COMPARATIVE STUDY OF OSINT TOOL FOR IOT

[1]Pinal Mistry, [2]Dr.Ravi Sheth, [3]Mr. Priyank Parmar
[1]M.Tech Student, [2]Assistant Professor, [3]Assistant Professor,
[1,2,3] School of Information Technology, Artificial Intelligence and Cyber Security,
[1,2,3] Rashtriya Raksha University, Gandhinagar, Gujarat India.

Abstarct: *With the rapid development and fast increasing use of Internet of Things (IoT) in day to day life, more devices are connected to Internet. In the smart home, smart wear, smart manufacturing, and smart health care and everyday life, IoT devices are commonly used. Therefor security vulnerabilities are increased endlessly. As more devices are connected to internet, increasing continuously huge amount of data and most of data are available publicly which means that we can access data from anywhere, anytime or by any user from Internet. Managing security of these devices are difficult task for security analyst. For security of devices OSINT on devices is requires. Open Source Intelligence (OSINT) is type of intelligence gathering from target which are publicly available. There are many OSINT tool available like Maltego, Shodan, and Censys for devices and network monitoring. In this paper, an inclusive survey of OSINT, types of OSINT tools and comparison of tools are described. The merits and demerits of each OSINT tool are presented. At last summarize conclusion and future work.*

Index Terms: Internet of Things (IoT), Open Source Intelligence (OSINT) Tools, Security, Vulnerability, Crawling

1. INTRODUCTION

The Internet of Things (IoT) is emerging platform, which connect everyday physical object to internet by wired or wireless medium. As we know that nowadays all things became "Smart" means connected internet require vast use of IoT devices. They have been used in smart home, smart city, smart work, smart healthcare and everyday life related fields.

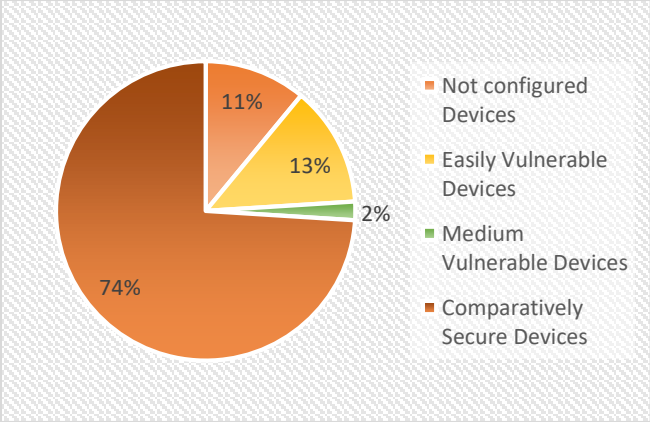

Fig.1. IoT Vulnerability Assessment

IoT system protection vulnerabilities are present, and they are very difficult to handle. HP estimates that 70% of IT products have security vulnerabilities and 25 vulnerabilities are accessible per unit. By leveraging the vulnerabilities of these machines, malicious attackers participate in illegal activity. The amount of data generated by this inter connected devices are huge which is available publicly. OSINT is used for this publicly available information.

OPEN SOURCE INTELLIGENCE (OSINT)

Open Source Intelligence (OSINT) is a very useful method to collect and analyze all the information from public sources, media, human resources, or the internet. OSINT includes a large amount of variety of intelligence for data collection and analysis. In my word, it's an art to creates and gather all data & information which is publicly available.

OSINT is type of intelligence gathering consist collecting, processing and analyzing of public information from open data source like social media, blogs, publication, internet connected devices. OSINT is mainly based on the target.

Nowadays, Open source Intelligence is used by law enforcement agency, government and military by fight against cybercrime. By gathering information from publicly available source about particular target attacker or pen tester can better understand characteristics and discover possible vulnerabilities. Information gathering from huge amount of source is s time consuming. A great start is with OSINT framework. This framework provide link to the large collection of resource for different task from personal information gathering to dark web scraping.

OSINT sources collected using three method: Passive, semi-passive and active.

