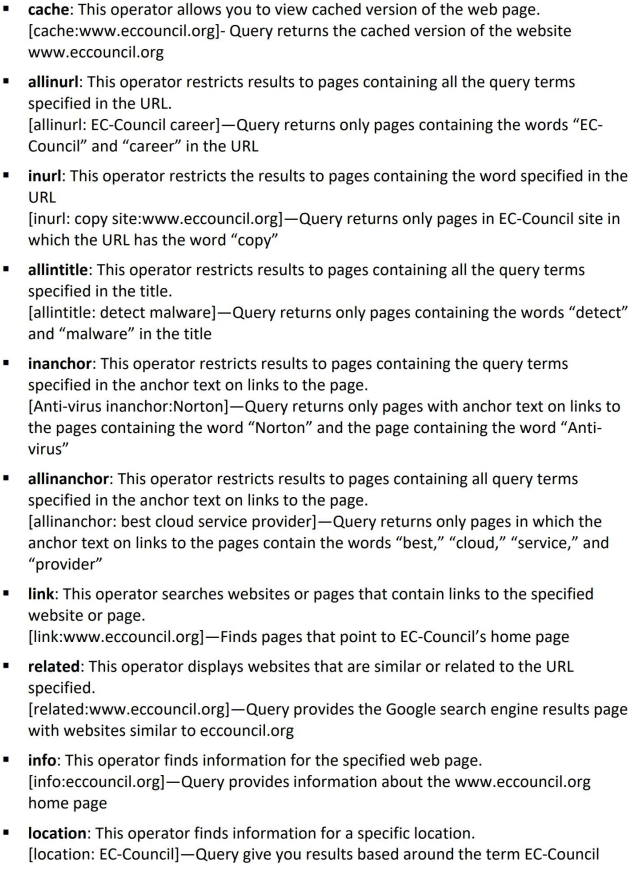
***FOOTPRINTING & RECONNAISSANCE***

LAB-1

1)GOOGLE ADAVNCE OPERATORS

Intitle:login sit:eccouncil.com

Ec-council filetype:pdf



2)info gathering with video search engines using youtube meta data

3)infogatering with FTP search engines

They are NAPALM FTP indexet(<https://www.searchftps.net/>)

4)IOT search engines

Shodan,Censys

LAB-2

1)Find Company Domain and Subdomains

\*netcraft (we need to go to site reports to find data)

\*Sublist3r

2)Personal Info Gathering

\*PeekYou

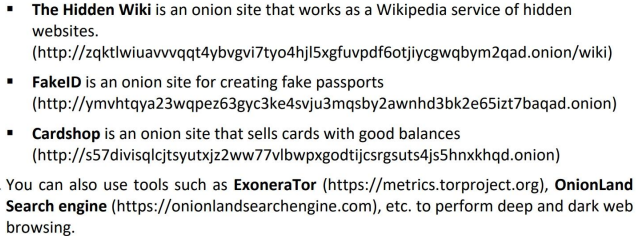
3)Gathering email using theHarvester

\*theHarvester

theHarvester -d domain.com -l 200 -b facebook

4)Deep and Dark web

Tor brouser,DuckDuckgo



5)Determinig target OS

\*Censys

\*Netcraft

LAB – 3

1)Gatering Employee’s information using theHarvester

theHarvester -d domain.com -l 200 -b linkedin

2)Social Networking

\*social sites

\*Sherlock.py

Python3 sherlock.py Krishna

3)Followerwonk

LAB-4

1)INFORMATION ABOUT A TARGET WEBSITE USING PING COMMAND

ping google.com -f -l 1500

1500 is the packet size.

