https://doi.org/10.46335/IJIES.2024.9.7.2 **e-ISSN: 2456-3463**
Vol. 9, No. 7, 2024, PP. 5 -9

International Journal of Innovations in Engineering and Science, www.ijies.net

OCTAVESTER TOOL: Traversing Reconnaissance Utilities

Vishal Injewar[1], Rohan Misalwar[2], Sarthak Manalwar [3], Shantanu Jangale [4], Komal Jaisinghani[5]

[1,2,3,4] Student, [5]Assistant Professor, Department of Computer Engineering, SVPCET, Nagpur

kjaisinghani@stvincentngp.edu.in

***Received on**: 5 May,2024* ***Revised on**: 29 June,2024* ***Published on**: 02 July ,2024*

Abstract -*The primary objective of this paper is to enhance security measures within the industry. It aims to study trends and issues in cyber security and analyze cyber security tooling. Primarily it is the evolving security threats over the globe that have directly or indirectly affected the fortunes as well as the masses. Octavester tool is a Linux-based tool that is CLI as well as GUI-based which is used to overcome a major and primary parameter of security staging i.e. Reconnaissance (gathering information). A comparative study of the pre-research and post-research period with implementation concluded the best hacking features and information on different parameters standardized according to research and analysis, the previous model developed named 'Crawler' was the platform used for features such as packet sniffing and professional security activities and finally the tool best for naïve users as well as security engineers based on the diversified analysis.*

***Keywords: CLI, Crawler,* GUI, Octavester, Reconnaissance.**

Introduction

With the addition of AI to the world, certainly, many things have shifted their focus from being the best to being very anonymous, everything has its assets and liabilities and so with the technology, the engrossing things within cybersecurity have always been concerning. The fact that many people don't know about is the technology they are using has certainly helped their survival but they are unaware that there is always a side that has stayed anonymous to them [1]. The recent trends and analysis from numerous giants as cited in their threat reports have utterly pronounced the types, trends, and strategies crackers have initiated to make things worse for the fortunes to secure their data which directly or indirectly have affected every person. So the information they are regulating is being secured by a particular mechanism or the other which is eventually controlled by the sustainable corporations. Security attacks on these sizable organizations have put our privileged data at risk which can be remarked as a compromise in the security that has paved the way concerning dark-net markets and operations not known by the individuals. The Octavester tool deals with both active & passive reconnaissance techniques which are subjected to the initial phase of hacking followed by scanning, gaining access, maintaining access, and clearing the tracks. To facilitate this, cyber security and ethical hacking methodologies have always been an attachable domain for the industry which has significantly commenced and standardized Linux-based tooling [2]. Particularly the tools have made working easier for professionals as well as for folks, it has simplified the procedures such as classifying, encapsulating, encoding, adapting, and inclusive report generation in a simultaneous processing mode hence the emphasis of this paper is on the concrete role of network security and importance of Open-source intelligence [8].

https://doi.org/10.46335/IJIES.2024.9.7.2 **e-ISSN: 2456-3463**
Vol. 9, No. 7, 2024, PP. 5 -9

International Journal of Innovations in Engineering and Science, www.ijies.net

Literature review

Previous works done in the field

The correspondence between technology congregation and firm performance can be discovered in the work of David Kennedy, Inc. TrustedSec (2020); their study showed an SE toolkit which is open source penetration testing framework designed for social engineering that has various custom attack vectors that permit you to make credible and feasible attack quickly[1]. Further, the study of LionSec (2016) Xerosploit is a penetration testing toolkit whose end in view is to simulate man-in-the- middle attacks for testing purposes. It brings various modules that allow to simulate well-regulated attacks and also enables to carry out Denial of Service attacks and port scanning [6]. Ryan Fedasiuk (2022), an analyst at the Center for Security and Emerging Technology [17], listed six tools that can be used to utilize operational security and guide toward internet safety. These include VPNs, URL and file scanners, antivirus software, IP trackers, and domain enumeration studies [14]. Further study of IP tracking from a research paper authentic IP and network tracking measurement study of hostile websites with HAZOP (2017) IP tracking focused on manipulating the real-time networks and bouncing of network locations.[4]

Study Variables

Data and variables

The research and implementation period stretches over 16 months 2022-2024, which is graded as the research and implementation period. Research phase includes the study of research papers, threats, attack vectors, and technologies required to develop a tool periodically. Kali Linux operating system is a base for implementations and study which is an open-source platform where an individual can study and implement representations and scripting according to their requisite.

