A PRIMER ON OSINT

Null/OWASP Bangalore

21st December, 2019

@ideaengine007 @ideaengine007 @ideaengine007

ABOUT ME

- ASE-T @T.C.S. Ltd
- Hyper Curious
- Musician
- Little Vulnerable

AGENDA

❑ *Getting Started*

❑ *Types of Intelligence Gathering*

❑ *A Scenario*

❑ *OSINT Gathering TTPs*

❑ *Applications*

❑ *Demos*

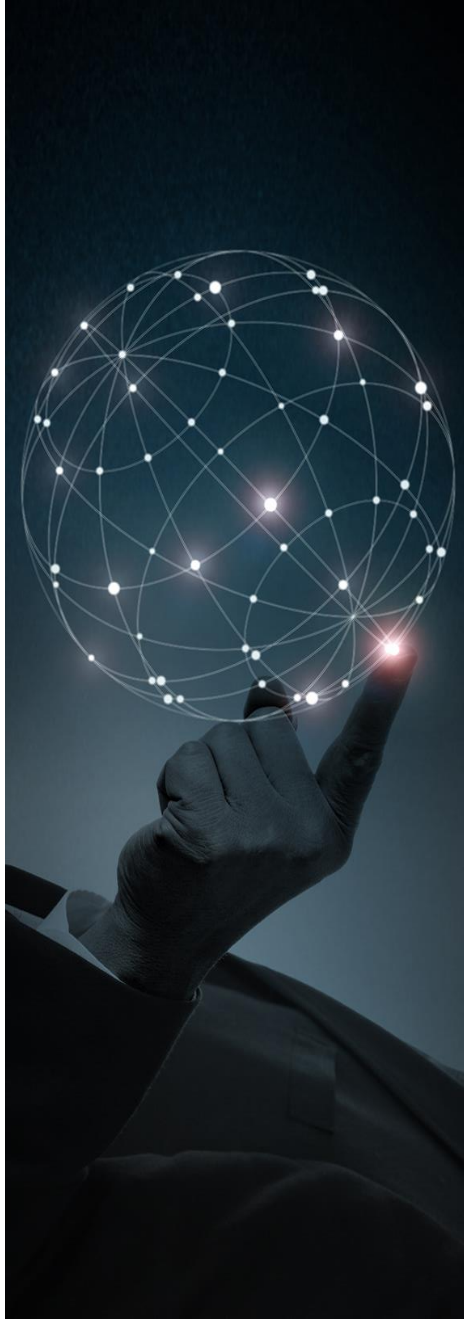
❑ *OSINT of OSINT*

❑ *References*

❑ *Conclusion*

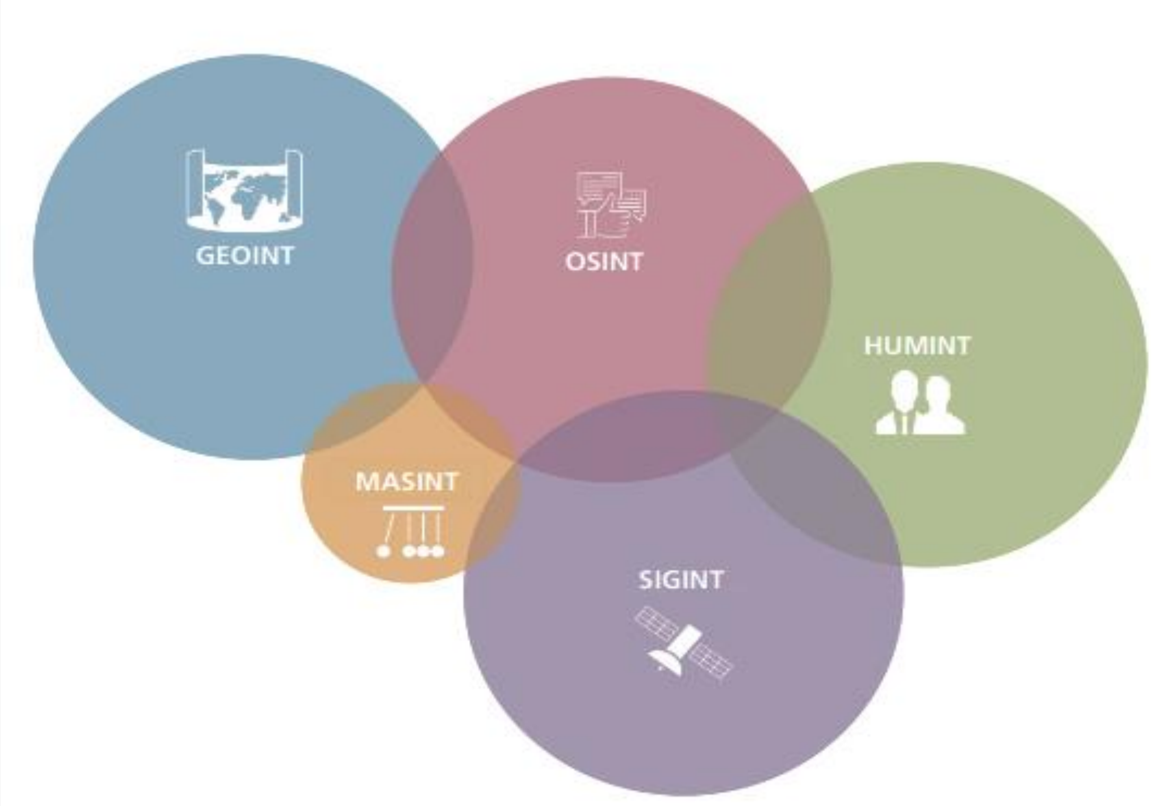
GETTING STARTED

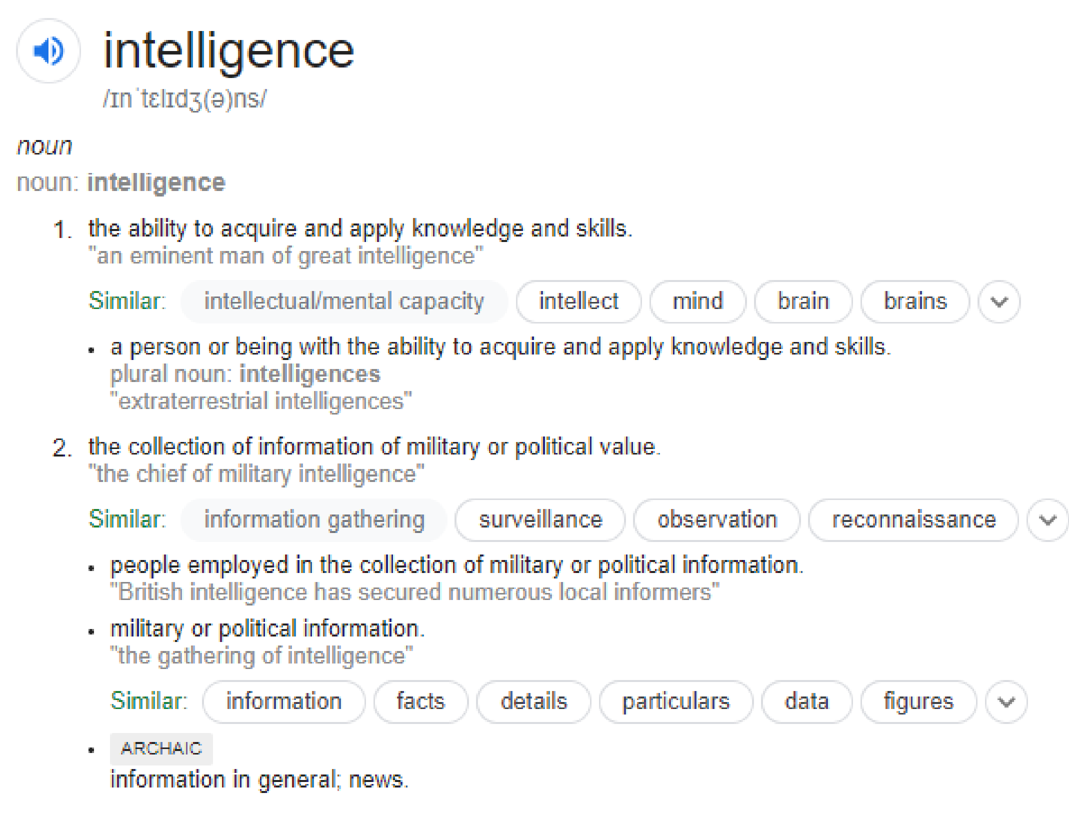
OSINT



“Gathering intelligence by exploiting publicly available resources.”

TYPES OF INTELLIGENCE GATHERING





intelligence

/ɪnˈtɛlɪdʒ(ə)ns/

noun

noun: **intelligence**

1. the ability to acquire and apply knowledge and skills.
   "an eminent man of great intelligence"

