OSINT (Open-source intelligence)

#Research_Task_2 by Sukhveer singh

1. OSINT –

OSINT stands for Open Source Intelligence. It is the practice of collecting and analyzing publicly available information from various sources to gather intelligence about a particular target, individual, organization, or event. OSINT encompasses a wide range of sources, including social media platforms, news articles, public records, government websites, and more.

OSINT Framework:

The OSINT Framework is a structured approach or methodology for conducting open source intelligence gathering. It provides a systematic way to organize and categorize different sources of information, tools, and techniques used in the OSINT process. The framework helps intelligence analysts and researchers to efficiently gather, process, and analyze relevant information from diverse sources.

Some categories -

- **Social Media:** Platforms like Twitter, Facebook, LinkedIn, and Instagram, where individuals and organizations share information publicly.

- **Search Engines**: Tools like Google, Bing, and DuckDuckGo, which allow users to search for information on the internet.

- **Public Records**: Government databases, court records, property records, and other publicly available documents.

- **Online Forums and Communities:** Discussion forums, message boards, and online communities where individuals share information and engage in discussions.

- Geospatial Data: Maps, satellite imagery, and geographical information systems (GIS) for analyzing locations and physical environments.

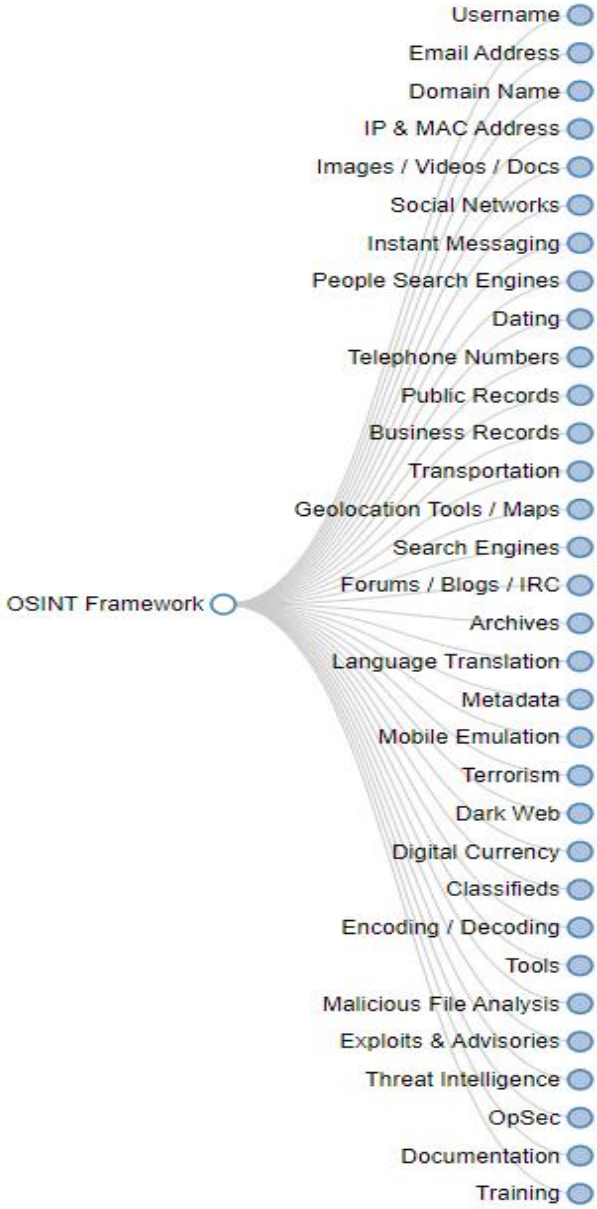
- **Dark Web:** Hidden parts of the internet not indexed by traditional search engines, where illicit activities and sensitive information may be found.