Methodology and model specifications

The primary objective of this section is to showcase the working procedure of the Octavester tool and a brief introduction to the tool used for different attacks and security. This study used the front end to ease the interaction for netizens as well as for professionals forwarded to the fact that security professionals can alter the methods and study in Linux. Initially, the tools are deactivated in Kali Linux, and you can activate them as needed and reveal all the connected networks nearby. By default, the functionalities are turned off through commands; you can enable them and proceed accordingly. The methodology of a tool depends on four phases:

- Planning
- Discovery
- Implementation
- Reporting

Scanning and initializing are involved to gain information to the greatest extent possible

Sr. No.	Developer	Development	Proposed Tool Study	Implementations
1	Biswajeet Ray, Security Engineer (Defenzelite)	Developed an OSINT Tool “Brahmastra OS”	To use this user will need to install or create a different virtual machine. [15]	The idea is to develop a tool that will run on Linux OS without creating any additional machines.
2	LionSec, Cyber Security Researcher known as King J. T. (presented the research on MITM attacks)	Developed Xerosploit tool which is functional and carries out various simulations	Xerosploit tool is majorly focused on security engineers and it is a MITM tool. [11]	Reconnaissance tool functionalities and Octavester tool is majorly based on information gathering which is always the first stage of penetration testing. [11]
3	David Kennedy, known as ReL1K	The open-source Social Engineering Toolkit framework conducts a range of simulations for SE attacks.[7]	SET is a publicly accessible software utility developed specifically for conducting social engineering assessments and penetration testing activities.[7]	Social engineering tools manipulate human behavior, leveraging psychological tactics to illicitly access systems, data, or sensitive information for malicious purposes.[7]

https://doi.org/10.46335/IJIES.2024.9.7.2 e-ISSN: 2456-3463
Vol. 9, No. 7, 2024, PP. 5 -9

including fetching and scrutinizing critical details concerning the tools and their underlying infrastructure. The tool will provide the specific functions and functionalities on the Linux system, for the execution. Initially, the tool needs to be downloaded by using this command
$ git clone https://github.com/vinjewar23/Ocatvester.git

Octavester is built using Python, featuring a command line interface (CLI) for user interaction. At the first instance, users will be presented with a menu displaying the various functions and options available. Users will input the corresponding option number to proceed with a specific action. The tool encompasses eight options, all of which are designed to execute ethical methodologies aimed at retrieving information from open-source platforms.
The tool will offer eight different features:

1. **Sub-domain enumeration**
   • Enumeration of the websites using the wordlist and request library.
2. **IP Geolocation grabbing**
   • Grabbing geolocation of IP address using free API.
3. **Contact number information enumeration**
   • Gather information on mobile numbers using internet archives.
4. **Location Grabber**
   • A link reveals the location with the specifics by studying latitude and longitude.
5. **Encryption & Decryption**
   • Encrypt and decrypt the message for the sender and the receiver.
6. **Email information**
   • To find if the emails have been previously pwned or not.
7. **IP Scanner**
   • Scans the IP for malicious forwarding and tracking.
8. **DNS Lookup**
   • This test will display DNS records for a domain sorted by priority.
   • It is conducted directly against the authoritative name server of the domain, ensuring immediate visibility of DNS record changes.

The central interface for the Ocatvester tool is exhibited in the figure after the installation and execution of the associated commands. For a more extensive understanding to illustrate profoundly, we will go with Location Grabber as an example.
Step 1: Begin by installing the tool.
Step 2: Install the tool's dependencies by executing pip install -r requirements.txt
Step 3: Run the tool using the command python main.py.
Step 4: Select the option within the tool for the location grabber functionality.
Step 5: Choose a suitable template from the available options.

