Proceedings of the Second International Conference on Edge Computing and Applications (ICECAA 2023)
IEEE Xplore Part Number: CFP23BV8-ART; ISBN: 979-8-3503-4757-9

Cybercheck – OSINT & Web Vulnerability Scanner

Shamunesh P[1], Vinoth S[2], L N B Srinivas[3*]
[1,2,3] Department of Networking and Communications
Faculty of Engineering and Technology
SRM Institute of Science and Technology, Kattankulathur
Tamilnadu-603203, India
[1]sp8274@srmist.edu.in, [2]vs8255@srmist.edu.in, [3*]srinival@srmist.edu.in

*Corresponding author: L N B Srinivas *email ID: srinival@srmist.edu.in

2023 2nd International Conference on Edge Computing and Applications (ICECAA) | 979-8-3503-4757-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICECAA58104.2023.10212207

***Abstract*— The objectives of "CyberCheck" are drafted very precisely to solve 2 important modules of the Penetration Testing Workflows. Open-Source Intelligence (OSINT) and Web Vulnerability Scanning are the most crucial practices fora penetration tester to keep track of their target andnot to leave any of their digital footprints in the process of scanning their endpoints. Often, a pen-tester must bedependent on a 3rd party service provider, those who provide all open-source tools to check on. But this stage is not always beneficial for a pen-tester to have a fully transparent scanning on their target. The idea is to develop an Open-Source user-customizable OSINT and Web Vulnerability scanner in Python environment scripts that are very transparent on the algorithm for performing OSINT search or Web Vulnerability scanning. This feature is a nightmare for any pen-tester to test or track on their target endpoints using open-source that is highly transparent in scanning ports and functions that they trust on. This also adds the pen-tester to work ethically by customizing the type and parameter he wants to scan instead of going unethical in an online 3rd party service provider.**

***Keywords*— OSINT (Open-Source Intelligence), Web Vulnerability, Penetration Testing, Vulnerability Assessment, Enumeration, Clickjacking**

I. INTRODUCTION

Cybersecurity has become the most important and demanded task for any data driven application. There has been a huge uprise in penetration testers and tools supporting it [1]. All these open-source service providers are beneficial, but there is a drawback on their transparency. The service providers themselves turns out to be unethical platform for the targets. The tools for open-source intelligence related activities, and web vulnerability scanning as a user-customizable platformgives a pen-tester enormous activities perform and to trust its process without any harm of their targets.

One important result that we took as a reference for adding up features into our work are the recent survey done in hacker one and bug crowd community platforms about the tools and scanner platforms used by pen-tester and its transparency. There was a high need of having an open-source customizable OSINT and web vulnerabilities scanner so that the pen-testers can work on their stages oftesting without worrying about the footprints and the type of parameters that may run in the backend for 3rd party service providers.

Whereas, here they have full control over what they wish to do so. A proper fieldwork has been taken before framing up a solution for a customizable web vulnerability scanner because it can be misused by the pen-tester upon unethical activities. But the action of adding unethical scripts into the python environment will be a bad result for the pen-tester itself, because of the highly transparent Open-source plugins we have added along with the package installation setup.

A. OSINT

Open-Source Intelligence (OSINT) is considered as a very crucial practice for a penetration tester to gather as such information possible about the target from the resources that are available online without any private access needed. OSINT scanners identify and target relevant data sources based on the specific requirements of the user. These sources can include websites, social media platforms, public databases, government records, online forums, blogs, and more.

The practices in OSINT include, getting the online presence of the target, social media activity and log monitoring, contacts mentioned anywhere, links and connection of networks, recently accomplished work, involved in any social activities via medias or publications [2].

B. Web Vulnerability

This practice mostly deals with the stage 2 in penetration testing phase, here the pen tester goes with some default methods of vulnerability scanning after the enough of OSINT.

Vulnerability is nothing but a loophole on a system or architecture, that allows a person to penetrate and give access to perform some unwanted activities that they are restricted to perform. Practices involved in web vulnerability scanning are clickjacking, host header injection, subdomain enumeration and reverse IP [3].

C. Penetration Testing

Penetration Testing is a crucial practice followed by Security Analyst to test the level of penetration they can perform from the identified loophole or vulnerability. Some tools for performing penetration testing are Burp Suite, Nmap, Shodan etc. [4]

D. Vulnerability Assessment

Vulnerability Assessment is a scanning process and comes on the second phase of penetration testing. The process of identifying the loophole on a system. There are a lot of vulnerability assessment tools available to scan the application and report the areas that holds bug.The OSINT practices are also the first stage in vulnerability assessment, most often the scanning is taken based on the OWASP TOP 10 results [5].

