

**OpenVuln Scanner**

OSINT Tool and Security Framework

**PHASE-I 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)**

**DEC 2022**

**KUMARAGURU COLLEGE OF TECHNOLOGY**

**COIMBATORE 641049**

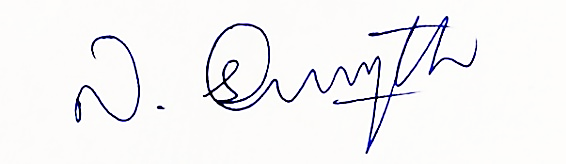
**(An Autonomous Institution Affiliated to Anna University, Chennai)**

**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

Computer Science and Engineering

Kumaraguru College of Technology

Coimbatore-641049

Professor

Computer Science and Engineering

Kumaraguru College of Technology

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:**

**DECLARATION**

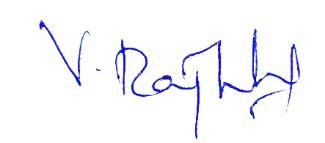
We affirm that the project work titled “OpenVuln Scanner” being submitted in partial fulfillment for the award of B.E Computer Science and Engineering is the original work carried out by us. It has not formed the part of any other project work submitted for the award of any degree or diploma, either in this or any other University.

**Diagram

Description automatically generated**

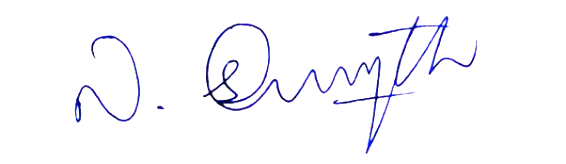


**SHARAT N (19BCS086) VISHAL S (19BCS103)**

****

**RAJHESHWAR V (19BCS105)**

I certify that the declaration made above by the candidates is true.



**Dr N. Suganthi,**

Professor,

Department of Computer Science and Engineering,

Kumaraguru College of Technology,

Coimbatore – 641049.

**ACKNOWLEDGEMENT**

We express our profound gratitude to the Management of Kumaraguru College of Technology for providing us with the required infrastructure that enabled us to successfully complete the project.

We extend our gratitude to our Principal, **Dr. D. Saravanan,** for providing us the necessary facilities to pursue the project.

We would like to acknowledge **Dr. P. Devaki,** Professor and Head, Department of Computer Science and Engineering, for her support and encouragement throughout this project.

We thank our project coordinator and guide **Dr. N. Suganthi,** Professor, Department of Computer Science and Engineering, for the constant and continuous effort, guidance and valuable time.

Our sincere and hearty thanks to staff members of Department of Computer Science and Engineering of Kumaraguru College of Technology for their well wishes, timely help and support rendered to us during our project. We are greatly indebted to our family, relatives and friends, without whom life would have not been shaped to this level.

-  **SHARAT N**

**VISHAL S**

**RAJHESHWAR V**

**ABSTRACT**

With the increasing need to protect the elements of information technology, such as assets and information, from rising threats, it has become imperative 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 of the information assets, such as the application servers of a business or an organization, with respect to an in-house security framework 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** |  | **TITLE** | **PAGE NO** |
| **NO** |  |  |  |
|  |  |  |  |
|  | ABSTRACT | | 4 |
|  |  |  |  |
|  |  | |  |
| 1 | INTRODUCTION | | 7 |
|  |  |  |  |
| 2 | LITERATURE REVIEW | | 8 |
|  |  |  |  |
|  | EXISTING SYSTEM | | 11 |
| 3 |  |  |  |
|  | 3.1 | DRAWBACKS OF EXISTING SYSTEM | 12 |
|  |  |  |  |
|  | PROPOSED SYSTEM | | 13 |
|  |  |  |  |
|  |  |  | 13 |
|  | 4.1 | BLOCK DIAGRAM |  |
| 4 | 4.2 | IMPLEMENTATION | 14 |
|  |  |  |  |
| 4.3 | METHODOLOGY | 15 |
| 4.4 | SECURITY FRAMEWORK | 22 |
|  | SYSTEM REQUIREMENTS | | 23 |
|  |  |  |  |
| 5 | 5.1 | HARDWARE REQUIREMENTS | 26 |
|  |  |  |  |
|  | 5.2 | SOFTWARE REQUIREMENTS | 26 |
|  |  |  |  |
| 6 | ADVANTAGES & LIMITATIONS | | 24 |
|  |  | |  |
| 7 | CONCLUSION AND FUTURE WORK | | 25 |
|  |  | |  |
| 8 | REFERENCES | | 29 |
|  |  |  |  |