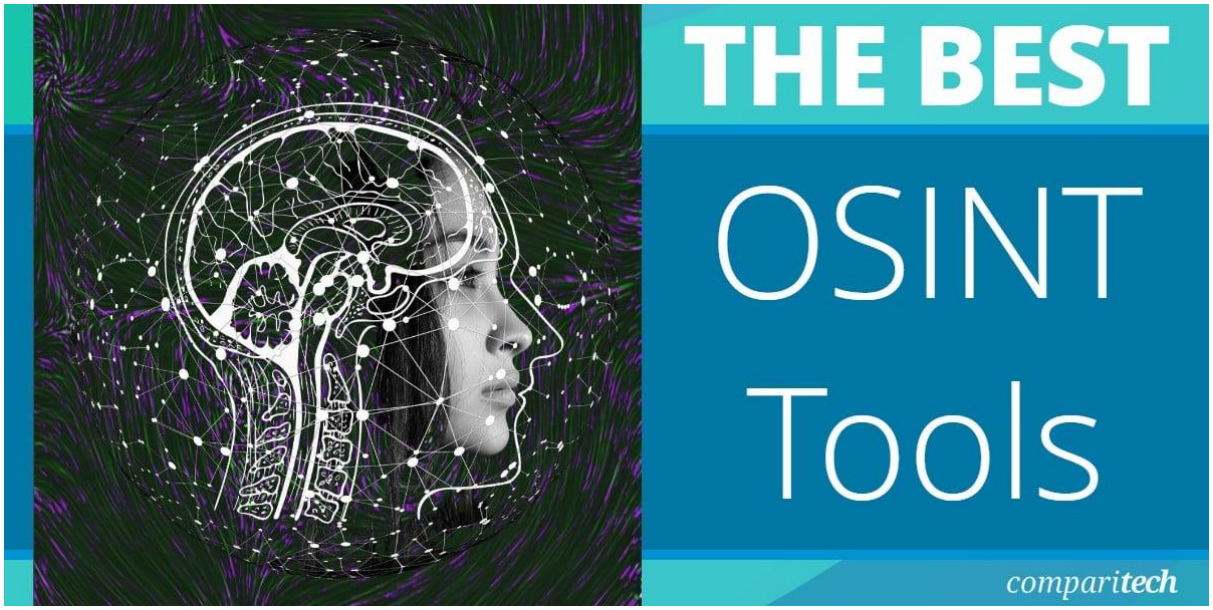
- **Tools and Techniques:** Software tools, techniques, and methodologies used for data collection, analysis, and visualization in the OSINT process.

- **Deep Web:** This category includes parts of the internet that are not indexed by standard search engines but are accessible with specific tools or credentials. It encompasses content that is not publicly available and may require specialized techniques to access.

- **Academic and Research Databases**: This category includes academic journals, research papers, and scholarly databases where researchers publish their findings. These sources provide valuable information on a wide range of topics and can be useful for in-depth analysis and understanding of specialized subjects.

- **Corporate and Business Information:** This category covers sources of information related to businesses, corporations, and commercial entities. It includes company websites, financial reports, regulatory filings, and industry publications. Analyzing corporate information can provide insights into business strategies, financial performance, market trends, and competitive intelligence.