2)information gatering using Photon

Python3 photon.py -u google.vom

3)information gathering using Central Ops

4)Web Data Extractor

5)mirror website using Httrack

6)gather information using GRecon

7)gather information using CeWL

LAB-5

Email footprinting

1)Email Tracker pro

2)analyze email hedder

LAB-6

Who is footprinnting

1)whoislookup

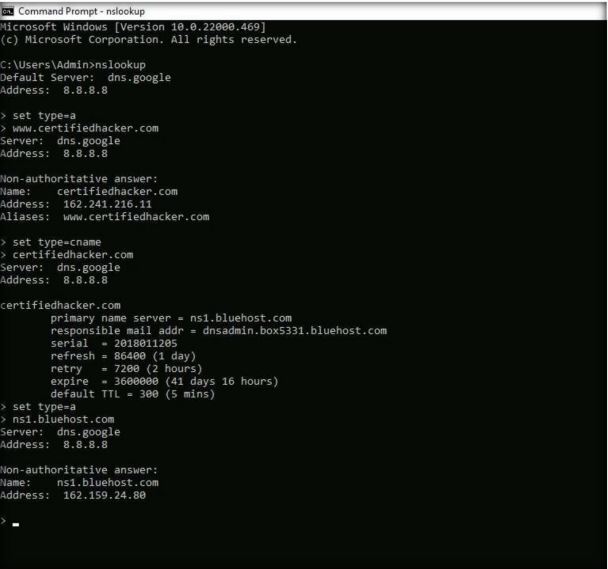
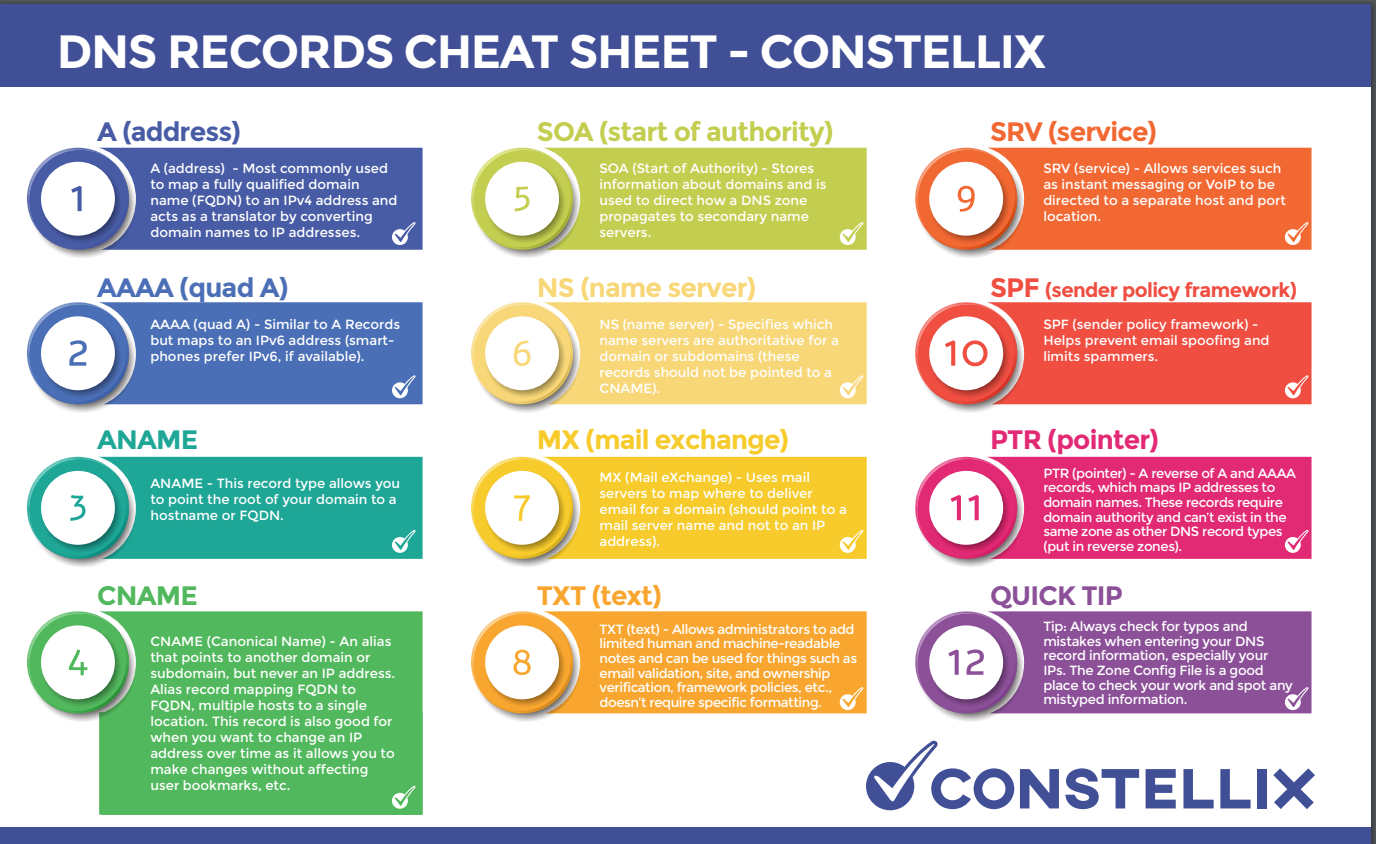
LAB-7

DNS footprinting

1)nslookup

DNS records

\*



Steps in nslookup

Nslookup

Set type=a

Google.com

\*we can also use type on dns in settype in a,mx,cname etc..

\*kloth.net (graphical nslookup)

2)perform reverse DNS Lookup using Reverse IP Domain Check and DNSRecon

Yougetsignal.com

./dnsrecon.py -r 162.168.216.0-55

Securitytrails.com

LAB -8

1)Secure dns lookup

Arin.net

2)network tracerouting

For windows11

Tracert google.com

For linux

Traceroute google.com

3)Advanced route tracing using path analyzer pro

LAB-9

1)Recon-ng(footprinting a target)

These are the commands

> marketplace install all

> modules search

> workspaces

>workspaces create CEH

>workspaces list

>db insert domains

>show domains

>modules load recon/domains-hosts/brute\_hosts

>run

>modules load recon /hosts-hosts/reverse\_resolve

>run

>show hosts

>back

>options set Customer Certifiedhacker Networks

>run

>options set SOURCE facebook.com

>run

>back

>options set creator kittu

>options set customer pandu

>run

Then open the saved file in browser

2)footprinting using maltego

3)domainfy

Domainfy –n eccouncil –f all

4)searchfy

Searchfy –q “Tim Cook”

5)footprinting using foca(win)

6)footprinting using BillCipher

6)osint

osintframework.com

7)namecheckr.com