OpenVuln Scanner

OSINT Tool and Security Framework

A PROJECT REPORT

Submitted by

SHARAT N (19BCS086)

VISHAL S (19BCS103)

RAJHESHWAR V (19BCS105)

in partial fulfilment for the award of the degree

of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

KUMARAGURU COLLEGE OF TECHNOLOGY

COIMBATORE 641049

(An Autonomous Institution Affiliated to Anna University, Chennai)

MAY 2023

KUMARAGURU COLLEGE OF TECHNOLOGY

COIMBATORE 641049

(An Autonomous Institution Affiliated to Anna University, Chennai)

BONAFIDE CERTIFICATE

Certified that this project report “**OpenVuln Scanner”** is the bonafide work of **“RAJHESHWAR V (19BCS105), SHARAT N (19BCS086), and VISHAL S (19BCS103)”** who carried out the project work under my Supervision.

SIGNATURE	**SIGNATURE**
Dr P. Devaki	Ms N. Suganthi,
HEAD OF THE DEPARTMENT	**PROJECT GUIDE**
Professor and Head	Professor
Computer Science and Engineering	Computer Science and Engineering
Kumaraguru College of Technology	Kumaraguru College of Technology
Coimbatore-641049	Coimbatore- 641049

The candidate with University Register Numbers **19BCS086, 19BCS103** and **19BCS105** were examined by us in Project Viva-Voce examination held on

________________________	________________________
INTERNAL EXAMINER	**EXTERNAL EXAMINER**
Name :	**Name :**
Designation:	**Designation:**

ACKNOWLEDGEMENT

We express our profound gratitude to our Founder **Padmabhushan Arutselvar Late Dr. N. Mahalingam B.S.c., F.I.E.,** Chairman **Dr. B. K. Krishnaraj Vanavarayar B.Com., B.I.,** Correspondent **Mr. M. Balasubramaniam M.Com., M.B.A.,** and Joint Correspondent **Mr. K. Shankar Vanavarayar M.B.A., PGDIEM.,** for giving a great opportunity to pursue this course.

We extend our gratefulness to our Principal **Dr. D. Saravanan Ph.D.,** for providing facilities to complete our project.

We would like to make a special acknowledgement and thanks to **Dr. P.Devaki Ph.D.,** Professor and the Head of the Department of Computer Science and Engineering, for her support and encouragement throughout the project.

We express our heartful thanks to our Project Guide **Ms N Suganthi,** Professor, Department of Computer Science and Engineering, for her wholehearted support during the project.

We would like to convey our honest thanks to all faculty members and non-teaching staff members of the department for their support.

ABSTRACT

With the increasing need to protect the elements of information technology such as assets and information and the constant number of increasing threats to them, it has become absolutely important to follow necessary practices, strategies and methods to protect them and eliminate vulnerabilities. This project aims to put forth a tool that can dig in and perform an advanced OSINT search and vulnerability analysis of the information assets such as web, application servers of a business or an organization with respect to an in-house security framework that we that we have defined expounding the security foundations of an entity such as businesses, organization, schools that do handle data and information.

Keywords: information technology, assets, information, OSINT search, vulnerability analysis, security framework.

TABLE OF CONTENTS

CHAPTER-1

INTRODUCTION

The fact of the matter is the world is increasingly reliant on technology than ever need. Every day, people handle and share a lot of information within an organization or even the Internet. The information includes sensitive data, personally identifiable information (PII), protected health information (PHI) of individuals, confidential information such as strategic corporate information, trade secrets, proprietary code, passwords, research plans etc. This has created a need for securing every aspect of our information as it's the "new gold" as information security professionals would put it. This information being stored and handled by businesses and organizations have to secure the assets they are stored in, the way they are organized, the way they are managed, they are used. To do the fore mentioned actions, various guidelines, process, practices have to be followed and specialized tools have to be used in order to do so. So, it's relatively important that an organization should have a security framework in place that defines each and every action that's taken in an organization as there are a lot of cases where people with malicious intent have been able to comprise the security of an organization.

CHAPTER-2
LITERATURE REVIEW

Paper / Title	Author	Year	Journal	Objective	Proposed Technique	Limitations/ Improvements
Framework for Improving Critical Infrastructure Cybersecurity	NIST	2018	National Institute of Standards and Technology	The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.	The Framework is developed under EO 13636, and continues to evolve according to CEA(Cybersecurity Enhancement Act) of 2014, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business and organizational needs without placing additional regulatory requirements on businesses	The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework.

Protecting Controlled Unclassified Information in Non-federal Systems and Organizations	Ron Ross Patrick Viscuso Gary Guissanie Kelley Dempsey Mark Riddle	2016	National Institute of Standards and Technology	The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies. This publication provides federal agencies with recommended security requirements for protecting the confidentiality of CUI. The requirements are intended for use by federal agencies in contractual vehicles or other agreements.		The purpose of this publication is to provide federal agencies with recommended security requirements for protecting the confidentiality of CUI when the CUI is resident in a nonfederal system and organization; But this paper doesn't really state any strategies, methods or practices for non-federal organizations.
IT Governance and Information Security – Guides, Standards and Frameworks	Yassine Maleh Mamoun Alazab Mustapha Belaissaoui	2022	Book published by CRC Press	discusses strategic information technology governance and information security: guides, practices, and maturity frameworks	Highlights ISO standards, IT Service Management (ITSM) frameworks such as ITILv4, IT Asset Management (ITAM), IT Security Management	

Cybersecurity Frameworks Comparing, Contrasting and Mapping	Matthew Hudnall, The University of Alabama	2019	IEEE Computer Society	Three current cybersecurity professional and academic program schemes target cyber education, training, and workforce roles. They have complementary elements that can serve as a pathway from learning cyber to working cyber if correctly navigated.—discusses the NICE 2.0, NSA CAE-CD, CSEC2017 cybersecurity frameworks	discusses the NICE (National Initiative on Cybersecurity Education) 2.0, NSA CAE-CD(Centers of Academic Excellence in Cyber Defense Education), CSEC2017 (Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity) cybersecurity frameworks	This paper goes in details about the frameworks proposed by the standard regulatory bodies such as NIST (National Institute of Standards and Technology), NSA (National Security Agency) and Centers of Academic Excellence in Cyber Defense Education (CAE-CD) boldly stating these frameworks as curricular foundations for cybersecurity without referencing the other ISO standards proposed for cybersecurity such as ISO/IEC 27002, ISO/IEC 27031, ISO/IEC 27032 etc.

