VIT
BHOPAL
www.vitbhopal.ac.in

Group 19!

Advanced Reconnaissance and Visualization Tool

Review-2

Presented To : Dr.Ajay Kumar Phulre Sir

Team Members

01	Rohit K Bhat	20BCY10056
02	G.Sharan Raghav	20BCY10102
03	Sai Maneesh CH	20BCY10186
04	S.V.Hareshwara Reddy	20BCY10181
05	B.Shiva Sai	20BCY10056

INTRODUCTION

Definition of Reconnaissance:

- **Theory:** Reconnaissance, commonly known as "recon," is the preliminary phase in strategic planning and information gathering. It involves collecting data about a target to understand its characteristics, vulnerabilities, and potential threats.
- **Practical Knowledge:** In the digital realm, reconnaissance includes activities like network scanning, open-source intelligence (OSINT), and social engineering to gather information about a target system or organization.

Types of Reconnaissance:

- **Theory:** Reconnaissance can be categorized into passive and active forms. Passive reconnaissance involves collecting information without directly interacting with the target, while active reconnaissance involves direct engagement with the target system.
- **Practical Knowledge:** Passive reconnaissance might include monitoring public forums for information about a company, while active reconnaissance may involve scanning a network for open ports.

Objectives of Reconnaissance:

- **Theory:** The primary objectives of reconnaissance are to identify potential targets, understand their structure and vulnerabilities, and gather intelligence that can inform further actions.
- **Practical Knowledge:** In cybersecurity, for instance, reconnaissance aims to discover weak points in a network, such as open ports, and identify potential entry points for attackers.

Information Sources in Reconnaissance:

- **Theory:** Reconnaissance draws data from various sources, including public records, social media, network traffic, and human intelligence.
- **Practical Knowledge:** Cybersecurity professionals may utilize tools like WHOIS databases, social media monitoring, and network scanning tools to gather information about an organization's digital footprint

INTRODUCTION

Open-Source Intelligence (OSINT):

- **Theory:** OSINT involves collecting information from publicly available sources. It includes data from the internet, media, public records, and other openly accessible outlets.
- **Practical Knowledge:** Security analysts use OSINT to gather information about an organization's online presence, employee details, and potential vulnerabilities.

Social Engineering:

- **Theory:** Social engineering is a human-centric form of reconnaissance, involving manipulating individuals to divulge confidential information.
- **Practical Knowledge:** Phishing emails, pretexting, and impersonation are common social engineering techniques used to gather information by exploiting human psychology.

Network Scanning:

- **Theory:** Network scanning involves probing a target's network to identify active devices, open ports, and services running on those ports.
- **Practical Knowledge:** Tools like Nmap are employed to perform network scans, providing valuable insights into a system's structure and potential vulnerabilities.

Footprinting:

- **Theory:** Footprinting is the process of accumulating data about a target's network architecture, domain names, and network services.
- **Practical Knowledge:** Footprinting techniques may include DNS interrogation, network mapping, and service identification to build a comprehensive profile of the target.

INTRODUCTION

Digital Footprint:

- **Theory:** A digital footprint is the online trail of data left by an individual or organization. It includes websites visited, social media interactions, and other online activities.
- **Practical Knowledge:** Analysts use digital footprints to understand an entity's online presence, aiding in identifying potential attack vectors.

Risk and Threat Assessment:

- **Theory:** Reconnaissance contributes to risk assessment by identifying vulnerabilities and potential threats, allowing organizations to prioritize security measures.
- **Practical Knowledge:** Assessments based on reconnaissance findings guide the development of cybersecurity strategies to mitigate identified risks.

Legal and Ethical Considerations:

- **Theory:** Reconnaissance activities must adhere to legal and ethical standards. Unauthorized access or data collection can have severe legal consequences.
- **Practical Knowledge:** Security professionals must ensure that their reconnaissance activities comply with applicable laws and ethical guidelines to avoid legal ramifications.

Continuous Reconnaissance:

- **Theory:** Reconnaissance is an ongoing process. Regularly updating information and staying aware of emerging threats is crucial for maintaining effective security.
- **Practical Knowledge:** Cybersecurity strategies incorporate continuous reconnaissance to adapt to evolving threats and maintain a proactive security posture.

LITERATURE REVIEW

- Open Source Intelligence has become increasingly important in the field of cybersecurity
- As cyber threats continue to evolve, organizations need effective methods to gather and analyze relevant intelligence to identify potential risks and mitigate them.
- A comprehensive review of advanced OSINT frameworks reveals several key elements for scanning IP addresses, emails, websites, and organizations. These advanced frameworks leverage a wide range of sources to collect and analyze data, including publicly available information on the internet. Some of the sources used in these frameworks include social media platforms, public databases, search engines, and specialized tools for OSINT data collection.
- Furthermore, these frameworks employ various techniques to scan IP addresses, emails, websites, and organizations.

