



# Open Source Intelligence

Patricia Musomba

# Introduction



Open source intelligence: The use of publicly available data to gather information on a **target**, passively.

Intelligence - Actionable data. Data that can help in decision making.

Usually performed during the reconnaissance phase of redteaming/pentesting

# Types of OSINT



## Active OSINT:

- This involves **engaging** with the particular target.
- The target may be aware of active OSINT
- Example: scanning of the network infrastructure to find open ports and services

## Passive OSINT:

- No engagement with the target
- Information is available in the **public domain**
- Example: Websites, identifying people associated with the target (employees, contractors)

# Why is it important?



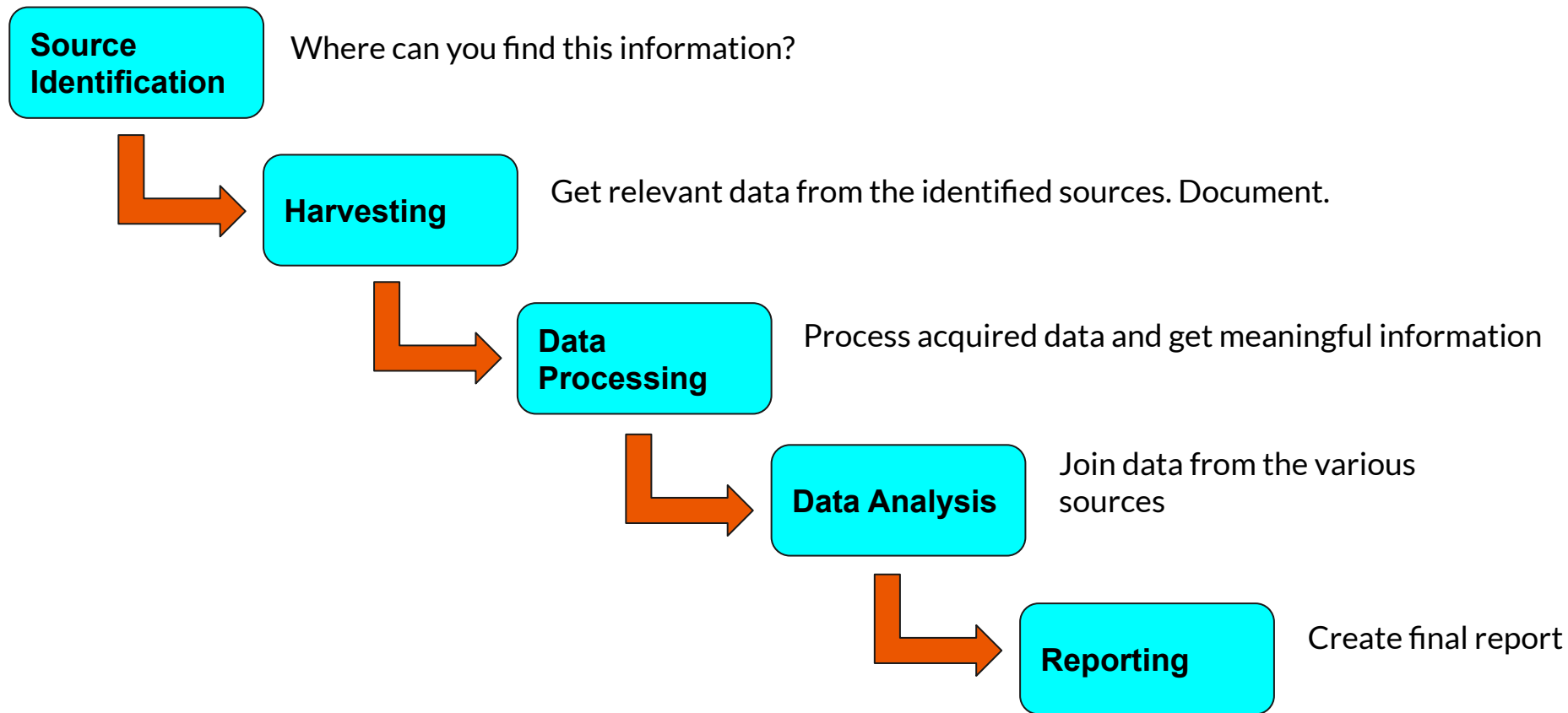
Information gathered determines the **Techniques, Tactics and Procedures(TTPs)** used during the pentesting/redteaming exercise

Determines a target's attack surface: vulnerabilities that can be exploited

Data of interest

- Technology infrastructure: ip, domains, services, hardware & software versions, OS info
- Database: documents, spreadsheets, configuration files
- Metadata: Emails, employee information

# OSINT Process





Search  
Engines

Network  
Recon

Email  
Harvesting

# OSINT TOOLS

Domain/Su  
bdomain

Social  
Media

Web Data

# Search Engines



Search engine scraping: process of harvesting URLs, description or other information from the search engine

## Tools:

1. Shodan <https://www.shodan.io/>
2. Censys <https://censys.io/>
3. Google <https://google.com>

Let's try some:

On Google:

related:<domain>

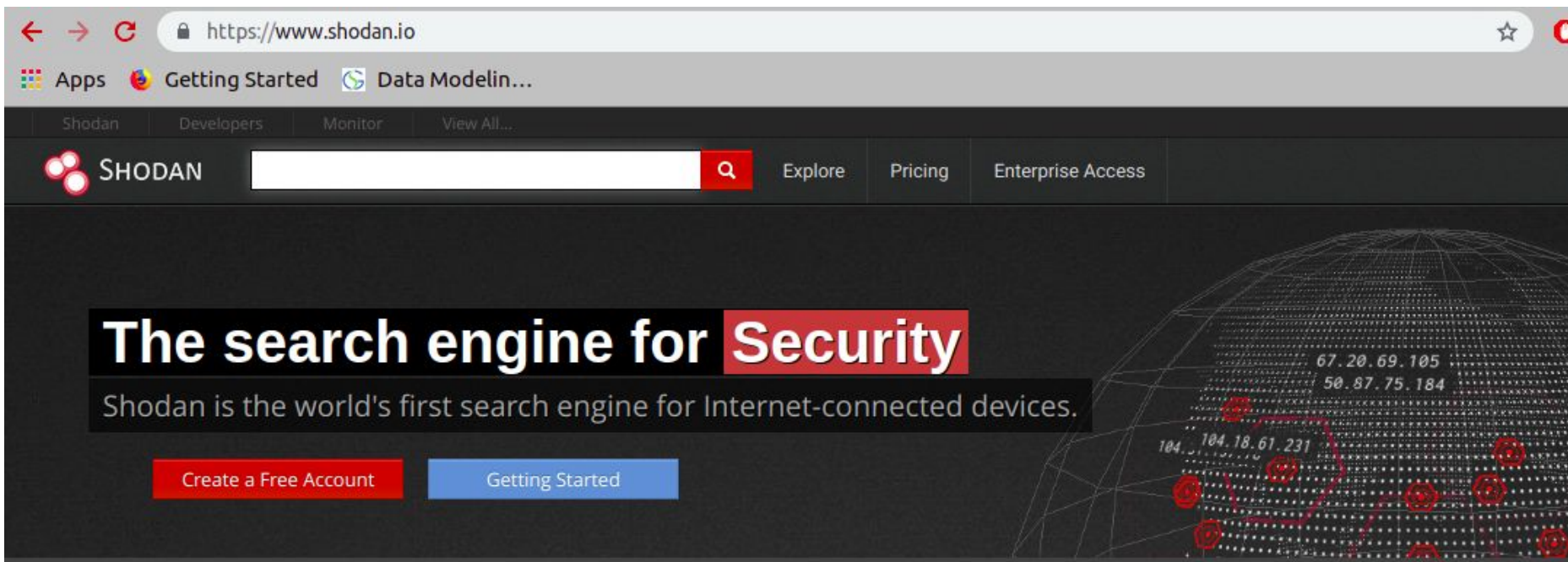
info:<domain>

site:<domain> filetype:<>

Other operators:

<https://ahrefs.com/blog/google-advanced-search-operators/>

Shodan <https://www.shodan.io/>



The screenshot shows the Shodan website homepage. At the top is a browser address bar with the URL <https://www.shodan.io/>. Below the address bar is a navigation bar with links for 'Apps', 'Getting Started', and 'Data Modelin...'. The main header features the Shodan logo, a search bar, and links for 'Explore', 'Pricing', and 'Enterprise Access'. The background of the header is a dark, stylized globe composed of a grid of lines and dots, with some IP addresses like '67.20.69.105' and '50.87.75.184' visible. A large, bold headline reads 'The search engine for Security', with 'Security' highlighted in a red box. Below the headline, a sub-headline states 'Shodan is the world's first search engine for Internet-connected devices.' At the bottom of the header are two buttons: 'Create a Free Account' (red) and 'Getting Started' (blue).

← → ↻ <https://www.shodan.io/> ☆

Apps Getting Started Data Modelin...

Shodan Developers Monitor View All...

SHODAN  🔍 Explore Pricing Enterprise Access

# The search engine for Security

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started



## Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



## See the Big Picture

Websites are just one part of the Internet. Ther refrigerators and much more that can be found v



# Web Data



Why? Find vulnerabilities in web applications, servers

Tools:

1. Proxy web applications - burpsuite, WebShag
2. CLI tools:
  - Nikto
  - Wpscan
  - Dirsearch
3. APIs
4. Google Analytics

# Email Harvesting

**Why?** Emails discovered are used for social engineering eg phishing

## **Tools:**

- theHarvester
- SimplyEmail
- Hunter.io
- Infoga



The harvester helps us in

- Entities Implementation
- Target Prioritization
- Passive & Active Discovery
- Username Searches

```
root@kali:~# theharvester
```

```
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when
ion.
```

[illegible]

```
Usage: theharvester options
```

```
-d: Domain to search or company name
-b: data source: baidu, bing, bingapi, censys, crtsh, dogpile,
    google, google-certificates, googleCSE, googleplus, google-pro
    hunter, linkedin, netcraft, pgp, threatcrowd,
    twitter, vhost, virustotal, yahoo, all
-g: use Google dorking instead of normal Google search
-s: start in result number X (default: 0)
-v: verify host name via DNS resolution and search for virtual hosts
```

# Hunter.io

No installation  
required

Just sign up on

<https://hunter.io/>

On the free plan, you  
get 50 monthly  
searches

Searches and verifies  
email addresses

 Finder  Verifier  Bulks  Leads  Outreach



## Domain Search ?

africahackon.com

 africahackon.com



☒ All ☐ Personal ☐ Generic

Support (1)

Support

info@africahackon.com 

Every email you find on Hunter can be  
saved as a lead.

CSV

Next



11 sources ▾

# Network Recon



Network recon is getting as much information about you target's network as possible.

Data that can be collected:

- IP addresses
- IP address geolocation
- Remote location recon
- Wireless networks
- DNS Data

## Tools

1. [Recon-NG](#)
2. [Nmap](#): More on Nmap [High on Coffee Cheat sheet](#)
3. [Nslookup](#)
4. [Netdiscover cheat sheet](#)

# Social Media



Sites:

1. Facebook
2. Twitter
3. Instagram
4. LinkedIn
5. Google+
6. Snapchat
7. Dating sites

You can get information that can be used for effective social engineering





# Thank you.

