd], IP[192.168.0.1], RedirectLocation[login.asp]
URL : http://192.168.0.1
Status : 302
Country
Description: Shows the country the IPv4 address belongs to. This uses the GeoIP IP2Country database from http://software77.net/geo-ip/. Instructions on updating the database are in the plugin comments.
String : RESERVED
Module : ZZ
HTTPServer
Description: HTTP server header string. This plugin also attempts to identify the operating system from the server header.
String : httpd (from server string)
IP
Description: IP address of the target, if available.
Kali Linux Tutorials
www.kalilinuxtutorials.com
kalilinuxtutorials.com


File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
http://192.168.0.73 ERROR: No route to host - connect(2)
http://192.168.0.105 ERROR: Connection refused - connect(2)
http://192.168.0.104/ [403]
http://192.168.0.110/ [200]
http://192.168.0.104 [403] Apache[2.4.6][mod_wsgi/3.4], Country[RESERVED][ZZ], Email[webmaster@example.com], HTTPServer[Red Hat Linux][Apache/2.4.6 (Red Hat) OpenSSL/1.0.1e-fips mod_wsgi/3.4 Python/2.7.5], IP[192.168.0.104], OpenSSL[1.0.1e-fips], PoweredBy[Apache,the], Python[2.7.5], Title[Test Page for the Apache HTTP Server on Red Hat Enterprise Linux]
URL : http://192.168.0.104
Status : 403
Apache
Description: 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. - homepage: http://httpd.apache.org/
Version : 2.4.6 (from HTTP Server Header)
Module : mod_wsgi/3.4
Country
Description: Shows the country the IPv4 address belongs to. This uses the GeoIP IP2Country database from
Kali Linux Tutorials
www.kalilinuxtutorials.com
kalilinuxtutorials.com


File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
String : Test Page for the Apache HTTP Server on Red Hat Enterprise Lin
ux (from page title)
http://192.168.0.102/ [200]
http://192.168.0.102 [200] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[Ubuntu
Linux][Apache/2.2.8 (Ubuntu) DAV/2], IP[192.168.0.102], PHP[5.2.4-2ubuntu5.10], Tit
le[Metasploitable2 - Linux], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]
URL : http://192.168.0.102
Status : 200
Apache
Description: 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. - homepage: http://httpd.apache.org/
Version : 2.2.8 (from HTTP Server Header)
Country
Description: Shows the country the IPv4 address belongs to. This uses
the GeoIP IP2Country database from
http://software77.net/geo-ip/. Instructions on updating the
database are in the plugin comments.
String : RESERVED
Kali Linux Tutorials
www.kalilinuxtutorials.com
kalilinuxtutorials.com


File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
Module : ZZ
HTTPServer
Description: HTTP server header string. This plugin also attempts to
identify the operating system from the server header.
Os : Ubuntu Linux
String : Apache/2.2.8 (Ubuntu) DAV/2 (from server string)
IP
Description: IP address of the target, if available.
String : 192.168.0.102
PHP
Description: PHP is a widely-used general-purpose scripting language
that is especially suited for Web development and can be
embedded into HTML. This plugin identifies PHP errors,
modules and versions and extracts the local file path and
username if present. - Homepage: http://www.php.net/
Version : 5.2.4-2ubuntu5.10
Title
Description: The HTML page title
String : Metasploitable2 - Linux (from page title)
Kali Linux Tutorials
www.kalilinuxtutorials.com
kalilinuxtutorials.com