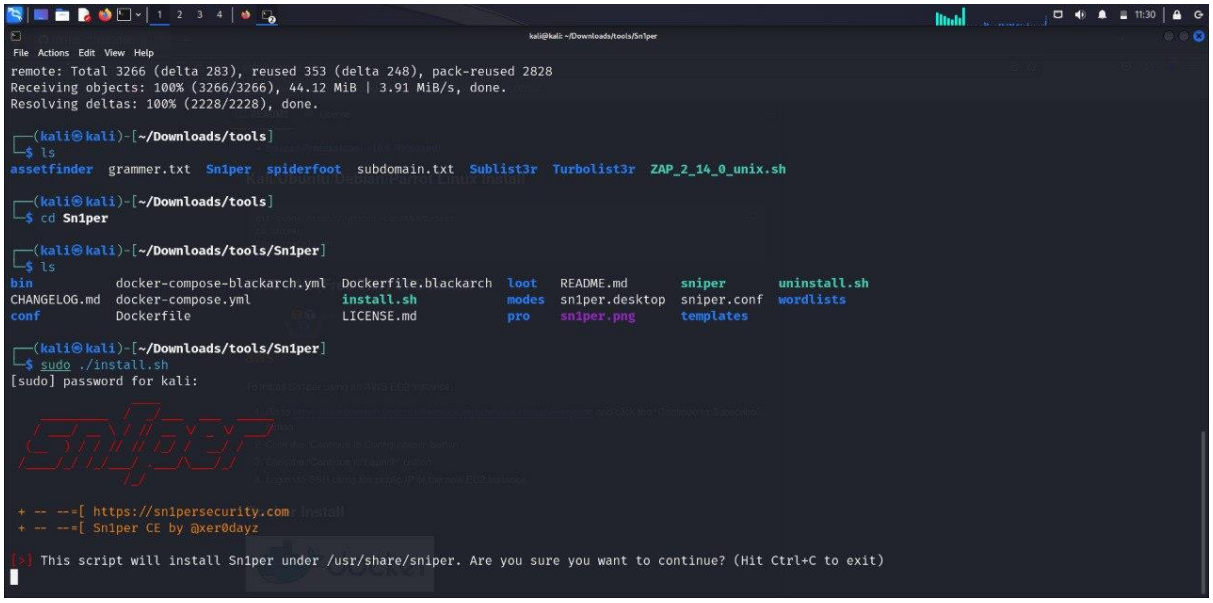

OSINT Framework
Username
Email Address
Domain Name
IP & MAC Address
Images / Videos / Docs
Social Networks
Instant Messaging
People Search Engines
Dating
Telephone Numbers
Public Records
Business Records
Transportation
Geolocation Tools / Maps
Search Engines
Forums / Blogs / IRC
Archives
Language Translation
Metadata
Mobile Emulation
Terrorism
Dark Web
Digital Currency
Classifieds
Encoding / Decoding
Tools
Malicious File Analysis
Exploits & Advisories
Threat Intelligence
OpSec
Documentation
Training



2. 4 Best OSINT tools

1. Tool Name: - SN1PER

a. **Description:** - SN1PER is a powerful reconnaissance tool used for automated scanning and enumeration of web applications, networks, and systems. It is designed to gather comprehensive information about potential targets, including open ports, services running, vulnerabilities, and possible attack vectors.



b. Usage:

SN1PER is used for automated scanning and enumeration of web applications, networks, and systems. It streamlines the reconnaissance process by gathering comprehensive information about potential targets, including open ports, services running, vulnerabilities, and attack vectors.

c. Advantages:

Automation: SN1PER automates the reconnaissance process, saving time and effort for security analysts.

Comprehensiveness: It provides detailed information about the target, including open ports, services, and vulnerabilities.

Customization: Users can customize scanning parameters and options to suit their specific requirements and target environments.

Ease of Use: Despite its powerful capabilities, SN1PER is designed to be user-friendly, making it accessible to security professionals of all levels of expertise.

d. Features:

Information Gathering: SN1PER gathers comprehensive information about the target, including open ports, services, and potential vulnerabilities.

