**Module 2: Foot printing and Reconnaissance**

1. Foot printing through Search Engines:

# Information Gathering (Google Searching):

* Accessing login page directly:

Goto Google.com> type(intitle:login site:eccouncil.org)

* Searching pdf files:

type(file name)filetype.pdf

eg: type ethnical hacking filetype.pdf

* For all details Search:

allinurl: needed details field

Eg: allinurl:eccouncil carrer

* For Information Search

into:url

eg: into:www.laba.com

* For Address Search

Forlocation:url

Eg: forlocation: laba.com.np

# Information Gathering (youtube searching):

-www.mattwo.io

(pasting youtube videos and channel link into url for detail information)

Information Gathering (Ftp Open Source Data Searching):

* [www.searchftps.net](http://www.searchftps.net)

# Web application Searching:

* <https://www.netcraft.com> – netcraft tool

#Site details Searching:

* [www.websiteinformer.com](http://www.websiteinformer.com)

# Tool for Searching Personal Information:

* <https://www.peekyou.com>

Kali linux tool for Searching Detail Information

* theHarvester

command: $theHarvester -d domain -b source

eg: $theharvester -d facebook.com -b yahoo

# Social Media Searching

(for collecting personal and domain information)

* Sherlock Tool (in kali os)

**Installing sherlock tool in kali**

github > search “Sherlock” tool/Script > copy url> open terminal> type “git clone” > paste url> install Sherlock tool

**after installation:**

ls> cd sherlock> ls> cd Sherlock\_project > ls> pip3 install -r requirements.txt

final command: Sherlock Username

eg: Sherlock hari

* Photon tool

(web crawler to extract URLs with parameters, also able to fuzz them, Secret AUTH keys and a lot more)

* installation

same as sherlock

-After installation in terminal

ls> cd photon > ls> sudo pip3 install -r requirements.txt

help command: python3 photon.py -h

command: python3 Photon.py -u (url)

eg: python3 Photon.py -u <https://www.certifiedhacker.com>

* GRecon tool: (for Site Cloning )
* installation: same as sherlock tool
* After installation: ls> Python3 grecon.py

then define target url

* Cewl Tool (for unique word collection from Sites)
* installation

Same as sherlock

- After Installation: ls>cd CeWL

Commands: ls> ccewl -h > ls ceWL -d 3 -m 8 Url -w directory

(-h for help, -d for depth, -m for minimum word length, -w for output file)

* HTTrack Website Copier (Website mirroring tools)

install HTTrack Website Copier tool

(goto vm lab and open win 11)

win 11> backup E:> module2> website mirroring tools> HTTrack website copier> Install

* Email Tracking:

tool- EmailTrackerpro (in win11 vm)

* install EmailTracekerpro > select “trace headers” > select “trace an email i have received” >

Paste Email Headers > trace

* Domain Tracking:

site: [https://whois.domaintools.com](https://www.whois.domaintools.com)

* Domain Tracking in windows:
* NSLOOKUP command

CMD as Administrator > nslookup

* “A” record: >set type =a > domain
* “SOA” record: >set type =soa>domain
* “MX” record: >set type=mx> domain (mail exchange record)

Finding mail Server ip:

>Set type=a> mail.certifiedhacker.com

* Reverse Domain Tracking:

Site: <https://www.yougetsignal.com> > reverse ip domain check

* Domain Tracking in kali os:

installing dnsrecon tool - sudo apt install dnsrecon > dnsrecon

command: dnsrecon -d domain -n name server

eg: dnsrecon -d certifiedhacker.com -n ns1.bluehost.com

(-d for dictionary , -n for name server)

* Ip address tracking:

web tool: <https://search.arin.net> > paste ip for detail information

* recon-ng: Framework- combination of tools.

(mainly used for Reconsinance)

modules - tools

1. Installing modules: sudo recon-ng > help> Marketplace > marketplace ? > marketplace install all

* Commands:

To Check modules: Modules search

To Create Project: Workspaces

To Check Projects: Workspaces list

To Create Project: Workspaces Create (Input Project Name)

1. After Installing Modules:

* To Create Project ( cmd: Workspaces Create Project\_Name)
* To Check List of Project ( cmd: Workspaces list)
* To Load Project ( cmd: Workspaces load Project\_Name)
* To Insert Domain (cmd: db insert domains)
* To Check Inserted Domain ( cmd: show domains)
* To delete domain (cmd: db delete domain)
* To load modules ( cmd: modules load “module”)
* To Run loaded Modules( cmd: run)

1. For Creating Report:

* modules load report > modules load reporting/html > Options list > options Set CREATOR name > Options Set CUSTOMER Customer name > Options Set FileName “File Name/Directory/Path” > run
* maltego ( Open Source Intelligence in kali linux)
* gather, analyze, and visualize publicly available information, uncovering relationships and patterns between entities like domains, IP addresses, social media profiles, and more
* Billcipher tool: information gathering on the basis of ip/host

**Installing Billcipher tool in kali**

github > search “Billcipher” tool/Script > copy url> open terminal> type “git clone” > paste url> install Billcipher Tools

**after installation:**