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework	Rodney Petersen Danielle Santos; Karen A. Wetzel Matthew C. Smith Greg Witte	November 2020	NIST Special Publication 800-181	describes the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), a reference structure that describes the interdisciplinary nature of the cybersecurity work. It serves as a fundamental reference resource for describing and sharing information about cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization.	Uses the NICE Cybersecurity Workforce Framework), as a reference that describes the interdisciplinary nature of the cybersecurity work.	This framework proposes tasks , roles and drafts strategies for cybersecurity workforce and employees in the field of cybersecurity but it doesn't incorporate strategies and methods for maintaining and managing assets that hold sensitive and confidential data where other frameworks do.

The challenges of cybersecurity frameworks to protect data required for the development of advanced maintenance	Jaime Campos Pankaj Sharma Erkki Jantunen David Baglee Luca Fumagalli	2016	Open access article published by Elsevier B.V	highlight the important aspects of the data management in condition monitoring and maintenance, especially when the emergent technologies, such as the cloud computing and big data, are to be considered in the maintenance department. In addition, one of the main data management elements highlighted in the current work are the cybersecurity issues which might be one of the biggest obstacles hindering the development of cloud based big data for condition-based maintenance (CBM) purposes.	References the cloud computing framework proposed by NIST and other frameworks proposed by Cloud Security Alliance (CSA).	This paper puts forth a lot of reasons to why people hesitate to store their confidential and sensitive data in the cloud servers and the risk associated with it while talking about the advantages associated with the cloud. While it highlights the benefits and disadvantages of cloud computing and data storage and maintenance in it, it completely leaves out the theoritical principles, strategies, methods and countermeasures in various aspects of cybersecurity.

OSINT in the Context of Cyber-Security	Fahimeh Tabatabaei, Douglas Wells	January 2021	Book published by Springer Publications	The impact of cyber-crime has necessitated intelligence and law enforcement agencies across the world to tackle cyber threats. All sectors are now facing similar dilemmas of how to best mitigate against cyber-crime and how to promote security effectively to people and organizations. Extracting unique and high value intelligence by harvesting public records to create a comprehensive profile of certain targets is emerging rapidly as an important means for the intelligence community. As the amount of available open sources rapidly increases, countering cyber-crime increasingly depends upon advanced software tools and techniques to collect and process the information in an effective and efficient manner.	Provides a complete insight on methods, practices and methodologies in Open Source Intelligence.	

Cyber Intelligence and OSINT: Developing Mitigation Techniques against Cybercrime Threats in Social Media	Abel Yeboah-Ofori, Allan Brimicombe	2015	Paper published on International Journal of Cyber-Security and Digital Forensics (IJCSDF) - Hong Kong e	Open Source Intelligence (OSINT) involve the collection or processes of gathering data and profiling of publicly available private and public sector information sources about individuals and business intelligence purposes. These sources includes internet and other social media platforms such as Facebook, emails, twitters, what's apps for. Much debate and research has been done on the threats, vulnerabilities and the impact of the use of social media sites but this study is to minimize bias.		
Cobit: An International Source for Information Technology Controls	John Lainhart IV	January 2010	Article published on EDPACS Newsletter	The article dives in and provides a complete insight of the COBIT framework	The researcher has done a comprehensive study on the framework and proposes some guidelines on performing an audit using the framework	The study talks only how good the COBIT Framework but doesn't tell how it stands against other frameworks such as NIST.

ISO/IEC 27001	Published by ISO/IEC organization	ISO/IEC standard gets revised every year	------	This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks.	This International Standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's n Information Security Management System (ISMS).	--------
How HIPPA can crush your medical practice –Why most medical practices don't have a clue about cybersecurity or HIPAA and what to do about it?	Craig A. Petronella	Book published in the year 2016		This book describes how complying to the old HIPAA act can lead to a disaster.	It discusses the risks and threats to the PHI (Personal Health Information) in both medical and cybersecurity point of view in context of HIPAA act.	Though it states the facts and truth about HIPAA, it just mentions the much secure HITECH act.

ISA/IEC 62443	Series of standards by put forth by International Electrotechnical Commission (IEC)	Gets revised every year	---------	This standard provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs)	Provides a comprehensive guideline and absolute effectiveness in securing information and OT systems.	------
IEC 61850 standard	Standard defined by International Electrotechnical Commission (IEC)	Gets revised every year	--------	International standard that defines communication protocols to provide communication between different equipment located in a substation, such as protection, control, and measurement equipment, as well as (IEDs) intelligent electronic devices.	Discusses object-oriented methods to provide logical communications between substations, primary process equipment, and secondary devices	-------
Applying a holistic cybersecurity framework for global IT organizations	Maurice Dawson	2018	Article published on Business Information Review	This article illustrates how cybersecurity can be broken into these three core areas and used together to address issues such as developing training environments for teaching real cybersecurity events	This study examines the research gaps within cybersecurity as it relates to core themes in an effort to develop stronger policies, education programs and hardened technologies for cybersecurity use.	This article doesn't state the guidelines and practices based on any specific standard or frameworks. It just puts forth common best security practices and guidelines for organizations.

CHAPTER-3

EXISTING SYSTEM

Maltego is a commercial, freemium tool that specializes in uncovering relationships among people, companies, domains, and publicly accessible information on the internet. 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.

Shodan is also a freemium tool that works as a search engine to find different IT assets such as web servers, mail servers, application servers, CCTV cameras and even IoT devices such as smart cameras, smart voice assistants etc. The free version comes with a few OSINT tools such as HOISWHOIS database lookup, DNS lookup and such. The premium version comes loaded with more features such as vulnerability analysis, network exposure monitoring etc.

Spiderfoot is an OSINT tool that automates OSINT for various cybersecurity actions such as asset discovery, attack surface monitoring, security assessments and such. But like the above-mentioned tools, premium version offers more features, and it is said to report a lot of false positives compared to its competitors.

Apart from these, there a lot of individual tools for individual functions such as discovery, reconnaissance developed as scripts, modules, and even wholesome tools in programming languages like Python, Bash, Lua etc. Even people who are into the field of cybersecurity, contribute a lot on their part to the world of OSINT tools.

3.1 DRAWBACKS OF EXISTING SYSTEM:

Currently, there are tools in the market available to perform functions such as

- WHOIS Lookup
- Subdomain Enumeration
- DNS Records Lookup
- Geolocation
- OS Detection etc.

But these tools are available individually and require a lot of effort to install as there are a lot of problems associated such as mismatch and non-availability of dependencies, incompatibility of the modules associated with the operating system etc.

Like this problem, the forementioned tools are mostly freemium – meaning though free versions of those tools are available, they do not offer you a lot of features that the paid, premium version do. The price of these tools is too high such that an individual who wants to experience the full potential of these OSINT tools may or may not be able to afford to. Considering organizations, they would have to pay a hefty amount for buying multiple licenses, further increasing the CapEx (Capital Expenditure) of an organization. Organizations might not even purchase these tools as it does not assure them ROI (Return on Investment) on buying these tools.

