OSIF

Open Source Intelligence Framework

whoami

Eskie Cirrus James Maquilang
KPMG Philippines

- Cybersecurity Lead Consultant
- Software Engineer
- Knights of Columbus
- General Santos City, PH

whoami

Al Francis

- Lead Information Security Analyst
- Software Engineer
- Project-AG

OSIF

OPENSOURCE INTELLIGENCE FRAMEWORK

OSIF is an open-source framework dedicated to OSINT. For the ease of use, the interface has a layout that looks like Metasploit.

Project was initiated by laet4x, it was started on year 2022.

```
─$ ./osif

                                                  ##    ####   #####   ######
                                                 #  #   #   #    #     #
                                                #    #  #        #     #
                                                #    #   ####    #     ####
                                                #    #       #   #     #
                                                 #  #   #   #    #     #
                                                  ##    ####   #####   #

                                                    >> OSINT Framework
                                                       >> @laet4x


       -=[ 1 api           ]=-
       -=[ 2 dns           ]=-
       -=[ 1 social        ]=-
       -=[ 1 subdomain     ]=-
       -=[ 1 uncategorized ]=-

[!] There are some issues ; use 'show issues' to see more details
osif > use dns/dns_records
osif dns(dns_records) > show options

Module options
==============

   Name    Value       Required  Description
   ----    -----       --------  -----------
   DOMAIN  google.com  Y         Provide your target Domain

osif dns(dns_records) >
```

Open Source Intelligence Framework

- Attack Surface
- Blockchain
- Email
- Geolocation
- Host Enumeration
- IoC
- Mobile
- Social Media
- Web Enumeration

https://github.com/fr4nc1stein/osint-framework

Modules

Email Hunter

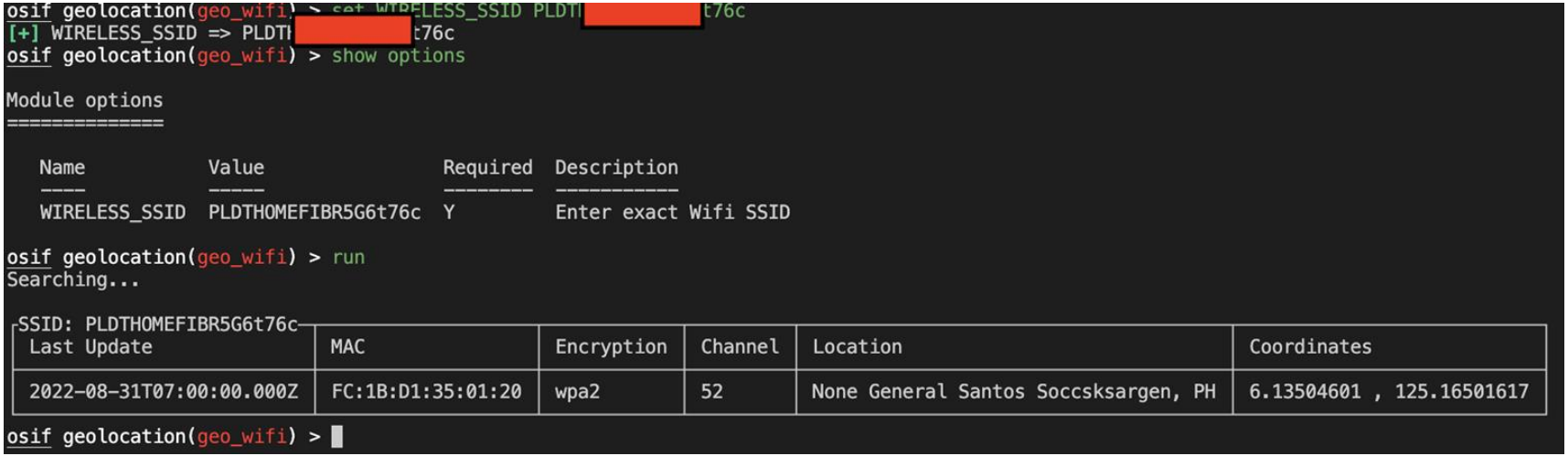
```
osif > use email/hunter_email
osif email(hunter_email) > set DOMAIN google.com
osif email(hunter_email) > run

Analyzing 'google.com'...

Extracted Emails::

google.com
```

