UDC 621.39

OPEN SOURCE INTELLIGENCE (OSINT)

Nser A.M., Minochkin D.A.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: nser.anzhela@gmail.com, dmytro.minochkin@gmail.com

РОЗВІДКА НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ

У статті наводиться опис технологій, методик та можливості розвідки з на основі відкритих джерел (OSINT - Open-source intelligence). А саме буде розглянуто методи та приклади використання, фреймворки та рекомендації з оперуванням певного роду інформації.

The article describes the technologies, methods, and exploration of open-source intelligence (OSINT). Namely, methods and examples of use, frameworks, and recommendations for the operation of certain types of information will be considered.

Open-source intelligence (OSINT) is information collected from public sources such as those available on the Internet, although the term isn't strictly limited to the internet, rather means all publicly available sources.

The U.S. Department of Defense (DoD) defines OSINT as follows: “Open-source intelligence (OSINT) is an intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement” [1].

OSINT sources are distinguished from other forms of intelligence because they must be legally accessible by the public without breaching any copyright or privacy laws. That’s why they are considered “publicly available.” This distinction makes the ability to gather OSINT sources applicable to more than just security services. For example, businesses can benefit from exploiting these resources to gain intelligence about their competitors.

OSINT can be passive or active. Passive methods are those that do not involve interaction with target systems and are not subject to automatic detection. In active data collection, analysts interact with target systems, which can involve employing advanced techniques or even simple interactions such as registering on an organization’s website to get materials available to registered users only [2].

A great place to start is the OSINT Framework put together by Justin Nordine [3]. The framework provides links to a large collection of resources for a huge variety of tasks from harvesting email addresses to searching social media or the dark web. OSINT framework focused on gathering information from free tools or resources.

Let’s look at practical tools for OSINT. And we will start with the easiest and most used in real life is Google dorking.

In simple words one can say Google Dorks are a technique that makes use of Google's advanced search services to locate valuable data or hard-to-find content.

Let’s look at the most popular Google Dorks operators and what they do.

- intitle: used to search for various keywords inside the title, for example, intitle:security tools will search for titles beginning with “security” but “tools” can be somewhere else in the page;

- filetype: used to search for any kind of file extensions, for example, if you want to search for pdf files you can use: email security filetype: pdf;

- intext: useful to locate pages that contain certain characters or strings inside their text, e.g. intext:"safe internet";

- site: will show you the full list of all indexed URLs for the specified domain and subdomain, e.g. site:securitytrails.com;

- cache: this dork will show you the cached version of any website, e.g. cache:securitytrails.com.

Maltego specializes in uncovering relationships among people, companies, domains and publicly accessible information on the internet. It’s also known for taking the sometimes enormous amount of discovered information and plotting it all out in easy-to-read charts and graphs. The graphs do a good job of taking raw intelligence and making it actionable, and each graph can have up to 10,000 data points [4].

The Maltego program works by automating the searching of different public data sources, so users can click on one button and execute multiple queries. A search plan is called a “transform action” by the program, and Maltego comes with quite a few by default that include common sources of public information like DNS records, whois records, search engines and social networks. Because the program is using public interfaces to perform its searching, it’s compatible with almost any source of information that has a public interface, so adding more searches to a transform action or making up a whole new one is easily possible.

Once the information is gathered, Maltego makes connections that can unmask the hidden relationships between names, email addresses, aliases, companies, websites, document owners, affiliations and other information that might prove useful in an investigation, or look for potential future problems. The program itself runs in Java, so it works with Windows, Mac and Linux platforms.

Shodan is a network security monitor and search engine focused on the deep web & the internet of things. It was created by John Matherly in 2009 to keep track of publicly accessible computers inside any network.

It is often called the 'search engine for hackers', as it lets you find and explore different kinds of devices connected to a network like servers, routers, webcams, and more.

Shodan is pretty much like Google, but instead of showing you fancy images and rich content / informative websites, it will show you things that are more related to the interest of IT security researchers like SSH, FTP, SNMP, Telnet, RTSP, IMAP and HTTP server banners and public information. Results will be shown ordered by country, operating system, network, and ports.

Shodan users are not only able to reach servers, webcams, and routers. It can be used to scan almost anything that is connected to the internet, including but not limited to traffic lights systems, home heating systems, water park control panels, water plants, nuclear power plants, and much more.

Nmap is one of the most popular and widely used security auditing tools, its name means "Network Mapper". Is a free and open source utility utilized for security auditing and network exploration across local and remote hosts.

Some of the main features include [5]:

- Host detection: Nmap has the ability to identify hosts inside any network that have certain ports open, or that can send a response to ICMP and TCP packets.

- IP and DNS information detection: including device type, Mac addresses and even reverse DNS names.

- Port detection: Nmap can detect any port open on the target network, and let you know the possible running services on it.

- OS detection: get full OS version detection and hardware specifications of any host connected.

Version detection: Nmap is also able to get application name and version number.

In this article, I have covered the basic idea of OSINT and why it’s useful. We’ve looked at a great place where you can discover many OSINT tools to help you with virtually any kind of information gathering you need to do, and we’ve also given you a taste of a few individual tools and shown how they can work.

Gathering OSINT is also a great way to understand what information you are gifting potential attackers. Once you are aware of what kind of intel can be gathered about you from public sources, you can protect this information and develop better defensive strategies.

References

1. Hassan, Nihad A.; Hijazi, Rami (2018). Open Source Intelligence Methods and Tools doi:10.1007/978-1-4842-3213-2.
2. OSINT (Open-source intelligence). Kaspersky IT Encyclopedia. (n.d.). URL: https://encyclopedia.kaspersky.com/glossary/osint.
3. Justin Nordine. OSINT framework. URL: https://osintframework.com/
4. Sharma, (2021, June 28). 15 top open-source intelligence tools. CSO Online. https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-intelligence-tools.html.
5. Borges, E. (2021, October 19). Top 25 OSINT Tools for Penetration Testing. URL: https://securitytrails.com/blog/osint-tools.