**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**

Intelligence and law enforcement organisations must now combat cyber risks due to the impact of cybercrime. The best way to combat cybercrime and the most effective way to educate people and businesses about security is through current universal problems that affect all sectors. A crucial tool for the intelligence community is quickly emerging: extracting unique and valuable intelligence from public records to build thorough profiles of specific targets. The ability to collect and analyse information effectively and efficiently rely increasingly on cutting-edge software tools and methodologies as the amount of open sources available rise quickly. [7]

Open-Source Intelligence (OSINT) is the gathering of information from publicly accessible, private and public sector sources about specific people or an organization for business intelligence objectives. These sources include the internet, emails, Twitter, Facebook, and other social media websites and apps. The risks, weaknesses, and effects of using social media sites have been the subject of much discussion and research, but this study aims to reduce prejudice. [8]

NIST places a strong emphasis on utilising business objectives to direct cybersecurity efforts and taking cybersecurity risks into account as part of the organization's risk management procedures. When it comes to managing cybersecurity risk for critical infrastructure, there is no one solution that fits all. Organizations will still face distinct risks from various threats, vulnerabilities, and risk tolerances. They will also differ in how they adapt the Framework's recommended practises. [1]

Federal agencies place a high priority on protecting Controlled Unclassified Information (CUI) stored in non-federal systems and organisations. In this paper, federal agencies are given suggested security standards for safeguarding CUI confidentiality. Federal agencies are expected to use the standards in contracts and other legal documents. It offers federal agencies suggested security standards for safeguarding the CUI in a system and organisation that are not federal. [2]

The Cybersecurity Workforce Framework (NICE Framework), developed by the National Initiative for Cybersecurity Education (NICE), is a model for reference that explains the interdisciplinary nature of cybersecurity work. It acts as a key reference tool for outlining and exchanging knowledge about cybersecurity work and the knowledge, skills, and abilities (KSAs) required to finish projects that can improve an organization's cybersecurity posture. [5]

All the fundamental components of effective risk management and cyber defence are combined under security governance. Without this oversight, there will always be risky gaps and assets would be compromised. Business strategies, information architecture, security policies and procedures, and operating practises are all determined by governance, which is the method through which these risk values are reflected in the direction and judgement. The "hidden ingredients" in the company's risk or security management plan are compliance audits and reviews, which guarantee that security policies and procedures are properly followed. [3]

Education, policy, and technologies are the three main pillars of cybersecurity. The education section offers advice on creative methods to teach cybersecurity material, including talking about the organisations that accredit courses in computer science or information technology (IT). The governing rules, resources, and methods that can be advanced in cybersecurity education must be examined by an organisation. The framework's policy topic includes numerous guidelines, requirements, legislation, and best practises. These can be regulations from the Department of Defense (DoD), National Institute of Standards and Technology (NIST), the US military, and more in the US. These rules serve as the foundation for additional advice and guidance that companies can use to create their own policies.The framework's technologies section incorporates information on cutting-edge technology, including gadgets with Internet access. In order to assure compliance with cybersecurity regulations, these technologies, which include mobile phones, operating systems (OSs), software, and other devices, go through an evaluation of their security posture. [14]