Email	First Name	Last Name	Position	Phone	Linkedin	Twitter
[redacted]@google.com	[redacted]		None	None	None	None
[redacted]google.com			None	None	None	None
[redacted]@google.com			None	None	None	None
[redacted]gle.com		[redacted]er	None	None	None	None
[redacted]in@google.com			None	None	None	None
[redacted]google.com			None	None	None	None
[redacted]@google.com			None	None	None	None
[redacted]ogle.com			None	None	None	None
[redacted]r@google.com			None	None	None	None
[redacted]ogle.com			None	None	None	None

```
osif email(hunter_email) >
```

Modules

GeoWifi



Modules

Shodan Attack Surface

```
osif > use attack-surface/shodan_search
osif attack-surface(shodan_search) > set HOST_IP 18.205.222.128
osif attack-surface(shodan_search) > run

Analyzing '18.205.222.128'...

SHODAN
 HOST       18.205.222.128

 ASN        AS14618
 HOSTNAME   backerkit.com,ec2-18-205-222-128.compute-1.amazonaws.com
 ORG        Amazon Technologies Inc.
 ISP        Amazon.com, Inc.
 PORTS      80,443
 SERVICES   http,https

osif attack-surface(shodan_search) >
```

Modules

Bitcoin Balance

```
osif blockchain(bitcoin_balance) > run

BALANCE
 ADDRESS                 bc1qktj7rdvczswrmwlqz6ktfrwd9csdfczjs4e85u

 address                 bc1qktj7rdvczswrmwlqz6ktfrwd9csdfczjs4e85u
 received                0.39656787
 sent                    0.0
 balance                 0.39656787
 tx_count                2
 unconfirmed_tx_count    1
 unconfirmed_received    105001
 unconfirmed_sent        39656787
 unspent_tx_count        0
 first_tx
 last_tx

osif blockchain(bitcoin_balance) >
```

Installation - Docker

```
git clone https://github.com/fr4nc1stein/osint-framework osif

cd osif

docker-compose up -d

docker exec -ti osif bash

  ./osif
```

Installation

```
git clone https://github.com/fr4nc1stein/osint-framework osif

cd osif

pip3 install -r requirements.txt
```

Roadmap

Adding more modules:

- Attack Surface (censys)
- Email (snov.io)
- Repositories (searchcode)

How to contribute

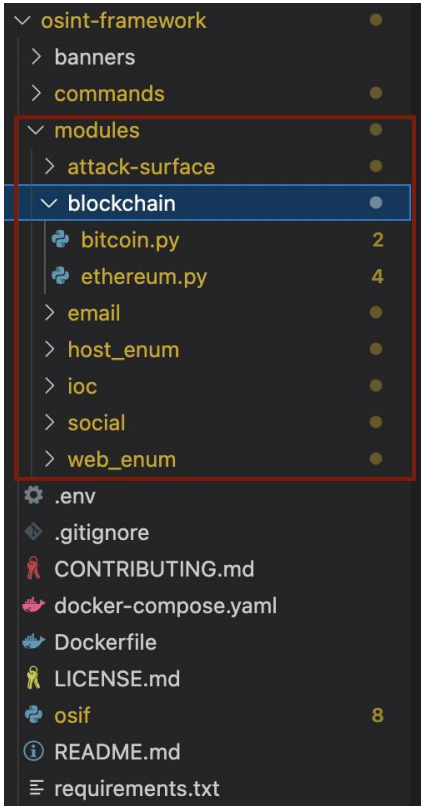
There are many ways to contribute to the OSIF project. This overview summarizes the most important steps to get you started as a contributor.

- Report bugs to the OSIF issue tracker.
- Make suggestions for changes, updates, or new features to the OSIF issue tracker.
- Contribute bug fixes, example code, documentation, or tutorials to OSIF.
- Contribute new features to OSIF.

Contribute new modules

- *Fork it!*
- *Create your feature/module branch:* ***git checkout -b my-new-module***
- *Commit your changes:* ***git commit -am 'Add some module'***
- *Push to the branch:* ***git push origin my-new-module***
- *Submit a pull request*

How to contribute




```python
from sploitkit import *
import requests

class dnsRecords(Module):
    """ This module find DNS information
    Author:  laet4x
    Version: 1.0
    """
    config = Config({
        Option(
            'DOMAIN',
            "Provide your target Domain",
            True,
        ): str("laet4x.com"),
    })

    def run(self):
        domain = self.config.option('DOMAIN').value
        print("\n"" Analyzing '%s'..." % (domain))
        request = requests.get("https://api.hackertarget.com/dnslookup/?q=" + domain)
        res = request.text
        print("\n", res)
```