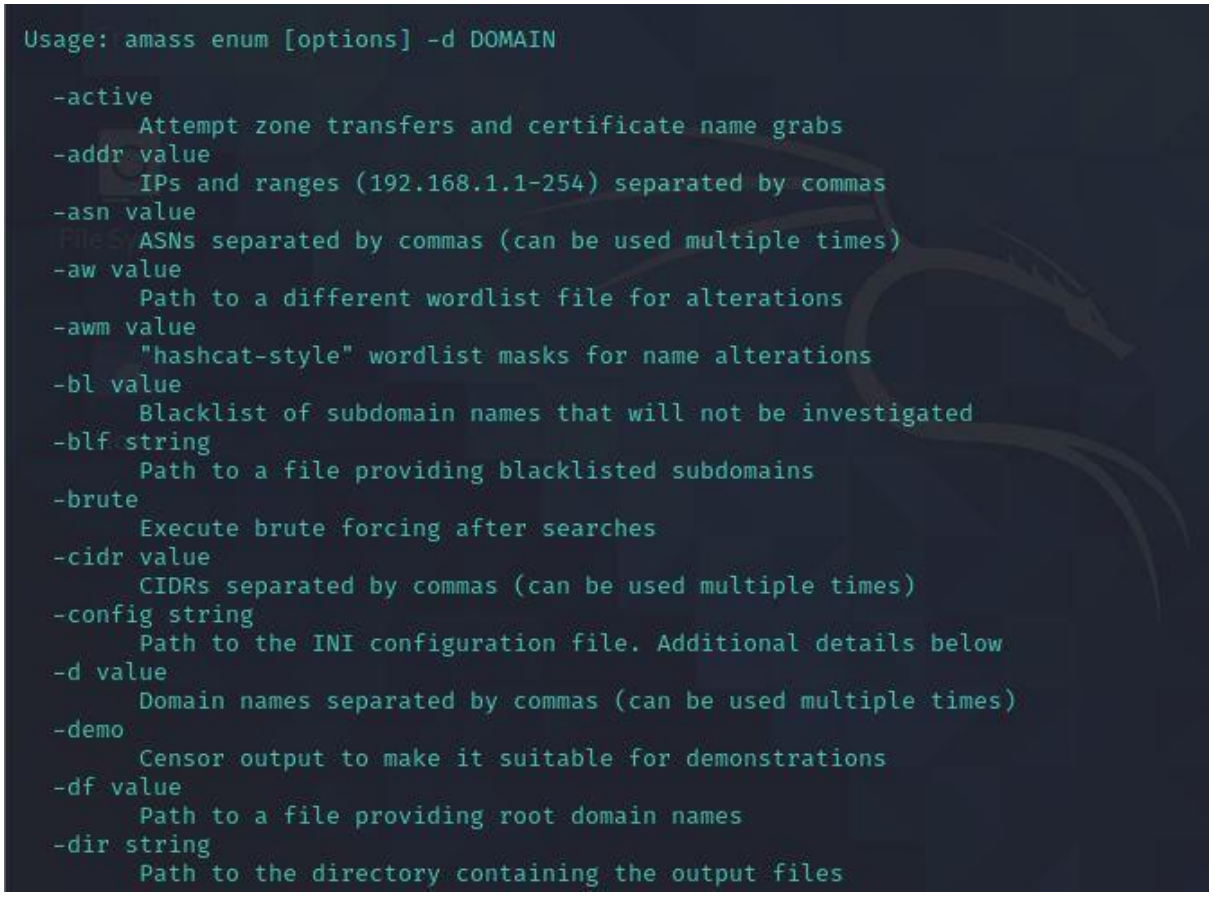
Vulnerability Detection: It identifies vulnerabilities in the target system, such as outdated software versions or misconfigurations.
Reporting: SN1PER generates detailed reports summarizing the findings of the reconnaissance process, facilitating further analysis and remediation.
Customizable Scans: Users can tailor scanning parameters and options according to their specific requirements and target environments.
Accessibility: SN1PER is designed to be user-friendly, making it accessible to both experienced security professionals and beginners in the field.

2. Amass –

I. Introduction to Amass: -

Amass is a powerful open-source tool used for network mapping and reconnaissance. It is designed to help security professionals and researchers discover and map the attack surface of target networks by gathering information about domain names, subdomains, IP addresses, and other related infrastructure components.

II. Uses of Amass: -



Discovery of Assets: Amass is used to discover and enumerate domain names, subdomains, IP addresses, and other network assets associated with a target organization or domain.