URL: Link To Referred Research Paper

EXISTING WORKS

- Maltego
- Mitaka
- SpiderFoot
- Spyse
- BuiltWith
- Intelligence X

NOVELTY OF PROJECT

1. **Comprehensive Scanning Capabilities:** The integration of tools like Wave, Photon, and Recon Dog suggests that our tool aims to offer a wide array of scanning capabilities. This could include scanning IP addresses, emails, websites, and organizations, providing a comprehensive view of the target's digital presence.
2. **Aggregation and Visualization:** The ability to aggregate raw data from different sources and present it on a dashboard is a valuable feature. This can simplify the analysis process for security professionals, making it easier to interpret the gathered information.
3. **User Base:** The project's target audience, including Infosec Researchers, Penetration Testers, Bug Hunters, and Cyber Crime Investigators, indicates a focus on practical usability and relevance for security professionals.
4. **Alerting and Monitoring:** Incorporating features for real-time alerting and monitoring enhances the proactive nature of the tool. This is crucial for identifying potential threats or changes in the target's digital footprint promptly.
5. **Open Source Nature:** Being an open-source project allows for collaboration and contributions from the cybersecurity community. This can lead to continuous improvement, updates, and a broader range of supported features.

REAL-TIME USAGE

- Performs advanced scan on a IP Address, Emails, Websites, Organizations and find out information from different sources.
- Correlates and collaborate the results, show them in a consolidated manner.
- Use specific script / launch automated OSINT for consolidated data.
- Currently available in only Command Line Interface (CLI).
- Can be used by Infosec Researchers, Penetration Testers, Bug Hunters and Cyber Crime Investigators to find deep information about their target.

REQUIREMENTS

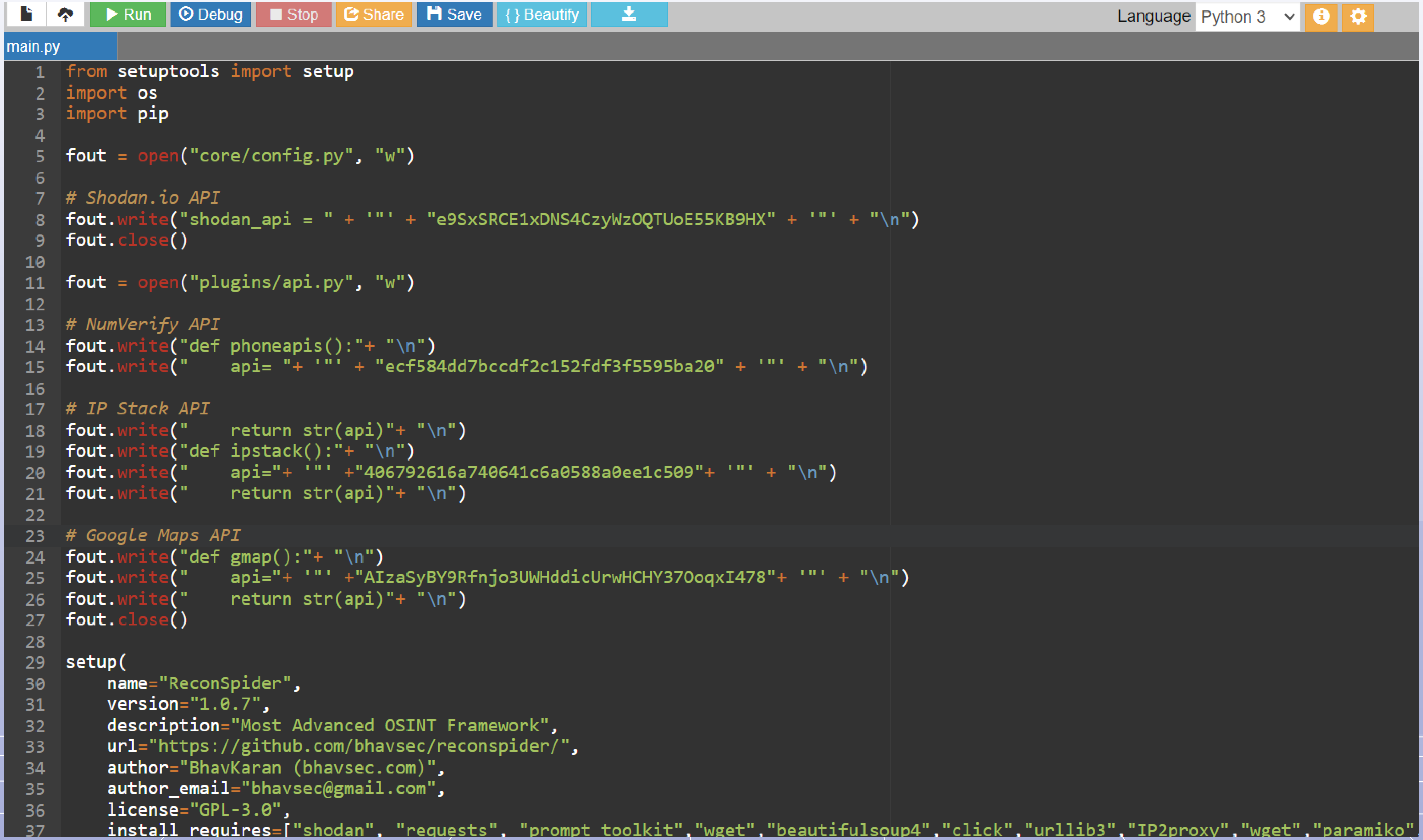
- **Data Collection and Aggregation:** The tool must collect and aggregate data from diverse sources, including network traffic, logs, and external threat feeds, ensuring comprehensive threat intelligence.
- **Real-time Monitoring and Analysis:** It should provide real-time monitoring and analysis capabilities to detect and respond to emerging threats promptly.
- **Effective Visualization:** The tool must offer advanced data visualization features, such as interactive dashboards and reports, to help security professionals quickly understand the threat landscape.
- **Security and Compliance:** The tool should adhere to security standards and compliance requirements, with role-based access control and data encryption to safeguard sensitive information.
- **Integration and Compatibility:** It should seamlessly integrate with existing security infrastructure, including SIEMs and threat intelligence providers, and be compatible with various operating systems and network configurations.