**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 WHOIS 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.

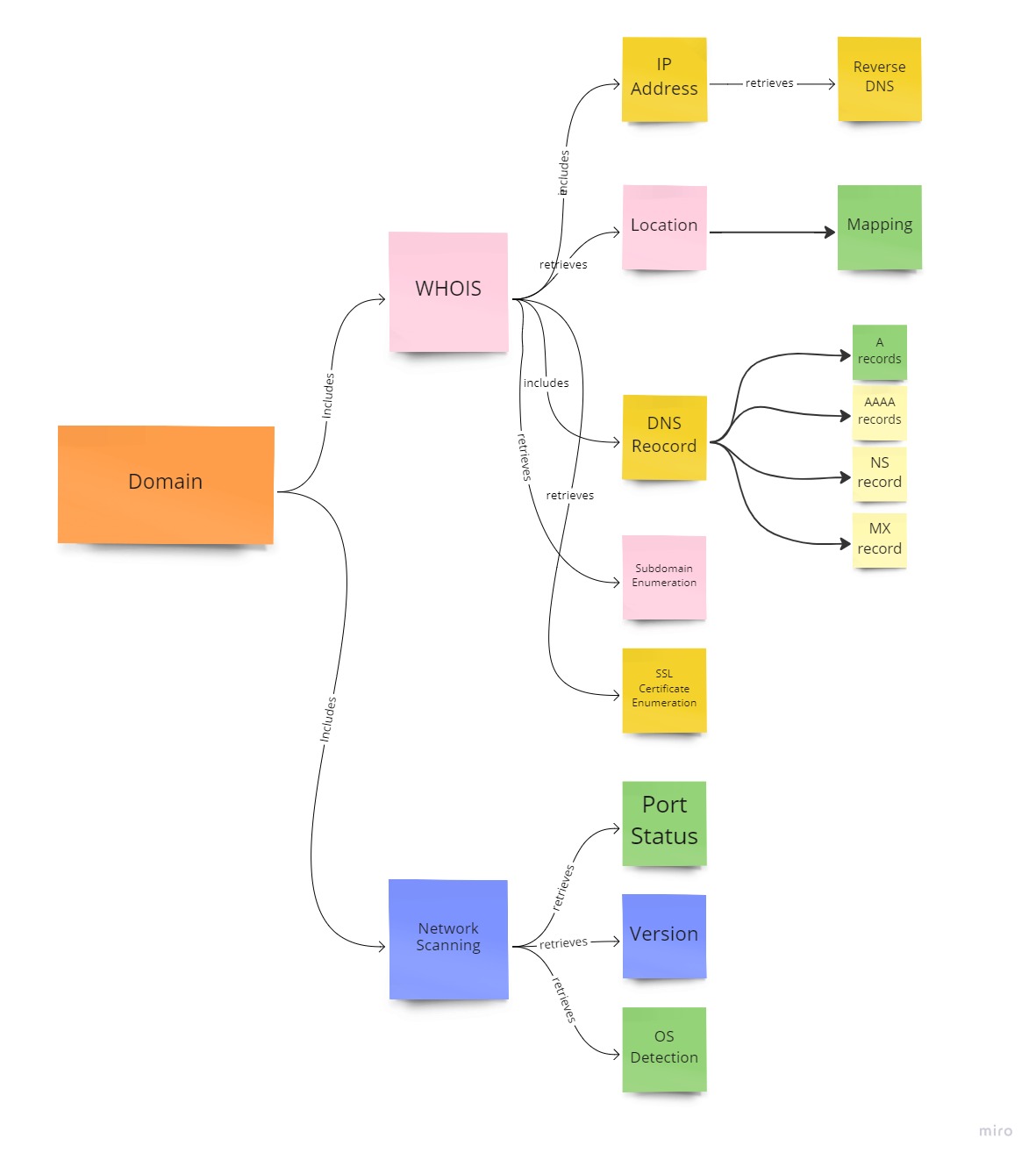
Like this problem, the forementioned tools are mostly freemium – meaning though free versions of those tools are available, they do not offer you a lot of features that the paid, premium version do. The price of these tools is too high such that an individual who wants to experience the full potential 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**

Our solution is to provide a handy tool that is useful for Open-Source Intelligence. This gathers free, publicly available data about an organization (i.e., a domain) on the internet. We have a dashboard **Fig. 4.2.a** that shows cumulative results. We have interconnective modules. So, our tool works in a strategical manner to gather information **Figure 4.1.a**. We provide an industrial-level standard security framework for Identity and Access Management, IT Assets Management. That can be used in all types of industries, Hospitals and Educational Institutions.

**4.1 Block Diagram:**



**Figure 4.1.a Block Diagram of Open Vuln Scanner**

**4.2 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.

Graphical user interface, application, Teams

Description automatically generated

**Fig. 4.2.a Main Dashboard**

**4.3 METHODOLOGY**

**4.3.1. 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. The dashboard **Fig. 4.3.1.a** displays all the detailed gathered WHOIS details.

