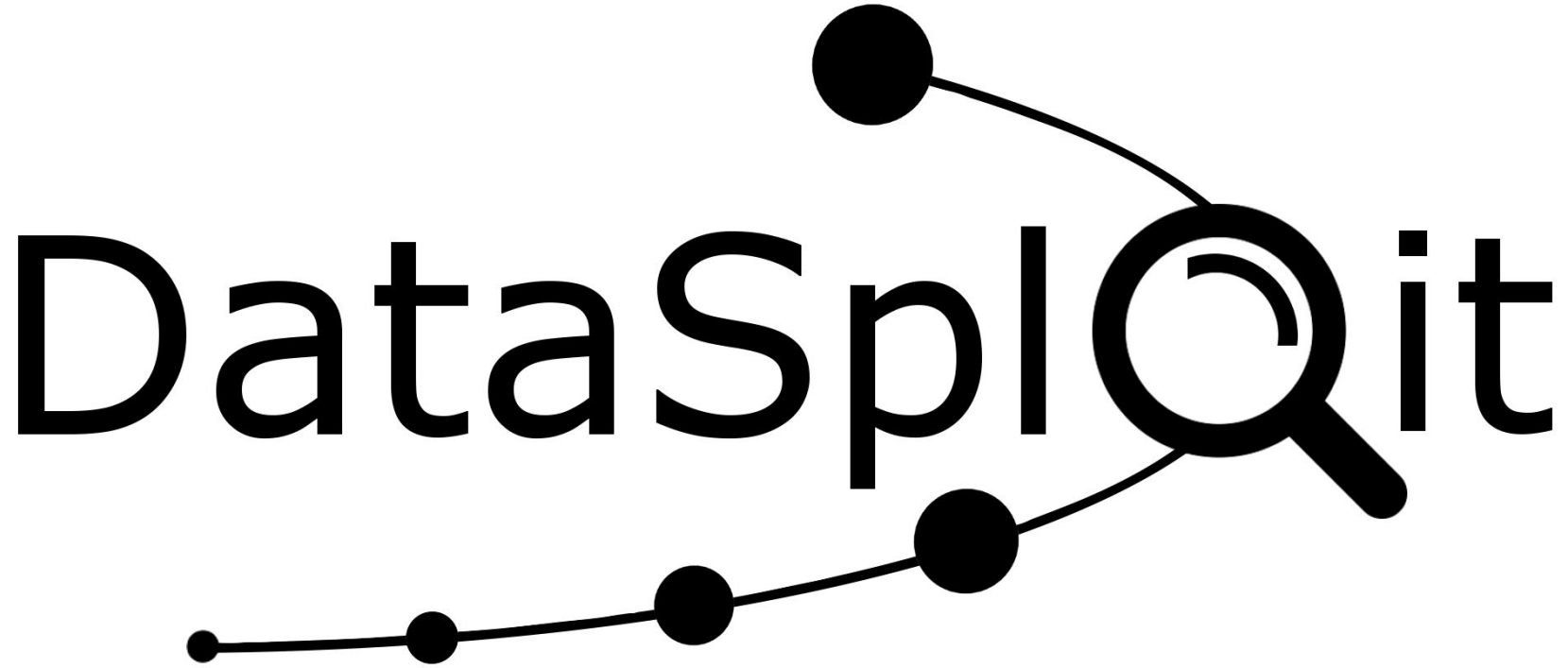


Open Source Assistant for #OSINT

https://github.com/datasploit/datasploit

http://datasploit.info | @datasploit

[shubhammittal:// $ whoami

- Just another Pen-tester.
- Security Consultant @ NotSoSecure
- 5+ Years of Experience

- Twitter - @upgoingstar
- Email - upgoingstaar@gmail.com

What’s DataSploit?

- Automated OSINT Tool for Domain / Email / Username / IP Addresses
- Fetches information from multiple HIDDEN sources.
- Works in passive mode.
- Written in Python.
- Multiple report formats available.

- Customized for Pen-testers / Product Security Guys / Cyber Investigators.

Why DataSploit?