TABLE I. Comparisons of few 3rd party service providers and its transparency

TOOLS	FEATURE	INTERFACE	OPEN SOURCE	LIMITATIONS
Shodan	IoT device search engine, vulnerability scanner, and port scanning [6]	GUI, API	No	Code and implementation details are not available, not open source, search engine can be misused by attacker,complex to understand
Censys	IoT search engine with vulnerability detection and filtering	Web	Partial	Require account creation after someinteraction with search engine, does not support IPv6
Nmap	OS fingerprinting, port scanning, host detection, and fundamental vulnerabilities	Command line	Yes	Hard to master, onlybasic vulnerability provides
Maltego	OSINT tool for reconnaissance [7]	Web	No	Complex

II. ALGORITHM USED

The use of an algorithm-based implementation comesonly on the web scrapping modules of our work. Algorithm used for Subdomain Enumeration: An enumeration algorithm is an algorithm that enumerates the answers to a computational problem [9] The goal of an enumeration algorithm is to generate and list all the possible arrangements or subsets of a given set. This algorithm generates all possible subsets of a set of objects. It starts with an empty subset and systematically adds elements to generate different subsets. This can be useful for solving problems that involve searching through a large solution space or finding all possible solutions. [8]. Formally, such an algorithm applies to problems that take an input and produce a list of solutions, similarlyto function problems. Fig 1 mentioned below is the flowchart of the enumeration algorithm.

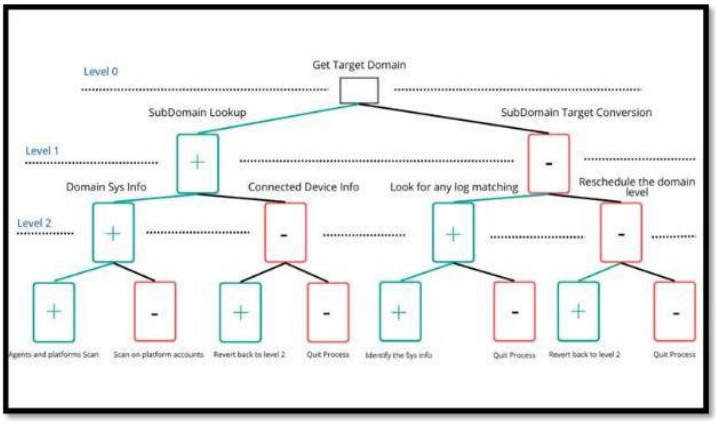

Fig. 1. Flowchart of Enumeration Algorithm

III. IMPLEMENTATION

A. Architecture

The Architecture diagram gives a clear-cut idea of how the workflow is structured and the modules are linked one other and works seamless. The Fig 2 gives a better understanding of our architecture.

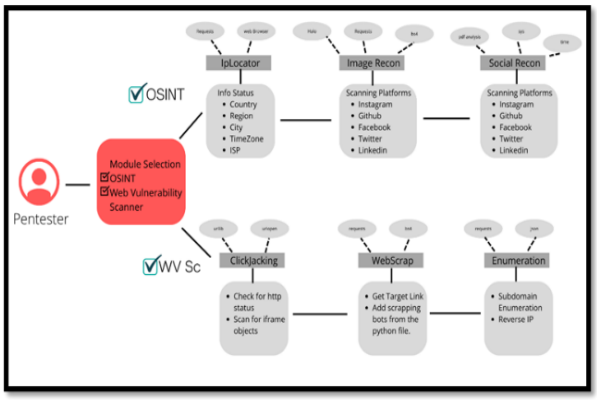

Fig. 2. Architecture

Diagram

B. Use Case Diagram:

The UML (Unified Modeling Language), Use case diagram gives the proper idea of how the user will interact with the modules. Use case diagram is veryessential if there are multiple properties involved inan application. Fig 3 gives the use case diagram of this work.

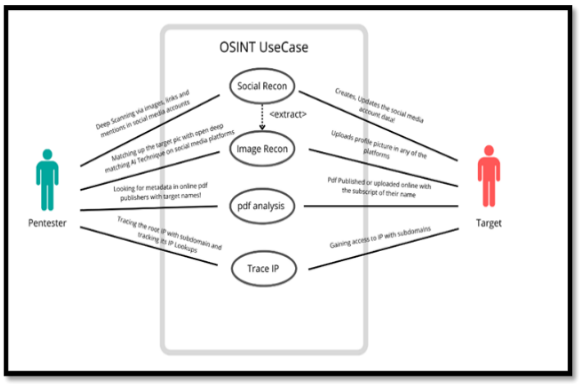

Fig. 3. Use Case Diagram

C. Envy / Packages:

Here, discussed all the dependencies involved and the kind of scanning parameters that are provided in the OSINT and web vulnerability options of the checklist. The working model's entire environment was scripted in python, because of the inbuilt scanning and browser-dependent packages python provides as open-source for pen-testing.