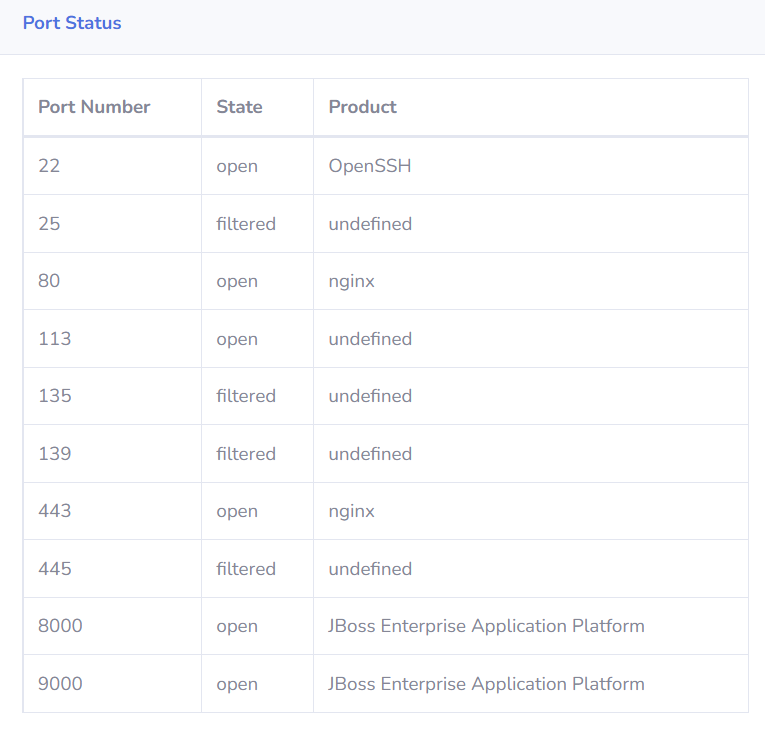
**Table

Description automatically generated**

**Fig. 4.3.1.a WHOIS Details**

**4.3.2. 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 section **Fig. 4.3.2.a** 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.

****

**Fig. 4.3.2.a Network Analyzer**

**4.3.3. 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. This section **Fig. 4.3.3.a** displays the OS Details.

****

**Fig. 4.3.3.a OS Detection**

**4.3.4. 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 in **Fig. 4.3.4.a** will be useful to find exploits in the attacking phase.

**Table

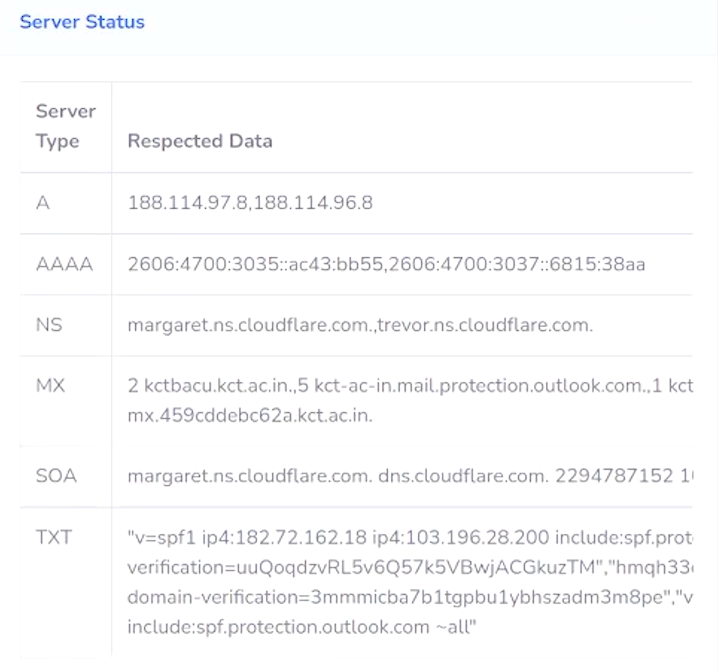
Description automatically generated**

**Fig. 4.3.4.a Technology Stack Detection**

**4.3.5. DNS Records**

DNS Records module uses a Python script that we have developed to enumerate the DNS records in **Fig. 4.3.5.a** like

