EyeQ Dot Net
LEARN FROM REAL HACKERS

TASK 4

Information Gathering tools

ABSTRACT

Information Gathering tools are a set of specialized software designed for collecting valuable data from various public sources, platforms, and databases. These tools aid in the process of open-source intelligence (OSINT) gathering, enabling individuals such as security professionals, researchers, and analysts to compile comprehensive insights about specific targets. By systematically extracting information such as domain names, IP addresses, social media profiles, email addresses, and more, these tools help paint a detailed picture of a target's online presence. The data collected can be analyzed to identify potential security vulnerabilities, map connections between entities, and facilitate decision-making in various contexts. It is important to use these tools responsibly and ethically, adhering to legal regulations and authorization protocols.

SUBMITTED BY

Bibitha V R | 14-08-2023

Harvesting Knowledge: Exploring the Landscape of Information Gathering Tools

- Research below tools to get information of the target.

1. Maltego
2. OSINT Framework
3. Reccon FTW
4. Recon-Ng
5. Spiderfoot
6. Aquatone

---

1. Maltego:

Tool Description:

Maltego is a commercial tool that specializes in visual link analysis. It allows users to collect, analyse, and visualize data from a wide range of sources. By mapping out connections between entities like people, organizations, websites, and infrastructure, Maltego helps analysts uncover hidden relationships and potential attack vectors. Maltego offers both a graphical user interface (GUI) and a command-line interface (CLi), catering to both beginner and advanced users.

Website: https://www.maltego.com/

Advantages/Features/Uses:

- Visualizes complex relationships between entities.
- Collects data from various sources, including social media, public records, and websites.
- Generates interactive graphs and charts for better understanding.
- Aids in threat intelligence, digital forensics, and cybersecurity investigations.

Installation in kali:

1. Open the terminal window in your Kali Linux virtual machine.

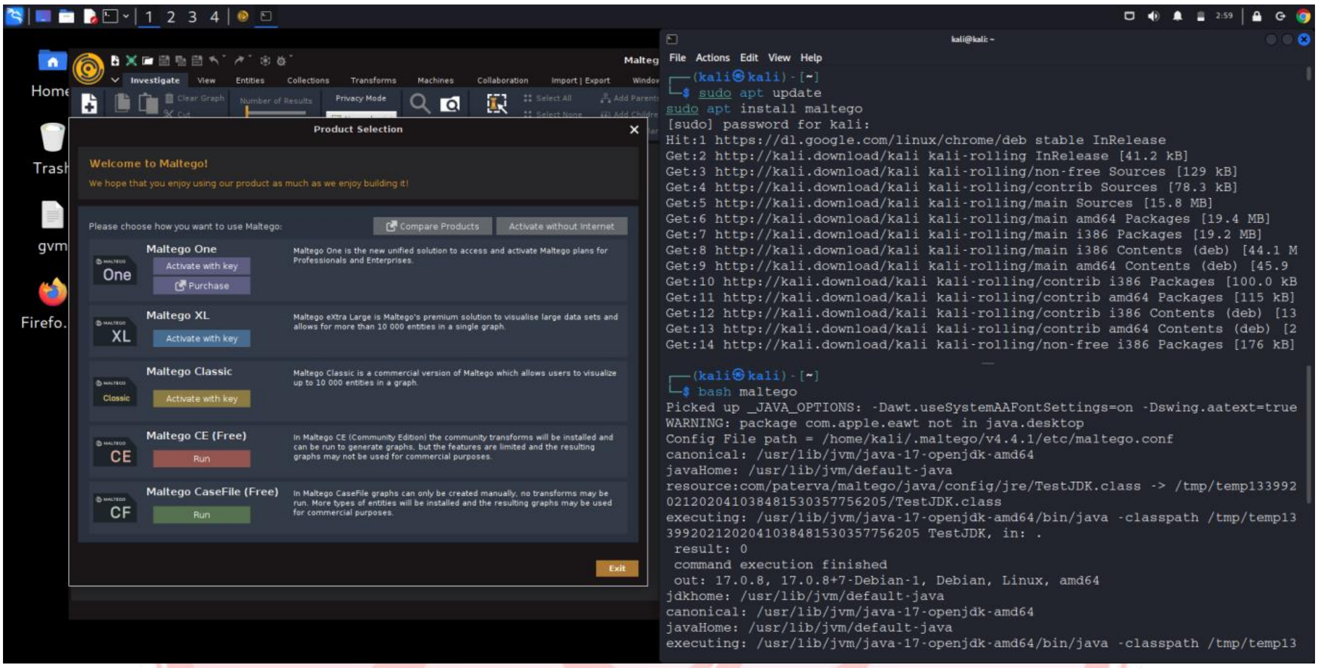
2. First update the Kali Linux and then install the required packages by typing the following command-

```
sudo apt-get update
sudo apt install maltego
```

