



**OpenVuln Scanner**  
**OSINT Tool and Security Framework**

**U18CSP8701 - PROJECT PHASE-II 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)**

**APRIL 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**

Dr P. Devaki

**HEAD OF THE DEPARTMENT**

Professor and Head

Computer Science and Engineering

Kumaraguru College of Technology

Coimbatore-641049

**SIGNATURE**

Dr. N. Suganthi,

**PROJECT GUIDE**

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**

## DECLARATION

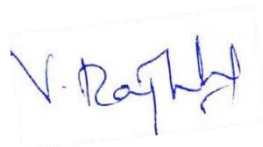
We affirm that the project work titled “OpenVuln Scanner” being submitted in partial fulfillment for the award of B.E Computer Science and Engineering is the original work carried out by us. It has not formed the part of any other project work submitted for the award of any degree or diploma, either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



**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 **Dr. L. Latha** 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 NO	TITLE		PAGE NO
	ABSTRACT		5
1	INTRODUCTION		7
2	LITERATURE REVIEW		8
3	EXISTING SYSTEM		11
	3.1	DRAWBACKS OF EXISTING SYSTEM	12
4	PROPOSED SYSTEM		13
	4.1	BLOCK DIAGRAM	13
	4.2	IMPLEMENTATION	14
	4.3	METHODOLOGY	15
	4.4	SECURITY FRAMEWORK	24
5	PERFORMANCE REVIEW		25
6	SYSTEM REQUIREMENTS		27
	6.1	HARDWARE REQUIREMENTS	27
	6.2	SOFTWARE REQUIREMENTS	27
7	ADVANTAGES & LIMITATIONS		28
8	CONCLUSION AND FUTURE WORK		29
9	PLAGARISM REPORT		30
10	REFERENCES		31

# **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**

NIST focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. It 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. [1]

The protection of Controlled Unclassified Information (CUI) resident in non-federal 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. It provides federal agencies with recommended security requirements for protecting the CUI in a non-federal system and organization. [2]

Security governance brings together all the basic elements of cyber defence and effective risk management. Without this governance, dangerous gaps persist and assets are inevitably compromised. Governance is the mechanism by which these risk values are reflected in the direction and judgment that determine business plans, information architecture, security policies and procedures, and operating practices. Compliance audits and reviews are the 'secret ingredients' that ensure security policies and processes are strictly adhered to, by the company's risk or security management strategy. [3]

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.[5]

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. [7]

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 include 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. [8]

Cybersecurity can be broken into these three core areas - education, policy, and technologies. The education part provides insight on innovative ways to teach cybersecurity coursework to include discussing the accrediting bodies for programs related to information technologies (IT) or computer science. An organization must review governing policies, tools, and techniques that can be brought forward in cybersecurity education. The policy theme of the framework incorporates multiple directives, standards, mandates, laws, and best practices. In the US, these can include policies from the Department of Défense (DoD), National Institute of Standards and Technology (NIST), US military, and more. These policies provide the baseline for further guidance and direction for organizations to set their own policies. The technologies portion of the framework brings in data about emerging technologies such as those that include Internet-enabled devices. These technologies include mobile phones, operating systems (OSs), software,

and other devices that undergo a review of security posture to ensure compliance cybersecurity policies. [14]

Opensource intelligence developed along with technological innovation. Many actors, including business corporations, antisocial individuals, governmental organisations, law enforcement agencies, etc., have been persuaded to incorporate opensource intelligence for their own gain by the enormous amounts of data that have accumulated in the public domain as a result of the development of social media platforms. The accessibility to the internet has made it possible for people to easily locate and post any kind of information. (Edwards et al., 2017) [19]

According to Hayes & Cappa (2018) [21], OSINT can be used to perform risk analyses for the business in order to guard against future cyberattacks on its vital infrastructure, which was a component of the US electrical grid. The company's network, apps, devices, and crucial IT resources were profiled using a vulnerability assessment and other open-source intelligence analysis processes.

Wiradarma & Sasmita (2019) [22] suggested a similar approach for examining website vulnerabilities. The victim's information is gathered from open sources using OSINT tools like Maltego and others during the information gathering stages of penetration testing. Combining information from OSINT, penetration testing, and the ISO 31000 risk assessment standard resulted in a suggestion for system improvement.

