OSINT

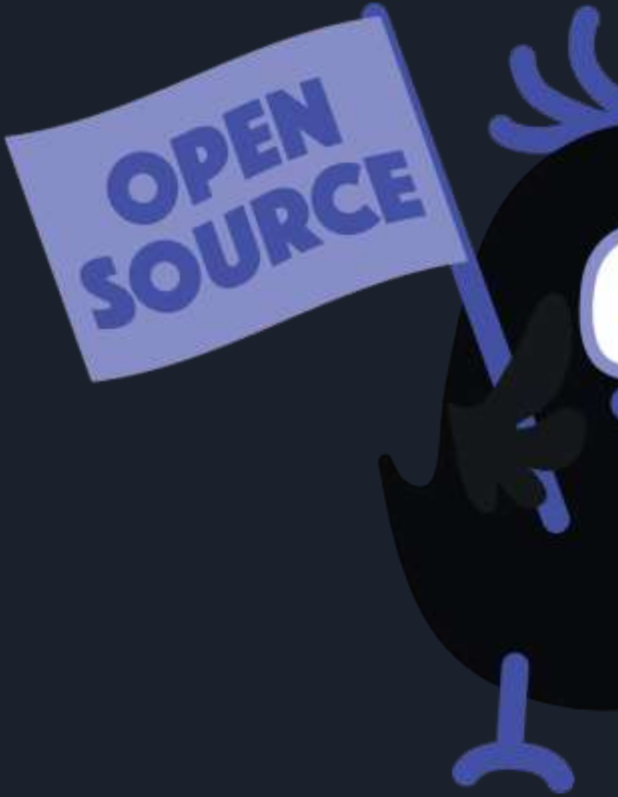
Name: Vicky Aryan

VTF ID: 1379675

What We Cover:

- ❑ What is OPEN SOURCE ?
- ❑ What is OSINT ?
- ❑ Intelligence Life Cycle
- ❑ Overview of Sock Puppets
- ❑ Search Engine Operator
- ❑ Reverse Image Search
- ❑ Exif data view

What is open source data?



Open source data is any information that is available to the public or can be made available by request.

Source of open-source :

- Newspaper and magazine articles, as well as media reports
- Academic papers and published research
- Books and other reference materials
- Social media activity
- Census data
- Telephone directories
- Court filings
- Arrest records
- Public trading data
- Public surveys
- Location context data
- Breach or compromise disclosure information
- Publicly shared cyberattack indicators like IP addresses, domain or file hashes
- Certificate or Domain registration data
- Application or system vulnerability data

What is OSINT?

Open-source intelligent is a multi-method methodology for collecting, analyzing and making decision about data accessible in publicly available source to be used in an intelligent context.

In the intelligent community, the term “open” refers to overt, publicly available sources.

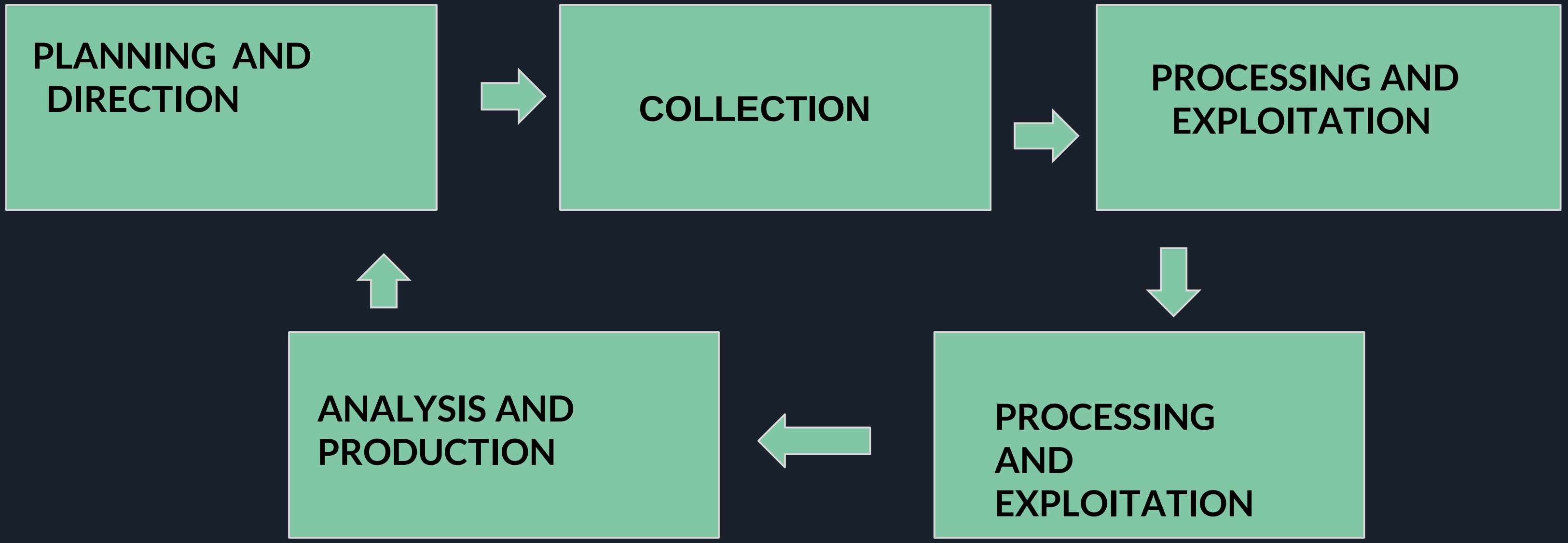
OSINT
A NUMBER OF STATISTIC S AND
REGULARLY USE
OSINT METHO
TO JUDICI
CRIMINAL
ANALYSIS THAT PROVIDE INFORMATI ON TH
AND SOCIAL NETWORK ANALYSIS
THERE ARE A NUMBER OF
MANY ORGANIZATION S ARE NOW