3. Run maltego by typing the following command-

```
Bash maltego
```

This should open maltego client.



Product Selection

Welcome to Maltego!

We hope that you enjoy using our product as much as we enjoy building it!

Please choose how you want to use Maltego:

Maltego One – Maltego One is the new unified solution to access and activate Maltego plans for Professionals and Enterprises.

Maltego XL – Maltego eXtra Large is Maltego's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.

Maltego Classic – Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.

Maltego CE (Free) – In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.

Maltego CaseFile (Free) – In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
sudo apt install maltego
[sudo] password for kali:
Hit:1 https://dl.google.com/linux/chrome/deb stable InRelease
Get:2 http://kali.download/kali kali-rolling InRelease [41.2 kB]
Get:3 http://kali.download/kali kali-rolling/non-free Sources [129 kB]
Get:4 http://kali.download/kali kali-rolling/contrib Sources [78.3 kB]
Get:5 http://kali.download/kali kali-rolling/main Sources [15.8 MB]
Get:6 http://kali.download/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:7 http://kali.download/kali kali-rolling/main i386 Packages [19.2 MB]
Get:8 http://kali.download/kali kali-rolling/main i386 Contents (deb) [44.1 M
Get:9 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [45.9
Get:10 http://kali.download/kali kali-rolling/contrib i386 Packages [100.0 kB
Get:11 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:12 http://kali.download/kali kali-rolling/contrib i386 Contents (deb) [13
Get:13 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [2
Get:14 http://kali.download/kali kali-rolling/non-free i386 Packages [176 kB]

