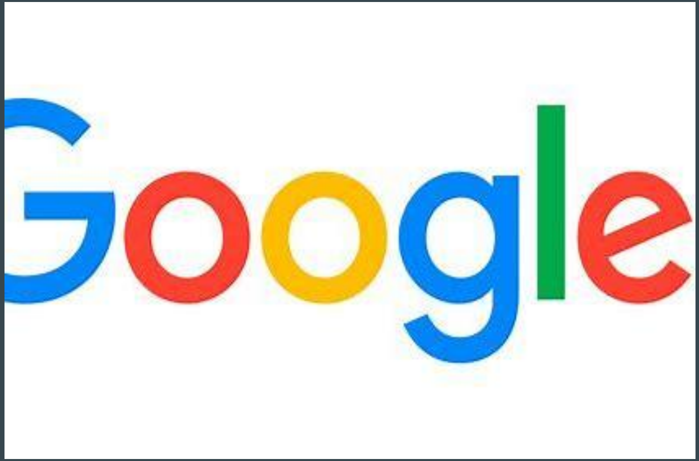
OSINT

(OPEN SOURCE INTELLIGENCE)

INTRODUCTION TO OSINT

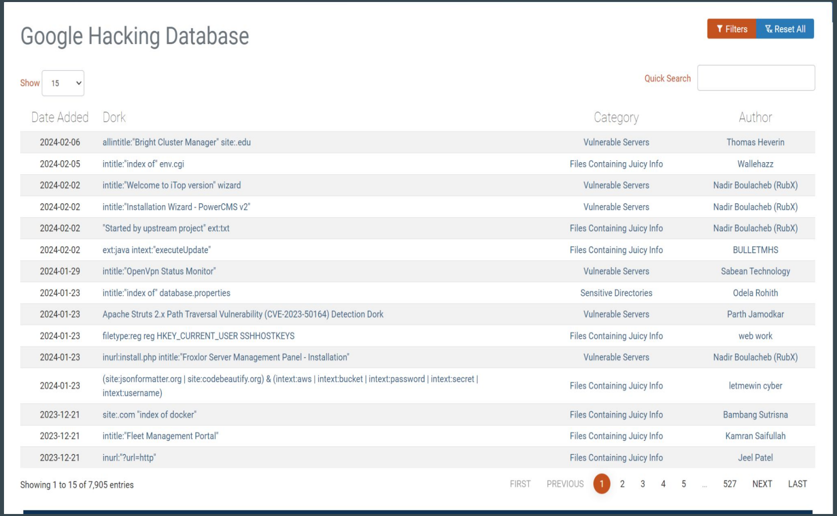


What is OSINT

- OSINT is the collection, analysis and dissemination of information that is legally and publicly accessible via open sources.
- Open sources such as the internet and discarded items (papers containing info)
- Used by hackers, pentesters, journalists, and federal law enforcement
- Two ways of conduction OSINT
- Passive and Active
- Passive is monitoring and using the internet to gather info
- Active OSINT requires physical or riskier actions to get certain info
- *OSINT should ALWAYS be the first step to any successful hack or pentest!

How to use OSINT

- OSINT can be used via the internet or physical efforts
- On a KALI Linux machine or via your own device (PC/PHONE) open Google
- Navigate to the "Google Hacking Database" (GHDB)
- Once there click on any link that is listed (see below)
- You can use the links provided to "Dork"



