IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101225

OPEN-SOURCE INTELLIGENCE TECHNIQUE(OSINT) SPIDER

Abhishek Mishra[1], Anish Bhowmick[2], Mehul Jain[3], Nimisha Jain[4] Dr. Sonal Sharma[5]

Department of Computer Science and Engineering FET- Jain University Bangalore, Karnataka, India[1-5]

Abstract: - The search, collection, analysis, and use of information from open sources, as well as the methodologies and tools used, is referred to as open-source intelligence (OSINT). OSINT arose from a military requirement to acquire relevant and publicly available data. Since its inception, several studies have been conducted suggesting and creating new ways to use OSINT in various situations. SINT Spider attempts to combine the most common and necessary OSINT techniques into one nice convenient package. It is a great toolkit for anyone who does any penetration testing, or just wants a head start on their exploitation. The tool is still in its early stages, however it does everything it sets out to do minus any GUI makers. You can use the toolkit on any system with the necessary dependencies and requirements to install and run the packages. In addition, I would recommend creating your own scripts and adding things on top of this toolkit if you plan to use it in every attack. This is the toolkit to use if you are a newer pen tester and want to get into information gathering and learn new techniques for information gathering. It also provides a reference if you need to run one of these tools outside of Kali (which is sometimes necessary). The tool will be built on a framework which will merge tools with a common command line interface. Each tool will play a role in reducing the effort required to run multiple tools. The initial plan is to merge the following tools - Reverse Image Search - Email Hunting - Username Hunting - IP Tracing

***Key-words*:** - Pap smear, Debris, Poisson noise, Image Processing

1. INTRODUCTION

OSINTSpider is most Advanced Open-Source Intelligence (OSINT) Framework for scanning IP Address, Emails Organizations and find out information from different sources. OSINTSpider can be used by Infosec Researchers, Penetration Testers, Bug Hunters and Cyber Crime Investigators to find deep information about theirtarget. OSINTSpider aggregate all the raw data, visualize it on a dashboard and facilitate alerting and monitoring on the data.
As we all know, Open-Source Intelligence is essentially acquiring publically available information for the person or resource we're looking for. Today, Everything is happening

digitally from payment industries to educational institutes every thing is going in digital form. It may be blackhat hackers looking for a huge bounty by exploiting networks, it might a group or a company looking to launch a large-scale ransomware attack, or it may be a state-sponsored advanced threat persistant threats (APT) groups which is responsible for attacks such as solarwinds as we saw in this pandemic. In such cases the blue team operations, incident responders or government groups responsible for cybercrime divisions comes into play. For example, in case of ransomware attacks first they need to look for the cryptographic keys in the memory or the anonymous servers where the keys are stored and if it is done by some same group which reportedto pursue this kind of attack earlier this can be used to find out the pattern of the attacks. For a cyberterrorist if a certain IP address is found then it can be traced back to where the IP is originating. All this test cases depends highly on Open-Source Intelligence (OSINT) techniques to locate the asset.
The OSINT have many techniques associated with it but the main problem is there are so many tools or websites to perform the same search but there are no such tools that can be used to perform multiple operations. This is where OSINT Spider comes into play. It consists of four tools to perform, Email OSINT, Username OSINT, IP tracing and Reverse Image Search.

2. LITERATURE SURVEY

The gathering of information from publicly available sources and the analysis of that information to create actionable intelligence is known as open-source intelligence (OSINT). OSINT's scope includes not only cybersecurity but also corporate, business, and military intelligence, as well as other domains where information is important. There are websites dedicated to persons searches, which can be conducted using a genuine name, username, email address, or phone number. People search websites allow users to opt out, but after people opt out of listings, new search services using their records surface. The reason for this is that multiple services buy and use the same dataset. Some