   Similar: intellectual/mental capacity · intellect · mind · brain · brains

   - a person or being with the ability to acquire and apply knowledge and skills.
     plural noun: **intelligences**
     "extraterrestrial intelligences"

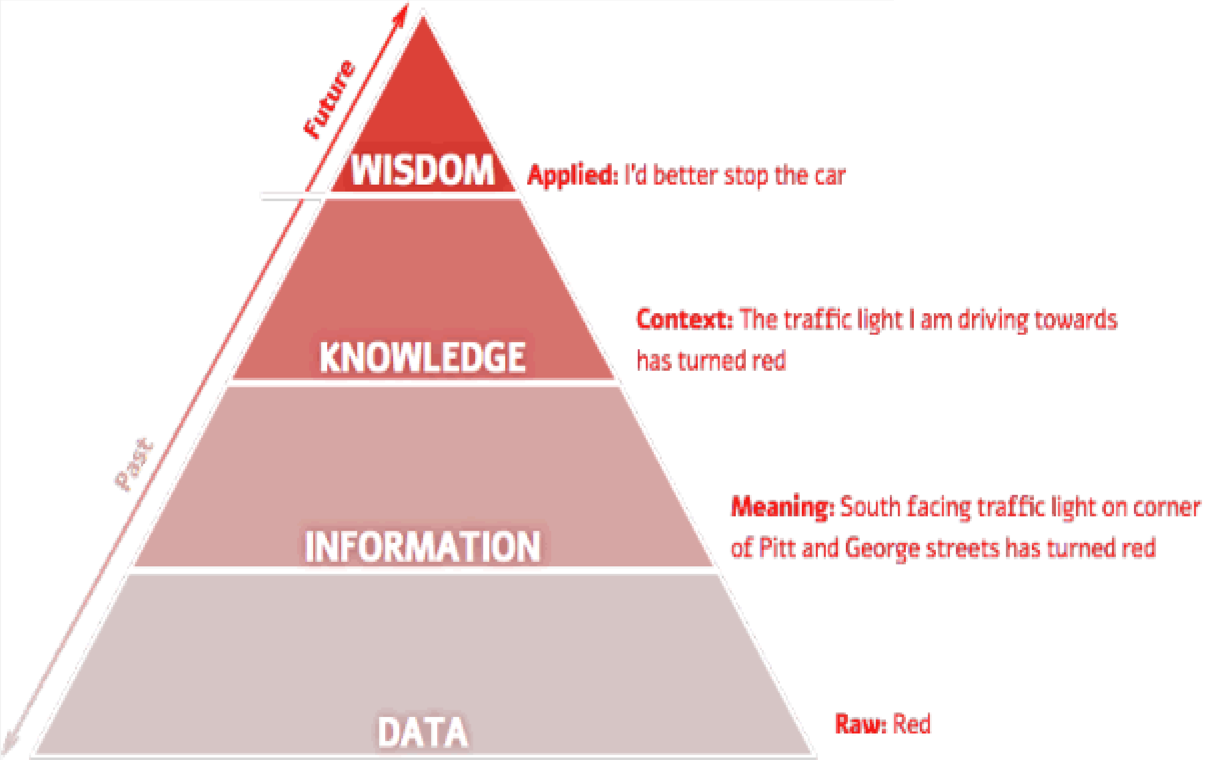
2. the collection of information of military or political value.
   "the chief of military intelligence"

   Similar: information gathering · surveillance · observation · reconnaissance

   - people employed in the collection of military or political information.
     "British intelligence has secured numerous local informers"
   - military or political information.
     "the gathering of intelligence"

     Similar: information · facts · details · particulars · data · figures

   - ARCHAIC
     information in general; news.