- **Passive**: All OSINT intelligence method use passive collection because OSINT main goal is to gather information about target with publicly available resource only.
- **Semi-passive**: In this method, sends limited request to target server for acquire information about it. We are not able to in depth investigating of target, only basic investigation is performed.
- **Active**: In this collection method we directly connected to target to gather information about it. Target can be aware of reconnaissance process so person use advanced gathering information to access data like open port, vulnerabilities, Operating system, scanning web application and more. In this method accurate result is obtained due to direct connect with target.

Process of OSINT on any target is performed as shown in below Fig.

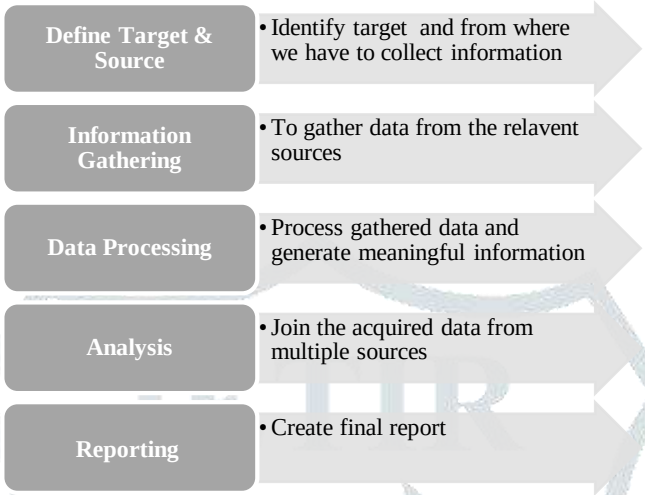

Fig.2. Open Source Intelligence (OSINT) Process

The merits of OSINT (Open Source Intelligence) are as follows:

- Less Risky: OSINT use publicly available information for collect intelligence has no risk as compared to other intelligence gathering technique.
- Cost effective: less expensive compared to other.
- OSINT sources are available anywhere and always up to date.
- Most of OSINT resources are shared by other parties without any copyright license.
- OSINT techniques can be used by law enforcement for fighting against cyber-crime.

The merits of OSINT (Open Source Intelligence) are as follows:

- **Complexity of data management**: The data gathered by OSINT is huge amount, so it's challenging to handle id effectively.
- **Unstructured information**: Publicly available information is disorganized. So information gathered by OSINT is heterogeneous and difficult to classify.
- **Misinformation**: There are many possibilities that information gathered are fake or misleading. OSINT is always deal with correct information and ensure positive outcome.
- **Data sources reliability**: Authenticity of information is key point for OSINT. Data sources from where information are gathered are always trustworthiness and reliable

There are many OSINT tools are available for information gathering from different sources like social media, IoT devices, blogs, and publication. This tools are used by pen- tester, malicious attacker, security researcher. Some of them are listed below:

- Maltego
- Shodan
- Censys
- Sublist3r
- theHarvester
- google dorks
- Spiderfoot
- Spyse
- Metagoofil
- Nmap

- openVAS
- Many others

2. LITERATURE REVIEW

Shodan: It is online search engine for Internet of Things (IoT) that furnish massive amount of information about devices connected to Internet. This devices include workstation, phone, printer, computer, router, CCTV camera, switches etc.[1]. It continuously search for device, which are available publicly and attacked by malicious attacker with a purpose of IoT exploration, Network security monitoring. Shodan is based on SYN scanning and banner grabbing, which are behavior based technique [2] Shodan provide result by scanning the IP addresses, tries to identify which service is available on which port, header information, location.[3]

Censys: It is a search engine that allows user to scan device and network on the internet [5]. Censys keeps its database updated with information about devices which exposed on the internet. It is also 4 based on the SYN scanning banner grabbing technique. Recently, Censys scan the following protocol: HTTP, HTTPS, SMTP, POP3, and FTP. With the use of Censys possible to get details of devices that responded as well as technical details about their software, encryption algorithm, configuration, and certificate. Additionally, information present on Censys can be used to prevent large scale attack by informing the vulnerable devices about potential danger. [4].