Google Hacking Database

Show 15

Quick Search

Date Added	Dork	Category	Author
2024-02-06	allintitle:"Bright Cluster Manager" site:.edu	Vulnerable Servers	Thomas Heverin
2024-02-05	intitle:"index of" env.cgi	Files Containing Juicy Info	Wallehazz
2024-02-02	intitle:"Welcome to iTop version" wizard	Vulnerable Servers	Nadir Boulacheb (RubX)
2024-02-02	intitle:"Installation Wizard - PowerCMS v2"	Vulnerable Servers	Nadir Boulacheb (RubX)
2024-02-02	"Started by upstream project" ext:txt	Files Containing Juicy Info	Nadir Boulacheb (RubX)
2024-02-02	ext:java intext:"executeUpdate"	Files Containing Juicy Info	BULLETMHS
2024-01-29	intitle:"OpenVpn Status Monitor"	Vulnerable Servers	Sabean Technology
2024-01-23	intitle:"index of" database.properties	Sensitive Directories	Odela Rohith
2024-01-23	Apache Struts 2.x Path Traversal Vulnerability (CVE-2023-50164) Detection Dork	Vulnerable Servers	Parth Jamodkar
2024-01-23	filetype:reg reg HKEY_CURRENT_USER SSHHOSTKEYS	Files Containing Juicy Info	web work
2024-01-23	inurl:install.php intitle:"Froxlor Server Management Panel - Installation"	Vulnerable Servers	Nadir Boulacheb (RubX)
2024-01-23	(site:jsonformatter.org | site:codebeautify.org) & (intext:aws | intext:bucket | intext:password | intext:secret | intext:username)	Files Containing Juicy Info	letmewin cyber
2023-12-21	site:.com "index of docker"	Files Containing Juicy Info	Bambang Sutrisna
2023-12-21	intitle:"Fleet Management Portal"	Files Containing Juicy Info	Kamran Saifullah
2023-12-21	inurl:"?url=http"	Files Containing Juicy Info	Jeel Patel

Showing 1 to 15 of 7,905 entries

Tools for OSINT

- Using various OSINT tools gives you the upper hand for recon
- Reverse image searches, facial recognition software, and Google Dorks
- Google Dorking is narrowing down searches to find info that is hidden yet accessible
- For example typing “gaming computers” on google will give millions of sites
- But typing in “site:amazon.com gaming computers” will show only Amazon results
- Cool huh???
- To look up somebody, tools like thatsthem.com or typing in their name in Google can give results to their address, name, height, weight etc...

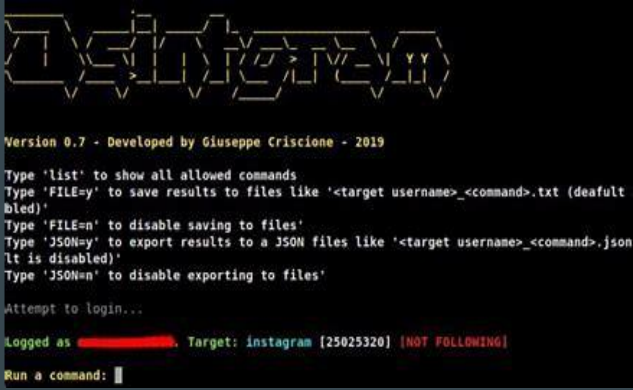
Tools for OSINT PT.II

- If a target’s EMAIL was found through Google Dorking, tools like haveibeenpwned or epios.com can look for anything related to the email
- Social Media gives lots of info, look up on IG or FACEBOOK or TWITTER #newjob or anything related to that phrase
- There are also tools like OSINTGRAM or TWINT which can scrape a persons IG or TWITTER account(s) (TWINT uses geolocation!! & Bypasses Twitter API!)
- Social-searcher.com or checkusernames.com looks for social media accounts of a target when there full name is given or username given
- For scanning faces tools like facecheck.id uses AI to look for a targets face on the internet

Additional Tools

- Tineye-Reverse Image Search
- Shodan-IOT device search engine
- Yandex.ru-Russian search engine similar to Google
- PicTriev-Age guesser
- WayBack-Machine Archives
- Haveibeenpwned-email data breach/leak analyzer
- Maltego-Automated OSINT framework (KALI LINUX TOOL)
- Github Clones-OSINT tools made for Linux based machines
- KALI LINUX-This pentesting OS has apps that are made for OSINT (check them out!)
- Dumpster Diving or Social Engineering

OSINTGRAM Installation



```
Version 0.7 - Developed by Giuseppe Criscione - 2019

Type 'list' to show all allowed commands
Type 'FILE=y' to save results to files like '<target username>_<command>.txt (deafult
bled)'
Type 'FILE=n' to disable saving to files'
Type 'JSON=y' to export results to a JSON files like '<target username>_<command>.json
lt is disabled)'
Type 'JSON=n' to disable exporting to files'

Attempt to login...

Logged as [redacted]. Target: instagram [25025320] [NOT FOLLOWING]

Run a command: 
```