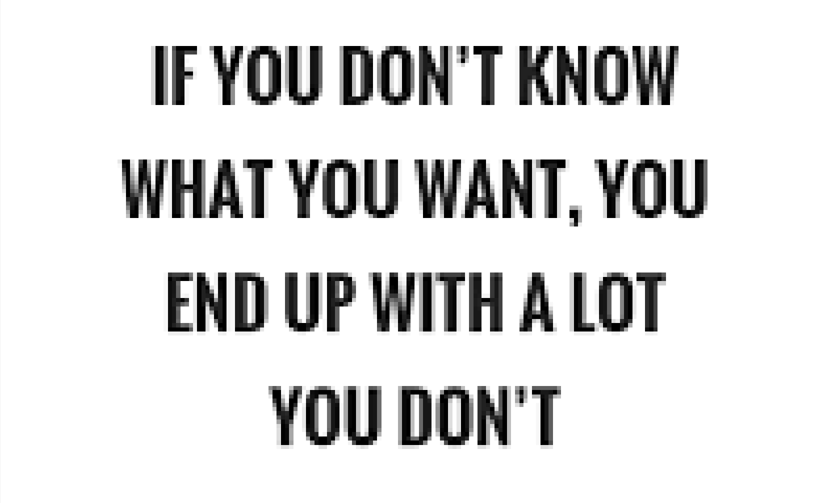


Applied: I'd better stop the car

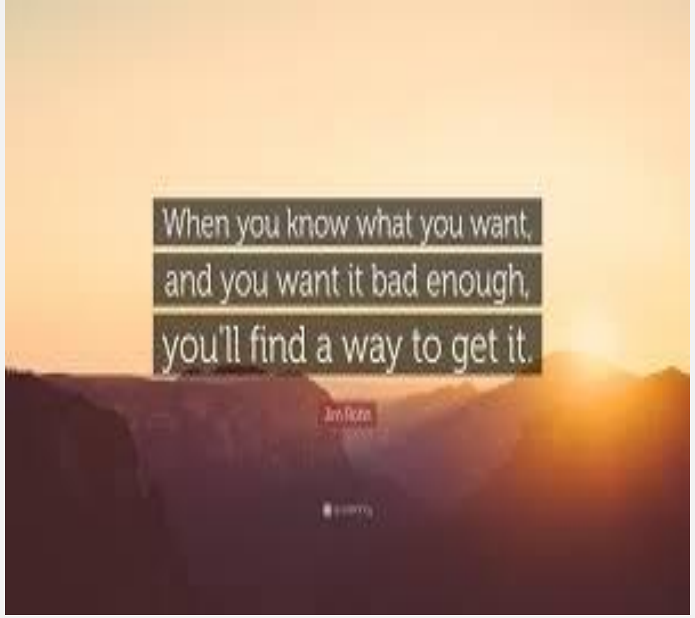
Context: The traffic light I am driving towards has turned red

Meaning: South facing traffic light on corner of Pitt and George streets has turned red

Raw: Red

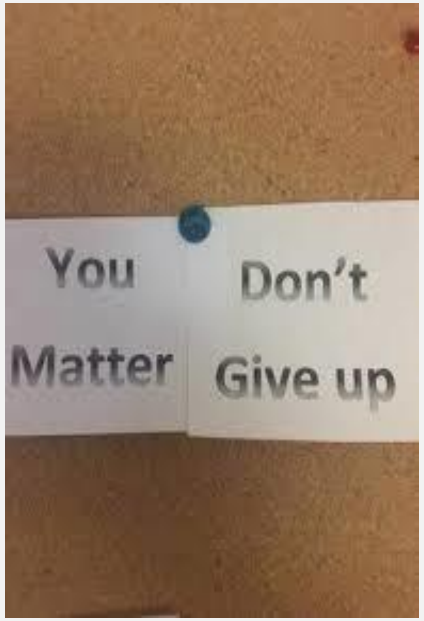


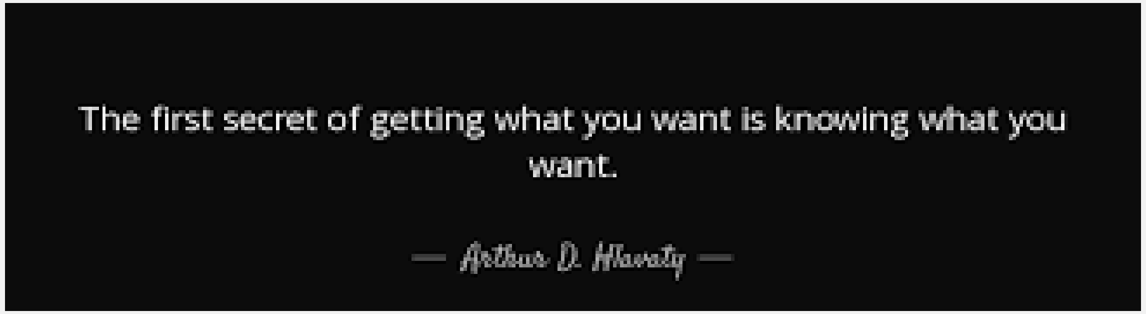
IF YOU DON'T KNOW WHAT YOU WANT, YOU END UP WITH A LOT YOU DON'T



When you know what you want, and you want it bad enough, you'll find a way to get it.