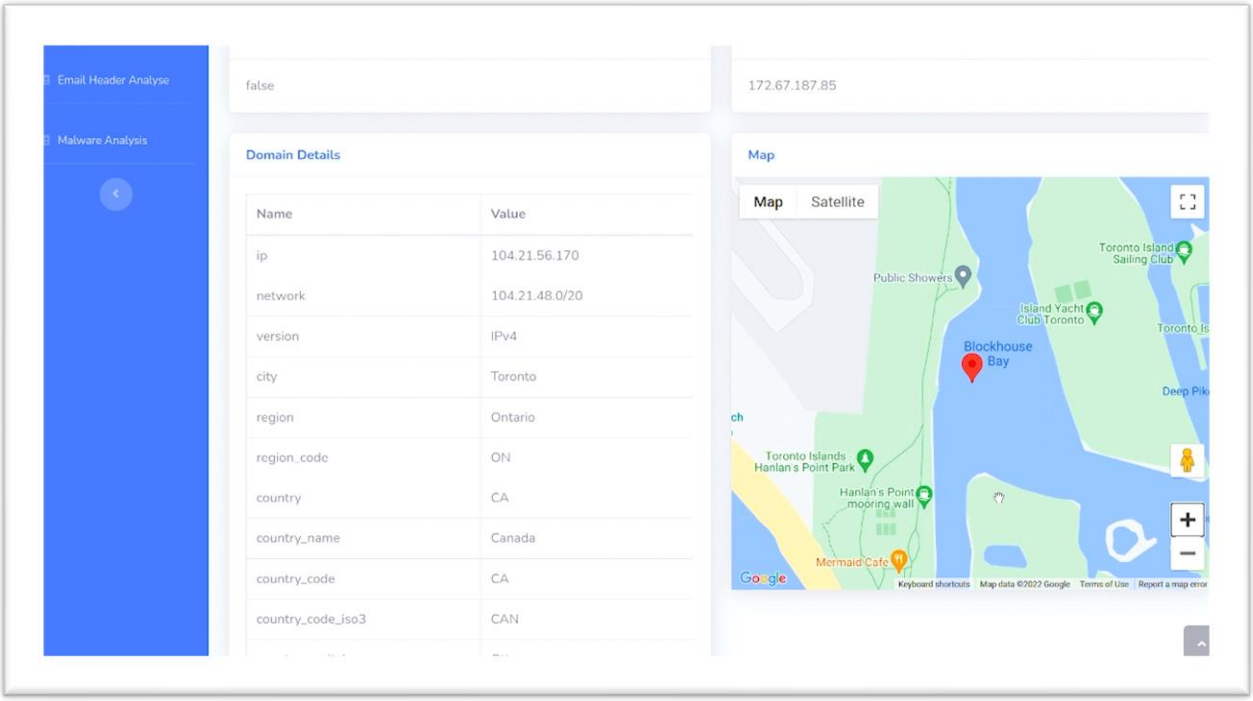
CHAPTER-4

PROPOSED SYSTEM

4.1 IMPLEMENTATION:

Our tool Open Vuln Scanner is an Open-Source Intelligence (OSINT) tool which would fetch details from the user and collect the details of the domain and generate an OSINT report.

Our tool comprises of various modules to perform OSINT which includes WHOIS details gatherer, Network Scanner, Operating System (OS) detection, Domain Name System (DNS) Enumeration, Subdomain Enumeration, IP Address Lookup, SSL Certificate Enumeration and Adult Content Detection. The details gathered from this tool will help us in attacking phase.



false

172.67.187.85

Domain Details

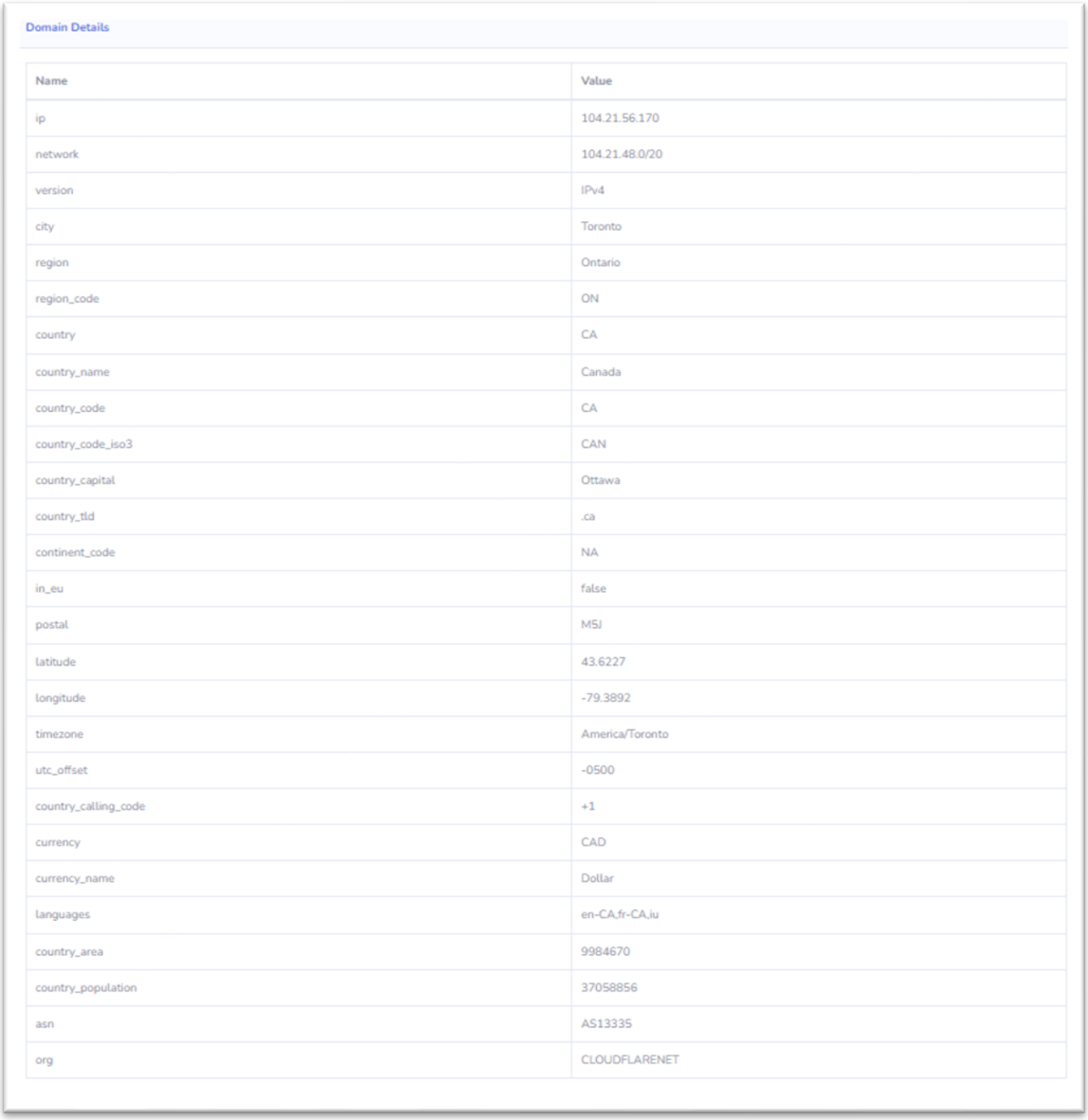
Name	Value
ip	104.21.56.170
network	104.21.48.0/20
version	IPv4
city	Toronto
region	Ontario
region_code	ON
country	CA
country_name	Canada
country_code	CA
country_code_iso3	CAN

