2. Footprinting & Reconnaissance

Practical 1: Google Hacking

Using Google dorks while searching on google can help filtering unwanted results.

Following are some helpful google dorks:

site: If you are looking for specific website.
inurl: If you are looking for the keyword in the address bar.
intitle: If you are looking for the keyword in the title bar.
intext: If you are looking for the keyword in any webpage or file.
filetype: or ext: If you are looking for specific files
index.of/ If you are looking for file servers or directory listings
cache: If you are looking for lastly captured snapshot from google for any website.

Using multiple google dorks helps you to filter searches on google.
For more google dorks developed by others you can access GHDB (Google Hacking Database) from following link:
https://www.exploit-db.com/google-hacking-database/

To avoid indexing of your web content over google, you have to create and maintain robots.txt file in the root directory of the website.
To check the syntax of the file, you can access the robots.txt file for any website as follows:
www.site.com/robots.txt

For example:
www.wipro.com/robots.txt
www.virginia.edu/robots.txt

Practical 2: Using netcraft site report

You can search on google as “netcraft site report” to locate the online tool and find following link:

http://toolbar.netcraft.com/site_report

There you can enter your targets URL to find out some basic details about it.

Practical 3: Using yougetsignal for reverse ip lookup

Reverse IP lookup means checking for existence other domains/sub domains on our victims IP address. You can search on google as “reverse ip lookup” to locate following link:

www.yougetsignal.com/tools/web-sites-on-web-server

Over there you can either enter domain name or IP address of your target, it shows you all other domains, sub domains for that server.

Practical 4: Using the way back machine to check deleted pages

The way back machine can be used to see the cached pages or web sites which are deleted. You can search on google as “the way back machine” to locate the link:

https://archive.org/web/

Over there you can enter some deleted URL and find cached pages from there tool.
For example you can enter : www.cyanogenmod.org. This website got shutdown on 31st December 2016. But using the way back machine you can still view the past pages.

Practical 5: Using Mozilla Firefox addon “Wappalyzer”

Wappalyzer is one very useful addon available for Mozilla Firefox web browser, its also available as an extension for Google Chrome web browser. You need to install the addon on Firefox from following link:
For Firefox:
https://addons.mozilla.org/en-US/firefox/addon/wappalyzer/

For Chrome:
https://chrome.google.com/webstore/detail/wappalyzer/gppongmhjkpfnbhagpmjfkannfbllamg?hl=en

After installation is successful, you can visit any website and wappalyzer addon will detect there backend technology like, Web server, plugins etc.

Practical 6: Using whatweb tool from Kali Linux

In Kali Linux, we get a reconnaissance tool called whatweb. Using this tool does the same activities like wappalyzer. For running this, you have to start a terminal windows and enter command in following syntax:

whatweb <target website>

For example:
whatweb www.wipro.com

Practical 7: Using whois tool to find domain owner details

In Kali Linux, we get a reconnaissance tool called whois. Using this tool, you can find out the domain owner details of your target. For running it, you need to start a terminal window and enter the command in following syntax:

whois <domain name>

For example:
whois wipro.com

Practical 8: Using the harvester tool to find email addresses and other info

In Kali Linux, we get a reconnaissance tool called theharvester. Using this tool you can find much more details about your target thats available from social media. For running it, you need to start a terminal windows and entering command with following syntax:

theharvester -d <domain name> -b <source>

For example:

theharvester -d wipro.com -b google

You can enter : theharvester -h to get complete list of all options available.

Practical 9: Using Maltego tool

Maltego is one of the best tool used for reconnaissance, it comes pre-installed with Kali Linux and also available for all other platforms. You need to create an account with them and have to get logged in with that in Maltego. You can visit the following link for registration:

https://www.paterva.com/web7/community/community.php

On starting Maltego, you need to click on New Graph at top, and then on left side you should get a palette. You need to drag and drop an entity towards graph on right and provide required settings. For example you can drag and drop domain from palette and chane the name to you target like wipro.com and then right click on it and click on run all transforms. Similarly you can drag and drop person from left and enter your target's name example "Rahul Chitale" then right click on it and click Run all transforms. It will find out all possible info from social media.

Apart from all these, you can also try on some social networking sites like Facebook, Instagram, Twitter, Linkedin etc.