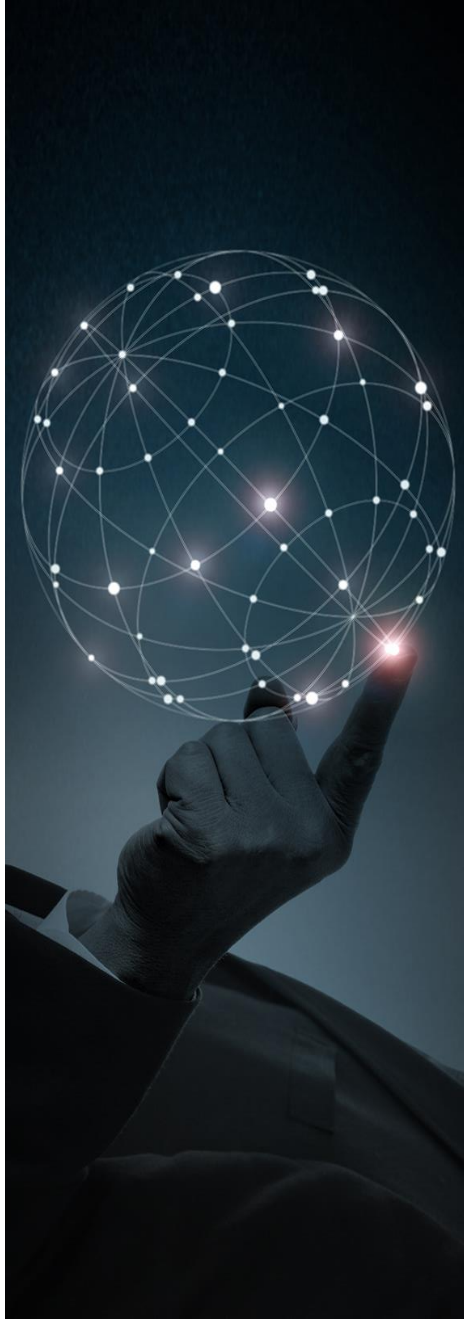
Jim Rohn



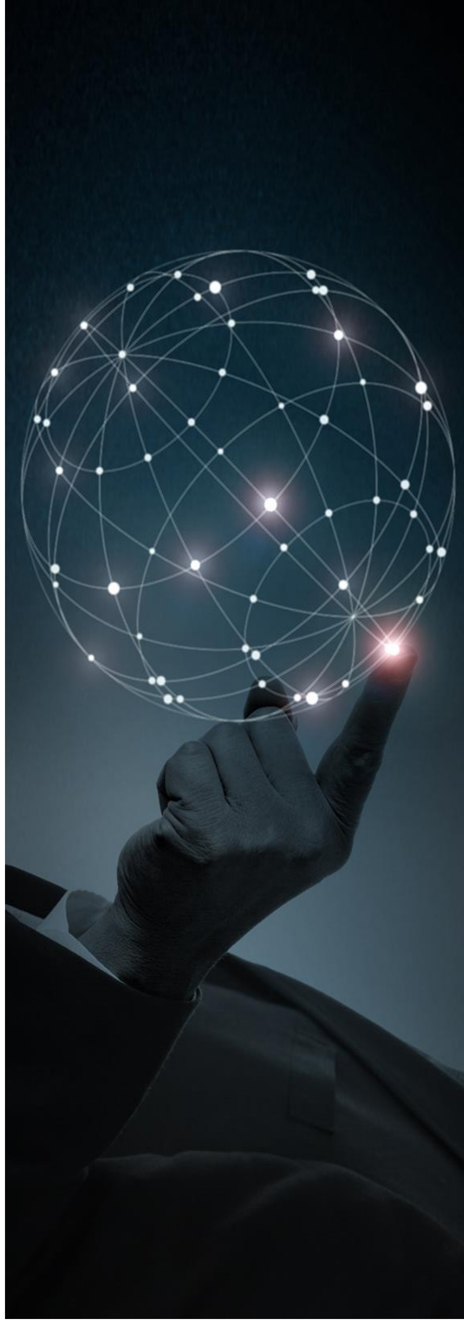


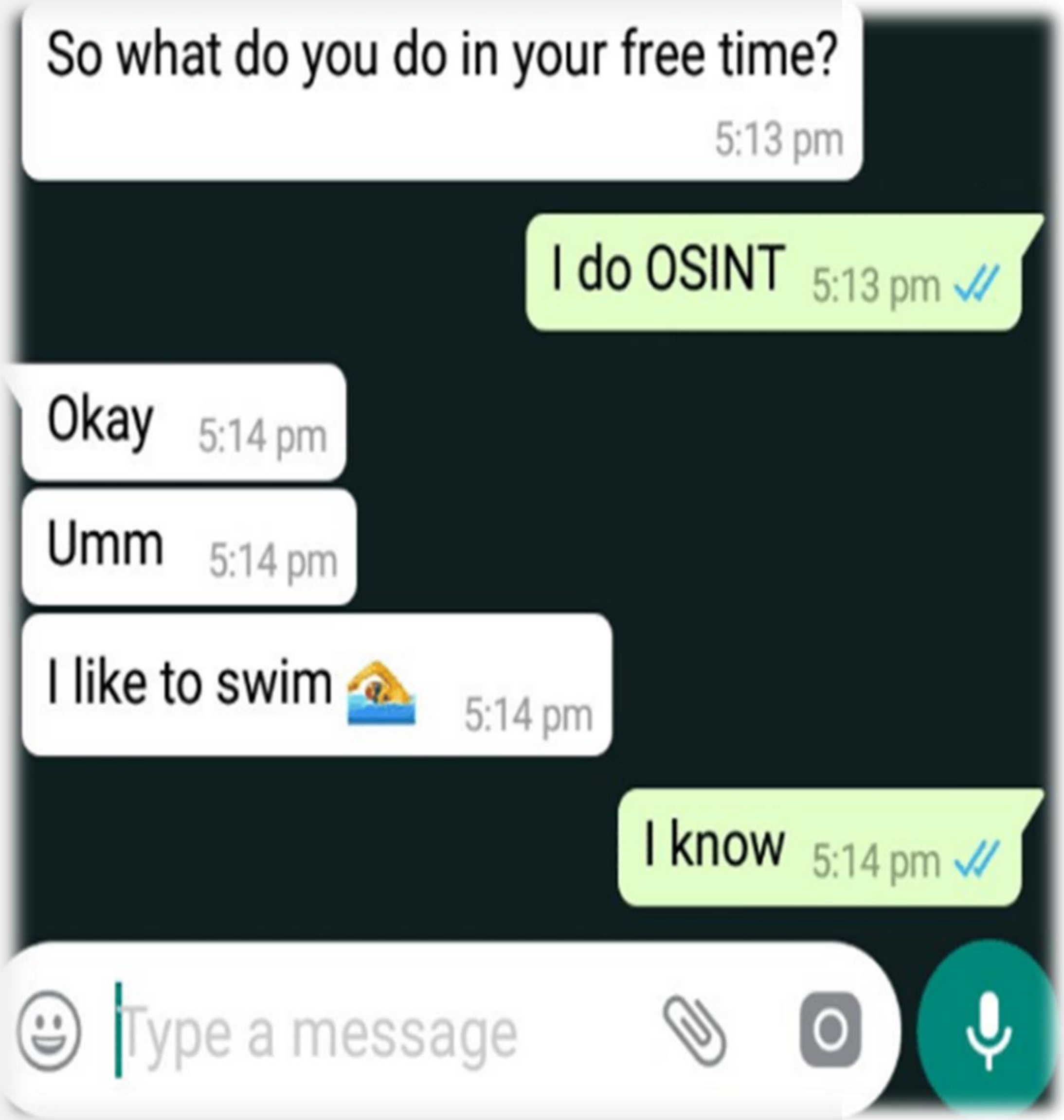
The first secret of getting what you want is knowing what you want.