Fig. 4.1.a Main Dashboard

4.2 METHODOLOGY

4.2.1. WHOIS Details

The WHOIS details gathering module will get the details like IP address, Network ID, Registrant Name, Registrant Organization, Country, City, Latitude and Longitude details, and ASN ID. We have integrated a map feature. The location details of the server is mapped in the dashboard. By this map feature, user can use the 360 ° viewer for extensive OSINT. This gives basic details, but this will be helpful in reconnaissance phase.



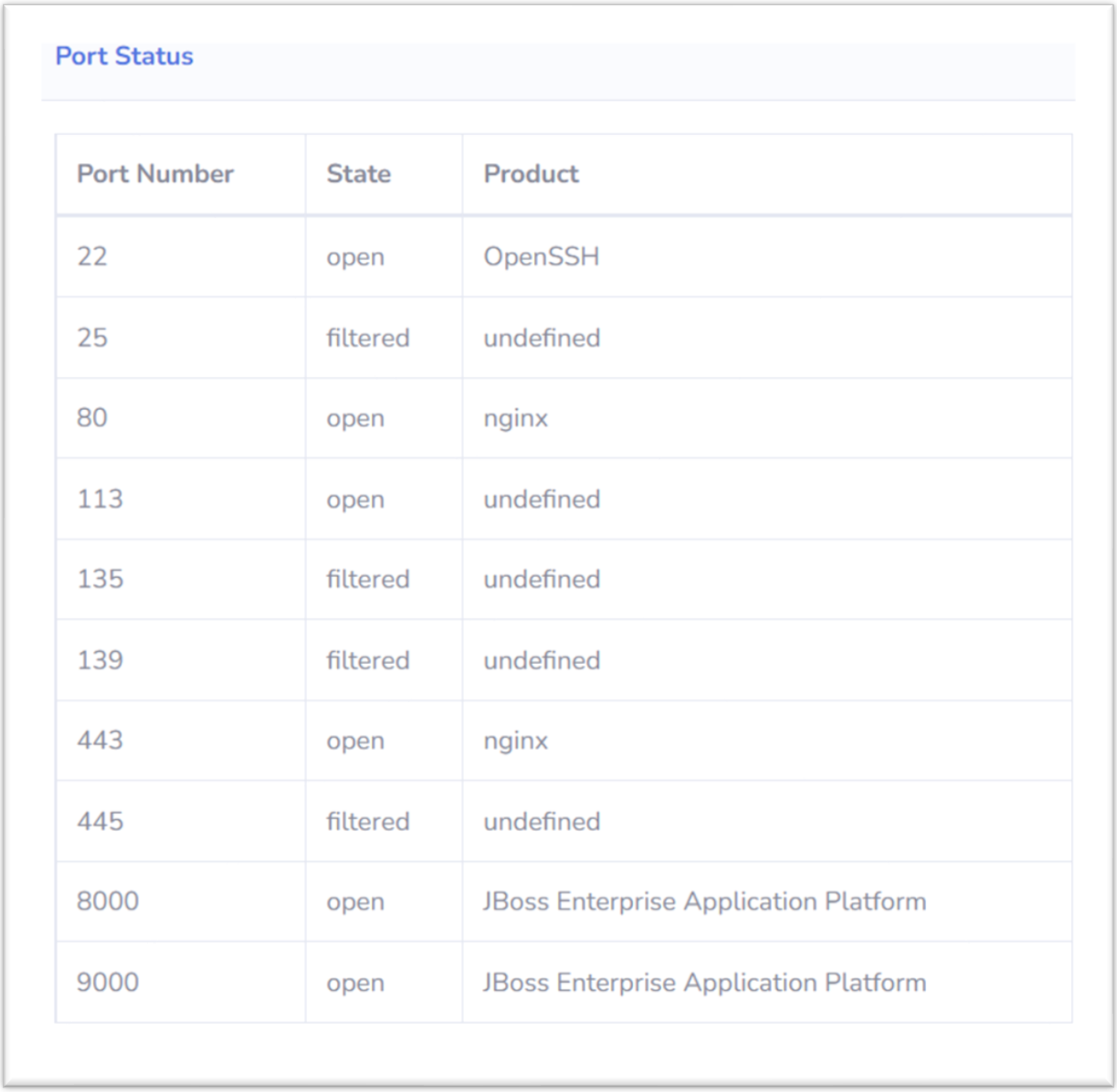
Domain Details

Name	Value
ip	104.21.56.170
network	104.21.48.0/20
version	IPv4
city	Toronto
region	Ontario
region_code	ON
country	CA
country_name	Canada
country_code	CA
country_code_iso3	CAN
country_capital	Ottawa
country_tld	.ca
continent_code	NA
in_eu	false
postal	M5J
latitude	43.6227
longitude	-79.3892
timezone	America/Toronto
utc_offset	-0500
country_calling_code	+1
currency	CAD
currency_name	Dollar
languages	en-CA,fr-CA,iu
country_area	9984670
country_population	37058856
asn	AS13335
org	CLOUDFLARENET

Fig. 4.2.1.a WHOIS Details

4.2.2. Network Analyzer

Network analyzer is a python-based module that scans the status of the ports in the server where the website is hosted and the services running in the port. This will give you the details such as the service, its version running on the respective port. These details will be useful to find exploits to attack the site.