CODING AND IMPLEMENTATION

The Tool will contain options like:

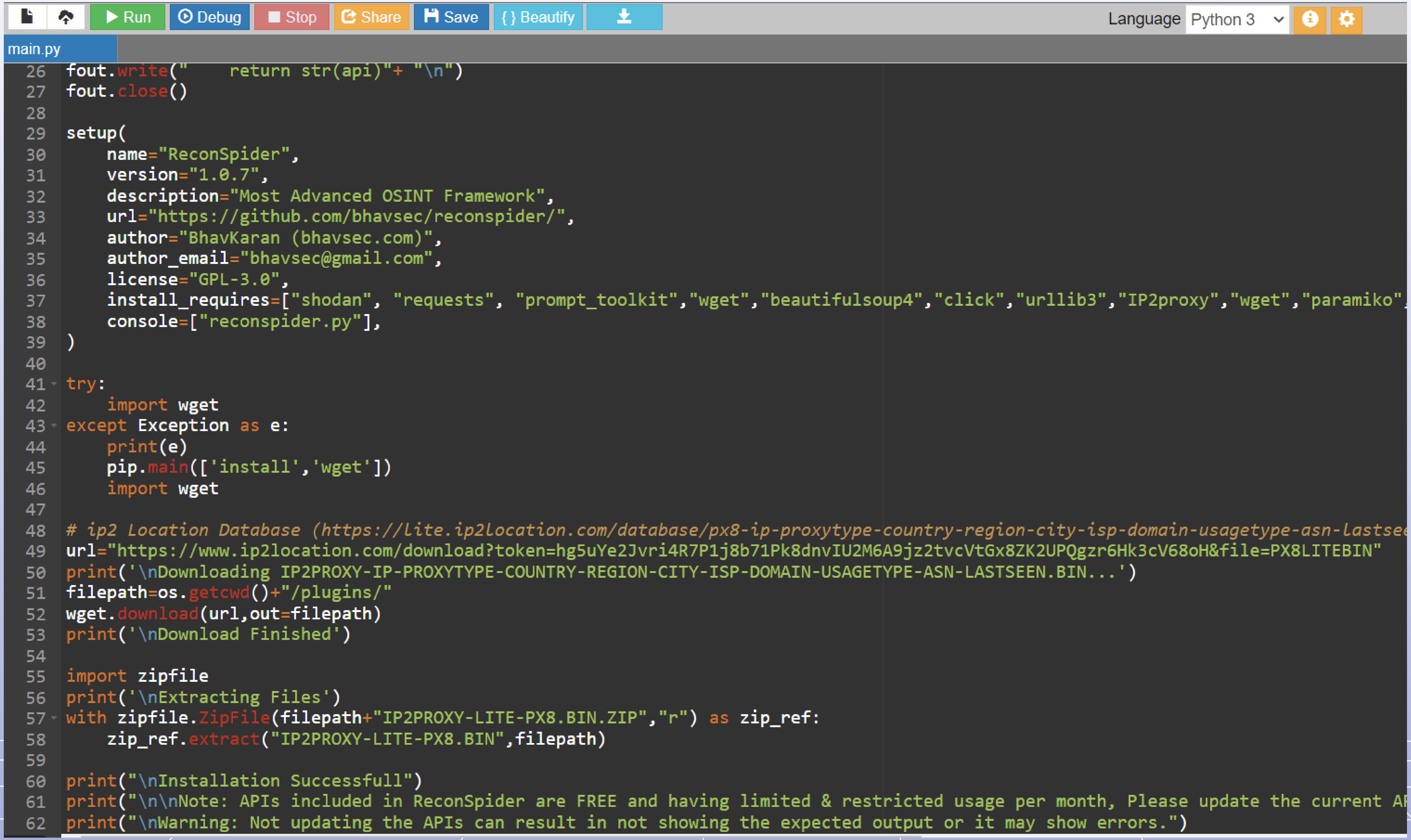
1.	**IP**	**Enumerate information from IP Address**
2.	**DOMAIN**	**Gather information about the given DOMAIN**
3.	**PHONE NUMBER**	**Gather information about the Phone number**
4.	**DNS MAP**	**Map DNS records associated with the target**
5.	**METADATA**	**Extract all metadata of the given file**
6.	**REVERSE IMAGE SEARCH**	**Obtain domain name or IP address mapping**
7.	**HONEYPOT**	**Check if it's honeypot or a real system**
8.	**MAC ADDRESS LOOKUP**	**Obtain information about give Mac address**
9.	**IPHEATMAP**	**Draw out a heatmap of locations of IP**
10.	**TORRENT**	**Gather the torrent download history of the IP**
11.	**USERNAME**	**Extract Account info. from social media**
12.	**IP2PROXY**	**Check whether IP uses any VPN / PROXY**
13.	**MAIL BREACH**	**Checks given domain has breached Mail**