Step 6: Input the required information as prompted by the selected template.
Step 7: The tool will start a server listening on port 8080.
Step 8: Share the generated link with the intended target.
Step 9: Upon the target clicking the link, their device information and precise location coordinates will be retrieved and displayed.
Step 10: Exit the tool – exit.

The fundamental operational sequence of Octavester is outlined in the Figure below this schematic maps out the comprehensive process by which the Octavester tool operates.
If we focus on the most important cyber reconnaissance technique and depict their expansion and evolution. We establish the subsequent classification consisting of four distinct categories.

Social Engineering: In essence, it is the system and practice of working that is done to delude the victim by exploiting their trust and persuading them to share privileged information or to perform activities that can be functional to an attacker.

Open-source Intelligence: Internet intelligence acts as both the offensive and defensive section for OSINT it is esoteric and unique to the information available on the Internet for the netizens. For example- shodan, and Google Dorking.

Network Information Gathering: When data availability is inadequate, the attacker must directly interact with the victim's framework. This allows for the delineation of a remote network or identification of the systems in use. Among the preferred tools for such tasks are tcpdump and Wireshark.

Side Channels: It usually defines the attack to draw responsive information from computing devices. For illustration, it has been demonstrated that information or signals leak from the display monitors and input devices can be used to recover login capabilities based on that reasoning it is important to carefully value and process the obtained information or data.

Functionality and Results

https://doi.org/10.46335/IJIES.2024.9.7.2 e-ISSN: 2456-3463
Vol. 9, No. 7, 2024, PP. 5 -9