## 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.

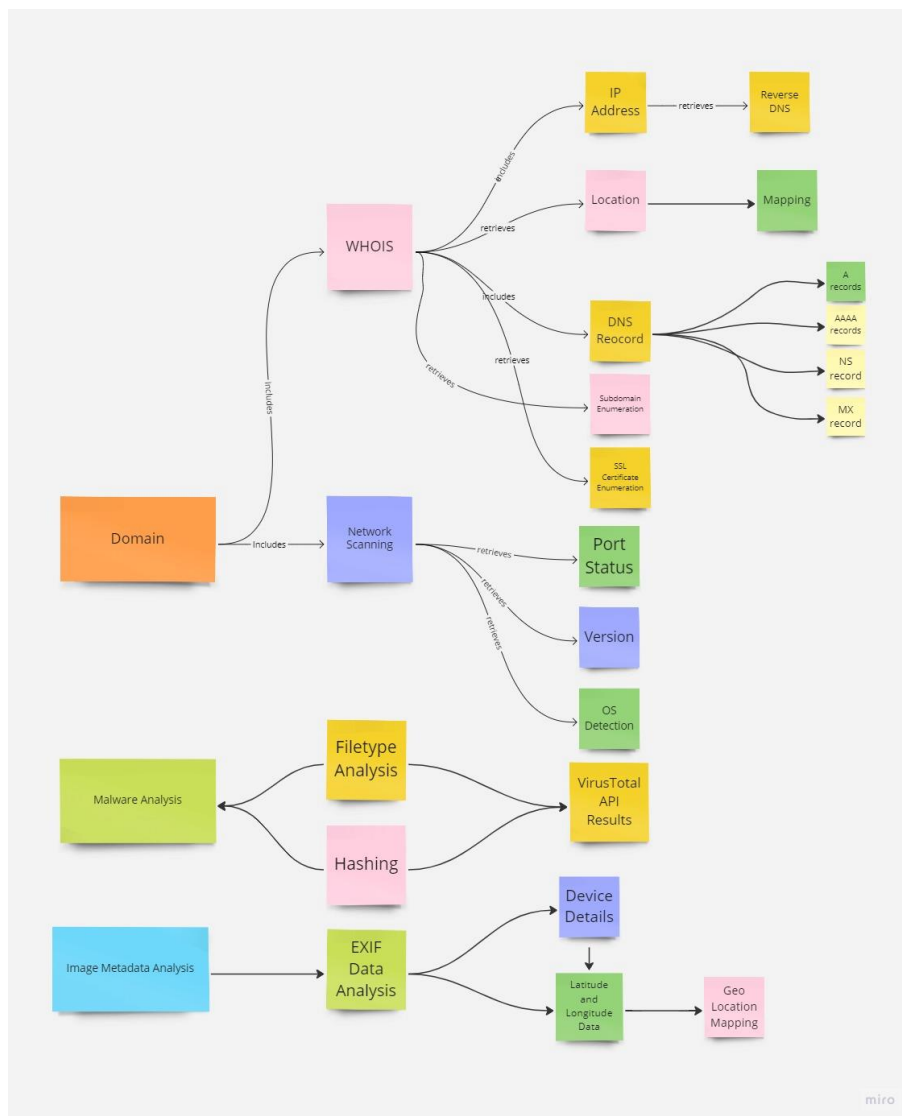
Like this problem, the forementioned tools are mostly freemium – meaning though free versions of those tools are available, they do not offer you a lot of features that the paid, premium version do. The price of these tools is too high such that an individual who wants to experience the full potential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

