TOP 3 OSINT TOOLS

1.Mr.G.SEENUVASAN, MCA, M.PHIL, NET.
Assistant Professor, Department of Computer Applications,
SrimathSivagnanaBalayaSwamigal Tamil Arts And Science College, Mailam.
2.Mr.I.JAYAKUMAR,
I M.Sc. Computer science,
Department of Computer science,
St. Joseph's College of Arts & Science, Cuddalore

Introduction

OSINT stands for *Open Source Intelligence,***Open source intelligence** (**OSINT**) is information collected from public sources such as those available on the Internet.It is not related to open-source software or collective intelligence. All our data are available on social media like Facebook, Instagram, LinkedIn profile and more social networks. But OSINT is even simpler, you know; many of us associate OSINT to cyber war, cyber-attacks, cybersecurity, etc. And while those things are a part of it, OSINT is much more explicit and uncomplicated.

The first step in a target attack – or a penetration test or red team activity – is gathering intelligence on the target. While there are ways and means to do this covertly, intelligence gathering usually starts with scraping information from public sources, collectively known as open source intelligence or OSINT. There is such a wealth of legally collectible OSINT available now thanks to social network and the prevalence of online activities that this may be all that is required to give an attacker everything they need to successfully profile an organization or individual.

What is OSINT used for?

Gathering OSINT on yourself or your business is also a great way to understand what information you are gifting potential attackers. Once you are aware of what kind of intel can be gathered about you from public sources. Gathering publicly available sources of information about a particular target an attacker or friendly penetration tester can profile a potential victim to better understand its characteristics and to narrow down the search area for possible vulnerabilities

Disclaimer

This article for informational and educational purposes only. We believe that ethical hacking, information security and cyber security should be familiar subjects to anyone using digital information and computers. We believe that it is impossible to defend yourself from hackers without knowing how hacking is done. Only for those who are interested to learn about Ethical Hacking, Security, Penetration Testing and malware analysis. Hacking tutorials is against misuse of the information and we strongly suggest against it. Please regard the word hacking as ethical hacking or penetration testing every time this word is used.

#1 Sherlock

When researching a person using OSINT (open source intelligence) the target is to find the information about a person into a bigger picture. Find username across social Networks to get images, videos, activity and more data of that person. Brand/Screen names are perfect for this because they are using unique and link data together, reuse them in accounts across the internet. With Sherlock, we can instantly hunt down social media accounts created with unique screen name.

For a single clue like email address or screen name, Sherlock can generate their accounts link across the internet. Now we can check about their activity on the internet through their profile info.

Requirements for install

- It runs all platform with python3
- Python 3.6 or higher is required
- Package manager pip3 to install Sherlock on your computer
- Properly install the requirements

Installation steps

- Open Kali Linux terminal
- First to update the packages run the following commands one by one
- **sudo apt-get update**
- **git clone https://github.com/sherlock-project/sherlock.git**

- **python3 -m pip install -r requirements.txt (or)**
- **pip install –r requirements.txt**

Usages

```
$ python3 sherlock.py  --h
Syntax :  sherlock.py [-h] [--version] [--verbose] [--rank]
                [--folderoutput FOLDEROUTPUT] [--output OUTPUT] [--tor]
                [--unique-tor] [--csv] [--site SITE_NAME]
                [--proxy PROXY_URL] [--json JSON_FILE]
                [--proxy_list PROXY_LIST] [--check_proxies CHECK_PROXY]
                [--timeout TIMEOUT] [--print-found]
                USERNAMES [USERNAMES ...]


positional arguments:
  USERNAMES             One or more usernames to check with social media
optional arguments:
  -h, --help            show this help message and exit
  --version             Display version information and dependencies.
  --verbose, -v, -d, --debug
                        Display extra debugging information and metrics.
  --rank, -r            Present websites ordered by their Alexa.com global
                        rank in popularity.
  --folderoutput FOLDEROUTPUT, -fo FOLDEROUTPUT
                        If using multiple usernames, the output of the results
                        will be saved to this folder.
  --output OUTPUT, -o OUTPUT
                        If using single username, the output of the result
                        will be saved to this file.
  --tor, -t             Make requests over Tor; increases runtime; requires
                        Tor to be installed and in system path.
  --unique-tor, -u      Make requests over Tor with new Tor circuit after each
```

request; increases runtime; requires Tor to be installed and in system path.

--csv Create Comma-Separated Values (CSV) File.