Zoomeye: Zoomeye is search engine for IoT devices, which is alternative of Shodan and Censys. Zoomeye has two detection engine Xmap and Wmap targeting devices in cyber space. It uses a keyword based search criteria target on specific parameter like application, location, port number, host name, IP address. Set of APIs are also available for defining more complex queries. [6]

Thingful: It is search engine for IoT devices, which is basically centered on the geo-location. This tool collect data coming from connected devices and sensors which generate real time data. This tool provide data regarding air quality monitoring, flood monitoring, radiation measurements [7]. Thingful tool is based on propriety algorithm for the identification of data [8].

Nmap: Nmap is most popular Open Source Intelligence (OSINT) tool used by the network scanner. It is free and open source tool for network discovery and auditing. Nmap is used by attacker in reconnaissance phase to gather information on weakness within network [9]. Nmap's basic features include Host Discovery, Port Search, Service, OS Fingerprinting, and detection of basic vulnerabilities. Nmap scans large high-speed networks. [10].

Maltego: Maltego is powerful Open Source Intelligence (OSINT) tool. It is used by pen tester during reconnaissance phase. It automate the process of discovering network resource[11].Maltego can be used to discover DNS server associated with target, Email account associated with target, and social media information. It provide graph view of gathered information so it can easily use by penetration tester [1].

IVRE: Instrument de Veille sur les Reseaux Ext' erieurs (IVRE)' is an open-source network identification system also known as DRUNK (Dynamic Recon of Unknown Networks). [12].Its main goal is to reconnaissance network traffic, by gathering information through Internet-wide scanning and then investigating gathered information for the purpose of explore vulnerable resources and their activities[13].This tool is main used in digital forensic, Intrusion detection, information gathering and identify vulnerabilities on network. IVRE based on Nmap, Zmap, Masscan. [12]

PunkSpider: It is a vulnerability search engine for web application that allows user to identify numbers and types of vulnerability on website with internet quickly. Vulnerabilities identified by this tools are: Blind SQL Injection, Cross site scripting, Operating system Command injection. This tool take URL as search query[4].

OpenVAS: The Open Vulnerability Assessment System (OpenVAS) is a comprehensive and effective vulnerability scanning and vulnerability management solution platform for many resources and tools. [14]. Open Vulnerability Assessment System is a scanning tool for network 5 security purposes provided under GNU. Its main capability include full network scanning, web server scanning [15]

SpiderFoot: It is another reconnaissance tool that automatically goes through lots of publicly available data source to compile information. Input for this tool are IP address, subnet, domain name, email address, host name. The result of this tool is represented by Graph of node with all entities and relationship. This tool is used to initiate penetration tests to detect data breaches and vulnerabilities, support threat intelligence [16]

theHarvester: This tool is used for collecting public information related to domain or company through search engine. It is efficient for supplying information such as company emails and host names, subdomains, and IP addresses. It also provides a user-friendly view of the findings in HTML or XML. In the reconnaissance stage, this resource is used [17].

Table. 1 Comparison Table for OSINT Tools

Tool	Main feature	Interface	Open Source	Limitation
Shodan	Search engine for IoT devices, vulnerability assessment tool, port scanning	GUI,API	No	Code and implementation details are not available, not open source, search engine can be misused by attacker, complex to understand
Censys	Search engine for IoT, discover vulnerability, filtering	Web	Partial	Require account creation after some interaction with search engine, does not support IPv6
Zoomeye	Search engine for IOT, find data related to network(IP, service, host)	Web	Yes	Require specific word to search, manual search
Thingful	Gather large scale data, provide geographical index of data	Web	Partial	Not open source, fast expiration of data due to dynamic nature of IoT devices
Nmap	Port scanning, Host discovery, basic vulnerability, OS fingerprinting	Command line	Yes	Hard to master, only basic vulnerability provide
Maltego	OSINT tool for reconnaissance	Web	NO	Complex
IVRE	Network scanning, graph view of output ,reconnaissance tool	Command line and web	Yes	Installation is time consuming, mostly has external decencies
PunkSpider	Search engine for vulnerability on web application	Web	No	Manually input, does not fit to IoT
OpenVAS	Network scanning OSINT tool, Vulnerability scanning	Command line	Yes	Cover few CVEs ,does not offer policy management
SpiderFoot	Multi target scanning, OSINT tool	Command line, GUI	Yes	Gathered information may be misuse
theHarvester	Gather information like email, subdomain, IP address, URLs	Command line	Yes	Gathered information may be misuse