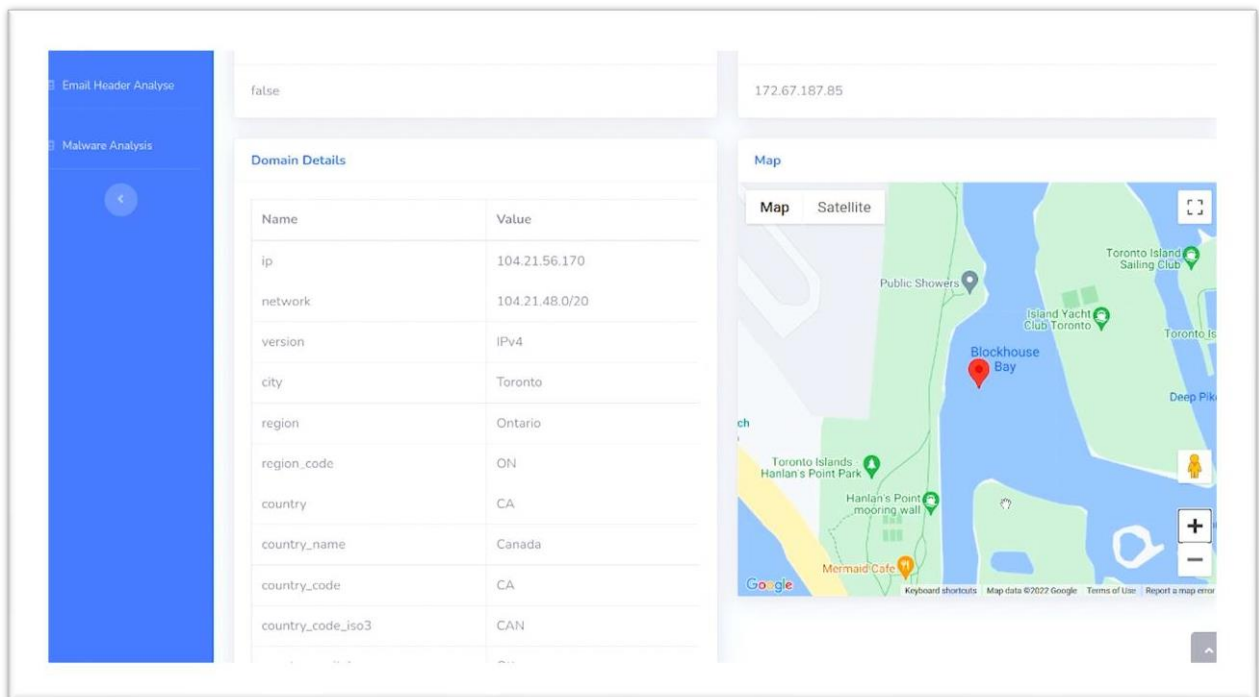


**Figure 4.1.a Block Diagram of Open Vuln Scanner**

## 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.



**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.

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,ju
country_area	9984670
country_population	37058856
asn	AS13335
org	CLOUDFLARENET

**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.

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. 4.3.2.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.



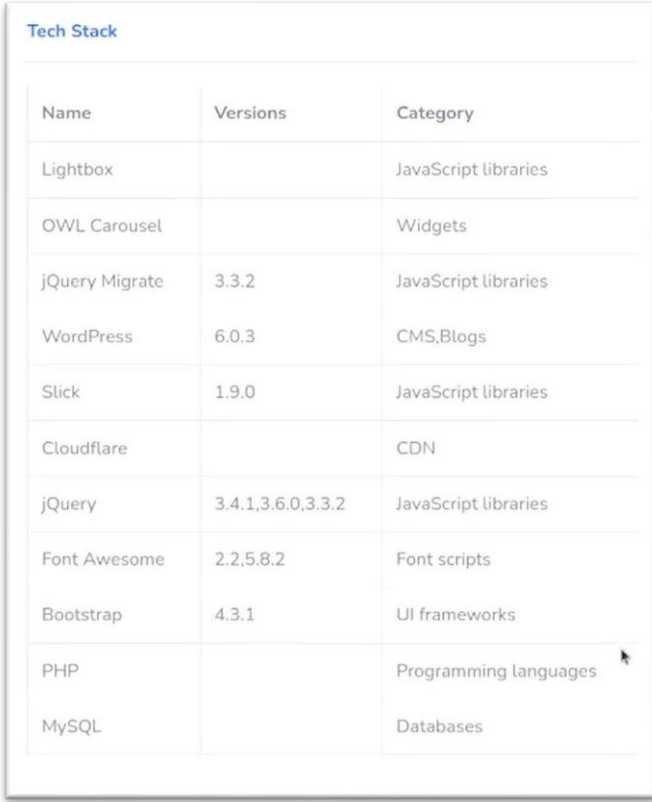
The screenshot shows a web interface titled "Os Scan" in blue text. Below the title is a table with three columns: "Accuracy", "CPE", and "Name". The table contains three rows of data representing detected Linux kernels.