┌──(kali㉿kali)-[~]
└─$ bash maltego
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
WARNING: package com.apple.eawt not in java.desktop
Config File path = /home/kali/.maltego/v4.4.1/etc/maltego.conf
canonical: /usr/lib/jvm/java-17-openjdk-amd64
javaHome: /usr/lib/jvm/default-java
resource:com/paterva/maltego/java/config/jre/TestJDK.class -> /tmp/temp133992
0212020410384815303577562O5/TestJDK.class
executing: /usr/lib/jvm/java-17-openjdk-amd64/bin/java -classpath /tmp/temp13
399202120204103848153035775620 5 TestJDK, in: .
 result: 0
 command execution finished
 out: 17.0.8, 17.0.8+7-Debian-1, Debian, Linux, amd64
jdkhome: /usr/lib/jvm/default-java
canonical: /usr/lib/jvm/java-17-openjdk-amd64
javaHome: /usr/lib/jvm/default-java
executing: /usr/lib/jvm/java-17-openjdk-amd64/bin/java -classpath /tmp/temp13
```

2. OSINT Framework:

The OSINT Framework is a community-driven collection of tools and resources for OSINT researchers. It provides a categorized list of tools, organized by data type (people, phone numbers, email addresses, social media, etc.), making it easy to find the right tool for a specific type of information. It's not a tool itself, but a valuable reference for anyone involved in OSINT research.

Website: https://osintframework.com/

Advantages/Features/Uses:

- Provides a categorized list of tools and resources.

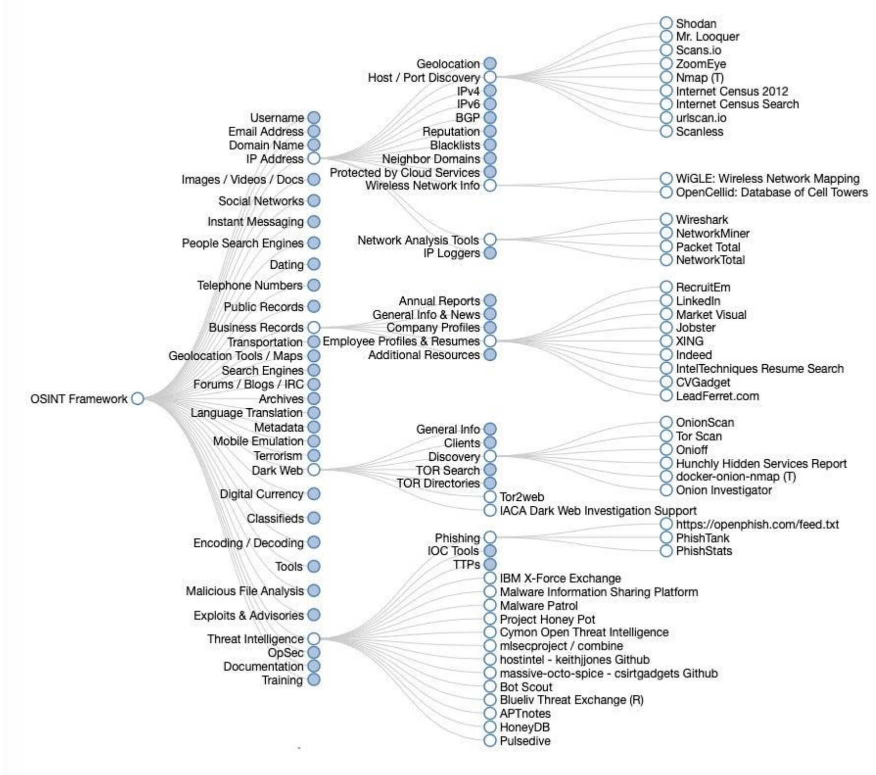
- Covers a wide range of data types and sources.

- Helps researchers discover the right tools for specific OSINT tasks.

- Offers a centralized reference point for OSINT practitioners.

Installation:

As OSINT Framework is not a tool with a graphical interface, there is no installation process. It's a website that you can access directly: - https://osintframework.com/ [OSINT Framework]



3. Reccon FTW:

Reccon FTW is an open-source reconnaissance framework written in Python. It allows security researchers and penetration testers to automate the process of gathering information from multiple sources. It supports modules for gathering information related to domains, subdomains, IP addresses, and more. Reccon FTW's modular architecture makes it easy to extend its capabilities.

GitHub Repository: - https://github.com/six2dez/reconftw

Advantages/Features/Uses:

- Simplifies domain reconnaissance and data collection.

- Provides quick information about subdomains and IP addresses.

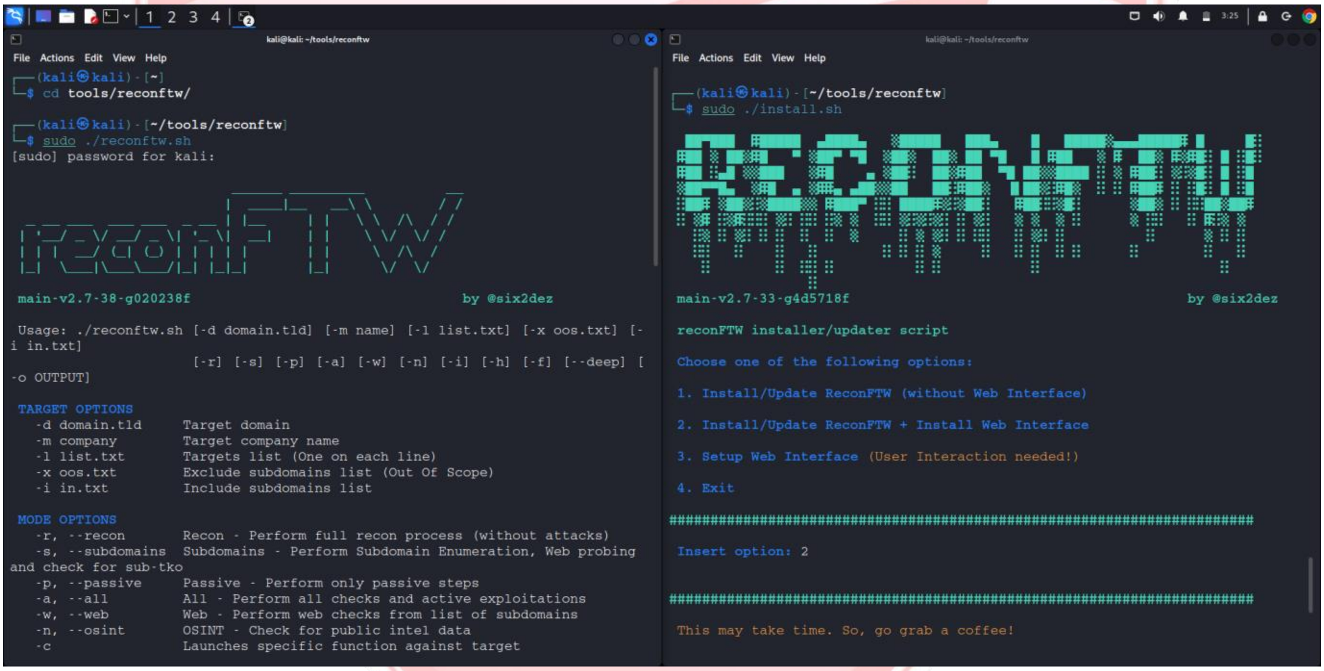
- Useful for penetration testers, bug bounty hunters, and security professionals

Installation:

1. Open terminal in your kali linux virtual machine.

2. Then update you kali linux machine and use the following command to install it-