- So much data.
  - Server’s Username / Passwords
  - Address
  - Email Id
  - Phone Number
  - Credentials
  - Interests
  - Friends
  - Preferences
  - Legacy Machines
  - Unnecessary Ports Information
  - Technologies in use, and blah blah..

Lets talk real time? History?

Well, you see it coming. What I found within 30 minutes was really stunning:

- 6 AWS access keys with their secret tokens
- 3 MongoDB connection URI (with login and password)
- 1 Twitter API credentials
- 1 Twilio API credentials
- 1 GitHub account credentials
- 1 Gmail account credentials
- And 1 Ravello Systems account credentials

Removed credentials Browse files

master

committed 9 days ago 1 parent commit

Showing 1 changed file with 5 additions and 5 deletions. Unified Split

10 group_vars/all View

```
@@ -1,11 +1,11 @@
 # Ravello's Credentials
-username: @redhat.com
-password:
-bucket:
+#username:
+#password:
+#bucket:
```

June 25, 2015

Study: Leaked credentials on P… linked to 47 gov't agencies

credentials leaked site:pastebin.com

All Images News Videos Maps More Settings Tools

About 1,140 results (0.40 seconds)

Leaked Steam Credentials <3 - Pastebin.com
pastebin.com/cDQX04AQ
Leaked Steam **Credentials** <3. a guest Jul 3rd, 2015 262 Never. Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

Philippine Information Agency Full Credentials Leaked - Pastebin.com
pastebin.com/TWuKVS95
Dec 28, 2013 - Philippine Information Agency Complete User **Credentials Leaked**. Website: http ://news.pia.gov.ph. Country: Philippines. Database: pianews.

FULL INSTAGRAM DATABASE LEAKED 2017 - Pastebin.com
pastebin.com/R6VfmHrJ
Jan 27, 2017 - Whether or not the **leaked** Instagram **credentials** are authentic, it never hurts to change ... Searches related to Instagram database **leak** ...

25+ Leaked TWC Account Login Credentials - **NEW MAY 2016 ...
pastebin.com/5tiyxT3E
25+ **Leaked** TWC Account Login **Credentials** - **NEW MAY 2016**. a guest May 25th, 2016 284 Never ... **Leaked** by: xjkn3rX. Full Dump: COMMENCED ...

Leaked User Credentials of Nice Print Photography & PIAP PH ...
pastebin.com/gy8HsghE
Leaked User **Credentials** of Nice Print Photography & PIAP PH. a guest Oct 11th, 2015 1,230 Never. Not a member of Pastebin yet? Sign Up, it unlocks many ...

Components

- Domain Osint
- Email Osint
- IP Osint
- Username Osint

- WIP
  - Company Scoping
  - Phone Number OSINT
  - Active Modules

Sources and Flow

Domain:

WhoIS
DNS Records
PunkSpider
Wappalyzer
Github
Email Harvestor
Domain IP History
Paste(s) Search
Pagelinks
Wikileaks
Links from Forums
Passive SSL Scan
ZoomEye
Shodan
Censys
Subdomains

Email:

Basic Email Checks
Work History
Social profiles
Enumerated Usernames
Location Information
Slides
Scribd Documents
Related Websites
HaveIBeenPwned

Username:

Git Details
Check username on various sites.
Profile Pics –Output saved in $username directory
Frequent Hashtags
Interaction on Twitter.

Active Modules

Setting it up..