OSINT Techniques

Passive recon involves gathering information about a target network or device without directly engaging with the system. OSINT analysts rely on third-party information using passive recon tools, such as Wireshark, which analyzes network traffic in real-time for Windows, Mac, Unix, and Linux systems. They piece together these different OSINT data points to find and map patterns.

Active recon directly engages with the target system, offering more accurate and timely information. OSINT analysts use active recon tools like Nmap, a network discovery tool that provides a granular view of a network's security.

Intelligence Life Cycle :



PLANNING AND DIRECTION

COLLECTION

PROCESSING AND EXPLOITATION

PROCESSING AND EXPLOITATION

ANALYSIS AND PRODUCTION

Overview of Sock Puppets:

Sock puppets are nothing but detailed created fake social media accounts to research in OSINT without giving up the true identity.

Sock Puppets are basically aliases, fictitious persona profiles created by someone else with specific goals in mind and is part of an OSINT Social Engineering technique.

Purpose of Sock puppets.

- Investigators can use the sock accounts to collect information and do research o some cases.
- Hackers can use sock accounts to do social engineering on the target to collect the information.
- Detective can use these type of accounts to collect information and to know the nature of someone related to their cases.

How to Create Sock Account?

You can use these resources as per of your requirement.

1. Name

https://www.fakenamegenerator.com/

2. Email Address

Now you have name and all sorts of details, you need a email address matching to that name.

You can use any mail provider to create email address make sure not to use your IP address while doing this.

Note:I recommend using mail.com to create email address and make sure you don’t use existing email address.

3. Face

https://thispersondoesnotexist.com/

4. Burner Phones and Sim Cards?

Burner means to use and through or a phone that is not connected to you in any way. A

Search Engine Operators:

Using search operators we were able to tailor the search to our needs and could conclude that no additional information on desired target.

Tools:
Google Advanced Search

Apart from google you might consider additional search engine.

Google Dorks

- “inurl: domain/” “additional dorks

A hacker would simply use in the desired parameters as follows:

- inurl = the URL of a site you want to query
- domain = the domain for the site
- dorks = the sub-fields and parameters that a hacker wants to scan

Some Useful google dorks:

Intitle:

Maps:

Book:

Define:

Related:

Link:

site:

phonebook:

inurl:

intext:

weather:

movie:

info:

Reverse Image Searching:

It is a method in which we put image on search engine and the search engine gives the result about that image.

Some useful search engines that might helps in reverse image searching

Exif Data View

EXIF stands for ‘Exchangeable Image File Format’ and refers to the basic metadata that is generated and stored by your camera whenever you take a photo.

- It can reveals more information like that geolocation, device name, and many other.

Tools:

Online Exif Viewer

EXIF.tools

Exiftool in kali linux and many more…..

OSINT Tools:

- Maltego
- Mitaka
- SpiderFoot
- Spyse
- BuiltWith
- Intelligence X
- DarkSearch.io
- Grep.app
- Recon-ng
- theHarvester
- Shodan
- Metagoofil
- Searchcode
- SpiderFoot
- Babel X

Thank you!

https://www.linkedin.com/in/vickyaryan/

https://twitter.com/pwn_b0y

https://pwnb0y.medium.com/