Attack Surface Mapping: It helps in mapping the attack surface of target networks by identifying all publicly accessible infrastructure components, including web servers, email servers, and other services.

Threat Intelligence: Amass can be used to gather threat intelligence by monitoring changes in the target's infrastructure, identifying new assets, and detecting potential security risks.

Penetration Testing: Security professionals use Amass during penetration testing engagements to gather reconnaissance information and identify potential entry points for attacks.

III. Advantages of Amass:

Comprehensive Reconnaissance: Amass provides comprehensive reconnaissance capabilities, allowing users to gather information about domain names, subdomains, IP addresses, and other network assets.

Automation: It automates the process of asset discovery and reconnaissance, saving time and effort for security analysts.
Integration with Other Tools: Amass can be integrated with other security tools and frameworks, such as Metasploit and Burp Suite, to enhance reconnaissance capabilities and streamline the penetration testing process.
Open Source: As an open-source tool, Amass is freely available for anyone to use, modify, and contribute to, making it accessible to the security community at large.

IV. Features of Amass:

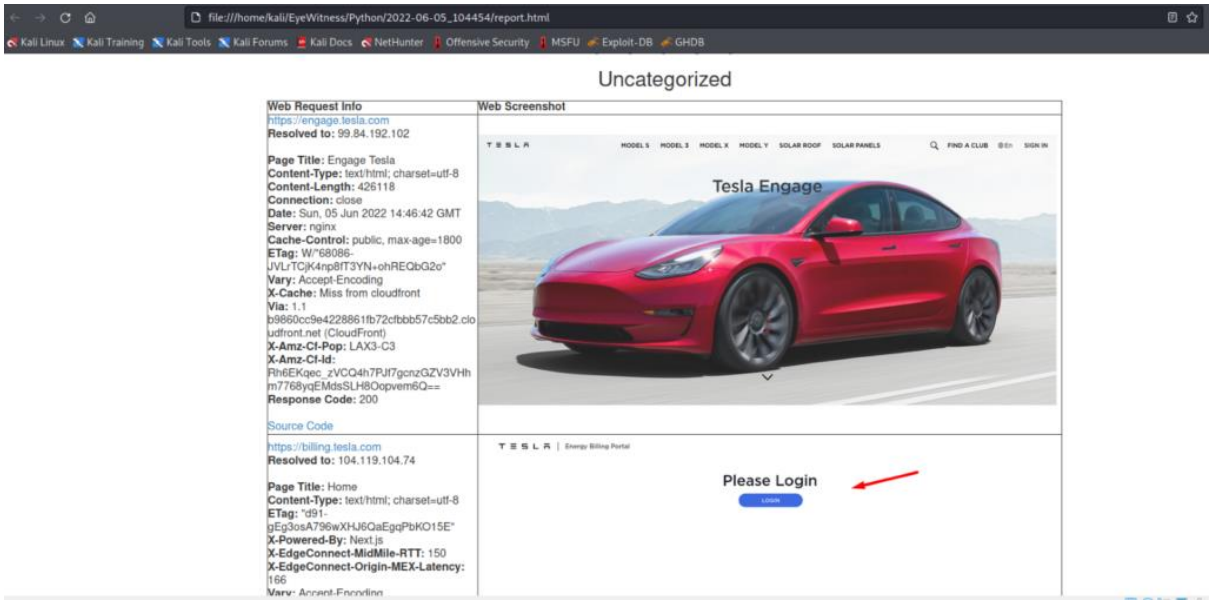
Subdomain Enumeration: Amass enumerates subdomains associated with a target domain, including wildcard subdomains and third-party services.
IP Address Discovery: It discovers IP addresses associated with domain names and subdomains, providing insights into the target's network infrastructure.
Passive Reconnaissance: Amass performs passive reconnaissance by collecting information from public data sources, DNS records, and other publicly accessible data repositories.
Active Reconnaissance: It also conducts active reconnaissance by performing DNS resolution, brute-force attacks, and other techniques to discover additional assets and subdomains.