— Arthur D. Hlavaty —



A SCENARIO





So what do you do in your free time? 5:13 pm

I do OSINT 5:13 pm ✓✓

Okay 5:14 pm

Umm 5:14 pm

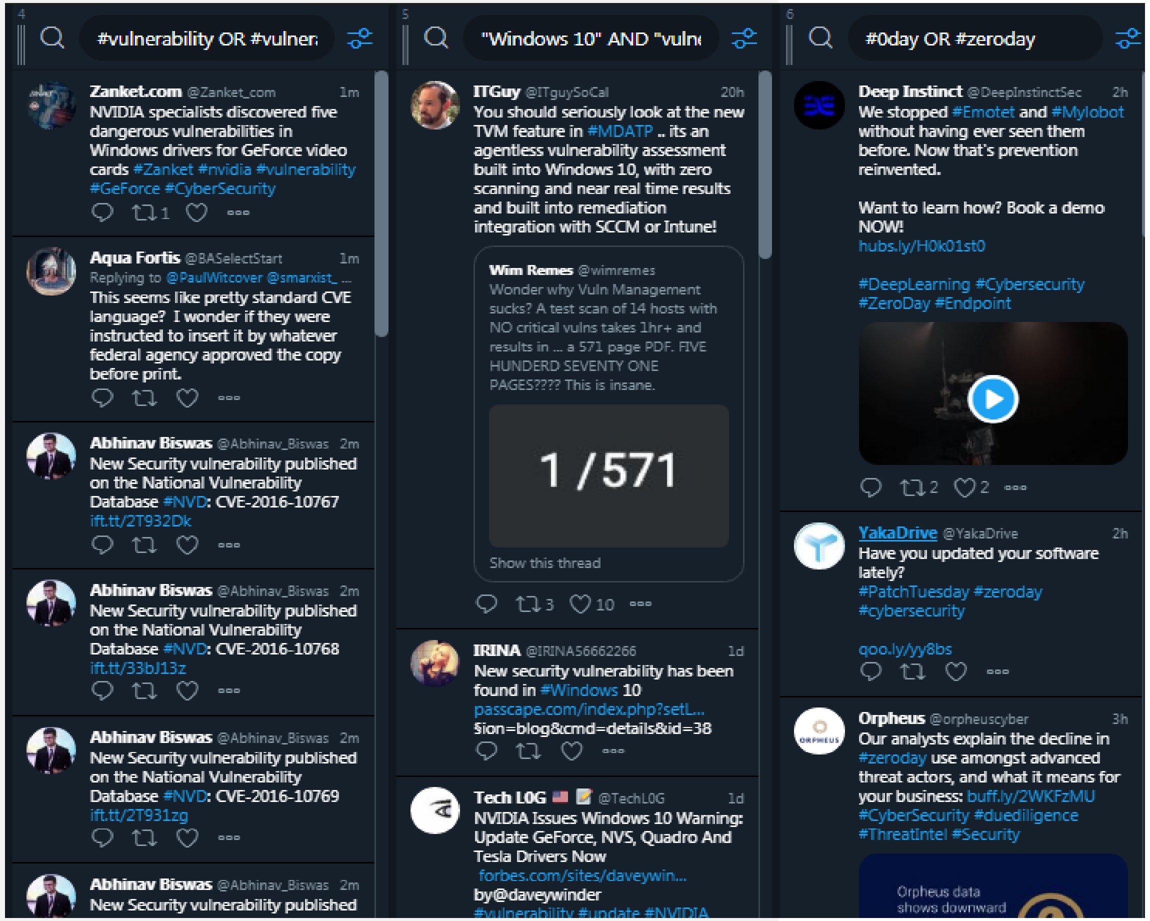
I like to swim 🏊‍♀️ 5:14 pm

I know 5:14 pm ✓✓

OSINT GATHERING TTPS

TweetDeck

- A social media dashboard application for management of Twitter accounts
- Customisable dashboard with unlimited columns to monitor trends, follow hashtags, and perform live searches
- Helps in observing events and incidents when supplied with proper filters
- You just need a Twitter Account [Click Here]
- Using Boolean Operators AND and OR, create filters



4 #vulnerability OR #vulner

Zanket.com @Zanket_com 1m
NVIDIA specialists discovered five dangerous vulnerabilities in Windows drivers for GeForce video cards #Zanket #nvidia #vulnerability #GeForce #CyberSecurity
1

Aqua Fortis @BASelectStart 1m
Replying to @PaulWitcover @smarxist_ ...
This seems like pretty standard CVE language? I wonder if they were instructed to insert it by whatever federal agency approved the copy before print.

Abhinav Biswas @Abhinav_Biswas 2m
New Security vulnerability published on the National Vulnerability Database #NVD: CVE-2016-10767 ift.tt/2T932Dk

Abhinav Biswas @Abhinav_Biswas 2m
New Security vulnerability published on the National Vulnerability Database #NVD: CVE-2016-10768 ift.tt/33bJ13z

Abhinav Biswas @Abhinav_Biswas 2m
New Security vulnerability published on the National Vulnerability Database #NVD: CVE-2016-10769 ift.tt/2T931zg

Abhinav Biswas @Abhinav_Biswas 2m
New Security vulnerability published

5 "Windows 10" AND "vulne

ITGuy @ITguySoCal 20h
You should seriously look at the new TVM feature in #MDATP .. its an agentless vulnerability assessment built into Windows 10, with zero scanning and near real time results and built into remediation integration with SCCM or Intune!

Wim Remes @wimremes
Wonder why Vuln Management sucks? A test scan of 14 hosts with NO critical vulns takes 1hr+ and results in ... a 571 page PDF. FIVE HUNDERD SEVENTY ONE PAGES???? This is insane.

1 / 571

Show this thread
3 10

IRINA @IRINA56662266 1d
New security vulnerability has been found in #Windows 10
passcape.com/index.php?setL...
$ion=blog&cmd=details&id=38

Tech L0G 🇺🇸 📝 @TechL0G 1d
NVIDIA Issues Windows 10 Warning: Update GeForce, NVS, Quadro And Tesla Drivers Now
forbes.com/sites/daveywin...
by@daveywinder
#vulnerability #update #NVIDIA

6 #0day OR #zeroday

Deep Instinct @DeepInstinctSec 2h
We stopped #Emotet and #Mylobot without having ever seen them before. Now that's prevention reinvented.