```
sudo apt-get update
git clone https://github.com/six2dez/reconftw
cd reconftw/
./install.sh
```



```
┌──(kali㉿kali)-[~]
└─$ cd tools/reconftw/

┌──(kali㉿kali)-[~/tools/reconftw]
└─$ sudo ./reconftw.sh
[sudo] password for kali:

 main-v2.7-38-g020238f                                    by @six2dez

 Usage: ./reconftw.sh [-d domain.tld] [-m name] [-l list.txt] [-x oos.txt] [-
i in.txt]
                      [-r] [-s] [-p] [-a] [-w] [-n] [-i] [-h] [-f] [--deep] [
-o OUTPUT]

 TARGET OPTIONS
   -d domain.tld     Target domain
   -m company        Target company name
   -l list.txt       Targets list (One on each line)
   -x oos.txt        Exclude subdomains list (Out Of Scope)
   -i in.txt         Include subdomains list

 MODE OPTIONS
   -r, --recon       Recon - Perform full recon process (without attacks)
   -s, --subdomains  Subdomains - Perform Subdomain Enumeration, Web probing
and check for sub-tko
   -p, --passive     Passive - Perform only passive steps
   -a, --all         All - Perform all checks and active exploitations
   -w, --web         Web - Perform web checks from list of subdomains
   -n, --osint       OSINT - Check for public intel data
   -c                Launches specific function against target
```

```
┌──(kali㉿kali)-[~/tools/reconftw]
└─$ sudo ./install.sh

main-v2.7-33-g4d5718f                                          by @six2dez

reconFTW installer/updater script

Choose one of the following options:

1. Install/Update ReconFTW (without Web Interface)

2. Install/Update ReconFTW + Install Web Interface

3. Setup Web Interface (User Interaction needed!)

4. Exit

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

Insert option: 2

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

This may take time. So, go grab a coffee!
```

4. Recon-NG:

Recon-NG is a full-featured open-source reconnaissance framework developed in Python. It's designed to automate the collection of information from various sources such as search engines, social networks, and public databases. Recon-NG provides a wide range of modules that can be customized and chained together to gather comprehensive information about a target.

GitHub Repository: https://github.com/lanmaster53/recon-ng

Advantages/Features/Uses:

- Automates OSINT tasks through modular design.
- Supports data collection from social media, search engines, DNS, and more.
- Allows customization and scripting for specific tasks.

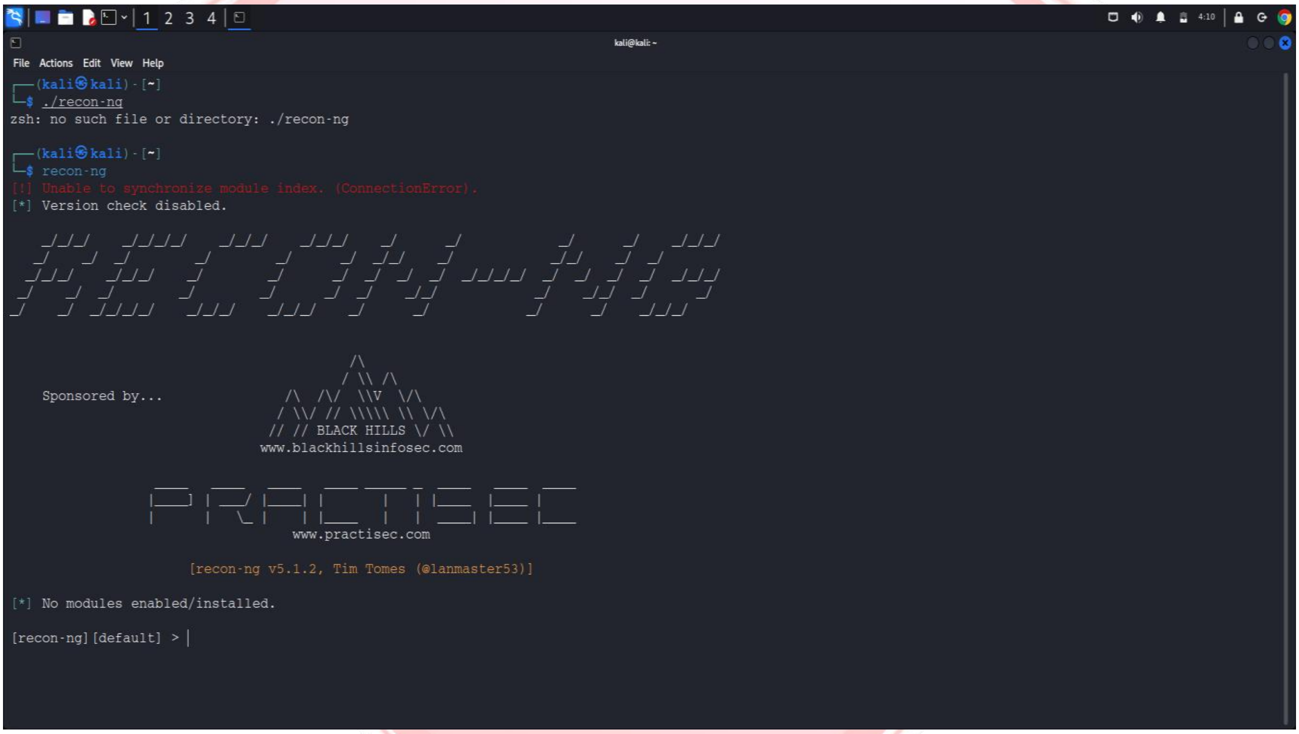
Installation:

1. Open terminal and then type the following commands to install recon-ng

```
sudo apt update
sudo apt install recon-ng
```

2. Start Recon-Ng:

```
bash recon-ng
```



```
┌──(kali㉿kali)-[~]
└─$ ./recon-ng
zsh: no such file or directory: ./recon-ng

┌──(kali㉿kali)-[~]
└─$ recon-ng
[!] Unable to synchronize module index. (ConnectionError).
[*] Version check disabled.

                                          /\
                                         / \\ /\
    Sponsored by...               /\  /\/  \\V  \/\
                                 / \\/ // \\\\\ \\ \/\
                                // // BLACK HILLS \/ \\
                               www.blackhillsinfosec.com