Python is a powerful tool and a scripting language to build and inherit the features and modules of ethical hacking or in general cybersecurity. And python is also the most widely used automation script used by cybersecurity professionals [10]. The Packages and its file structure of the work ismentioned in fig 4.

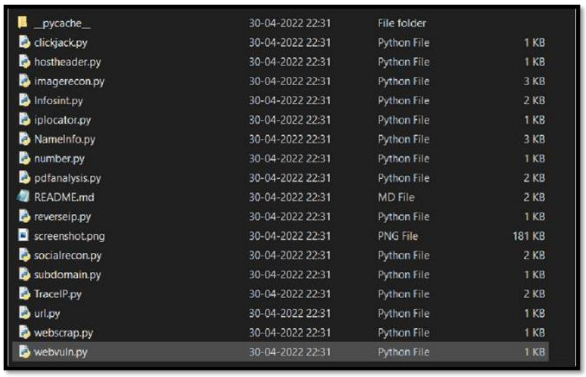

Fig. 4. File Structure

D. Working

The OSINT features and parameters for scanning we have added into the working model are fully open-source andfollow all the rules to be carried to ping an OSINT scan [11]. The python libraries import their dependencies and validate the user inputs with the browser web scrapping tools and platforms for OSINT. The Infosint.py file holds all root dependencies andthe main function calls to perform activities based on users' wishes. The imagerecon.py is the file to practice an open OSINT of social accounts based on the image loadedby the user.

Ip locator and traceip.py are filed to fetch some data about the IP input and relative registers held bythe IP. The pdfanalysis.py is the most important OSINTparameter file that gets metadata and relative information of the input keyword and opendocumentation available [12].

Files for the Web Vulnerability Scan

Clickjacking is a common web vulnerability performed by hackers to steal sensitive or unwanted harmful actions from the target. This file scans the domain site and checks for any trace of clickjacking.

The webvuln.py is the main header file for web vulnerability scanning that performs a clean overalldraft of a handful of scans [13].

IV. END RESULT

The OSINT tools and features added, work fine and depend only on the open-source resources, and the web vulnerabilities scanning are effective with different test cases tested.

A. WV Scan (Clickjacking):

4 important components were added in WV scanning, and expected results were obtained in scanning for clickjacking vulnerability. Figures 5 & 6 show that the target is logged on and not logged on to a 3rd party service respectively.

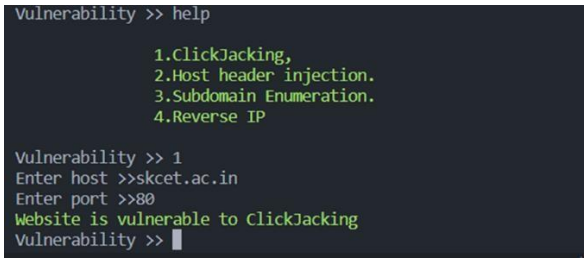

Fig. 5. Clickjacking Result (NOT OK)

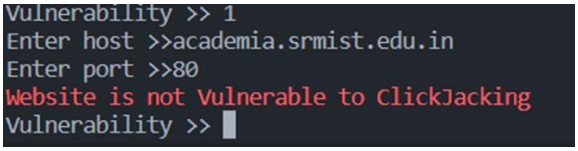

Fig. 6. Clickjacking Result (OK)

B. OSINT (IP Locator feature):

The IP location track is the task to be performed in the OSINT methods, the practice was compiled successfully, and the results obtained are shown in Fig. 7 & Fig. 8.

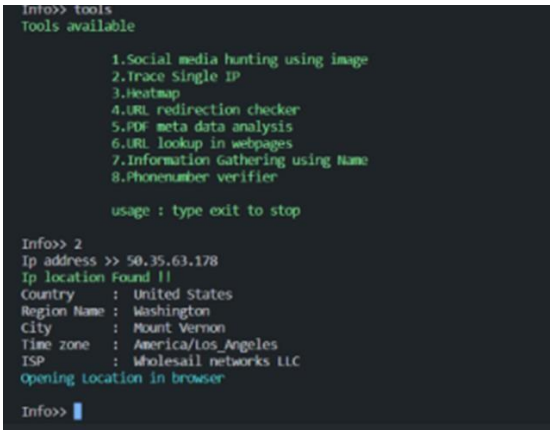

Fig. 7. IP Location Tracker

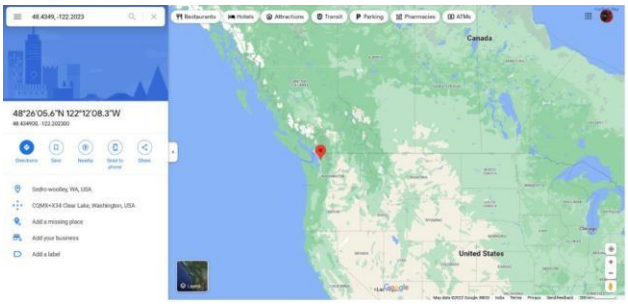

Fig. 8. IP Location Tracker via Google Maps

C. OSINT (PDF Metadata Analysis):

The PDF Metadata analysis was implemented, and the expected result obtained is shown in Fig. 9. This tool gets the hidden sensitive meta data of the PDF file.

