OPEN SOURCE INTELLIGENCE TOOLS

(OSINT FRAMEWORK TOOLS)

MALTEGO:

- It is an open-source software.
- Developed by Paterva from Pretoria, South Africa.
- Its stable release was on June 4, 2020.
- It is written in java program.
- Its suitable for windows, Mac OS, Linux operating system.

➢ **Uses of maltego tool:**

- it offers real-time data mining and information gathering.
- It presents the gathered information in the form of a node-based graph.
- It can connect up to 1 million objects at a time.
- MALTEGO has free as well as paid version.
- It exports the gathered information in the form of jpeg and pdf format.
- In reconnaissance it helps in gathering: IPv4 address, DNS names, NS records, network blocks and websites, GPS locations and coordinates, malware information such as hashes, network ports within the network, photos, email address, phone number and many more information.
- It is also used to find the relationships between the group of people through social networks.
- In maltego alone, users can query all types of data with data integrations of Shodan, whois, tin eye, etc.
- It has easily editable graphs.
- Allows us to search the darknet for closed websites without a login within more than 30 popular darknet resources.
- It can also retrieve address information, token, and transfer details to analyze activities and connect with other data.
- It can search the world's largest Yellow Papers, White papers, company registries, public documents.
- It mainly provides APIs of many recon tools.

METAGOOFIL:

- Metagoofil searches google for publicly hosted websites for files such as pdf, ppt, xls, docx, doc.
- It extracts the metadata from these files.
- Metadata means metadata is the data and information that is part of or attached to some other more obvious piece of data.
- Every file on a computer has some amount of metadata associated with it.
- After extracting all the data, this tool will generate a report which contains usernames, software versions, and servers or machine names that will help Penetration testers in the information-gathering phase.

➢ **Uses of metagoofil tool:**

- This tool can also extract MAC addresses from Microsoft office documents.
- This tool can give information about the hardware of the system by which they generated the report of the tool.
- with the instincts and intelligence of the attacker, Metagoofil can be used to guess type of operating system, network names, and so on.
- A brute force attack can then be performed, once enough information is gathered from the metadata of the files.
- With the metadata obtained through Metagoofil, it is possible to extract path information, which can be used to map the network.
- The results are displayed in HTML format.

SPIDER FOOT

- Spider-Foot tool automates OSINT for threat intelligence and mapping our attack surface.
- Spider-Foot can be used offensively in a red team exercise or penetration test for reconnaissance of the target or defensively to gather information about what our organization might have exposed over the internet.
- Spider-Foot's 200+ modules feed each other in a publisher/subscriber model to ensure maximum data extraction and most of which don't require API keys, and many of those that do require API keys.
- If our focus is solely on data collection, that is from small to medium targets and we wish to run Spider-Foot within our own infrastructure that we set up, secure and maintain with support from the community, the open- source version is best for us.
- When we want to collect and monitor OSINT data as well as quickly find what's important through rich data navigation and visualization features, spider HX is best for professionals.
- There are about 100 integrations and deep data analysis features.

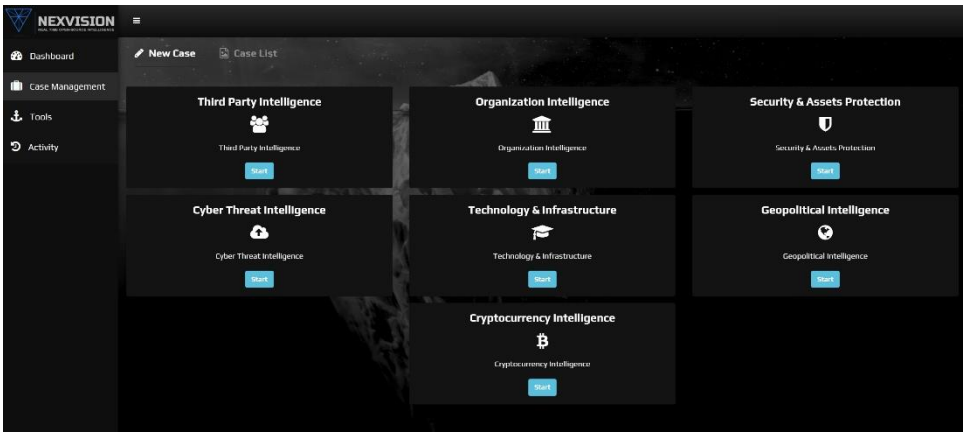
➢ **Uses of spider-foot**:

- we can target the following entities in a Spider-Foot scan: IP address, Domain/sub-domain name, Hostname, Network subnet (CIDR), ASN, E-mail address, Phone number, Username, Person's name, Bitcoin address.
- Spider-Foot HX takes things a step further with the following features:

1. **No installation or setup needed at all:** No Python dependencies to install, no virtual machines to spin up or ensuring we have enough compute/memory/disk to run a large scan.
2. **Investigations:** Sometimes, we don’t want full automation of our scan and want to step through the data collection process step-by-step, module-by-module. Investigations provide us with a visual way to take full control of the scanning process.
3. **Multi-target scanning:** In cases where we have multiple entities (domains, e-mail addresses, etc.) related to the same target, we can supply them all as targets of the one scan. This enables Spider-Foot to better identify relationships and find relevant information.

4. **Scans are faster:** Spider-Foot HX, scans run up to 10x faster than the open-source version.
5. **OSINT monitoring:** Run scans automatically on a daily, weekly or monthly basis at a time of our choice and have all changes between scans automatically tracked and alerted on.
6. **Email notifications:** Receive email notifications when Spider-Foot scans finish, or when scheduled scans identify changes between scan runs.
7. **More modules:** Spider-Foot HX adds additional modules for UDP port scanning, identification of languages used in content and screenshotting of certain content like social media profiles, dark web sites and security-sensitive webpages such as those that accept credentials.
8. **Reporting & Visualizations:** Slice and dice our scan results by data type, data family, module, module category and data source. Look at each data point in-depth to see how it was discovered, its relationships and more.
9. **Team collaboration:** With Spider-Foot HX, we can have multiple users with role-based access control, collaborating on scans and investigations.
10. **Annotations:** Add notes to scan results and pull them out with the API for rich integrations with internal SIEM tools, investigative platforms and ticketing systems.
11. **Security:** Two-factor authentication (2FA), role-based access control and a fully locked down cloud infrastructure that means we don't need to deal with the security of your OSINT platform and investigations.
12. **Anonymous:** Spider-Foot HX has TOR integration out of the box and provides no way for a scanned entity to know that it's we doing the scanning.
13. **Custom Scan Profiles:** With Spider-Foot HX, you can define scan profiles and re-use them for future scans.
14. **Spider-Foot HX API:** The Spider-Foot HX API is a fully documented RESTful API that supports virtually all UI functions so we can orchestrate the platform and extract data programmatically.

NEX VISION



- It is an advanced A.I.-powered OSINT solution that provides real-time intelligence from the Whole Web (Clear Web, Dark Web, and social media).
- It provides unprecedented access to Dark web searches through regular browsers like Chrome and Safari, without the use of anonymizing browser Tor.
- If we are looking to conduct background checks, due diligence, customer on-boarding compliance (KYC/AML/CFT), gather organization intelligence, third party intelligence, cyber threat intelligence, or even research on cryptocurrency addresses from a ransomware threat, Nex Vision provides accurate real-time answers.
- Nex Vision is primarily used by the military and governments
- Their service includes a direct subscription to their SaaS solution and purchasing intelligence reports.
- In the first step, its A.I. powered engine continually collects data, analyses it, and categorizes them, providing the largest commercially available data lake.
- In the second step, the engine uses machine learning to reduce false positives to provide highly accurate and contextualized results. This greatly reduces the man-hours and time required in investigations and the alert fatigue that analysts face when met with large amounts of irrelevant data.
- In the final step, all the results are reflected on the dashboard where users can easily visualize and make informed decisions.
- Penetration testers and red teamers should be able to use it during Open-Source Intelligence Assessments or while examining the external attack surface of their client