                                  www.practisec.com

                      [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] > |
```

5. Spiderfoot:

Spiderfoot is an open-source OSINT automation tool that focuses on gathering information from a wide range of sources. It can pull data from DNS records, WHOIS information, social media platforms, public databases, and more. Spiderfoot then compiles the data into a comprehensive report that helps analysts understand the online footprint of a target.

GitHub Repository: https://github.com/smicallef/spiderfoot

Advantages/Features/Uses:

Wide Data Source Support: Spiderfoot integrates with various data sources including search engines, social media platforms, WHOIS databases, DNS records, public APIs, and more. This comprehensive data collection approach ensures a thorough understanding of the target's online presence.

Automated Data Gathering: Spiderfoot automates the process of gathering data from different sources, saving time and effort for analysts. It combines information from multiple sources to build a more complete profile of the target.

Threat Intelligence: The tool can help security professionals gather threat intelligence by identifying potential vulnerabilities, weak points, and security risks associated with the target.

Reconnaissance for Vulnerability Assessment: Spiderfoot can be used to identify potential vulnerabilities by discovering exposed services, open ports, and outdated software associated with the target.

Email Address Analysis: It can extract email addresses associated with the target and perform additional analysis to find linked social media accounts and other online profiles.

Link Analysis and Visualization: Spiderfoot provides visualizations that help users understand relationships and connections between different entities, making it easier to spot patterns and potential threats.

Customization: Users can customize the tool's behavior by specifying modules to run, adjusting timeouts, and configuring which data sources to query.

Command-Line and Web Interfaces: Spiderfoot offers both a command-line interface (CLI) and a webbased interface, making it accessible to users with different preferences and skill levels.

Installation in Kali Linux (with Screenshots/Commands):

Here's how you can install Spiderfoot in Kali Linux:

1. Open a Terminal: Launch the terminal on your Kali Linux system.

2. Update Repositories: Run the following command to ensure your package repositories are up to date.

```
sudo apt update
```

3. Install Python and Dependencies: Install Python and other required dependencies using the following command.

```
sudo apt install python3 python3-pip
```

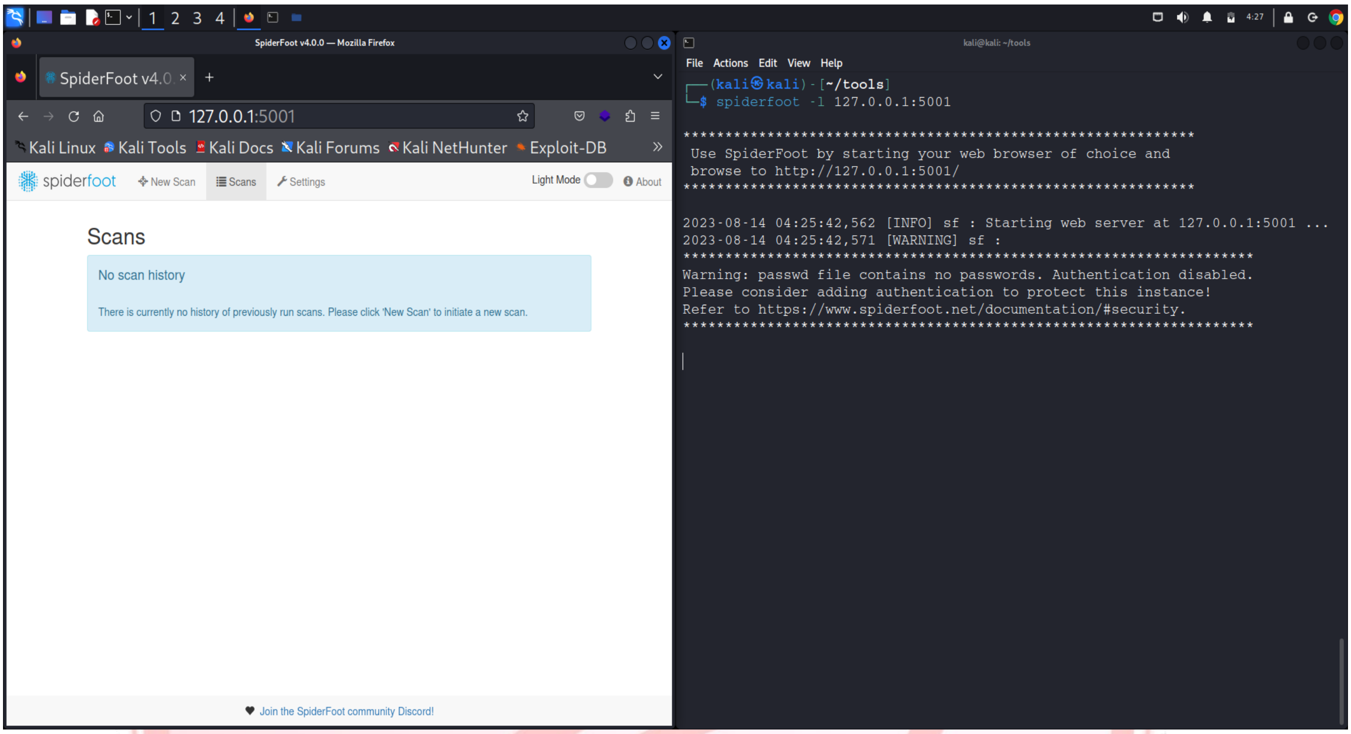
4. Install Spiderfoot: Use pip to install Spiderfoot with the following command.