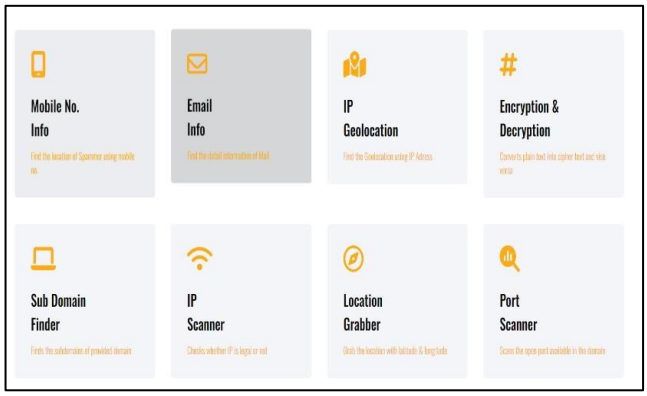


Fig 3. Depicts GUI hom

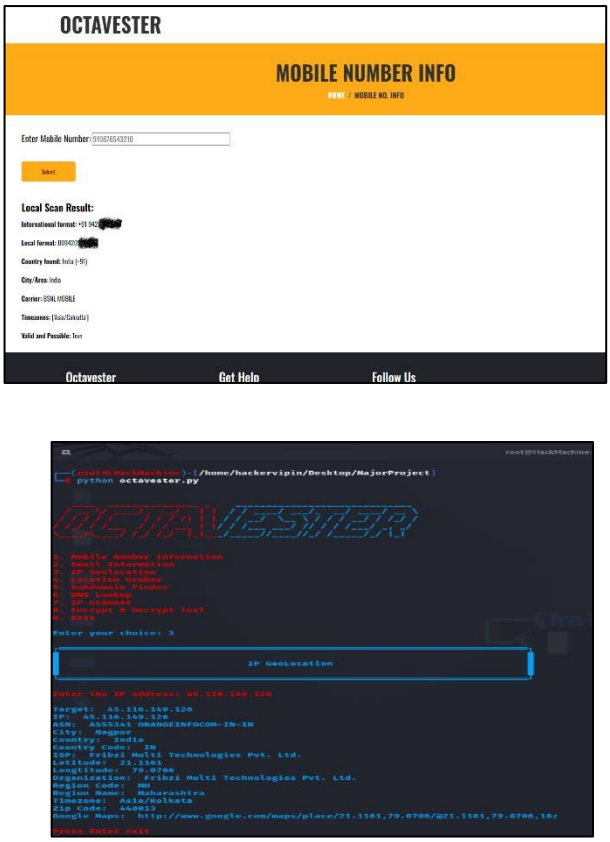


Fig 4. Contact Number information

Findings

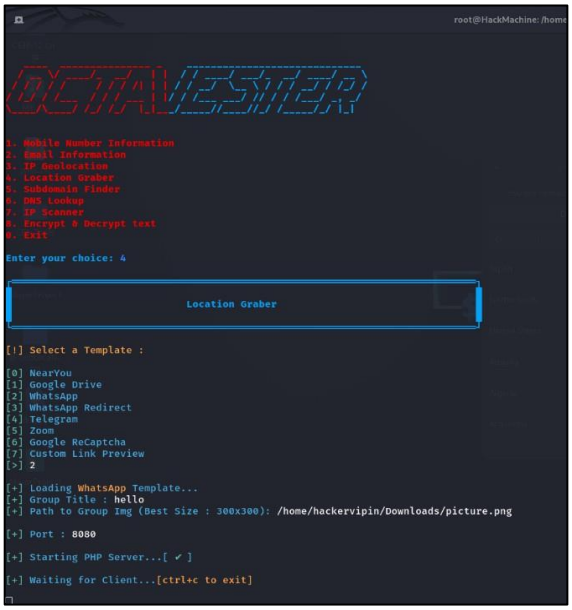
The Tool offers diverse functionalities aiding cybersecurity professionals in detecting and mitigating possible security risks. Email information is structured and offers insights into suspicious emails, blacklisted email sources, and malicious behavior. IP geolocation furnishes fundamental details about the country, region, city, ISP, ASN, and the physical location of active public IPv4 addresses. A location grabber sends out harmful links that reveal the target's device information and geographical location.

A subdomain locator hunts for existing subdomains, DNS lookup retrieves DNS records, while an IP scanner examines and lists open ports and services utilizing the Nmap library tool.

These findings outline the capabilities of a Cybersecurity tool. It emphasizes the various features of the tool such as email organization for detecting suspicious activities, IP geolocation for identifying the origin of IP addresses, and tools like subdomain finder,

DNS lookup, and IP scanner for comprehensive network analysis and security assessment. The tool's functionalities are designed to assist cybersecurity

.



CONCLUSION

This paper has enthralled the reconnaissance aspect which is the cornerstone for the entireness of cybersecurity attacks and pen testing methodologies. Swing adaptation and transformation in electronic devices boosted the volume of data that can be convened by the cracker and has also increased the scale of communication channels to execute the potential threat. Constructive changes in technology demand dedicated countermeasures which are as important as their advantages and precedence.

Social engineering attacks represent one of the most insidious and potentially disastrous threats in the realm of cybersecurity. What sets these attacks apart is their exploitation of human psychology and behavior rather than

technical vulnerabilities. Many people are not adequately informed about the various forms that social engineering can take, whether it's phishing emails, pretexting phone calls, or impersonation scams on social media. Consequently, they are more susceptible to falling victim to these deceptive tactics, often without realizing the potential consequences until it's too late. In consideration, the web cybersecurity Octavester tool we have developed offers a solution to tackle the challenges presented by cyber threats in the digital landscape.

According to the researchers, 95.2% of the tools enable users to collect information through the command line interface. Having evaluated it, we are equipped with a range of reconnaissance functionalities available via Command Line Interface (CLI) and Graphical User Interface (GUI), the tool enables users to detect and address potential risks existing throughout the internet. Through the utilization of advanced technologies, the Octavester

.

tool enables users to access verified information from open-source internet platforms, thereby aiding in the prevention of further exploitation. Its user-friendly design, featuring a GUI version, ensures accessibility for users of all technical proficiencies, including those less familiar with technology.

