OSINT Tools

Image and Location OSINT

- `sudo apt-get update`
- `sudo apt install libimage-exiftool-perl`
- `exiftool --help`
- `exiftool [image_name]`

Hunting Emails and Breached Data

- `theHarverster -d tcm-sec.com -b all`
- `theHarverster -d tesla.com -b google -l 100` not very aggresive

breach-parse
`./breachparse.sh @tesla.com tesla.txt`
h8mail
`h8mail -t shark@tesla.com -bc "/opt/breach-parse/BreachCompilation/" -sk`

Username and Account OSINT

- `whatsmyname -u thecybermentor`
- `sherlock thecybermentor`

Phone Number OSINT

- `phoneinfoga --help`
- `phoneinfoga scan 918590163664`

- `phoneinfoga serve -p 8080`

Social Media OSINT

Twint

- `pip3 install --upgrade -e git+https://github.com/twintproject/twint.git@origin/master#egg=twint`
- `pip3 install --upgrade aiohttp_socks`

A few simple examples to help you understand the basics:

- `twint -u username` - Scrape all the Tweets of a *user* (doesn't include **retweets** but includes **replies**).
- `twint -u username -s pineapple` - Scrape all Tweets from the *user*'s timeline containing *pineapple*.
- `twint -s pineapple` - Collect every Tweet containing *pineapple* from everyone's Tweets.
- `twint -u username --year 2014` - Collect Tweets that were tweeted **before** 2014.
- `twint -u username --since "2015-12-20 20:30:15"` - Collect Tweets that were tweeted since 2015-12-20 20:30:15.
- `twint -u username --since 2015-12-20` - Collect Tweets that were tweeted since 2015-12-20 00:00:00.
- `twint -u username -o file.txt` - Scrape Tweets and save to file.txt.
- `twint -u username -o file.csv --csv` - Scrape Tweets and save as a csv file.
- `twint -u username --email --phone` - Show Tweets that might have phone numbers or email addresses.

- `twint -s "Donald Trump" --verified` - Display Tweets by verified users that Tweeted about Donald Trump.
- `twint -g="48.880048,2.385939,1km" -o file.csv --csv` - Scrape Tweets from a radius of 1km around a place in Paris and export them to a csv file.
- `twint -u username -es localhost:9200` - Output Tweets to Elasticsearch
- `twint -u username -o file.json --json` - Scrape Tweets and save as a json file.
- `twint -u username --database tweets.db` - Save Tweets to a SQLite database.
- `twint -u username --followers` - Scrape a Twitter user's followers.
- `twint -u username --following` - Scrape who a Twitter user follows.
- `twint -u username --favorites` - Collect all the Tweets a user has favorited (gathers ~3200 tweet).
- `twint -u username --following --user-full` - Collect full user information a person follows
- `twint -u username --timeline` - Use an effective method to gather Tweets from a user's profile (Gathers ~3200 Tweets, including **retweets** & **replies**).
- `twint -u username --retweets` - Use a quick method to gather the last 900 Tweets (that includes retweets) from a user's profile.
- `twint -u username --resume resume_file.txt` - Resume a search starting from the last saved scroll-id.

https://github.com/sc1341/InstagramOSINT
https://github.com/Datalux/Osintgram

Website OSINT

- wappalyzer
- `whatweb`
- `whois tcm-sec.com`
- `httprobe`
  - `cat tesla.txt | sort -u | httprobe -s -p https:443`
  - To verify subdomain exist or not.
  - httprobe
- `assetfinder`
  - `assetfinder tcm-sec.com`
  - assetfinder
- `subfinder`
  - `subfinder -d tcm-sec.com`
  - subfinder
- `gowitness`
  - `gowitness file -f ./alive.txt -P ./pics --no-http`
  - gowitness
- `amass`
  - `amass enum -d tcm-sec.com`
  - amass

OSINT Frameworks

`recon-ng`

- `marketplace search`
- Doesn't need APIs
  - `marketplace install hackertarget`

        - `modules load hackertarget`
        - `info`
        - `options set SOURCE tcm-sec.com`
        - `run`
        - `show hosts`
    - `back`
    - `marketplace install profiler`
        - `modules load profiler`
        - `info`
        - `options set SOURCE thecybermentor`
        - `show profiles`

`maltego`

- Run maltego free
- Create a new graph
- Drag domain and double click to change

Other Tools

Hunchly - extension only runs in google chrome.