EXPLORING OPEN-SOURCE INTELLIGENCE (OSINT)

IST 110

Group 05

OSINT consists of the methods, tools, and use of publicly available information.

There are several key techniques including web scraping, social media analysis, active collection, advanced searching, and passive recon.

Businesses, individuals, and organizations of all types make use of OSINT daily for all aspects of operation.

The following presentation explores these critical techniques in more depth to answer the question:

What is OSINT?

OSINT Technique: Web Scraping

Web scraping is the primary technique used to harness the near infinite quantity of information available on the internet. It is a semi-automated process as a key aspect is human involvement in monitoring scraping tools to ensure ethical, accurate, and efficient collection of data.

OSINT Technique: Web Scraping

Concepts and Processes

Web scraping makes use of numerous programming languages from HTML & JavaScript to understand how websites are structured, Python to create scripts to automate data collection, and R to organize data. The term thusly encompasses the following concepts:

- Information source analysis
- Crawling (data collection from sources)
- Data organization

OSINT Technique: Web Scraping

Use Cases

A true master-list of all uses for web scraping is nigh impossible to craft, however highlights include:

- Market pricing/sentiment analysis
- Artificial Intelligence model training
- Journalism
- Political campaigning
- Marketing/advertising optimization

OSINT Technique: Social Media Analysis

Social media analysis is the ability to collect and analyze data from social media platforms to help a group or an organization's objectives. This technique can bring insight to human behavior and interests that can be used in a good or bad way based on a persons or organizations objectives.

OSINT Technique: Social Media Analysis

Use Cases

There are many use cases of social media analysis, specifically only off this technique are the following:

- Threat Detection and Monitoring
- Brand Monitoring and Competitive Intelligence
- Crisis Management (Disaster Response)
- Audience Analysis
- Investigative Research

OSINT Technique: Active Collection

Active Collection is when you find open ports and vulnerabilities in website and services that allow you to pull data out.

OSINT Technique: Active Collection

Use Cases

Use cases involved with active collection include:

- Gaining data from private social medias
- Finding archived or old data from websites
- Retrieving data from private sites or servers

OSINT Technique: Advanced Searching

Every day we use tools like Google to conduct basic search requests to find information that helps us complete works tasks, conduct research, or just to simply become more informed. When we use these types of simple searches, we often get a return with an overwhelming amount links or documents and many of them are usually not relevant to what we specifically want. This where is the technique of advanced searching can be extremely helpful and a good query can return exactly the information we want to find. It allows you to be very specific with finding key words in a context you want and will even search specific websites, file types, languages, and other criteria.

OSINT Technique: Advanced Searching

Use Cases

In a scenario where a company wanted to know specific details about competitors or customers, you can use Google search operators to do the following:

- **Conduct research on competitors**
- **Find email addresses for person of interest**
- **Look for indexed files**
- **Conduct customer research**

OSINT Technique: Passive Recon

Passive Recon is usually to gather OSINT intelligence. It can involve scraping publicly available websites, retrieving data from open-sourced APIs such as the Twitter API, or pulling data from deep web information sources.

ONSIT:

Passive Recon

For “penetration testers and security teams”, the goal of using ONSIT is to reveal public information about internal assets and other information accessible outside the organization.