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101225

organizations own those datasets, and even if a user removes a profile from one of their websites, the old data is repopulated on the new domain, resulting in the previously removed profile reappearing in the search. As a result, if folks performed a good job of cleaning up after themselves, you should be fine. As a result, if folks did a decent job cleaning up their junk, all you have to do now is wait for a fresh database to appear. One way to locate people who have opted out is to use the persons search tool, find a unique paragraph, and run a quoted Google search on it to find all of the company's domains. It's possible that in1information that was taken from site A is now on-site B. One of the websites that maps IP addresses to locations is iplocation.net. When you know which WI-FI access sites the user has used in the past, utilize wigle.net to map them and conduct additional in-depth investigation on Google Earth. When you have a photograph and want to find out where else it has been used, when did it originally emerge – use Google Images, to run a reverse picture search. Furthermore, Tin Eye's algorithms are not the same as Google's, and as a result, the results may differ. What is the benefit of that? As an investigator, you might be able to track down the person using their avatar, as most people don't bother changing their profile photographs on the numerous social media platforms they use. A photograph taken on the day of the event, for example, cannot be found using a date filter range that is earlier than the mentioned event. As a result, if the photograph is discovered, it was generated before to the incident and is therefore a forgery. Find clone and Findmevk.com for Vkontakte and karmadecay for Reddit will do the trick if you require a narrow search across the social network. It's also worth mentioning browser extensions: Image & RevEye for Chrome Search Options for Firefox.

3. METHODOLOGY

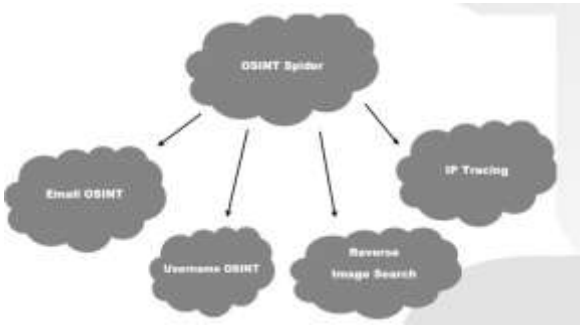

Fig 3.1(Flowchart of modules of OSINT SPIDER)

I. Email OSINT:

If someone named "Alex Issac" is working on an MNC and his work email is "Ales.I@MNC.com" now what we can see is that the MNC is using "Firstname.LastName's first Letter" as their email. This can be further used to list all employees email address just by seeing their names. If we want to take this to another step we can make a list of for example 1000 email records of their employee and check if their email was listed in a breach. We can check this by going to haveibeenpwned.com to see if they are breached. So for example if out of 1000 167 emails are in a breach earlier we can search for their passwords in sites like dehashed and try to login in their company email and if the user didn't change their passwords so we can successfully compromise employees of a MNC. This is a very small scenario what can happen but in reality the numbers are very huge and the scope increases. In the three techniques we mention i.e., checking for email accounts in breach and finding more accounts within the same organization can be automated by our Email OSINT package of OSINT Spider. It will first check if the provided email is in a breach and after that it will find each and every email account that is publicly available somewhere along with their linkedIN and twitter profiles.

II. Username OSINT

The Username OSINT is also helps in formulating email in the above-mentioned scenario but it can be used in other scenarios also. Social Media can reveal so much information such as the organization you work in, the position you are in, your previous organizations, your house, location, phone number, family members, hobbies etc. and this list can go long and long. This can be used to locate people or finding lost peoples, companies such as trace labs are doing amazing job in finding peoples by just using their digital footprints. People that were lost 10 years ago are found digitally, you can see the power of social media. Our Username OSINT will take a username as an input and will be searching on more than 70 social media sites and if that username was used atleast once it will provide you with the link of the social media site and their might be some false positive which will also be notified by our tool.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101225

III. REVERSE IMAGE SEARCH

The Reverse Image Search is very Important. To understand it let us assume a scenario, We found the name of the attacker and by searching in the social media sites we found a picture of the attacker. But we don't know where the place is ,in such cases reverse image search can come into play. A reverse image search technique is used in such scenarios to locate someone based on their recent activities. Traditionally what we do is upload the picture of the attacker in search engines such as google, Yandex etc. and they gave all the related images or almost same pictures of the places that the person is standing and helps us knowing the location. The Reverse Image Search is very powerful and can also be used in finding peoples. Our OSINT Spider also have a module of Reverse Image Search which can be used to doing exactly the same with just one click. You just have to enter the image path in the terminal and it will open the default web browser of the system and provide you with all related images.