--site SITE_NAME Limit analysis to just the listed sites. Add multiple options to specify more than one site.

--proxy PROXY_URL, -p PROXY_URL

Make requests over a proxy. e.g. socks5://127.0.0.1:1080

--json JSON_FILE, -j JSON_FILE

Load data from a JSON file or an online, valid, JSON file.

--proxy_list PROXY_LIST, -pl PROXY_LIST

Make requests over a proxy randomly chosen from a list generated from a .csv file.

--check_proxies CHECK_PROXY, -cp CHECK_PROXY

To be used with the '--proxy_list' parameter. The script will check if the proxies supplied in the .csv file are working and anonymous.Put 0 for no limit on successfully checked proxies, or another number to institute a limit.

--timeout TIMEOUT Time (in seconds) to wait for response to requests. Default timeout of 60.0s.A longer timeout will be more likely to get results from slow sites.On the other hand, this may cause a long delay to gather all results.

--print-found Do not output sites where the username was not found.

Commands to run

$Python3 sherlock.py username –r

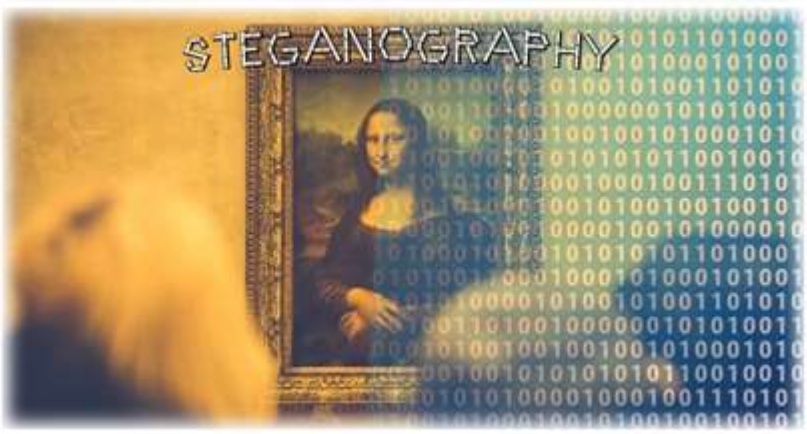
Example: python3 sherlock.py user123

Now Sherlock can check the all popular social networks which will search for accounts across the internet with the username "user123" and print only the results that it founded as a text file user123.txt

Not Found it denotes user123 has no account on that social media otherwise it generate account link. Sherlock can provide many information about target, we can use this information as clues to find the target full activity in social network.

#2 Steghide

Steghide is a steganography program that is used to hide data in various formats like images, audio file and video files. This program is pre-installed in Kali Linux operating system performing as data extracting and embedding into files.Steghide is a command line tool through which you can easy to use and understand only a few seconds to hide information in many files types. Its really useful in present and upcoming cyber security to hide and send data in secure way.



It used to embed the data into another file even extract the data with steghide. You can easily hide data in various kinds of images/audio files without loosing any quality of original file.

Features

- Encryption of embedded data
- Compression of embedded data
- Embedding of a checksum to verify the integrity of the extracted data
- Supports for JPEG, JPG, BMP, WAV, AU files
- Preventing personal data
- Increasing security and data assurance
- Hide data in plain sight

Installation steps

- Open the Kali Linux terminal and update the packages
- **sudo apt-get upgrade**

- Steghide is already available in Kali Linux repository just run the command below
- **sudo apt-get install steghide**