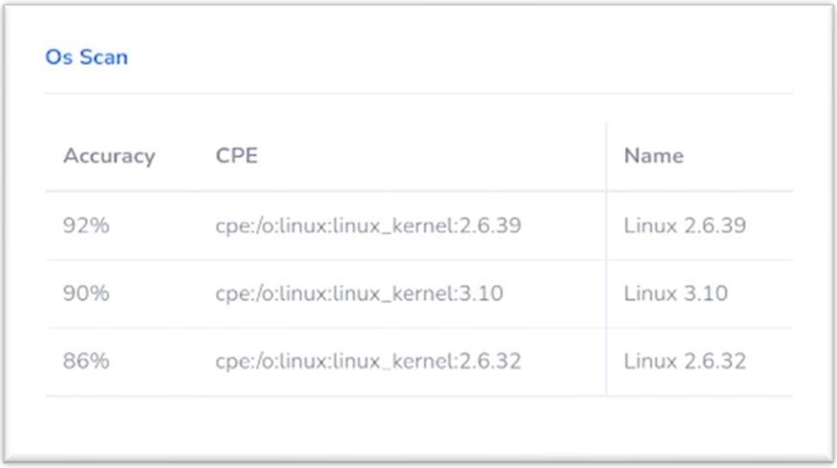
Port Status

Port Number	State	Product
22	open	OpenSSH
25	filtered	undefined
80	open	nginx
113	open	undefined
135	filtered	undefined
139	filtered	undefined
443	open	nginx
445	filtered	undefined
8000	open	JBoss Enterprise Application Platform
9000	open	JBoss Enterprise Application Platform

Fig. 4.2.2.a Network Analyzer

4.2.3. OS Detection

OS detection module enumerates the Operating System running on the server with the analysis of the banner that is fetched as a response from the server. This detail will be useful to find an exploit specific to the operating system.



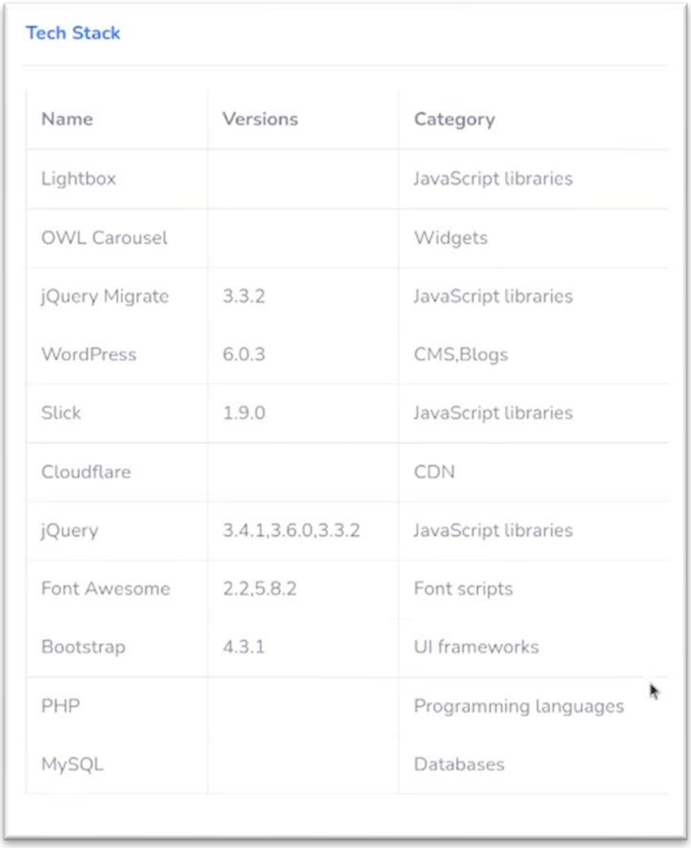
Os Scan

Accuracy	CPE	Name
92%	cpe:/o:linux:linux_kernel:2.6.39	Linux 2.6.39
90%	cpe:/o:linux:linux_kernel:3.10	Linux 3.10
86%	cpe:/o:linux:linux_kernel:2.6.32	Linux 2.6.32

Fig. 4.2.3.a OS Detection

4.2.4. Technology Stack Detection

Technology Stack detection module uses the Wappalyzer API to enumerate the web framework, plugins, and security systems they use in their website. These details will be useful to find exploits in the attacking phase.



Tech Stack

Name	Versions	Category
Lightbox		JavaScript libraries
OWL Carousel		Widgets
jQuery Migrate	3.3.2	JavaScript libraries
WordPress	6.0.3	CMS,Blogs
Slick	1.9.0	JavaScript libraries
Cloudflare		CDN
jQuery	3.4.1,3.6.0,3.3.2	JavaScript libraries
Font Awesome	2.2,5.8.2	Font scripts
Bootstrap	4.3.1	UI frameworks
PHP		Programming languages
MySQL		Databases

Fig. 4.2.4.a Technology Stack Detection

4.2.5. DNS Records

DNS Records module uses a Python script that we have developed to enumerate the DNS records like

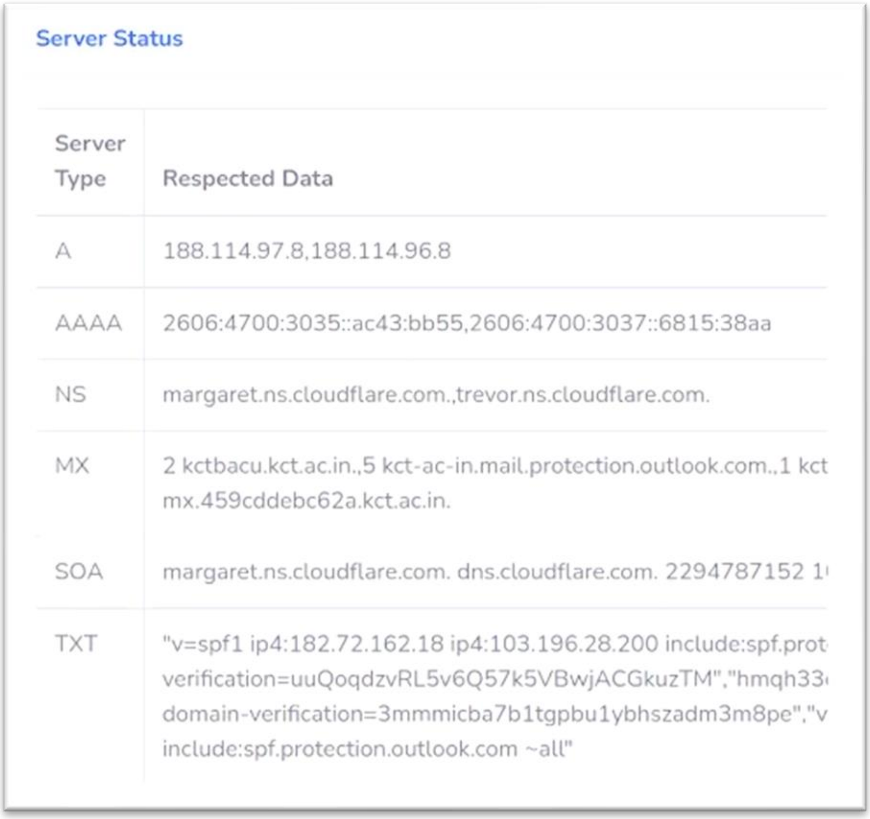
I. **A records -** DNS A records contain the IP address of a domain, specifically the IPv4 address.