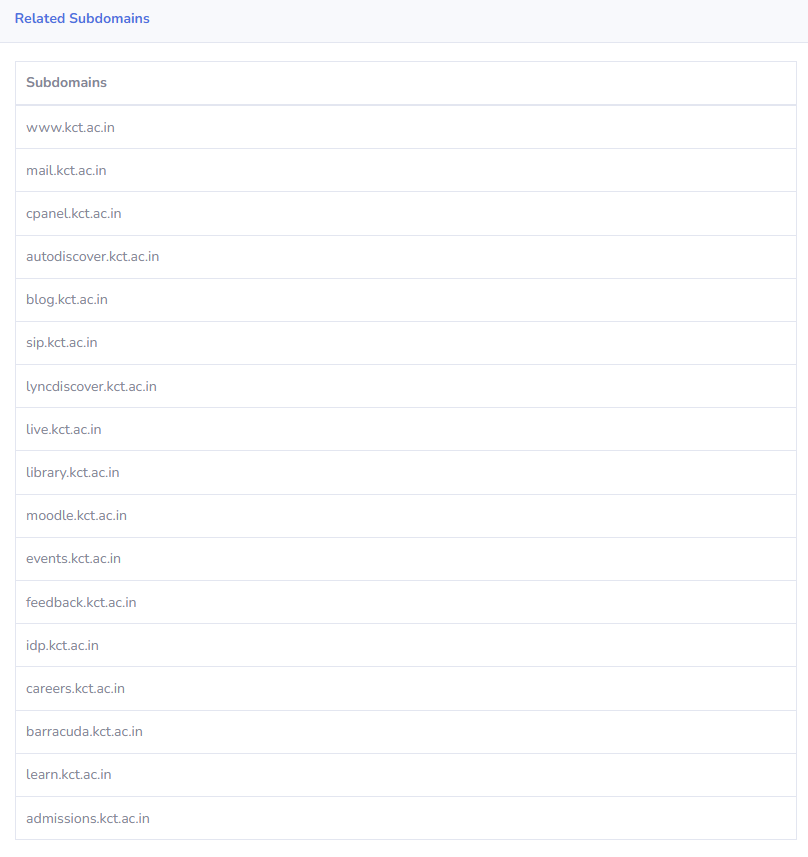
* 1. **A records -** DNS A records contain the IP address of a domain, specifically the IPv4 address.
  2. **AAAA records -** DNS AAAA records are exactly like DNS A records, except that they store a domain's IPv6 address instead of its IPv4 address.
  3. **NS –** Name Server record is a DNS record that contains the name of the authoritative name server within a domain or DNS zone.
  4. **MX –** A mail exchanger record specifies the mail server responsible for accepting email messages on behalf of a domain name.
  5. **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.



**Fig. 4.3.5.a DNS Records**

**4.3.6. Subdomain Enumeration**

Subdomain enumeration module enumerates the subdomain related to the domain. The details in **Fig. 4.3.6.a** 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.

****

**Fig. 4.3.6.a Subdomain Enumeration**

**4.3.7. 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 in **Fig. 4.3.7.a** will get the details of the registrant, organization, and certificate issuer.

Graphical user interface, table

Description automatically generated

**Fig. 4.3.7.a SSL Certificate Enumeration**

**4.4. Security Framework:**

The administration should ensure the following rules and regulations is followed in the organization.

* The proposed framework tries to cover all aspects of information security which includes methodology, practices, strategies, analysis, and technical details becoming a wealthy resource for defining a policy or a framework in your own place to perform the following Ensure the confidentiality, integrity, and availability (CIA Triad) of all the data they create, receive, maintain, or transmit [3]
* Protect against reasonably anticipated, impermissible uses or disclosures [5]
* Ensure amenability by their workforce
* Identify and protect against integrity of the information
* **Security Management and Evaluation** - A risk assessment should be done periodically. Security measures must be implemented to reduce the risk and vulnerabilities to ensure an appropriate level of security. [9]
* **Information Access Management –** The information access should be onlydone by authorized persons. Role-Based access should be implemented. [11]
* **Workforce Management and Training – Every workforce member must provide appropriate training** about the latest security policies and procedures. Take severe actions against the workforce member who violates the security policies and procedures.[12]
* **Datacenter and Device Security –** The administration should ensure the security while a user access to the electronic media such as Server, Hard Disk (HDD), Solid State Drive (SSD), Pendrive, Switches, Routers and Load Balancers. [14]
* **Audit -** A proper audit should be implemented to record and maintain the hardware, software and/or procedure mechanism in the information systems. [13]
* **Facility access and Control –** Only limited and authorized persons should be allowed to access the physical assets. There should be a strict restriction for transfer, removal, disposal, and reuse of data e-media. [15]

**CHAPTER-5**

**SYSTEM REQUIREMENTS**

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

**5.1 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

**5.2 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

● Python Libraries in the requirements file.

**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>

1. Cybersecurity Frameworks Comparing, Contrasting and Mapping **-** Matthew Hudnall, The University of Alabama - IEEE Computer Society
2. 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
3. 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
4. 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>
5. 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
6. Cobit: An International Source for Information Technology Controls - John Lainhart IV - EDPACS Newsletter
7. ISO/IEC-27001

<https://www.iso.org/isoiec-27001-information-security.html>

1. 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
2. ISA/IEC 62443 standard

<https://www.iec.ch/blog/understanding-iec-62443>

1. IEC 61850 standard

<https://ieeexplore.ieee.org/abstract/document/7543038>

1. Applying a holistic cybersecurity framework for global IT organizations – Maurice Dawson
2. Information Security – The Complete Reference 2nd Edition - Mark Rhodes Ousley – McGraw Hill Education