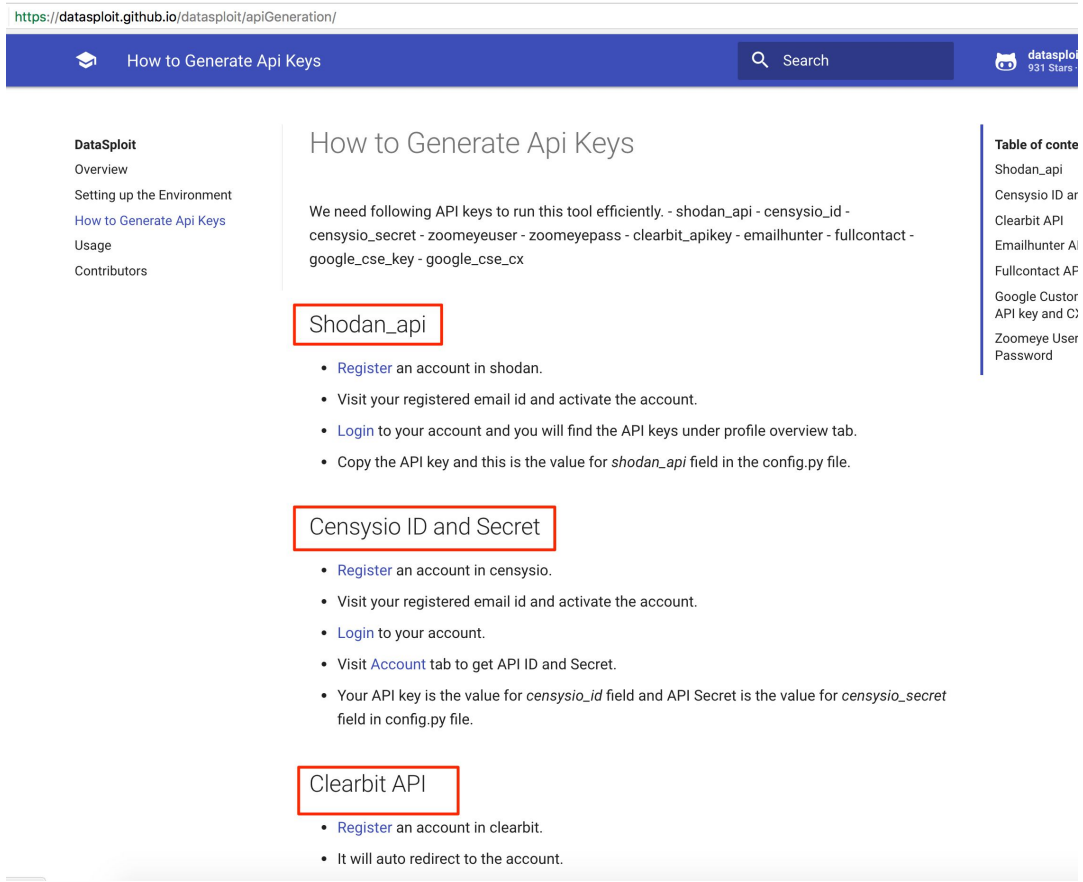
- Manual
  - Download from git (git clone or download)