Real-world testing has demonstrated the tool's performance, providing users with accurate details to make informed decisions regarding cybersecurity. Moreover, its beginner-friendly interface makes it accessible to a wider audience, including individuals with limited technological understanding.

Open-source tools are to be amended. Based on the results of Octavester scans, more advanced research should focus on developing a superlative set of methodologies to detect reconnaissance activities, which increases the percentage of endpoint security while minimizing the ratio of false positives.

References

1. W. Mazurczyk and L. Caviglione. 2021. Cyber Reconnaissance Techniques. Article in Communications of the ACM DOI: 10.1145/3418293.

2. D.R. Ingle, and A. Mate. 2022. Cybersecurity Tools and Methods. International Conference Proceedings IJCRT ISSN: 2320-2882.

3. V. Santhi, Dr K. Raja Kumar and B.L.V. Vinay Kumar. 2016. Penetration Testing using Linux Tools: Attacks and Defense Strategies. International Journal of Engineering Research & Technology ISSN: 2278-0181 Vol. 5 Issue 12.

4. M. Mansoori, I. Welch, K Raymond Choo and R. Maxion. 2017. Real-world IP and network tracking measurement study of malicious websites with HAZOP. International Journal of Computers and Applications. DOI: 10.1080/1206212X.2017.1283910

5. S. Matthew, S. Xiaoyu, K. Mingqing, W. Zuo, Li, Xiangyang, Dahbura, and Anton. (2024). Using a Computational Cognitive Model to Understand Phishing Classification Decisions of Email Users. Interacting with Computers. 10.1093/iwc/iwad054.

6. A. Mohammed. 2024. The Threats of DDoS and Social Engineering Attacks. 10.13140/RG.2.2.34130.32965.

7. Abbas, Asad. 2024. Social Engineering Attacks: Techniques, Impacts, and Mitigation Strategies. Article on ResearchGate. https://www.researchgate.net/publication/377382644_Social_Engineering_Attacks_Techniques_Impacts_and_Mitigation_Strategies.

8. Jeba, J & S., Rubin Bose, Köse, Utku, Rajan, Regin, Rajest, and Suman. 2023. In-Depth Analysis and Implementation of Advanced Information Gathering Tools for Cybersecurity Enhancement. 1. 130-146.

9. Y. Oles, Kharchenko, Vyacheslav, Pevnev, and Vladimir. 2023. Scanning of Web-Applications: Algorithms and Software for Search of Vulnerabilities "Code Injection" and "Insecure Design". 1005- 1010. 10.1109/IDAACS58523.2023.10348918

10. A. Halil & C. Ozkan. 2023. CYBER THREAT INTELLIGENCE SYSTEMS AND APPLICATIONS. https://www.researchgate.net/publication/377074580_CYBER_THREAT_INTELLIGENCE_SYSTEMS_AND_APPLICATIONS

11. K. Keshav, S. Vanshika & M. Prabhu. 2023. A Novel Approach for an Automated Advanced MITM Attack on IoT Networks. 10.1007/978-3- 031-23724-9_6.

12. Vishnu, V. & K. Praveen. 2022. Identifying Key Strategies for Reconnaissance in Cybersecurity. 10.1007/978-981-16-8012-0_3.

13. S. Jangale, R. Wagh, A. Babhulkar, O. Vispute, and A. Dadhe. 2022. Digital Forensics – Elevating Cyberspace. International Journal for Research Publication and Seminar NCASIT 2022 Conference proceedings ISSN: 2278-6848.

14. Kumaravel Archana. 2023. MONITORING OF NETWORK TRAFFIC DOWNTIME USING IP SCANNER VIA PROGRAMMABLE ROUTER. 16. 49-59. 10.37896/jxu16.11/008.

15. C. S. Fikiri, E. Stanley, O. Fadekemi, and I. Banwo. 2023. The Trends of Cybersecurity and Its Emerging Challenges in Africa. 10.1007/978-981-99-3057-9_4.