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. 4.3.3.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.



The screenshot shows a web interface titled "Tech Stack" in blue text. Below the title is a table with three columns: "Name", "Versions", and "Category". The table lists various web technologies and their associated versions or categories.

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. 4.3.4.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

- 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 10
TXT	"v=spf1 ip4:182.72.162.18 ip4:103.196.28.200 include:spf.protection.outlook.com verification=uuQoqdzvRL5v6Q57k5VBwjACGkuzTM","hmqh33 domain-verification=3mmmicba7b1tgpbu1ybhszadm3m8pe","v include:spf.protection.outlook.com ~all"

**Fig. 4.3.5.a DNS Records**

### 4.3.6. Sub-domain Enumeration

Sub-domain enumeration module enumerates the sub-domain related to the domain. The details in **Fig. 4.3.6.a** helps to broaden the attack surface, find hidden applications, and forgotten sub-domains. 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. 4.3.6.a Sub-domain 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.

SSL Validation				
Logged At	Not Before	Not After	Common 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. 4.3.7.a** SSL Certificate Enumeration

### 4.3.8. E-Mail Header Analysis

The tool also includes an email header analysis module which analyzes the email header of any email and gathers valuable information about the sender, the recipient, and the email's path through various email servers. The analysis can provide details such as the IP address of the sender, the email client used, the date and time the email was sent, and other important metadata as shown in **Fig 4.3.8a**. This can be useful in identifying potential phishing or spoofing attempts, as well as tracking down the source of suspicious emails. The email header analysis module in our tool provides a user-friendly interface to view and analyze email headers, and also includes a visual representation of the email's path through various email servers. With this module, our tool provides a comprehensive solution for conducting Open-Source Intelligence (OSINT) on a domain or organization, including both technical and non-technical information.

The screenshot displays a web-based interface for email header analysis. It features a central 'Summary' section with a table of email metadata, and two side-by-side sections for 'Emails Mentioned' and 'Urls Mentioned'.

Summary	
From	Pantech E Learning <certificate@pantechelearning.com>
To	RAJHESHWAR <rajheshwar02@gmail.com>
Cc	content-type:from:subject;to;bh=q3TZVlKpNckRlvsUqgUrszrZYKxO9fkQMvIVSK7;b=dOFEUIK7z19yC0alt6K85afYfZcbaqOOPeFUm4DFy/Fh+is1ImzdzhZvbaS44nxRtzQFXQyPi60Pev8h0Ub8xKE8xGr+JBg7x8pjXH6EPn3nEzk5WZG05ZdQ=
Subject	🔥 30 Days Masterclass on React JS - Open Source Li
MessageID	<d0uonn6zdvu0h4qekdqum@convertkit-mail2.com>

**Emails Mentioned**

- gmail.com@ckespa.pantechelearning.com
- rajheshwar02@gmail.com
- certificate@pantechelearning.com
- d0uonn6zdvu0h4qekdqum@convertkit-mail2.com
- abuse@convertkit.com

**Ip's Mentioned**

- 023.03.29.19
- 149.72.61.159

**Urls Mentioned**

- https://unsubscribe.convertkit-mail2.com/d0uonn6zdvu0h4qekdqum
- https://click.convertkit-mail2.com/d0uonn6zdvu0h4qekdqum/m2h7h5h8k24ex8cm/a=
- https://forms.gle/vkr3QTecvaXp8v5i8
- https://unsubscribe.convertkit-mail2.com/d0uonn6zdvu0h4qekdqum
- https://preferences.convertkit-mail2.com/d0uonn6zdvu0h4qekdqum
- https://click.convertkit-mail2.com/d0uonn6zdvu0h4qekdqum/dpkeh0h0zdp5xehm/a=

**Fig 4.3.8a E-mail header analysis**

### 4.3.9. Malware Analysis

Malware analysis is the process of analyzing malicious software, or malware, to determine its functionality and behavior. The goal of malware analysis is to identify how the malware works, what damage it can cause, and how to mitigate or eliminate its impact.