Want to learn how? Book a demo NOW!
hubs.ly/H0k01st0

#DeepLearning #Cybersecurity #ZeroDay #Endpoint
2 2

YakaDrive @YakaDrive 2h
Have you updated your software lately?
#PatchTuesday #zeroday #cybersecurity

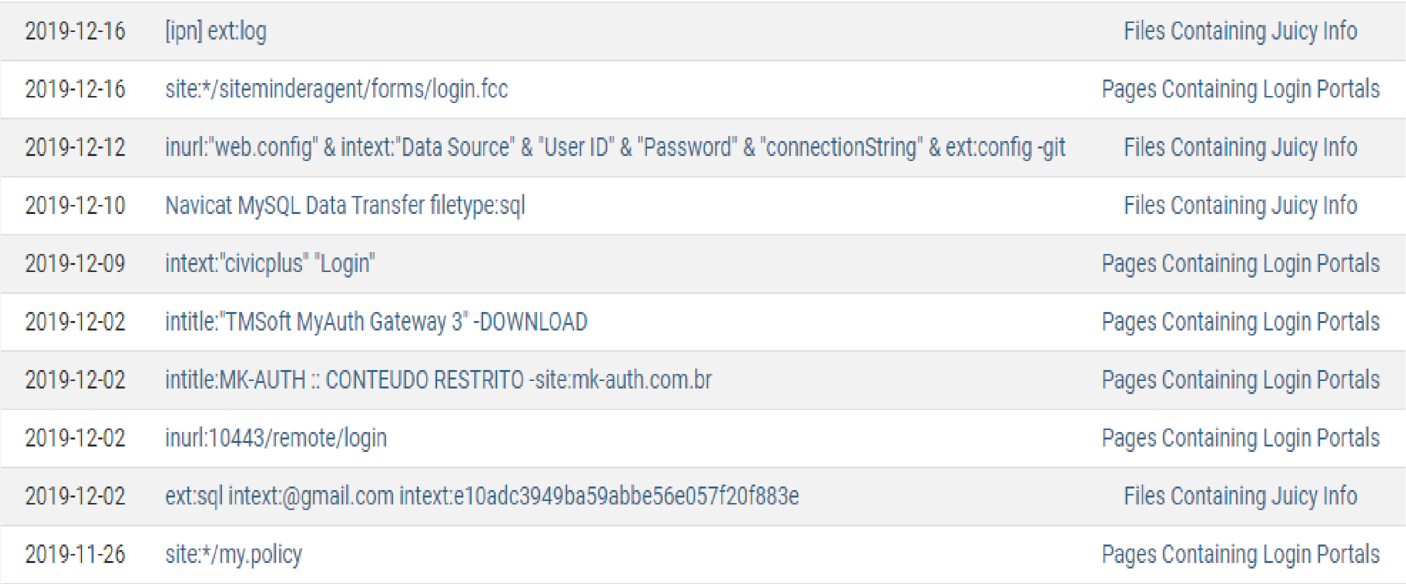
qoo.ly/yy8bs

Orpheus @orpheuscyber 3h
Our analysts explain the decline in #zeroday use amongst advanced threat actors, and what it means for your business: buff.ly/2WKFzMU #CyberSecurity #duediligence #ThreatIntel #Security

Orpheus data shows downward

Google Dorks

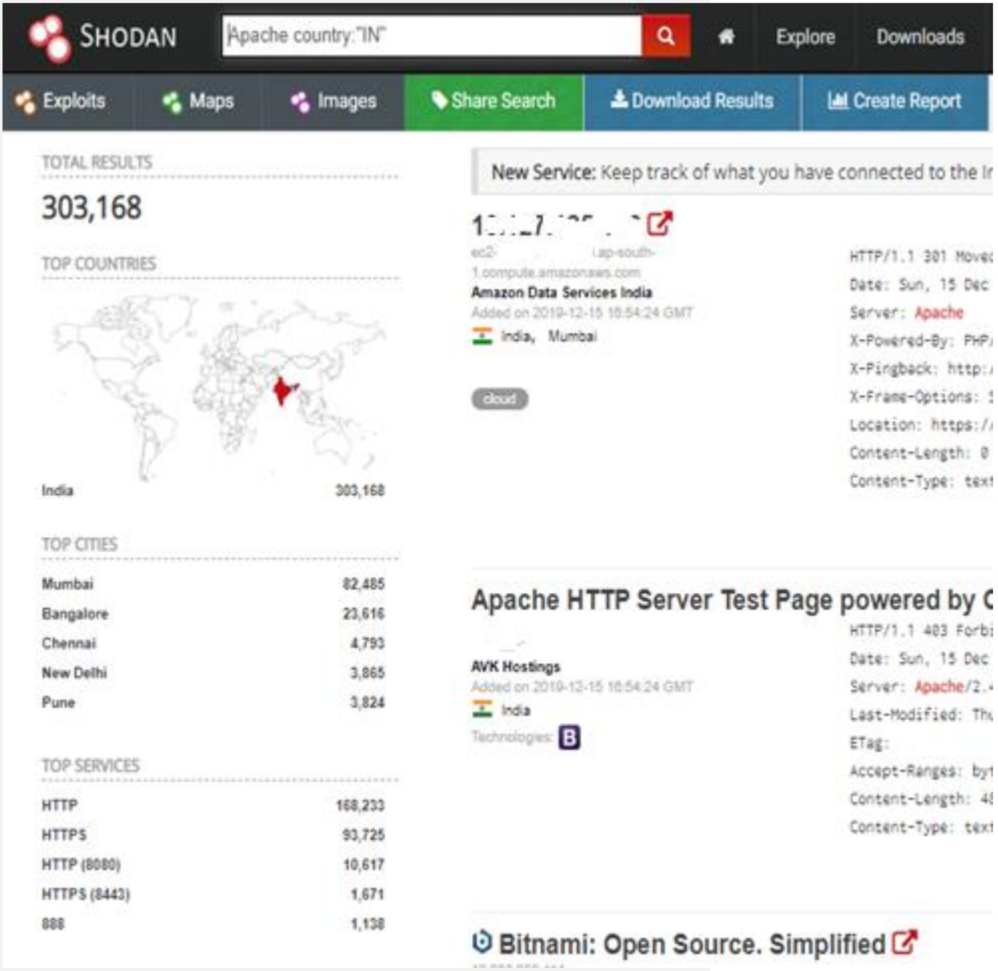
- Using Google Search for ‘focussed’ queries
- Finding vulnerable web applications and servers by using native Google search engine capabilities.
- Entire lists of queries with the formats are available to query ANYTHING.
- Dorks are populated on ExploitDB
- Interesting resources can be
  - Logs with ‘juicy’ info (eg. MySQL logs)
  - CSV files (eg. Payroll CSVs)
  - Login Pages (Admin portals)
  - Sensitive Directories and Files (eg. SSH keys)



