OSINT

!! FIRSTLY WHAT IS OSINT?

In addition to cybersecurity, OSINT is also frequently used by organizations or governments seeking to **monitor and influence public opinion**. OSINT can be used for marketing, political campaigns, and disaster management.

CYCLE : content -> collection -> process & exploit -> analysis & production -> integration ->repeat

NOTE TAKING:
notion , keep note , cherrytree , Cloud notes(e.x Microsoft) , Joplin

INTRODUCTION :
"*Open-source intelligence (OSINT) is an intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.*"

1. The internet is the main place where OSINT resources are found, indeed, many researchers differentiate between the online OSINT resources and the offline one by using the term "Cyber OSINT" to refer to internet resources exclusively. Internet resources include the following and more: blogs, social media websites, digital files (photo, videos, sound) and their metadata, technical footprinting of websites, webcams, deep web (government records, weather records, vital records, criminal's records, tax and property records), darknet resources, data leak websites, IP addresses, and anything published online publicly.
2. Traditional media channels such as TV, radio, newspapers, and magazines.
3. Academic publications such as dissertations, research papers, specialized journals, and books.
4. Corporate papers such as company profiles, conference proceedings, annual reports, company news, employee profiles, and résumés.
5. Geospatial information such as Online maps, commercial satellite images, geo-location information associated with social media posts, transport (Air, Maritime, Vehicles, and Railway) tracking.

Sock Puppets: A person whose actions are controlled by another ,a minion, - begginer osint

Fake Name Generator- generate person's information randomly with full info.

Privacy.com ? - generate credit card fakely
https://Privacy.com is used **to make secure online payments with masked card numbers**. Our customers shop more safely and privately using randomly-generated virtual card numbers instead of their real debit card or credit card numbers. You can also pause or close a Privacy Card at any time for an additional layer of security.
Person Does Not Exist - making a fake person photo

SEARCH ENGINE OPERATORS ?
Google , Yandex , Baidu , (Google dorking also included) , Google - Advance_search

REVERSE IMAGE SEARHING:
sites : images.google.com
yandex.com/images
tineye.com

VIEWING EXIF DATA:
site : exif.regex.info/exif.cgi
https://jimpl.com

PHYSICAL LOCATION OSINT
site: www.google.com/maps/

IDENTIFICATION GEOGRAPHICAL LOCATIONS
site: www.geoguessr.com
you can use yandex.com also

DISCOVERING EMAIL ADDRESSES:
site: hunter.io/search ,
https://phonebook.cz
https://tools.verifyemailaddress.io
emailchecker.net/validate
[connect extension] in gmail(main box)

PASSWORD OSINT:
Dehashed tool : https://dehashed.com (paid) (very powerfull tool!!)

linux tool (breach-parse)

HUNTING BREACHED CREDENTIALS :
https://haveibeenpwned.com/ ----- for checking mail/phone number data breach
https://weleakinfo.to/v2/
https://leakcheck.io

(MOST IMPORTANT TOOL)
https://scylia.sh (search by email (public exposed password (leak credentials)))

HUNTING USERNAMES AND ACCOUNTS:
Namech_k (just input name or keyword)
whatsmyname.app
namecheckup.com
kik.me
(Snapchat)is one of the best for find person's username and accounts etc...

SEARCHING FOR PE
OPLE ? : this osint is really good one just input the name and location/ without location for finding (public phone number)
1.Whitepages.com
2. fastpeoplesearch.com
3. fastbackgroundcheck.com
4. webmii.com
5. peekyou.com
6. 411.com
7. spokeo.com
8. thatsthem.com

VOTER RECORDS
voterrecords.com

HUNTING PHONE NUMBERS
1.google is the best overall (just search phone number and get all info regarding that)
e.x 4567890345 ,
(456)789-0345
(all this different methods available)
you can search with emojis()

2.Truecaller.com
3.callendtest.com
4.infobel.com (mainly freanch but you can change language and country)

DISCOVERING BIRTHDATES:
1.google dork ("ananta n" birthday)("ananta n " intext:"happy birthday" site:twitter.com)

SEARCHING FOR RESUMES
1. google dork ("name" resume)("name" resume site:drive.google.com)

TWITTER OSINT PART-1

1. dork (to:anyname & from:anyname & @anyname) used for find send / receive / tag people or profile here
2. from:anyname since:2019-02-01 until:2019-03
3. e.x : geocode(34.0207305, -118.6919133, 1km) https://twitter.com/search_advanced

TWITTER OSINT PART-2

1. socialbearing.com (unknown application . you should know)
2. twitenemy.com (all data (time spent and all of small sensitive data) about search person)
3. analytics.mentionmapp.com (analysis of network in twitter)
4. tweetbeaver.com (is used for find conversation of 2 person in twitter)
5. spoonbill.io (anytime change or update data analysis)
6. tinfoleak.com (potential leak info of twitter)

TWITTER OSINT PART-3
1. twittdeck.twitter.com (same dork as well as in part-1)

FACEBOOK OSINT PART-1
1. showdust.github.io
2. intelx.io

INSTAGRAM OSINT
1. wopita.com (general info)
2. instadp.com

SNAPCHAT OSINT

1. map.snapchat.com

REDDIT OSINT

1. google dork ("anyname" , site:reddit.com , intext:oscp)

in all Social media osint , you can use their's dorking system just like google dorking