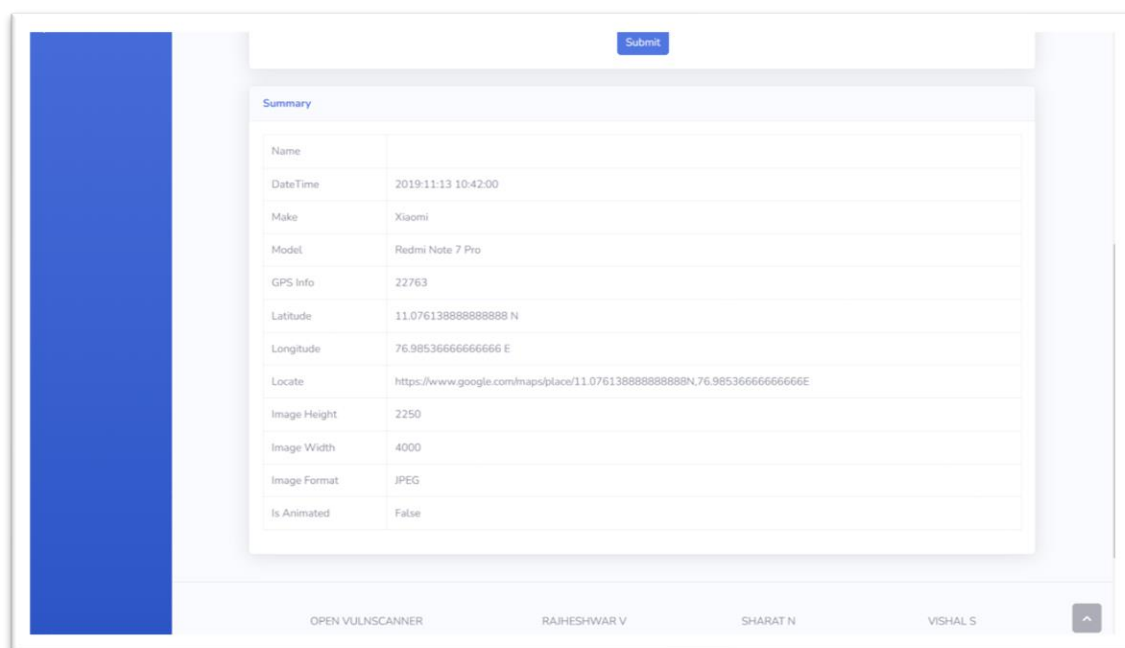
The malware analysis module of our tool is designed to detect and analyze any potential malware. The module utilizes various techniques such as file-type detection and malware signature-based detection. The malware analysis feature detects the file type and does creates a signature of the entire file. It then scans the file for malicious signatures with respect to the signature database. The feature also uses the VirusTotal API to generate a report based on the result of the scan as shown in **Fig 4.3.9a**. By detecting and analyzing malware, the tool helps organizations to prevent potential data breaches, protect their customers' data, and maintain their reputation.

Summary	
FileType	The filetype is /home/falcon/Desktop/Git Repo/Final-Year-Project/Feb/Spoor/media/media/786ab616239814616642ba4438df78a9_CcKh1y0.bin: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
Hashing	a29d02251f54567edb1d32f7c17ce4c04d5c54e317eb3b2bea2a068da728e59a /home/falcon/Desktop/Git Repo/Final-Year-Project/Feb/Spoor/media/media/786ab616239814616642ba4438df78a9_CcKh1y0.bin
Virus Total	{ "results": { "response_code": 0, "resource": "833c7210625f66cd447a42a80172548d7287d13a3ca10cbbec4add615678db7e", "verbose_msg": "The requested resource is not among the finished, queued or pending scans" }, "response_code": 200 }

**Fig 4.3.9a Malware Analysis**

### 4.3.10. Image Metadata Analysis

Image Metadata analysis is a valuable addition to our tool as it allows for a more comprehensive investigation of a target. In addition to the various modules described earlier, the tool also includes a metadata analysis module that can extract and analyze metadata from files such as images, documents, and PDFs. The metadata may contain sensitive information such as GPS coordinates, author names, and creation dates that can be used to track the origin of the file or reveal other useful details. The module can quickly scan and extract metadata from large numbers of files, providing valuable insights into an organization's digital assets. This feature eliminates the need for manual metadata analysis and allows for a more efficient and thorough assessment.