➢ **Uses of Nex Vision tool:**

- Results are delivered fast.
- making it easier for you to pinpoint vulnerabilities in your target environment
- help you find relationships between entities and understand how they're connected.
- It gathers information from the Dark Web and social media as well.
- NexVision provides the largest OSINT data pool (surface and dark web, social media data lake) and it uses artificial intelligence (AI), to remove false positives, so users get the most accurate intelligence
- AI/ML-powered engine with continuous collection, analysis and sorting of big data (from publicly available databases and the deep web)
- Provide real-time access to the whole web, including clear web and the dark web (where criminal activities occur), without the use of an anonymizing browser like Tor
- Greatly increasing data available whilst removing false positives
- Multilingual data support
- Equipped with natural language processing and steganography-decoding capabilities. Able to detect jargon and capture hidden information advanced threat actors employ to avoid detection.
- Dashboard that allows users to set keyword alerts, conduct investigations and analyze results whilst staying anonymous.
- Easy-to-use interface that is accessible to analysts without prior data science or computer science background.

- Provide alerts in real-time and send text/email alerts to the user
- Cloud-deployment solution with the ability to integrate with existing IoC stacks via API for easy adoption.
- Users can use NexVision to conduct background checks on people and organizations, gather social sentiment, monitor keywords throughout the whole web and NexVision will send an alert whenever there is new intelligence on the target.

TINEYE

- Tin Eye is the first reverse image search engine.
- We have to submit a proper picture to Tin Eye to get all the required information like where it has come and how it has been used.
- It uses different methods to function its tasks like image matching, signature matching, watermark identification, and various other databases to match the image instead of using keyword matching.
- Tin Eye applies neural networks, machine learning, pattern recognition, and image identification technology rather than keywords or metadata.
- Advanced image identification, label matching, image tracking, image verification, mobile image recognition, color search are its features.

➢ **Uses of tin eye tool**:

- Match Engine works with your own image collection and finds duplicate, resized and modified images. Powered by Tin Eye's unparalleled image recognition, Match Engine is engineered to deal with a broad range of image transformations, including resizing, cropping, edits, occlusions and color changes, amongst others.
- Match Engine is the API of choice for identifying duplicate images, profile and UGC image verification, fraud detection, image collection reconciliation and blacklisting unwanted images.
- Match Engine is scalable and it enables you to include image recognition capabilities in your own applications, enterprise solutions and web services.

- Win engine this service uses exceptional image recognition algorithms and neural networks to deal with the common problems encountered in user-supplied photographs: low resolution, bad lighting and color, improper framing and cropping, off-center angles and blurriness.
- It verifies images, moderate user-generated content, track images and brands, check copyright compliance, deploy fraud detection solutions, identify stock photos, confirm the uniqueness of an image.
- Mobile Engine makes it easy for you to add image recognition to your app. We provide a reference database of images (e.g., artwork, consumer packaged goods, book covers, catalog pages, etc.) and when your users photograph that object, Mobile Engine finds your matching reference image.
- Multicolor Engine automatically and consistently identifies the colors in your images.

REFERENCES:

https://www.computerweekly.com/photostory/2240160112/Nine-must-have-OSINT-tools/4/3-Metagoofil

https://www.hackingloops.com/metagoofil-tutorial-extract-information-from-docsimages-and-more/

https://www.computerforensics.com/news/what-is-metadata

https://www.kali.org/tools/metagoofil/

https://github.com/opsdisk/metagoofil/

https://cybersecuritynews.com/osint-tools/