II. **AAAA records -** DNS AAAA records are exactly like DNS A records, except that they store a domain's IPv6 address instead of its IPv4 address.

III. **NS** – Name Server record is a DNS record that contains the name of the authoritative name server within a domain or DNS zone.

IV. **MX** – A mail exchanger record specifies the mail server responsible for accepting email messages on behalf of a domain name.

V. **SOA -** Start of Authority record stores important information about a domain or zone such as the email address of the administrator, when the domain was last updated, and how long the server should wait between refreshes.



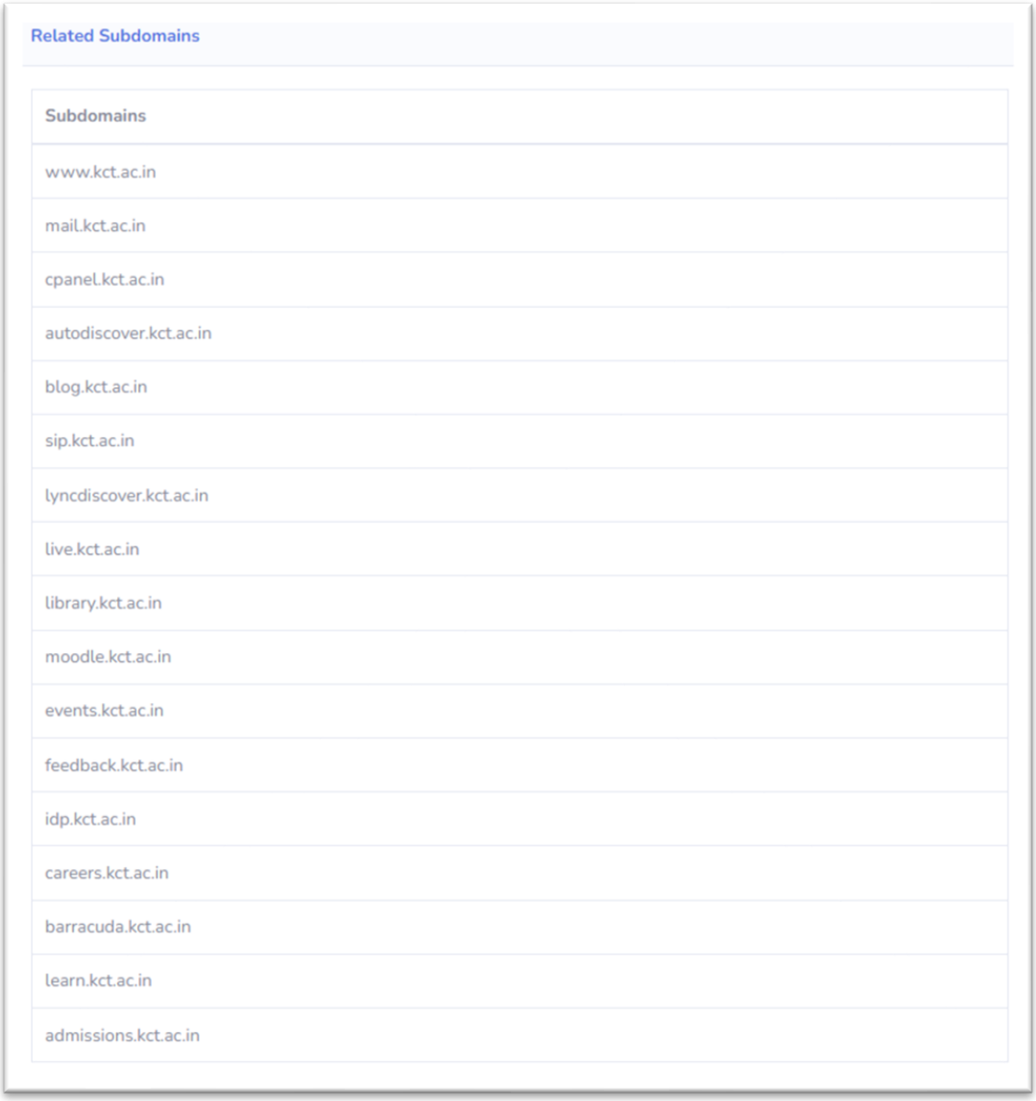
Server Status

Server Type	Respected Data
A	188.114.97.8,188.114.96.8
AAAA	2606:4700:3035::ac43:bb55,2606:4700:3037::6815:38aa
NS	margaret.ns.cloudflare.com.,trevor.ns.cloudflare.com.
MX	2 kctbacu.kct.ac.in.,5 kct-ac-in.mail.protection.outlook.com.,1 kct mx.459cddebc62a.kct.ac.in.
SOA	margaret.ns.cloudflare.com. dns.cloudflare.com. 2294787152 1
TXT	"v=spf1 ip4:182.72.162.18 ip4:103.196.28.200 include:spf.prot verification=uuQoqdzvRL5v6Q57k5VBwjACGkuzTM","hmqh33 domain-verification=3mmmicba7b1tgpbu1ybhszadm3m8pe","v include:spf.protection.outlook.com ~all"

Fig. 4.2.5.a **DNS Records**

4.2.6. Subdomain Enumeration

Subdomain enumeration module enumerates the subdomain related to the domain. It helps to broaden the attack surface, find hidden applications, and forgotten subdomains. Sometimes vulnerabilities may be present across multiple domains and applications of the same domain.