3. CONCLUSION

In recent times, the Internet of Things (IoT) is the most prominent, and the security of these IoT devices is a difficult task for security analysts. In this respect, OSINT (Open Source Intelligence) is used to collect information about an Internet-connected computer. From the comparison table, it was analyzed that the current tool has some drawbacks, such as non-open source, complex layout, time-consuming installation, accessible paid version, IPv4 support only, etc. There is therefore a great need to create an open source, user-friendly, command-line interface that is freely used to minimize the restriction of an existing IoT method. This can be achieve by combining more tools to get more accurate and powerful result. In this research, Combine Shodan tool with nmap, virus Total and many more provide more detailed information about targeted IoT device like IP addresses, List of Ports, Geographical information, latitude, longitude, malware analysis, list of exploitable vulnerabilities.

REFERENCES

[1] Brett, Mark & Parker, Jamie. (2019). A Guide To The Top Ten Open Source Tools For Network Defense And Improved Security. 10.6084/m9.figshare.9963722.

[2] S. Lee, S. H. Shin, and B. h. Roh. 2017. Abnormal Behavior-Based Detection of Shodan and Censys-Like Scanning. In 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN). 1048–1052. DOI:http://dx.doi.org/10.1109/ICUFN.2017.7993960

[3] John Matherly. Shodan Official Website. https://www.shodan.io/

[4] A review of network vulnerabilities scanning tools: types, capabilities and functioning. ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security August 2018 Article No.: 65 Pages 1–10https://doi.org/10.1145/3230833.3233287

[5] Censys, Available: https://www.censys.io/

[6] "Zoomeye," https://zoomeye.org/, 2019

[7] Thingful Official Website. http://umbrellium.co.uk/initiatives/thingful/,https://www.thingful.net/

[8] E. Aceves and V. M. Larios. 2015. White paper: Data Visualization for Georeferenced IoT Open Data Flows for a GDL Smart City Pilot. https://smartcities.ieee.org/images/tles/pdf/davgdl iotvisualinterface.pdf

[9] NMAP Official Page: https://nmap.org/

[10] Inside Nmap, the world's most famous port scanner. https://pentest-tools.com/blog/nmapport-scanner/

[11] Open source intelligence tools for pen testing. https://www.adminmagazine.com/Archive/2018/45/Open-source-intelligence-tools-for-pen-testing/(offset)/3

[12] Pierre Lalet, Florent Monjalet, and Camille Mougey. IVRE, a network recon framework. https://ivre.rocks/

[13] Linux Security Expert. IVRE tool review. https://linuxsecurity.expert/tools/ivre/

[14] https://www.showappslike.com/shodan/#

[15] W. Qianqian and L. Xiangjun. 2014. Research and design on Web application vulnerability scanning service. In 2014 IEEE 5th International Conference on Software Engineering and Service Science. 671–674.

[16] J. Pastor-Galindo, P. Nespoli, F. Gómez Mármol and G. Martínez Pérez, "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends," in IEEE Access, vol. 8, pp. 10282-10304, 2020, doi: 10.1109/ACCESS.2020.2965257.

[17] https://github.com/laramies/theharvester

[18] Yu, Miao & Zhuge, Jianwei & Cao, Ming & Shi, Zhiwei & Jiang, Lin. (2020). A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices. Future Internet. 12. 27. 10.3390/fi12020027.