3. EyeWitness tool –

i. Introduction to EyeWitness: -

EyeWitness is a reconnaissance tool used for capturing screenshots of web applications, websites, and network services. It is designed to help security professionals and penetration testers gather visual evidence of vulnerabilities, misconfigurations, and other security issues that may be present in target systems.

ii. Uses of EyeWitness:



Vulnerability Assessment: EyeWitness is used to perform vulnerability assessments by capturing screenshots of web applications and websites, allowing security analysts to identify potential security weaknesses.

Penetration Testing: It is used during penetration testing engagements to gather evidence of successful exploitation, document findings, and demonstrate the impact of security vulnerabilities.

Visual Reconnaissance: EyeWitness provides visual reconnaissance capabilities by capturing screenshots of network services, such as HTTP/HTTPS, FTP, and SSH, to identify exposed interfaces and potential attack vectors.

Reporting: EyeWitness generates comprehensive reports containing screenshots, HTTP response headers, and other relevant information, which can be used for documentation and communication of findings to stakeholders.

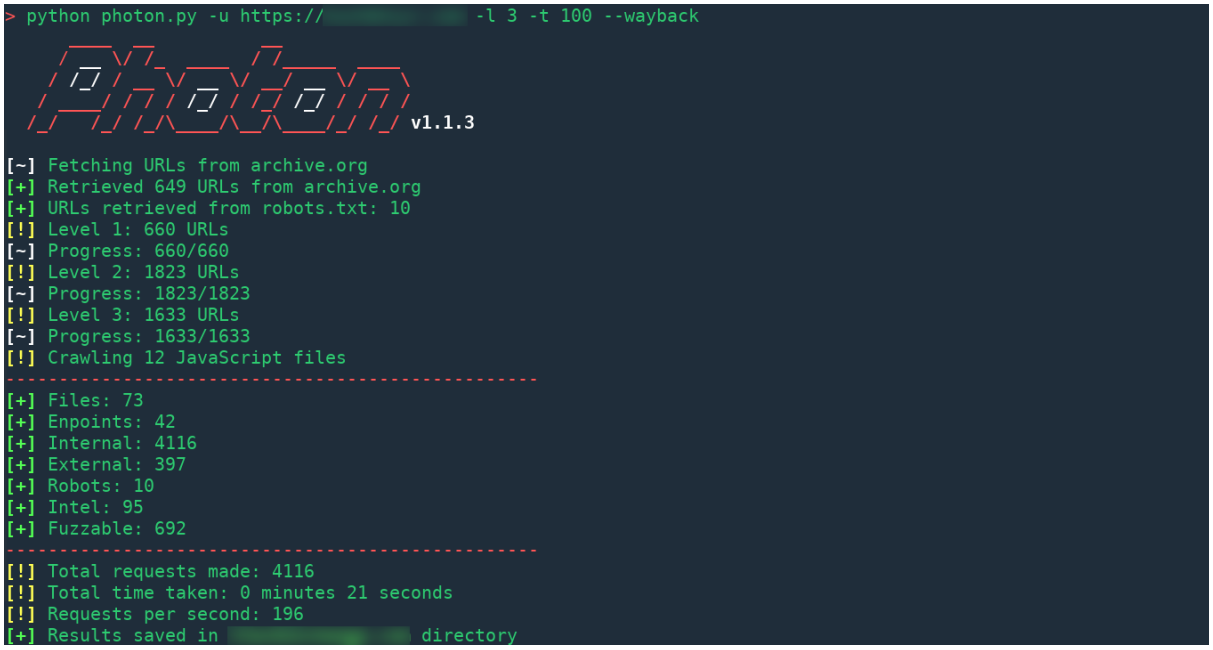
iii. Advantages of EyeWitness:

Automation: EyeWitness automates the process of capturing screenshots, saving time and effort for security analysts during reconnaissance and vulnerability assessment activities.
Comprehensive Reporting: It generates detailed reports containing screenshots, HTTP response headers, server banners, and other information, providing a comprehensive overview of the target environment.
Ease of Use: EyeWitness is user-friendly and easy to configure, making it accessible to security professionals of all levels of expertise.
Integration with Other Tools: It can be integrated with other security tools and frameworks, such as Metasploit and Burp Suite, to enhance reconnaissance capabilities and streamline the penetration testing process.

iv. Features of EyeWitness

Screenshot Capture: EyeWitness captures screenshots of web applications, websites, and network services using headless browsers, such as PhantomJS and Selenium.
HTTP Response Analysis: It analyzes HTTP response headers and server banners to gather information about the target system, including software versions, server configurations, and potential vulnerabilities.
Multiple Output Formats: EyeWitness supports multiple output formats, including HTML, XML, and CSV, for generating reports and exporting findings to other tools and frameworks.
Customization: Users can customize the behavior and configuration of EyeWitness to suit their specific requirements and target environments, including adjusting timeout settings, user agent strings, and screenshot sizes.

4. Photon tool –



1) Introduction to Photon:

Photon is a web application scanner designed for reconnaissance and enumeration. It is used to discover and extract URLs, parameters, cookies, and other relevant information from target web applications. Photon is commonly used by security professionals, penetration testers, and ethical hackers to gather intelligence about web applications and identify potential security vulnerabilities.

2) Uses of Photon:

Web Application Discovery: Photon is used to discover and enumerate web applications by scanning target domains and extracting URLs, directories, and files associated with the web server.
Parameter Enumeration: It extracts parameters from web application URLs and forms, allowing security analysts to identify input points and potential injection vulnerabilities.
Cookie Analysis: Photon analyzes cookies set by the web server to gather information about session management, authentication mechanisms, and potential security risks.
Link Crawling: It crawls through web pages and follows hyperlinks to discover additional pages, resources, and endpoints within the web application.

3) Advantages of Photon:

Comprehensive Reconnaissance: Photon provides comprehensive reconnaissance capabilities, allowing users to gather information about web applications, URLs, parameters, cookies, and other relevant data.
Automation: It automates the process of web application scanning and enumeration, saving time and effort for security analysts during reconnaissance activities.
Customization: Photon offers customization options for adjusting scan parameters, including the depth of crawling, the scope of scanning, and the type of information to extract.
Reporting: It generates detailed reports summarizing the findings of the reconnaissance process, including discovered URLs, parameters, cookies, and other relevant information.

4) Features of Photon:

URL Extraction: Photon extracts URLs from target domains and web pages, including directories, files, and resources accessible via the web server.
Parameter Enumeration: It identifies parameters present in web application URLs and forms, such as query parameters, POST data, and cookies.
Cookie Analysis: Photon analyzes cookies set by the web server to identify session management mechanisms, authentication tokens, and potential security vulnerabilities.
Link Crawling: It crawls through web pages and follows hyperlinks to discover additional pages, resources, and endpoints within the web application.
Custom Headers: Photon allows users to specify custom HTTP headers for requests, enabling advanced scanning techniques and bypassing certain security controls.

5. References –

https://osintframework.com/
https://www.blackberry.com/us/en/solutions/endpoint-security/osint

https://sectigostore.com/blog/open-source-intelligence-what-is-osint-how-does-it-work/
https://gbhackers.com/sn1per/
https://hakluke.medium.com/haklukes-guide-to-amass-how-to-use-amass-more-effectively-for-bug-bounties-7c37570b83f7
https://www.dionach.com/en-us/how-to-use-owasp-amass-an-extensive-tutorial/
https://github.com/RedSiege/EyeWitness
https://www.whiteoaksecurity.com/blog/screenshot-tool-part-1-eyewitness/
https://www.geeksforgeeks.org/photon-scanner-web-scraping-osint-tool/