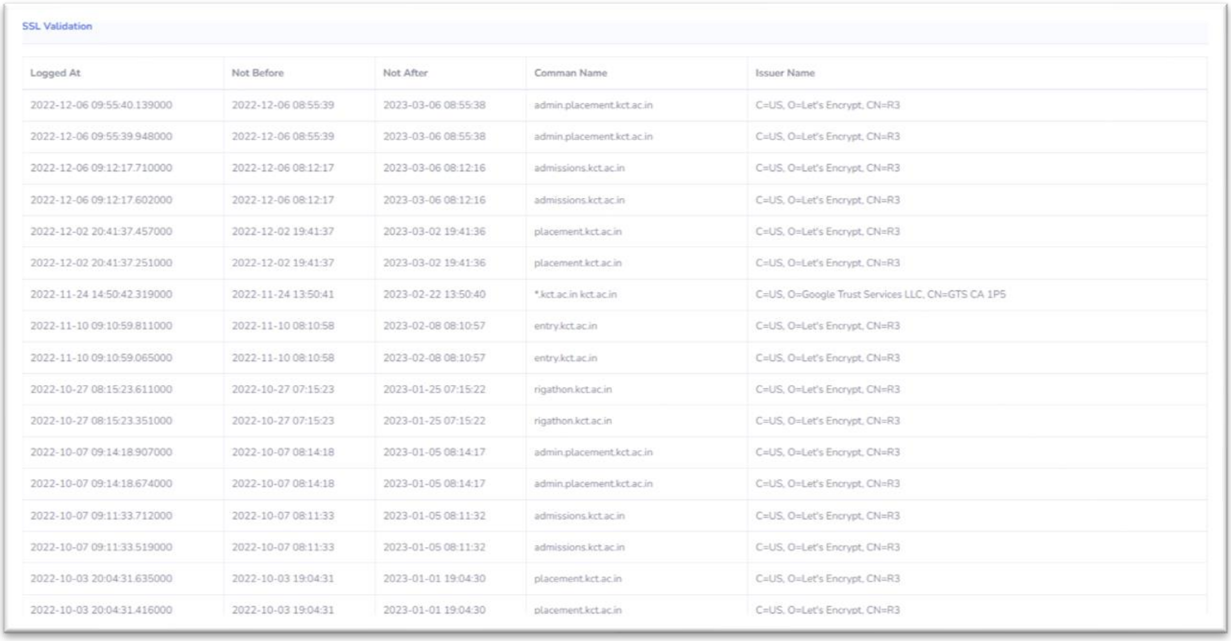
Related Subdomains

Subdomains
www.kct.ac.in
mail.kct.ac.in
cpanel.kct.ac.in
autodiscover.kct.ac.in
blog.kct.ac.in
sip.kct.ac.in
lyncdiscover.kct.ac.in
live.kct.ac.in
library.kct.ac.in
moodle.kct.ac.in
events.kct.ac.in
feedback.kct.ac.in
idp.kct.ac.in
careers.kct.ac.in
barracuda.kct.ac.in
learn.kct.ac.in
admissions.kct.ac.in

Fig. 4.2.6.a Subdomain Enumeration

4.2.7. SSL Certificate Enumeration

SSL certificate enumeration module enumerates the SSL certificates of the domain and its subdomains. Some WHOIS details would be hidden for user's privacy. But collecting the historical data there might be a chance of getting interesting details about the domain. These details will get the details of the registrant, organization, and certificate issuer.



SSL Validation

Logged At	Not Before	Not After	Comman Name	Issuer Name
2022-12-06 09:55:40.139000	2022-12-06 08:55:39	2023-03-06 08:55:38	admin.placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-12-06 09:55:39.948000	2022-12-06 08:55:39	2023-03-06 08:55:38	admin.placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-12-06 09:12:17.710000	2022-12-06 08:12:17	2023-03-06 08:12:16	admissions.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-12-06 09:12:17.602000	2022-12-06 08:12:17	2023-03-06 08:12:16	admissions.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-12-02 20:41:37.457000	2022-12-02 19:41:37	2023-03-02 19:41:36	placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-12-02 20:41:37.251000	2022-12-02 19:41:37	2023-03-02 19:41:36	placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-11-24 14:50:42.319000	2022-11-24 13:50:41	2023-02-22 13:50:40	*.kct.ac.in kct.ac.in	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
2022-11-10 09:10:59.811000	2022-11-10 08:10:58	2023-02-08 08:10:57	entry.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-11-10 09:10:59.065000	2022-11-10 08:10:58	2023-02-08 08:10:57	entry.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-10-27 08:15:23.611000	2022-10-27 07:15:23	2023-01-25 07:15:22	rigathon.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-10-27 08:15:23.351000	2022-10-27 07:15:23	2023-01-25 07:15:22	rigathon.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-10-07 09:14:18.907000	2022-10-07 08:14:18	2023-01-05 08:14:17	admin.placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-10-07 09:14:18.674000	2022-10-07 08:14:18	2023-01-05 08:14:17	admin.placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-10-07 09:11:33.712000	2022-10-07 08:11:33	2023-01-05 08:11:32	admissions.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-10-07 09:11:33.519000	2022-10-07 08:11:33	2023-01-05 08:11:32	admissions.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-10-03 20:04:31.635000	2022-10-03 19:04:31	2023-01-01 19:04:30	placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
2022-10-03 20:04:31.416000	2022-10-03 19:04:31	2023-01-01 19:04:30	placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3