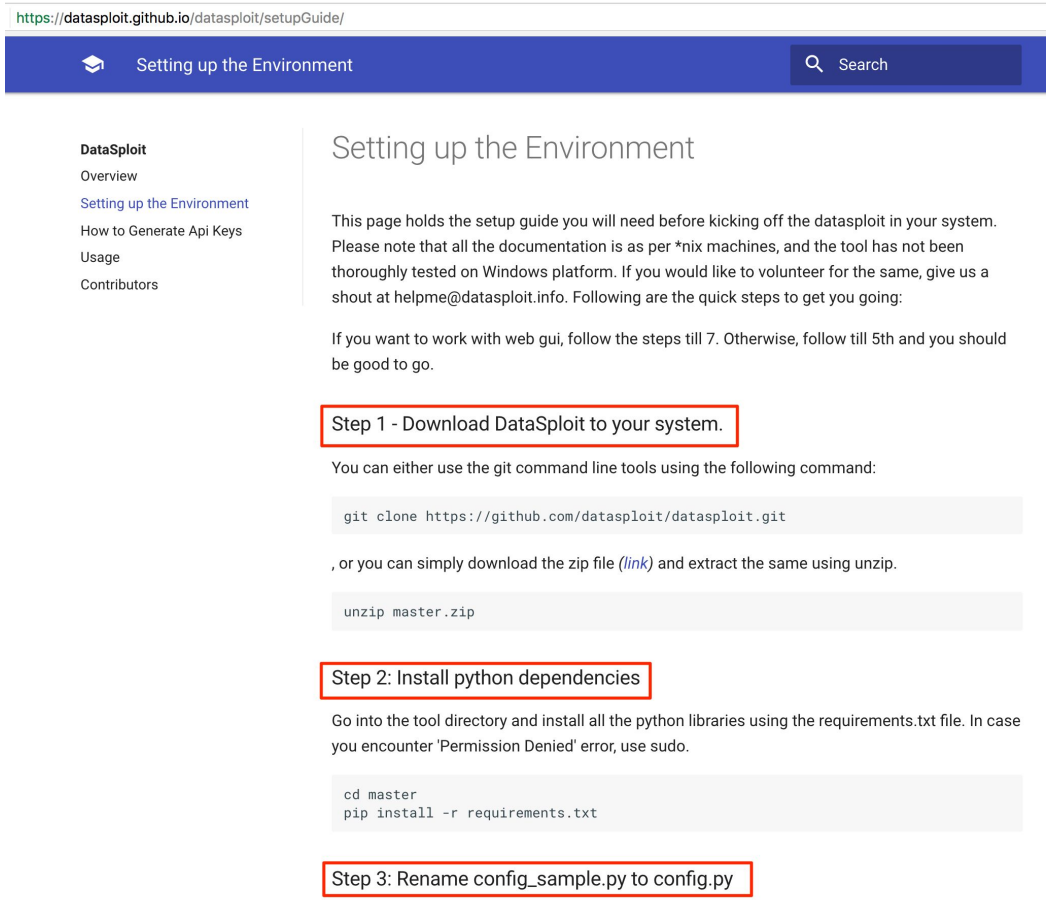
    git clone https://github.com/DataSploit/datasploit.git
  - pip install –r requirements.txt
  - config.py holds API keys
  - **domain_xyz.py** – running stand alone scripts.
  - **domainOsint / emailOsint / ipOsint** – automated OSINT
  - active_scan.py

- Automated
  - https://hub.docker.com/r/appsecco/datasploit/
  - https://hub.docker.com/r/ftorn/datasploit/

Documentation.