Once it's installed in to open the tool just typing steghide

The arguments are as follows

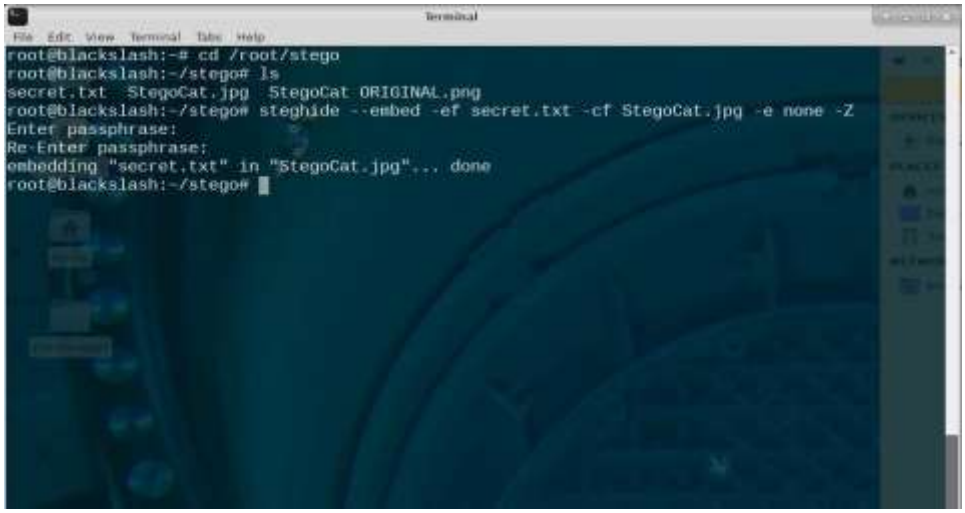
- **-ef** specifies the path of the file that you want to hide. You can embed any kind of file inside of the cover file, including Python scripts or shell files.
- **-cf** is the file that the data is embedded into. This is restricted to BMP, JPEG, WAV, and AU files.
- **-sf** is an optional argument that specifies the output file. If this is omitted, the original cover file will be overwritten by your new steganographic file.
- **-z** specifies the compression level, between 1 and 9. If you prefer not to compress your file, use the argument **-Z** instead.
- **-e** specifies the type of encryption. Steghide supports a multitude of encryption schemes, and if this argument is omitted by default, Steghide will use 128-bit AES encryption. If you prefer not use encryption, simply type **-e none**.

Embed hidden data into a file

To embed the data into another file by type the command line below.

- **Steghide embed –efsecret.txt –cf StegoCat.jpg –e none -z**

Here, embed – to embedding process, secret.txt – it denotes file to hidden into another file like text data file, StegoCat.jpg – it denotes as cover file,



Once you have executed the Steghide command, you will be prompted to set a password that will allow you to extract the embedded data later. So enter your passphrase and re-enter it to confirm. Once you get used to this process, it'll only take seconds to hide your data inside an image or audio file with Steghide.

Extract hidden data from the file

Extracting hidden data from a steganographic image is even easier. The command uses the syntax below.

$ steghide extract -sf stegoFile -xfoutputFile

Now you'll be prompted to enter the same password you created above in order to create the extracted file.

That you can hide data in plain sight, but you can really blow it if you don't follow some common sense rules. First, the small differences steganography introduces are hard to detect unless you have the original.

#3 EXIF Tool

EXIF Tool is usedto find the metadata, Metadata is simply data about data, or in our context, data about content. While the word has far reaching definitions, we will focus on how it applies to digital photos. Normally, this would contain information describing the type of image, when the image was created, and other details such as contrast, color and context.

Specially this tool used in cyber investigation to found the credential data from image like GPS position, Original time and date, device name and more. Exif Tool supports many different metadata formats including EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF and more.

For hackers or OSINT researchers gathering digital evidence, photos can be a rich source of data. Besides what's visible in the picture itself, metadata about when and where the photo was taken can also be recoverable. This data can include the device the photo was taken on, the GPS of the image and more unique data.

Installation steps

- Open Kali Linux terminal and upgrade packages
- **sudo apt-get upgrade**
- **sudo apt-get install ruby**
- **sudo apt-get install exif**
- Now the tool installed successfully

Usages

$ exif --help
-v, --version Display software version
-i, --ids Show IDs instead of tag names
-t, --tag=tag Select tag
-l, --list-tags List all EXIF tags
-|, --show-mnote Show contents of tag MakerNote
--remove Remove tag or ifd
-s, --show-description Show description of tag
-e, --extract-thumbnail Extract thumbnail