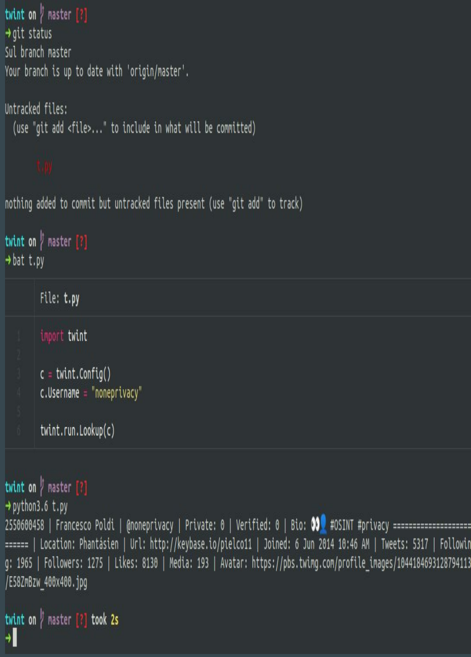
OSINTGRAM (Kali Linux):

- git clone https://github.com/Datalux/Osintgram.git
- cd Osintgram (navigates to the Osintgram directory)
- python3 -m venv venv (creating a virtual environment for Osintgram)
- source venv/bin/activate
- pip install -r requirements.txt
- Open credentials.ini file located in the config folder and put in credentials to your IG account. (MAKE A NEW IG ACCOUNT THAT CAN BE DISCARDED)
- python3 main.py <target username> --command <command> (This runs the script)
- Run this on your own Kali Linux machine don't use Cyber Range computers

TWINT Installation

TWINT (Kali Linux/Google Cloud Console):

- git clone –depth=1 https://github.com/twintproject/twint.git
- cd twint (changing directory into twint)
- pip3 install . -r requirements.txt
- TO USE/HELP
- twint -h (displays all the commands for twint to get more info)
- twint -u <target username>
- twint -u <target username> – limit <number of tweets>
- twint -u <target username> -s "enter keyword/phrase"
- twint -u <target username> –images (pulls up images)
- twint -s <keyword> –near <area> –since <full date> –min-likes <like number>
- twint -s <keyword> –since <full date> -g="<coordinates x,y>,<radius>"
- This also works using the google cloud console



```
twint on master [?]
➜git status
Sul branch master
Your branch is up to date with 'origin/master'.

Untracked files:
  (use "git add <file>..." to include in what will be committed)

        t.py

nothing added to commit but untracked files present (use "git add" to track)

twint on master [?]
➜bat t.py

       File: t.py

       import twint

       c = twint.Config()
       c.Username = "noneprivacy"

       twint.run.Lookup(c)


twint on master [?]
➜python3.6 t.py
2550600458 | Francesco Poldi | @noneprivacy | Private: 0 | Verified: 0 | Bio: 👀👤 #OSINT #privacy ===================
====== | Location: Phantásien | Url: http://keybase.io/pielco11 | Joined: 6 Jun 2014 10:46 AM | Tweets: 5317 | Followin
g: 1965 | Followers: 1275 | Likes: 8130 | Media: 193 | Avatar: https://pbs.twimg.com/profile_images/10441846931287941113
/E58ZmBzw_400x400.jpg

twint on master [?] took 2s
➜
```

PhoneInfoga Installation

PhoneInfoga(Kali Linux/Google Cloud Console):

- # Add --help at the end of the command for a list of install options
- bash <(curl -sSL https://raw.githubusercontent.com/sundowndev/phoneinfoga/master/support/scripts/install)
- Type phoneinfoga (this will see if it's downloaded)
- phoneinfoga scan -n <phone number> (Don't add dashes or symbols)
- In a browser type <Local IP Host:5000> (This will bring you to the GUI. Easier to use)
- The GUI also provides google dorks and other material

Objective

- Try Google Dorking and utilize the GHDB
- Use the quick search filter on the GHDB and look for “juicy information” (Open cameras, hidden login pages, PDFS of sensitive data, or admin pages
- Try using tools like pimeyes, facecheck.id or the Kali Linux OSINT tools
- Make a sock puppet account and use it for OSINTGRAM (OPTIONAL)
- Have fun and if you want to use OSINT daily check out tracelabs.