https://datasploit.github.io/datasploit/



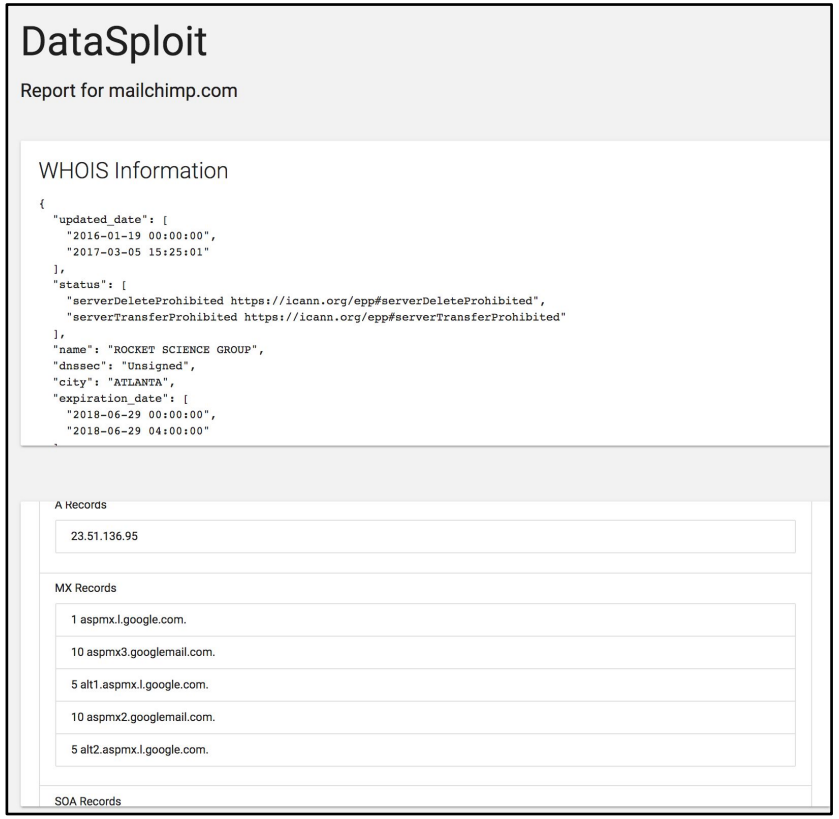


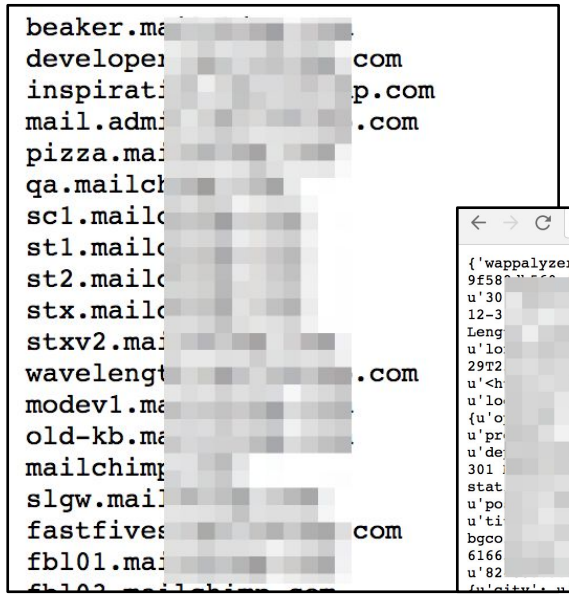
What's in there?

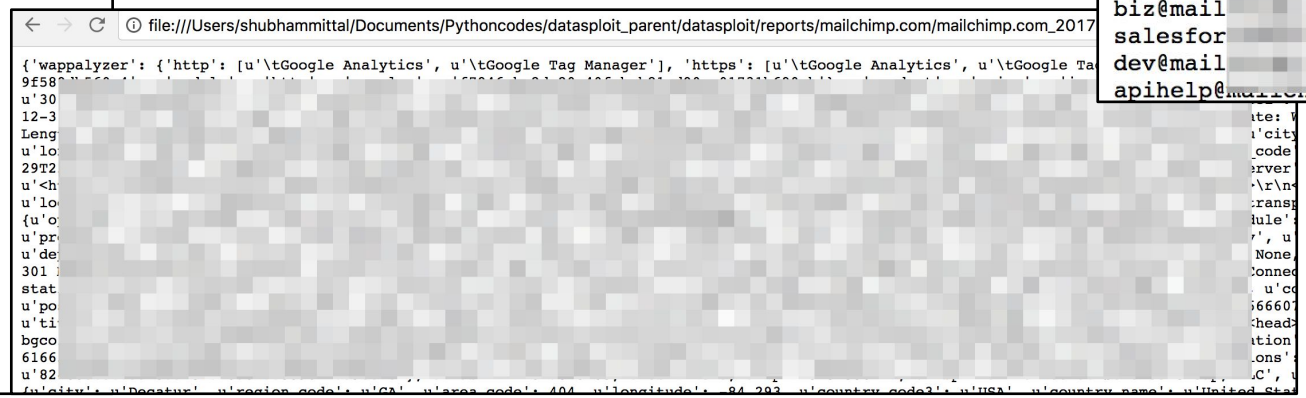
```
shubhammittal:datasploit/ (master*) $ ls
Finding                         datasploit.py                   domain_forumsearch.py
License.txt                     dochelp                         domain_forumsearch.pyc
Payload.class                   docs                            domain_github.py
Presentations                   domainOsint.py                  domain_github.pyc
README.md                       domain_GooglePDF.py             domain_history.py
active_default_file_check.py    domain_censys.py                domain_history.pyc
badges                          domain_censys.pyc               domain_pagelinks.py
check_urls.txt                  domain_checkpunkspider.py       domain_pagelinks.pyc
config.py                       domain_checkpunkspider.pyc      domain_pastes.py
config.pyc                      domain_dnsrecords.py            domain_pastes.pyc
config_sample.py                domain_dnsrecords.pyc           domain_shodan.py
contributors.txt                domain_emailhunter.py           domain_shodan.pyc
core                            domain_emailhunter.pyc          domain_sslinfo.pyc

domain_subdomains.py            email_basic_checks.pyc          mkdocs.yml
domain_subdomains.pyc           email_fullcontact.py            requirements.txt
domain_wappalyzer.py            email_fullcontact.pyc           roadmap.txt
domain_wappalyzer.pyc           email_pastes.py                 temptweets.txt
domain_whois.py                 email_pastes.pyc                test.py
domain_whois.pyc                generate_passwords.py           test_domainOsint.py
domain_wikileaks.py             hbp.py                          testhtml.html
domain_wikileaks.pyc            ipOsint.py                      testreg.py
domain_zoomeye.py               ip_asn.pyc                      upgoingstar
domain_zoomeye.pyc              ip_shodan.py                    usernameOsint.py
emailOsint.py                   ip_shodan.pyc                   username_gitscrape.py
emailOsint.pyc                  ip_whois.py                     username_reddit.py
email_basic_checks.py           ip_whois.pyc
```