2019-12-16	[ipn] ext:log	Files Containing Juicy Info
2019-12-16	site:*/siteminderagent/forms/login.fcc	Pages Containing Login Portals
2019-12-12	inurl:"web.config" & intext:"Data Source" & "User ID" & "Password" & "connectionString" & ext:config -git	Files Containing Juicy Info
2019-12-10	Navicat MySQL Data Transfer filetype:sql	Files Containing Juicy Info
2019-12-09	intext:"civicplus" "Login"	Pages Containing Login Portals
2019-12-02	intitle:"TMSoft MyAuth Gateway 3" -DOWNLOAD	Pages Containing Login Portals
2019-12-02	intitle:MK-AUTH :: CONTEUDO RESTRITO -site:mk-auth.com.br	Pages Containing Login Portals
2019-12-02	inurl:10443/remote/login	Pages Containing Login Portals
2019-12-02	ext:sql intext:@gmail.com intext:e10adc3949ba59abbe56e057f20f883e	Files Containing Juicy Info
2019-11-26	site:*/my.policy	Pages Containing Login Portals

Shodan

- Passive recon technique
- C.N.N. calls it the “scariest search engine of the world”
- Well, it’s just a search engine to find
  - Webcams
  - SCADA
  - Traffic Lights
  - Routers
  - Default Passwords (Oof!!)
- “It’s interesting. It’s exciting. It’s frightening.” – D.M.



TOTAL RESULTS

303,168

TOP COUNTRIES

India	303,168

TOP CITIES

Mumbai	82,485
Bangalore	23,616
Chennai	4,793
New Delhi	3,865
Pune	3,824

TOP SERVICES

HTTP	168,233
HTTPS	93,725
HTTP (8080)	10,617
HTTPS (8443)	1,671
888	1,138

New Service: Keep track of what you have connected to the Ir

[redacted]

ec2- [redacted] .ap-south-1.compute.amazonaws.com

Amazon Data Services India

Added on 2019-12-15 10:54:24 GMT

India, Mumbai

cloud

```
HTTP/1.1 301 Moved
Date: Sun, 15 Dec
Server: Apache
X-Powered-By: PHP/
X-Pingback: http:/
X-Frame-Options: S
Location: https:/
Content-Length: 0
Content-Type: text
```

Apache HTTP Server Test Page powered by C

AVK Hostings

Added on 2019-12-15 10:54:24 GMT

India

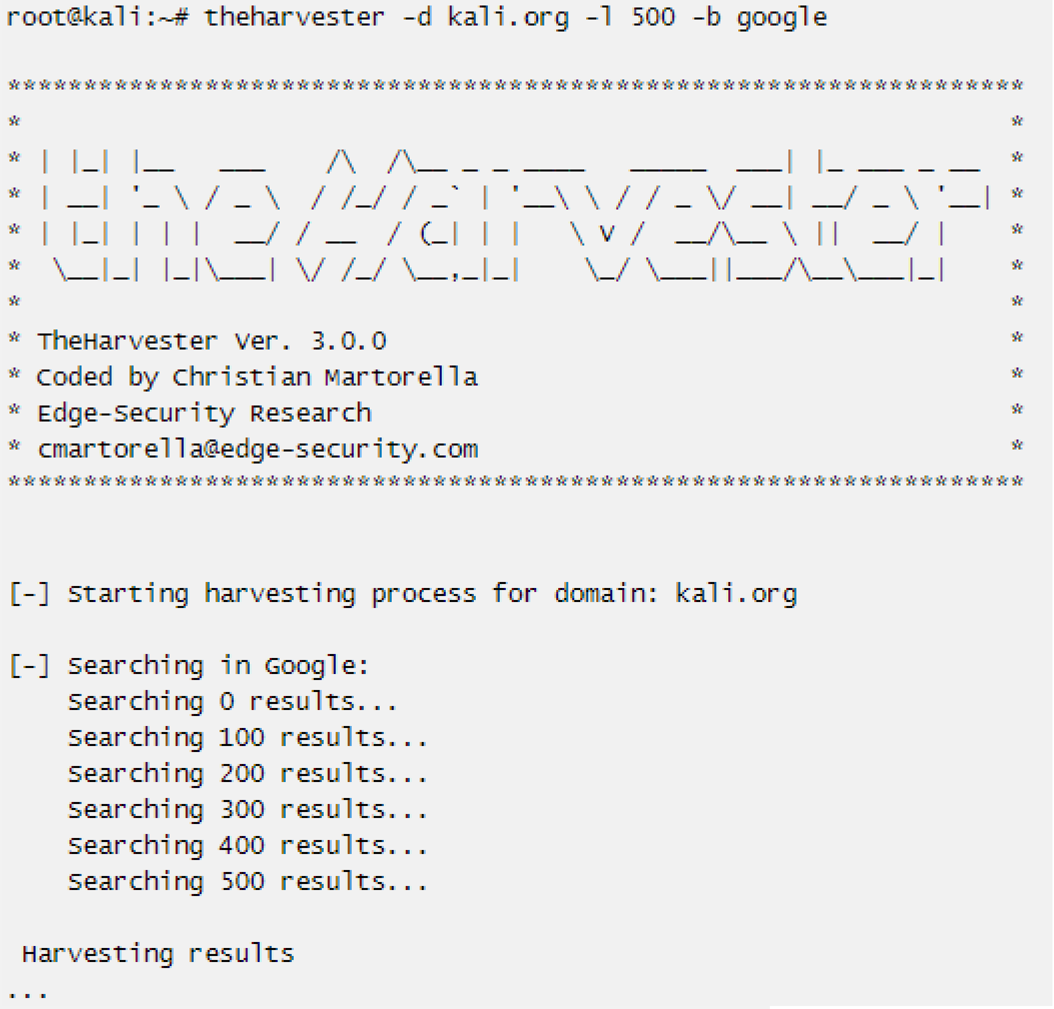
Technologies: B

```
HTTP/1.1 403 Forbi
Date: Sun, 15 Dec
Server: Apache/2.4
Last-Modified: Thu
ETag:
Accept-Ranges: byt
Content-Length: 48
Content-Type: text
```