REQUIREMENTS.PY



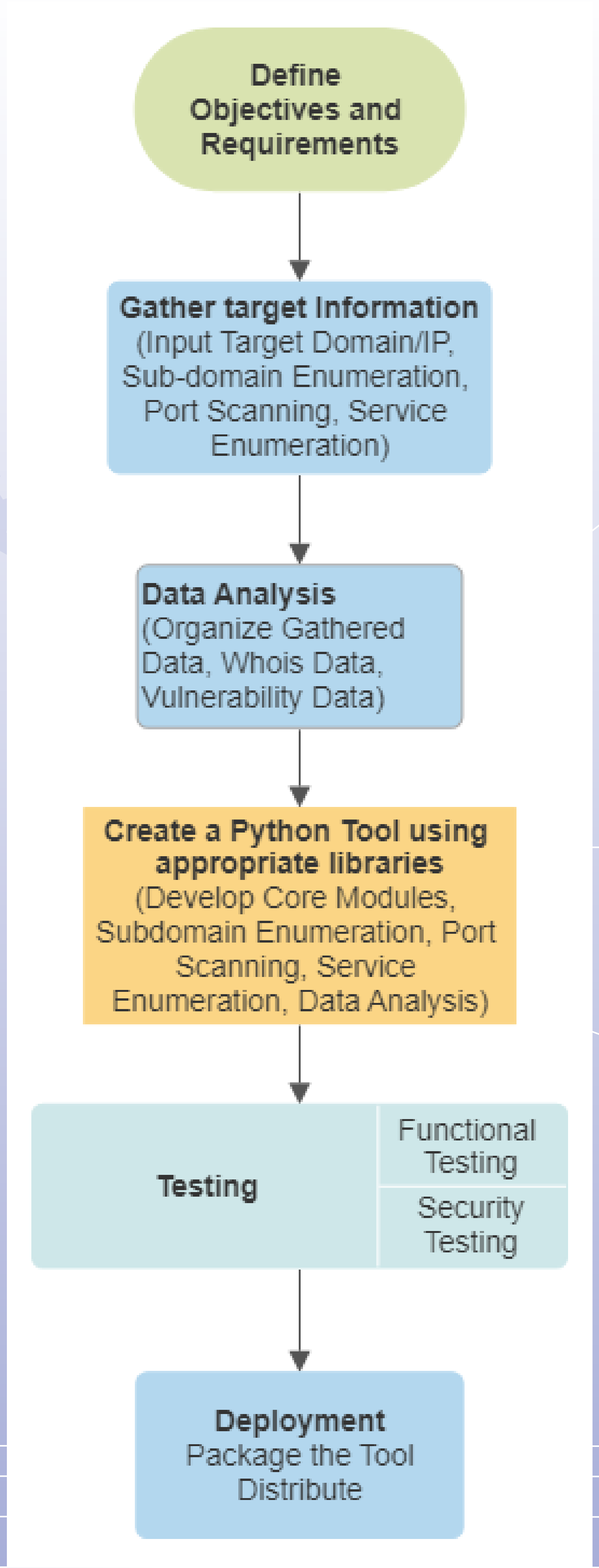
```python
from setuptools import setup
import os
import pip

fout = open("core/config.py", "w")

# Shodan.io API
fout.write("shodan_api = " + '"' + "e9SxSRCE1xDNS4CzyWzOQTUoE55KB9HX" + '"' + "\n")
fout.close()

fout = open("plugins/api.py", "w")

# NumVerify API
fout.write("def phoneapis():"+ "\n")
fout.write("    api= "+ '"' + "ecf584dd7bccdf2c152fdf3f5595ba20" + '"' + "\n")

# IP Stack API
fout.write("    return str(api)"+ "\n")
fout.write("def ipstack():"+ "\n")
fout.write("    api="+ '"' +"406792616a740641c6a0588a0ee1c509"+ '"' + "\n")
fout.write("    return str(api)"+ "\n")

# Google Maps API
fout.write("def gmap():"+ "\n")
fout.write("    api="+ '"' +"AIzaSyBY9Rfnjo3UWHddicUrwHCHY37OoqxI478"+ '"' + "\n")
fout.write("    return str(api)"+ "\n")
fout.close()

setup(
    name="ReconSpider",
    version="1.0.7",
    description="Most Advanced OSINT Framework",
    url="https://github.com/bhavsec/reconspider/",
    author="BhavKaran (bhavsec.com)",
    author_email="bhavsec@gmail.com",
    license="GPL-3.0",
    install_requires=["shodan", "requests", "prompt_toolkit","wget","beautifulsoup4","click","urllib3","IP2proxy","wget","paramiko",
```