The screenshot displays a web application interface for image metadata analysis. A blue sidebar is on the left. The main content area has a 'Submit' button at the top right. Below it, a 'Summary' section contains a table with the following data:

Name	
DateTime	2019:11:13 10:42:00
Make	Xiaomi
Model	Redmi Note 7 Pro
GPS Info	22763
Latitude	11.076138888888888 N
Longitude	76.98536666666666 E
Locate	<a href="https://www.google.com/maps/place/11.076138888888888N,76.98536666666666E">https://www.google.com/maps/place/11.076138888888888N,76.98536666666666E</a>
Image Height	2250
Image Width	4000
Image Format	JPEG
Is Animated	False

At the bottom of the interface, there is a footer with the text 'OPEN VULNSCANER', 'RAJHESHWAR V', 'SHARAT N', and 'VISHAL S'.

***Fig 4.3.10a Metadata Analysis***

#### **4.4. Security Framework:**

The tool generates a comprehensive report with respect to the in-house proposed security framework that includes information about the organization's security posture and gives a score that indicates the level of security of the organization.

The OSINT analysis includes gathering information about the organization's web presence, domain registration details, SSL certificate information, and email header analysis. It also includes a technology stack detection module that identifies the web framework, plugins, and security systems used by the organization. This information can be useful in identifying vulnerabilities and weaknesses in the organization's security posture.

The vulnerability assessment part of the framework involves running a suite of vulnerability tests to identify potential vulnerabilities in the organization's web assets. The tests include port scanning, network scanning, operating system detection, and service detection. These tests can help identify weaknesses in the organization's infrastructure and web applications that could be exploited by attackers.

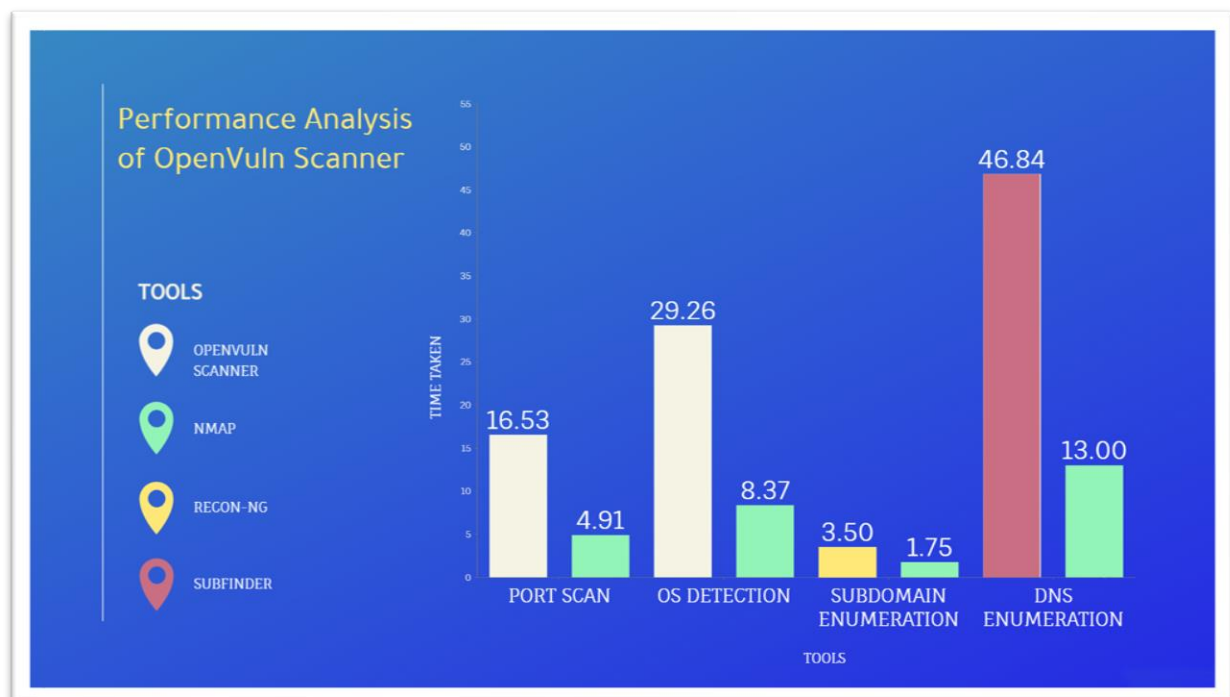
The generated report complies with industrial-level standard security frameworks providing a detailed analysis of the organization's security posture and includes recommendations for improving security. The report's score provides an indication of how secure the organization is and can be used as a baseline for future security assessments. Overall, the tool combined with the proposed framework provides a robust and thorough analysis of an organization's security posture that can help identify vulnerabilities and improve the organization's overall security.