Bitnami: Open Source. Simplified

TheHarvester

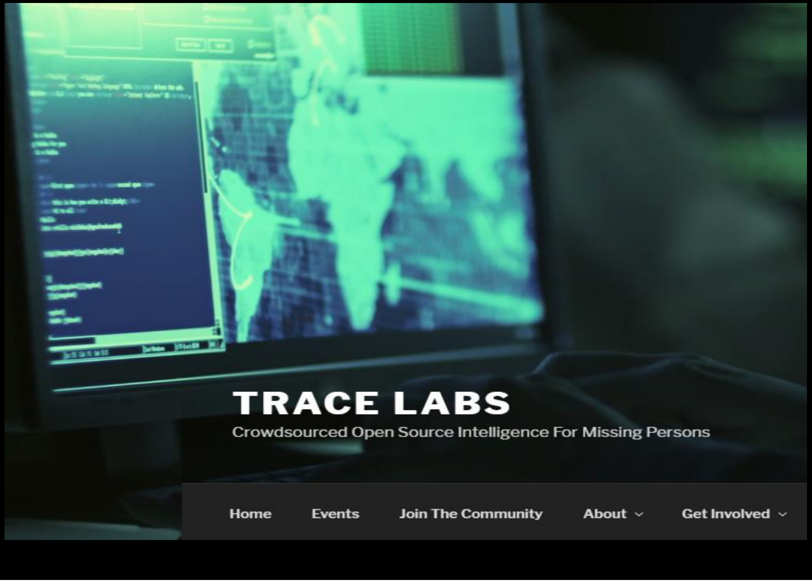
- Gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like various search engines, PGP key servers and SHODAN computer database
- Used for Passive Recon on targets



```
root@kali:~# theharvester -d kali.org -l 500 -b google

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 3.0.0                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Starting harvesting process for domain: kali.org

[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
    Searching 200 results...
    Searching 300 results...
    Searching 400 results...
    Searching 500 results...

 Harvesting results
...
```

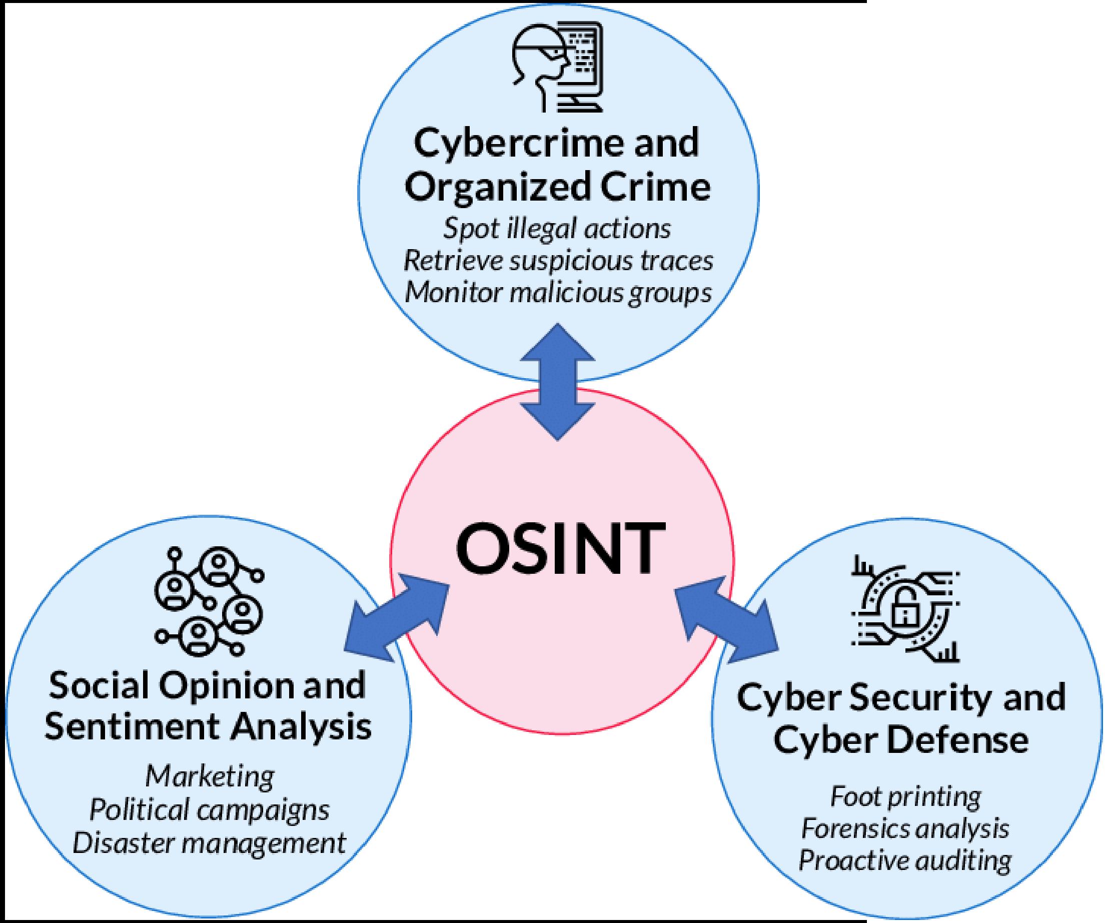
APPLICATIONS

- Reconnaissance, primary stage of P.T.
- Used by Companies to test their public presence
- Tracelabs, an OSINT based startup finds missing people by conducting CTFs
- Used/Applied by Threat Hunters, Security Professionals and alike ☺



TRACE LABS

Crowdsourced Open Source Intelligence For Missing Persons



OSINT

Cybercrime and Organized Crime

Spot illegal actions
Retrieve suspicious traces
Monitor malicious groups

Social Opinion and Sentiment Analysis

Marketing
Political campaigns
Disaster management

Cyber Security and Cyber Defense

Foot printing
Forensics analysis
Proactive auditing

DEMO

OSINT OF OSINT

- Twitter: @s0md3v, @midnight_comms, @OsintCurious
- Github: https://github.com/jivoi/awesome-osint
- Tracelabs: https://www.tracelabs.org/
- OSINT Framework: https://osintframework.com/
- OSINT Curious Podcast: https://osintcurio.us/
- OSINT Stash: https://osint.best/
- 2nd Generation OSINT for the Defense Enterprise: [link]
- Seclists by Daniel Miessler [link]
- The Privacy Security & OSINT Show [link]

REFERENCES

- https://danielmiessler.com/study/shodan/
- https://pen-testing.sans.org/blog/2015/12/08/effective-shodan-searches
- https://shodan.io
- https://github.com/laramies/theHarvester
- https://medium.com/hacker-toolbelt/the-harvester-osint-reconnaissance-91a18a294a30
- https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf
- https://tracelabs.org
- https://jakecreps.com/2018/09/28/advanced-osint-tools/
- https://www.researchgate.net/figure/OSINT-principal-use-cases_fig1_333703698

QUESTIONS,

YOU MUST ASK.

ME

THANK YOU :)