Fig. 4.2.7.a SSL Certificate Enumeration

4.3 BLOCK DIAGRAM:

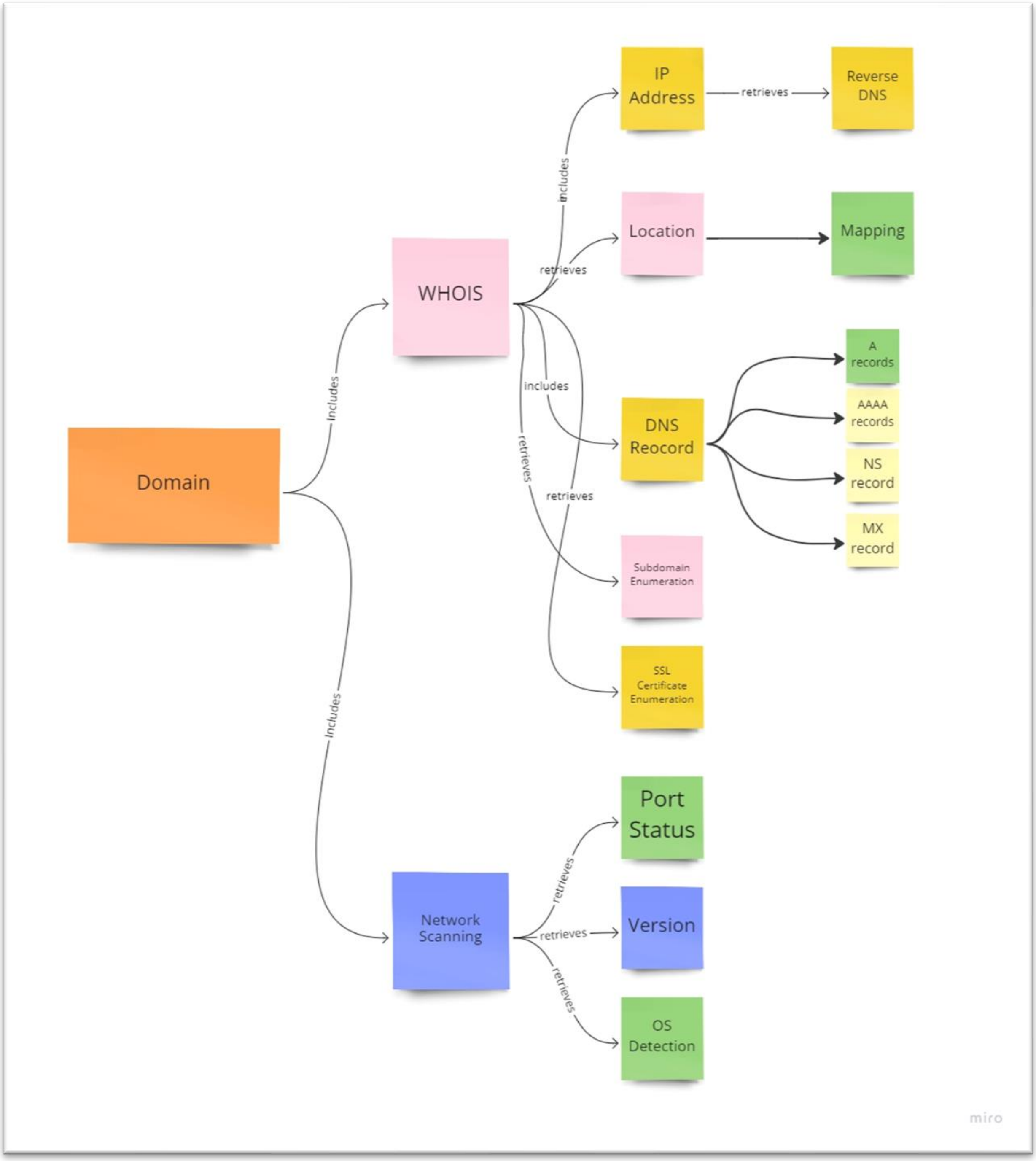


Figure 4.3.a Block Diagram of Open Vuln Scanner

CHAPTER-5

SYSTEM REQUIREMENTS

The Open Vuln Scanner consists of both hardware and software requirements for information gathering.

6.1 HARDWARE REQUIREMENTS:

- Processor: Intel Core i3 or AMD equivalent and above
- RAM: Minimum of 4GB is required
- Display such as monitor, or an external display is required
- Stable internet connection

6.2 SOFTWARE REQUIREMENTS:

- Windows/ Linux/ Unix Operating systems
- Chrome v93.0.4577 / Firefox v107.0 / Edge v88.0.705 and above
- Python 3.x and above
- Django
- SQLite 3

CHAPTER-6

ADVANTAGES & LIMITATIONS

ADVANTAGES:

- The time required for the report generation with all the details takes one day on average, whereas we automate the process and generate an easily interpretable report within few minutes.
- As the code is self-implemented in python you get to customize the implementation of the functionality to what you'll eventually be using your code for, so it's tailored to your workflow.
- The use of Django complements the project with features like Security, Scalability, Versatility, and Support of most OS and is Easy to work with.
- The software can be used by cyber security employees to assess the systems of their organization at ease.
- This software can be used by personnel ranging from amateur to experienced.

LIMITATIONS:

- As it is self-written code future developers working on the project have to go and learn the theory and best practices for our approach, but our code has been well refactored so that anyone can collaborate without any hassle
- It does a complete, comprehensive OSINT search which consumes a tad more time more than other tools.
- Since the tool comes in integrated with many modules, the module dependency chain is high.

CHAPTER-7

CONCLUSION AND FUTURE WORK

The future work is to implement this project in real time helping people ranging from beginners to professionals to easily perform an advanced OSINT search and vulnerability analysis without any hassle that enable them to modify their security practices, methodologies and strategies already in place and put forth security defense mechanisms in the form of hardware, software and security professionals based on the factors such as risk, ALE (Annual Loss Expectancy) and the cost based on the vulnerabilities found by the tool with respect to the proposed security framework along with this tool. Furthermore, this project can be improved by adding more modules and capabilities related to scanning, analyzing and preventing cyber security threats evolving everyday in this modern digital world making it an all-in-one cyber security tool similar to the commercial, proprietary ones available in the market.

CHAPTER-8

REFERENCES

1. Framework for Improving Critical Infrastructure Cybersecurity – NIST https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

2. Protecting Controlled Unclassified Information in Non-federal Systems and Organizations - Ron Ross, Patrick Viscuso, Gary Guissanie , Kelley Dempsey, Mark Riddle - National Institute of Standards and Technology

3. IT Governance and Information Security – Guides, Standards and Frameworks - Yassine Maleh, Mamoun Alazab, Mustapha Belaissaoui https://www.researchgate.net/publication/356649134_IT_Governance_and_Information_Security_Guides_Standards_and_Frameworks

4. Cybersecurity Frameworks Comparing, Contrasting and Mapping - Matthew Hudnall, The University of Alabama - IEEE Computer Society

5. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework - Rodney Petersen Danielle Santos; Karen A. Wetzel Matthew C. Smith , Greg Witte - NIST Special Publication 800-181

6. The challenges of cybersecurity frameworks to protect data required for the development of advanced maintenance - Jaime Campos Pankaj Sharma Erkki Jantunen - Elsevier B.V Publications

7. Tabatabaei, F., Wells, D. (2016). OSINT in the Context of Cyber-Security. In: Akhgar, B., Bayerl, P., Sampson, F. (eds) Open Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-319-47671-1_14

8. Cyber Intelligence and OSINT: Developing Mitigation Techniques against Cybercrime Threats in Social Media- Abel Yeboah-Ofori, Allan Brimicombe - International Journal of Cyber-Security and Digital Forensics (IJCSDF) - Hong Kong

9. Cobit: An International Source for Information Technology Controls - John Lainhart IV - EDPACS Newsletter

10. ISO/IEC-27001 https://www.iso.org/isoiec-27001-information-security.html

11. How HIPPA can crush your medical practice –Why most medical practices don't have a clue about cybersecurity or HIPAA and what to do about it? - Craig A. Petronella

12. ISA/IEC 62443 standard https://www.iec.ch/blog/understanding-iec-62443

13. IEC 61850 standard https://ieeexplore.ieee.org/abstract/document/7543038

14. Applying a holistic cybersecurity framework for global IT organizations – Maurice Dawson

15. Information Security – The Complete Reference 2nd Edition - Mark Rhodes Ousley – McGraw Hill Education