## CHAPTER-5

### PERFORMANCE REVIEW

The cloud platform hosting and lightweight framework used in the tool make it highly performant compared to other tools that require local installation and utilize local computing resources. The tool's deployment on cloud platforms like Azure ensures that it benefits from high-performance cloud IaaS infrastructure, resulting in faster performance and reduced latency. Moreover, the tool's use of lightweight frameworks like Django complements its performance by providing a minimalistic and efficient environment for executing code. The combination of cloud hosting and lightweight frameworks makes the tool highly responsive, reducing the time taken for scans and assessments. Performing a comprehensive assessment and enumeration of a whole domain can be a time-consuming process, and the proposed tool is no exception. However, this is a trade-off for the comprehensive and detailed analysis that the tool provides. In comparison to other tools available in the market, the time taken by the proposed tool is similar, if not better, considering the comprehensive nature of its analysis.



(Fig 7.1) Performance metrics of the application

In our research, we compared the proposed framework with other existing frameworks and found that it is more comprehensive and covers all security aspects of an organization. Unlike other security guidelines such as HIPAA, which focus on only one security aspect such as the storage of health data, our proposed framework covers all aspects of security, making it a wholesome solution. Furthermore, the proposed framework allows organizations to create a security policy that is tailored to their specific needs rather than providing one-size-fits-all guidelines. This level of customization ensures that organizations can develop a security policy that is practical, effective, and feasible for their specific environment. Overall, our performance review indicates that the proposed framework is a robust and comprehensive solution for enhancing the security posture of organizations. Overall, the proposed tool along with the framework provides a good balance between performance and comprehensive analysis, making it a valuable addition to any security team's arsenal.

## **CHAPTER-6**

### **SYSTEM REQUIREMENTS**

The OpenVuln 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
- Python Libraries in the requirements file.