```
pip3 install spiderfoot
```

5. Run Spiderfoot: After installation, you can start Spiderfoot using the following command.

```
spiderfoot -l 127.0.0.1:5001
```

This will start Spiderfoot's web interface, accessible at `http://127.0.0.1:5001` in your web browser.



Scans

No scan history

There is currently no history of previously run scans. Please click 'New Scan' to initiate a new scan.

```
┌──(kali㉿kali)-[~/tools]
└─$ spiderfoot -l 127.0.0.1:5001

**************************************************************
 Use SpiderFoot by starting your web browser of choice and
 browse to http://127.0.0.1:5001/
**************************************************************

2023-08-14 04:25:42,562 [INFO] sf : Starting web server at 127.0.0.1:5001 ...
2023-08-14 04:25:42,571 [WARNING] sf :
*********************************************************************
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*********************************************************************
```

6. Aquatone:

Aquatone is an open-source reconnaissance tool primarily used for gathering information about subdomains. It scans a given domain, discovers subdomains, and collects information such as IP addresses and server headers. Additionally, Aquatone takes screenshots of web pages associated with the subdomains, allowing analysts to quickly review the visual appearance of the sites.

GitHub Repository: https://github.com/michenriksen/aquatone

Advantages/Features/Uses:

Subdomain Enumeration: Aquatone assists in identifying subdomains associated with the target domain. This helps in understanding the broader online presence of the organization and any potential vulnerabilities.

Port Scanning: The tool performs port scanning on the identified subdomains to determine which ports are open. This can provide insights into possible entry points for attackers.

Web Technology Detection: Aquatone identifies the technologies and services used on the target domain. This information is crucial for understanding potential attack vectors and vulnerabilities associated with specific technologies.

Screenshot Capture: One of the unique features of Aquatone is its ability to capture screenshots of web pages associated with the subdomains. These screenshots offer visual context and may reveal any visible security issues or misconfigurations.

Data Visualization: The tool generates reports and visualizations in HTML format, making it easier to present findings to stakeholders. The reports include information about subdomains, open ports, and screenshots of web pages.

Integration: Aquatone can be integrated into larger workflows and automated processes due to its command line interface, making it suitable for both manual and automated reconnaissance tasks.

Installation in Kali Linux: Here's a step-by-step guide to installing Aquatone on Kali Linux along with relevant commands and screenshots:

1. Open Terminal: Launch the terminal on your Kali Linux system.

2. Install Golang: Aquatone is built using Golang, so you need to install Golang if you don't have it already.

```
sudo apt update

sudo apt install golang-go
```

3. Set GOPATH: Set up your GOPATH environment variable to specify the directory where Go packages will be installed. You can add the following line to your `.bashrc` or `.zshrc` file:

```
export GOPATH=$HOME/go

export PATH=$PATH:$GOPATH/bin
```

4. Install Aquatone: Install Aquatone using `go get` command.