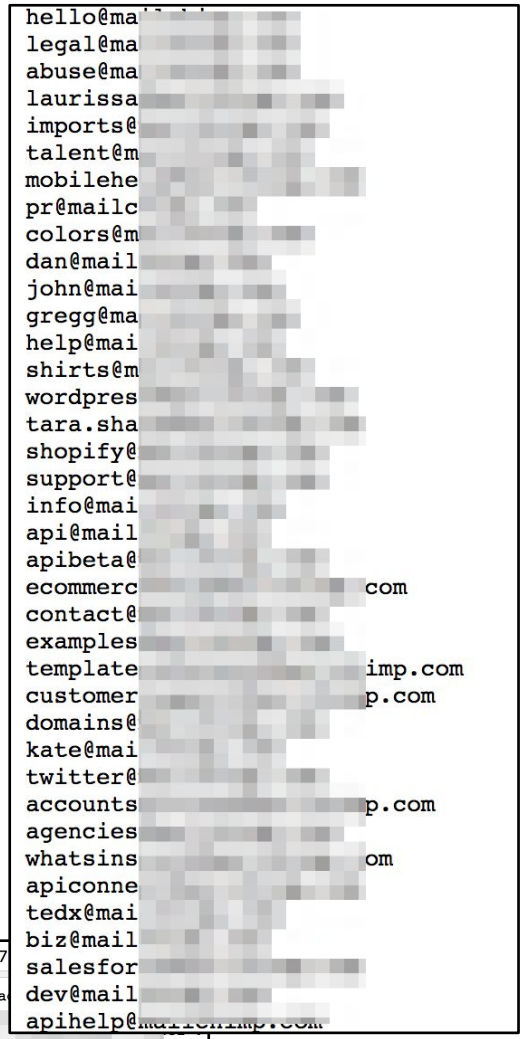
Output Formats

- HTML
- JSON
- Emails List (txt file)
- Subdomains List (txt file)










DEMO TIME
LET'S HOPE THE DEMO-GODS ARE SMILING!
memegenerator.net

Twitter:

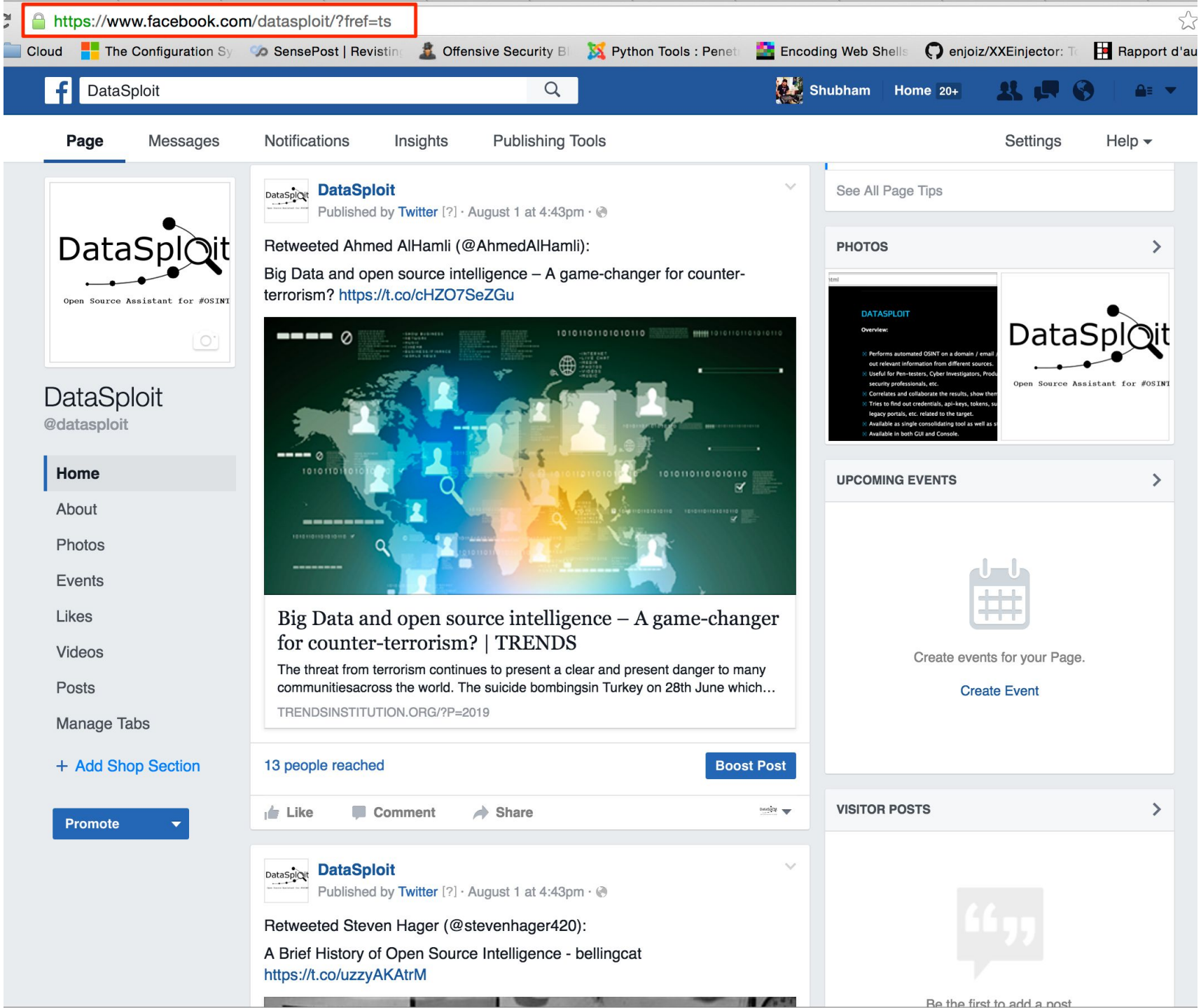
@dataspoloit

https://twitter.com/dataspoloit

Facebook:

/datasploit

https://www.facebook.com/datasploit/



Roadmap

- Allows to set up periodic scans and alerting for product security companies.
- Intelligence on co-relation and identity verification.
- Reports in CSV.
- Reverse Image Search and profile validation.
- Works closely with various social network APIs.
- Refine Pastebin and Github Searches.
- IP Threat Intelligence.
- Organization Scoping.
- Integration with SE other tools.
- Cloud related OSINT and active modules.
- pip install datasploit (to be installed as both library as well as script)

Coverage

OSINT Framework

How to Contribute

- Help us in testing the tool
- Expand : Write/Suggest modules
- Give Feedback: raise issues, tweet, drop an email.
- Use / Promote / Write about the tool.
- Write OSINT blogs / tool walkthrough(s) / etc.

- Report issues at https://github.com/datasploit/datasploit/issues

Core Contributors.

- Shubham Mittal (@upgoingstar)
- Nutan Kumar Panda (@nutankumarpanda)
- Sudhanshu (@sudhanshu_c)
- Kunal (@KunalAggarwal92)

- Kudos to
  - @anantshri for mentoring.
  - @ bnchandrapal for feedbacks, suggestions and other help around issues.

Thanks. g0t questions?

https://github.com/DataSploit/datasploit

Follow @datasploit for OSINT news and latest updates.

Tweet / DM to ***@datasploit***

upgoingstaar@gmail.com