-r, --remove-thumbnail Remove thumbnail

-n, --insert-thumbnail=FILE Insert FILE as thumbnail

--no-fixup Do not fix existing tags in files

-o, --output=FILE Write data to FILE

--set-value=STRING Value of tag

-c, --create-exif Create EXIF data if not existing

-m, --machine-readable Output in a machine-readable (tab delimited) format

-w, --width=WIDTH Width of output

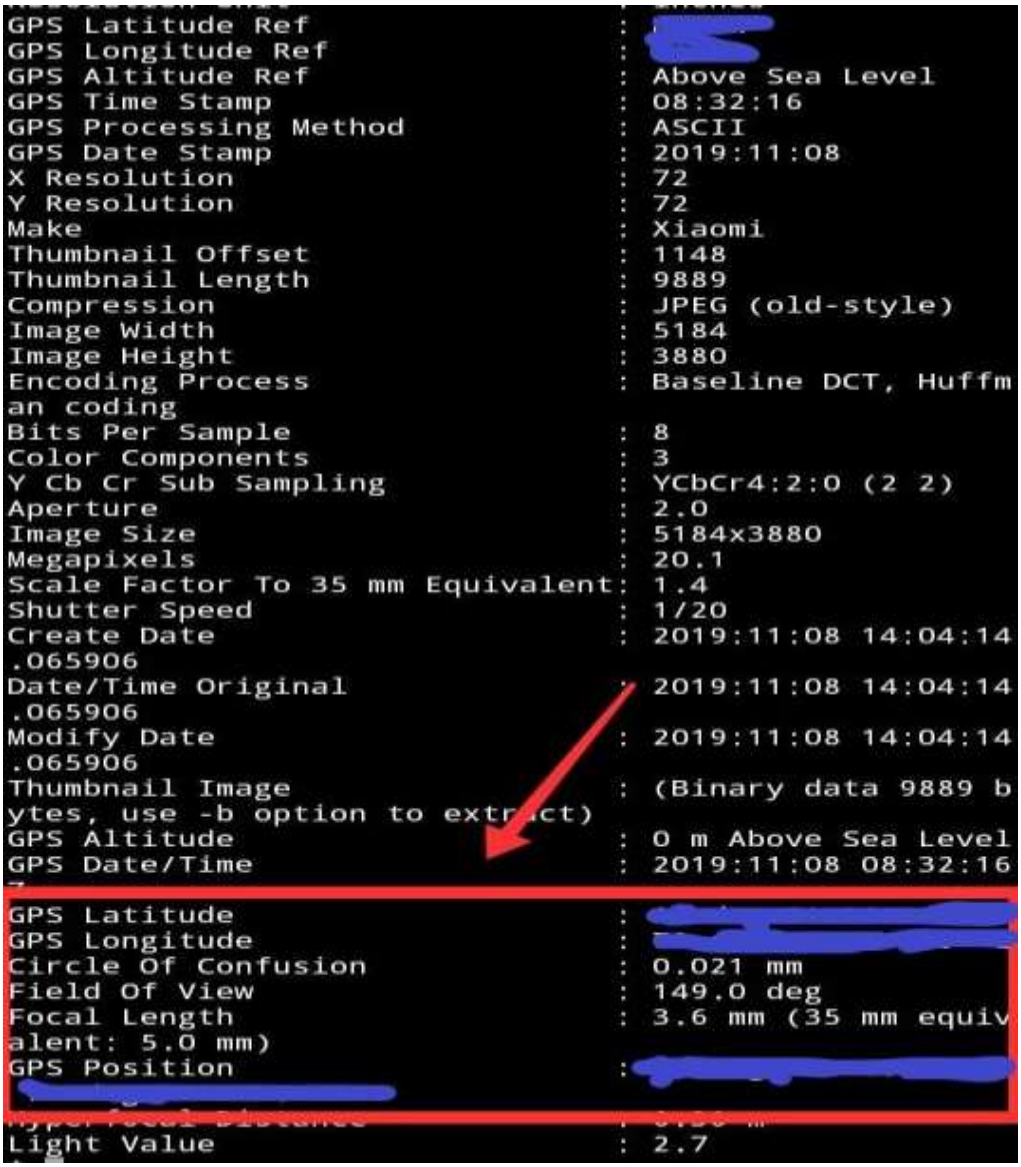
-x, --xml-output Output in a XML format

-d, --debug Show debugging messages

Run the Tool

- **exif [path/filename.jpg] –attribute**
- **exif /root/home/images/flower.jpg –o**

Now exif tool to find the metadata of given image



Understanding metadata in images is critical. You might find yourself looking for someone else, or not wanting to be found at all. It's wise for the paranoid to check pictures that they're in for GPS tags and other possible identifying information, such as dates and software watermarks.

Reference :

1. https://www.yeahhub.com/use-steghide-stegosuite-steganography-tools-kali-linux/
2. https://null-byte.wonderhowto.com/how-to/hunt-down-social-media-accounts-by-usernames-with-sherlock-0196138/
3. http://jtechcode.blogspot.com/2019/11/exif-tool-obtain-valid-metadata-from.html
4. https://youtu.be/UNkrDHfE2Qo
5. https://youtu.be/dgRrR-0qpok
6. https://github.com/sherlock-project/sherlock
7. https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools
8. J TECHCODE - Youtube Channelhttps://www.youtube.com/jtechcode