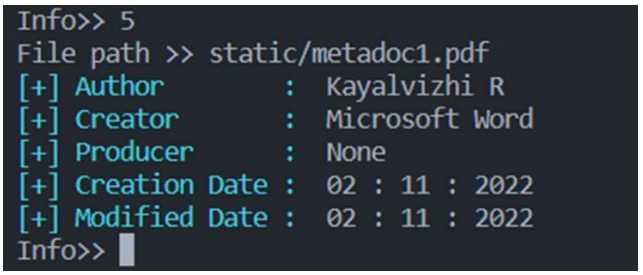

Fig. 9. PDF Metadata Analysis

E. OSINT (URL Redirection Check):

The URL Redirection check scanner was implemented successfully as shown in Fig 10. The scanner checks for any URL redirection on the 301 status.

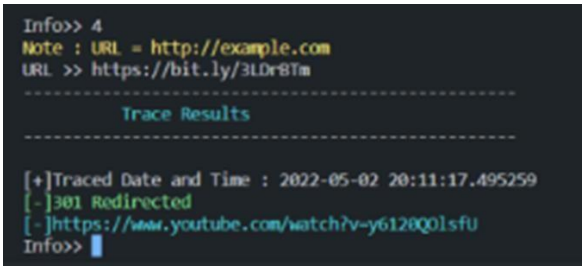

Fig. 10. URL Redirection Check

V. CONCLUSION

The OSINT tools and features added, work fine and depend only on the open-source resources and the web vulnerabilities scanning are effective with different test cases tested. OSINT scanners will likely incorporate advanced data analysis techniques, such as network analysis, link analysis, and data visualization, to provide deeper insights into collected information. These techniques can help uncover hidden connections, patterns, and trends that may not be immediately apparent.

The scope of the research is thus analyzed, and the parameters have been drafted successfully. Therefore, the objectives mentioned above have been successfully implemented and the resultsare verified and as expected. Therefore, the scope of the research are drafted as, Social media hunting using image, trace Single IP, heat map, URL redirection checker, PDF metadata analysis, URL lookups, information gathering using the name and phone number verifications.

VI. REFERENCES

[1] Clive Best, OSINT, the Internet and Privacy https://www.computer.org/csdl/proceedings-article/eisic/2012/4782a004/12OmNCbU37A

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

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

[4] Ivo Vacas, Ibéria Medeiros, Nuno Neves - Detecting Network Threats using OSINT Knowledge-Based IDS https://www.computer.org/csdl/proceedings-article/edcc/2018/806000a128/17D45VTRoD6

[5] 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 1–10 https://doi.org/10.1145/3230833.3233287

[6] Shodan Search Engine: https://www.shodan.io/

[7] Thingful Official Website. https://umbrellium.co.uk/projects/thingful/

[8] E. Aceves and V. M. Larios. 2015. Data Visualization for Georeferenced IoT Open Data Flows for a GDL Smart City Pilot. IEEE-GDL CCD smart cities white paper (2012): 1-5.

[9] 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

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

[11] A review of network vulnerabilities scanning tools: types, capabilities and functioning. ARES 2018: Proceedings of the13th International Conference on Availability, Reliability and Security August 2018 Article No.: 65 Pages 1– 10
https://doi.org/10.1145/3230833.3233287

[12] Rajamäki, Jyri; Sarlio-Siintola, Sari; Simola, Jussi. European Conference on Cyber Warfare and Security. Jun 2018, The Ethics of Open Source Intelligence Applied by Maritime law Enforcement Authorities https://usnwc.libguides.com/c.php?g=494120&p=3420732#:~:text=The%20Ethics%20of%20Open%20Source%20Intelligence%20Applied%20by%20Maritime%20law%20Enforcement%20Authorities

[13] Brett, Mark & Parker, Jamie. (2019). A Guide To The Top Ten Open Source Tools For Network Defense And Improved Security. https://www.researchgate.net/publication/336391115_A_Guide_To_The_Top_Ten_Open_Source_Tools_For_Network_Defense_And_Improved_Security.

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

[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. https://www.researchgate.net/publication/286672358_Research_and_design_on_Web_application_vulnerability_scanning_service