```
go get github.com/michenriksen/aquatone
```

5. Navigate to Aquatone Directory: Navigate to the Aquatone directory within your GOPATH.

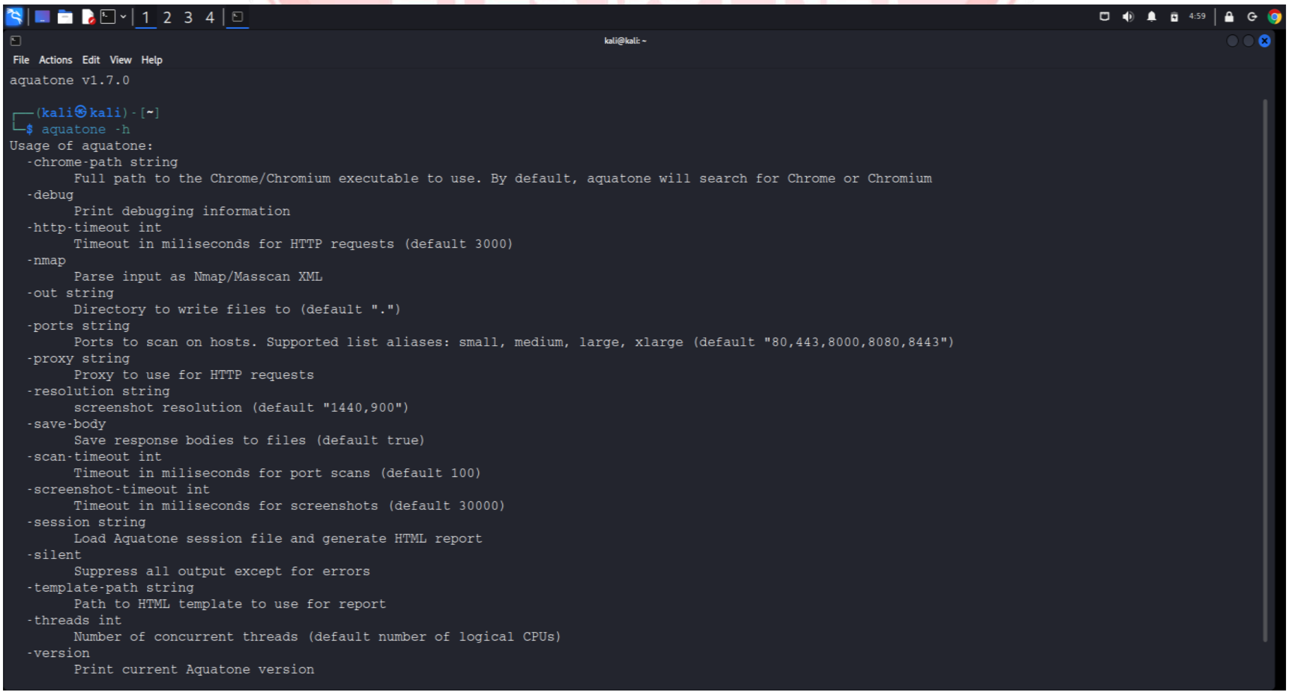
6. Build Aquatone:

Build the Aquatone tool using Go.

```
go install
```

7. Usage: After installation, you can use Aquatone from the command line.

```
aquatone -h
```



```
aquatone v1.7.0

┌──(kali㉿kali)-[~]
└─$ aquatone -h
Usage of aquatone:
  -chrome-path string
        Full path to the Chrome/Chromium executable to use. By default, aquatone will search for Chrome or Chromium
  -debug
        Print debugging information
  -http-timeout int
        Timeout in miliseconds for HTTP requests (default 3000)
  -nmap
        Parse input as Nmap/Masscan XML
  -out string
        Directory to write files to (default ".")
  -ports string
        Ports to scan on hosts. Supported list aliases: small, medium, large, xlarge (default "80,443,8000,8080,8443")
  -proxy string
        Proxy to use for HTTP requests
  -resolution string
        screenshot resolution (default "1440,900")
  -save-body
        Save response bodies to files (default true)
  -scan-timeout int
        Timeout in miliseconds for port scans (default 100)
  -screenshot-timeout int
        Timeout in miliseconds for screenshots (default 30000)
  -session string
        Load Aquatone session file and generate HTML report
  -silent
        Suppress all output except for errors
  -template-path string
        Path to HTML template to use for report
  -threads int
        Number of concurrent threads (default number of logical CPUs)
  -version
        Print current Aquatone version
```

Conclusion:

These tools collectively provide a range of capabilities for OSINT researchers, penetration testers, and security analysts to gather and analyze publicly available information about a target. Always ensure you understand the legal and ethical boundaries of using these tools in your research.

References:

- https://www.upguard.com/
- https://www.ecpi.edu/
- https://www.simplilearn.com/
- https://www.sans.org/in_en/
- https://portswigger.net/