REQUIREMENTS.PY



```python
fout.write("    return str(api)"+ "\n")
fout.close()

setup(
    name="ReconSpider",
    version="1.0.7",
    description="Most Advanced OSINT Framework",
    url="https://github.com/bhavsec/reconspider/",
    author="BhavKaran (bhavsec.com)",
    author_email="bhavsec@gmail.com",
    license="GPL-3.0",
    install_requires=["shodan", "requests", "prompt_toolkit","wget","beautifulsoup4","click","urllib3","IP2proxy","wget","paramiko"
    console=["reconspider.py"],
)

try:
    import wget
except Exception as e:
    print(e)
    pip.main(['install','wget'])
    import wget

# ip2 Location Database (https://lite.ip2location.com/database/px8-ip-proxytype-country-region-city-isp-domain-usagetype-asn-lastsee
url="https://www.ip2location.com/download?token=hg5uYe2Jvri4R7P1j8b71Pk8dnvIU2M6A9jz2tvcVtGx8ZK2UPQgzr6Hk3cV68oH&file=PX8LITEBIN"
print('\nDownloading IP2PROXY-IP-PROXYTYPE-COUNTRY-REGION-CITY-ISP-DOMAIN-USAGETYPE-ASN-LASTSEEN.BIN...')
filepath=os.getcwd()+"/plugins/"
wget.download(url,out=filepath)
print('\nDownload Finished')

import zipfile
print('\nExtracting Files')
with zipfile.ZipFile(filepath+"IP2PROXY-LITE-PX8.BIN.ZIP","r") as zip_ref:
    zip_ref.extract("IP2PROXY-LITE-PX8.BIN",filepath)

print("\nInstallation Successfull")
print("\n\nNote: APIs included in ReconSpider are FREE and having limited & restricted usage per month, Please update the current AP
print("\nWarning: Not updating the APIs can result in not showing the expected output or it may show errors.")
```

FLOWCHART



Define Objectives and Requirements

Gather target Information
(Input Target Domain/IP, Sub-domain Enumeration, Port Scanning, Service Enumeration)

Data Analysis
(Organize Gathered Data, Whois Data, Vulnerability Data)

Create a Python Tool using appropriate libraries
(Develop Core Modules, Subdomain Enumeration, Port Scanning, Service Enumeration, Data Analysis)

Testing

Functional Testing

Security Testing

Deployment
Package the Tool
Distribute

THANK YOU