## **CHAPTER-7**

### **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-8**

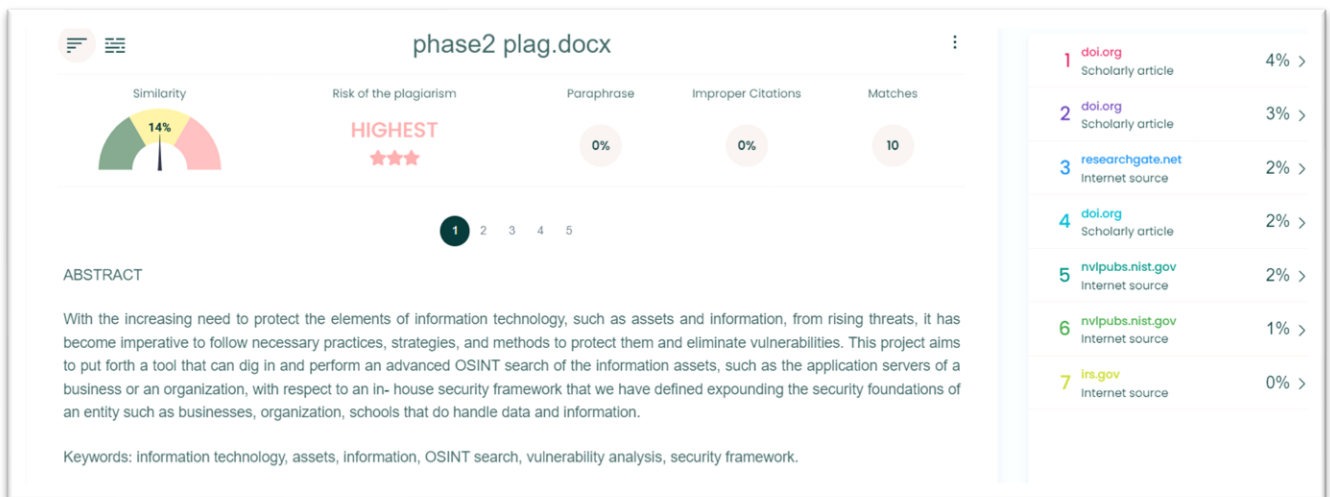
### **CONCLUSION AND FUTURE WORK**

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-9

## PLAGARISM

## REPORT



## **CHAPTER-10**

### **REFERENCES**

1. Framework for Improving Critical Infrastructure Cybersecurity (APRIL 2018) – NIST <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>
2. Ron Ross, Patrick Viscuso, Gary Guissanie , Kelley Dempsey, Mark Riddle (2020) -Protecting Controlled Unclassified Information in Non-federal Systems and Organizations - National Institute of Standards and Technology
3. Matthew Hudnall, The University of Alabama (29 March 2019) - Cybersecurity Frameworks Comparing, Contrasting and Mapping - IEEE Computer Society
4. Yogish Pai, U. & Krishna Prasad, K. (2021). Open Source Intelligence and its Applications in Next Generation Cyber Security - A Literature Review. International Journal of Applied Engineering and Management Letters (IJAEM)
5. Rodney Petersen Danielle Santos; Karen A. Wetzel Matthew C. Smith , Greg Witte (NOVEMBER 2020) - National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework - NIST Special Publication 800-181
6. Jaime Campos Pankaj Sharma Erkki Jantunen (2016) - The challenges of cybersecurity frameworks to protect data required for the development of advanced maintenance - 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](https://doi.org/10.1007/978-3-319-47671-1_14)

8. Abel Yeboah-Ofori, Allan Brimicombe (2018) - Cyber Intelligence and OSINT: Developing Mitigation Techniques against Cybercrime Threats in Social Media- International Journal of Cyber-Security and Digital Forensics (IJCSDF) - Hong Kong
9. John Lainhart IV - Cobit: An International Source for Information Technology Controls - EDPACS Newsletter
10. 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
11. Maurice Dawson (2018) - Applying a holistic cybersecurity framework for global IT organizations –
12. Information Security – The Complete Reference 2<sup>nd</sup> Edition - Mark Rhodes Ousley – McGraw Hill Education
13. Hassan, N. A., & Hijazi, R. (2018). The evolution of open Source intelligence. In Open source intelligence methods and tools a practical guide to online intelligence (pp. 11–11). essay, APRESS.
14. Glassman, M., & Kang, M. J. (2012, March). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Computers in Human Behavior, 28(2), 673–682.
15. Klaus, S., Franziska, S., & Reiner, C. (2020). Conception and implementation of professional laboratory exercises in the field of open source intelligence (OSINT). Society for Imaging Science and Technology, 2020(3), 1-99.
16. Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017, August).



Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security*, 69, 18–34.

17. Lee, S., & Shon, T. (2016). Open source intelligence base cyber threat inspection framework for critical infrastructures. 2016 Future Technologies Conference (FTC), 4(1), 1375-1384.
18. Hayes, D. R., & Cappa, F. (2018, September). Open-source intelligence for risk assessment. *Business Horizons*, 61(5), 689–697.
19. Wiradarma, A. A. B. A., & Sasmita, G. M. A. (2019, December 8). IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company). *International Journal of Computer Network and Information Security*, 11(12), 17–29.
20. Herrera-Cubides, J. F., Gaona-García, P. A., & Sánchez-Alonso, S. (2020, October 29). Open-Source Intelligence Educational Resources: A Visual Perspective Analysis. *Applied Sciences*, 10(21), 7617.
21. Yassine Maleh, Mamoun Alazab, Mustapha Bellaissaoui (2022) - IT Governance and Information Security – Guides, Standards and Frameworks -  
[https://www.researchgate.net/publication/356649134\\_IT\\_Governance\\_and\\_Information\\_Security\\_Guides\\_Standards\\_and\\_Frameworks](https://www.researchgate.net/publication/356649134_IT_Governance_and_Information_Security_Guides_Standards_and_Frameworks)
22. ISA/IEC 62443 standard  
<https://www.iec.ch/blog/understanding-iec-62443>
23. IEC 61850 standard  
<https://ieeexplore.ieee.org/abstract/document/7543038>
24. ISO/IEC-27001  
<https://www.iso.org/isoiec-27001-information-security.html>