IV. IP TRACING

The IP tracing is in the security industry for quite some time. As we see in movies someone is traced it can all be done with IP tracing. For groups such as APT it is very important for an incident responder to find the IP source of the Attack. It becomes very important to know the location of the attackers so that we can run operations to catch them. The IP tracing will give information such as in which zone the IP is, which organization the IP is registered, what is the coordinate or the geolocation of the IP address etc can be retrived from a single IP. So in after hack scenarios, it becomes very important to trace an IP address. Our tool OSINT Spider also have a IP tracing module which efficiently find all the above mentioned searches and more with just one click and output it in a very readible format so that it is easy for the forensic investigators, threat hunters or incident responders to read.

4. RESULT

These are the four parts that have been integrated into a single application. OSINT Spider can be used by incident responders and also by someone who is looking for someone who is missing or by a Pentester in the reconnaissance phase for the penetration test they are performing for their client. This one tool can be used to utilize four huge Open-Source Intelligence Techniques in a very easy manner through a command line. The tool is fully scripted with python and with use of python modules and Application Programming Interface (apis) wherever necessary. This is a pure command line-based tool which are more powerful than the GUI based frameworks and it also gives the command line geeks a huge advantage to fast utilize this tool.

Reverse search Image

Fig 4.1(Result of Reverse search Image)

Email OSINT

Fig 4.2(Result of Email OSINT)

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101225

Username OSINT

Fig 4.3(Result of Username OSINT)

IP TRACING

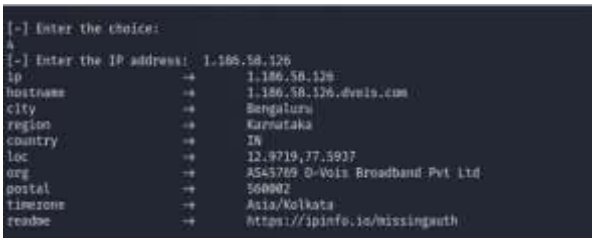

Fig 4.4(Result of IP Tracing)

5. FUTURE SCOPE AND CONCLUSION

According to the CIA, this OSINT is intelligence "derived from publicly available material." Most intelligence specialists broaden that term to include information aimed at the general public. OSINT is information that can be obtained without the use of specialized skills or technologies, but it can also contain sources that are exclusively available to subscribers, such as paywall content in newspapers or subscription journals. OSINT, according to the CIA, includes data obtained from the internet, the news, specialist journals and study, pictures, and geographical data. The Bellingcat MH17 inquiry used several of these sources. Exponents of OSINT are not required to hack into systems or utilise private credentials to gain access to data. Using someone's login data to unearth private information is not OSINT, but viewing their public profile on social media is. OSINT is a phrase used by intelligence agencies to describe information obtained from non-classified sources. Advancements in analytics, are projected to gain popularity in the Open Source Intelligence Market, resulting in increased revenue creation. Other factors driving the open-source intelligence market growth include the rapid expansion of open-source public databases and the rise in cyber security threats. Governments all across the world are deploying open-source intelligence technologies aggressively, adding to market spread.

For example, Open Government Data Platform is an open data initiative launched by the government of India in collaboration with the US government.

What our project involves is a set of software tools typical to aspiring security professionals. It is important that one understands how to work with these tools in their entirety before seeing

.Our OSINT Spider will help Threat Hunters to locate the threat actors, it will give forensic investigator to locate IP addresses after an incident. It will make government agencies, police to locate peoples by using their digital identity or digital footprints. It will help NGOs who are looking for missing persons and will help them reunite to their families. It will also help a beginner cybersecurity student to help understand the Open Source Intelligence techniques and will help them add a new skill to their arsenal.

6. REFERENCES

1. Shinde, P.S. and Ardhapurkar, S.B., 2016, February. (pp. 1-5). IEEE.
2. Shah, S. and Mehtre, B.M., 2013. Int JElectron Commun Comput Eng, 4(6), pp.47- 52.
3. https://shorturl.at/mDNTUhttps://shorturl.at/ehzCO
4. https://www.paessler.com/it-explained/packet- sniffing
5. https://en.ryte.com/wiki/Crawler
6. https://ieeexplore.ieee.org/document/7491568
7. https://ieeexplore.ieee.org/document/7119262
8. https://www.researchgate.net/publication/ 263779662_Network_Scanning_Vulnerabilit
9. https://ieeexplore.ieee.org/document/1166 620
10. https://www.sciencedirect.com/topics/com puter-science/packet-sniffer
11. https://www.researchgate.net/publication/ 309230926_Survey_of_Keylogger_Technol