

DART | DATA ANALYSIS FOR RED TEAMER

Submitted in partial fulfillment of the
requirements for the award of
Bachelor of Technology degree in Information Technology

By

B PRIYADHARSHANI (Reg.No - 39120086)
M KALAIVANI (Reg.No – 39120050)



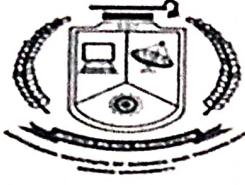
DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF COMPUTING

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

**Accredited with Grade “A” by NAAC | 12B status by UGC | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHISALAI,
CHENNAI - 600119**

MAY - 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **B Priyadharshani** (Reg.No - 39120086) and **M Kalaivani** (Reg.No - 39120050) who carried out the Project Phase-2 entitled "**DATA – DATA ANALYSIS FOR RED TEAMER**" under my supervision from January 2023 to May 2023.

24/4/23
Internal Guide

Dr. A. SIVASANGARI, M.E., Ph.D

10/5/23
Head of the Department

Dr. R. SUBASHINI, M.E., Ph.D.

Submitted for Viva voce Examination held on 10/05/2023

[Signature]
Internal Examiner

[Signature]
External Examiner

DECLARATION

I, **B PRIYADHARSHANI** (Reg.No- 39120086), hereby declare that the Project Phase-2 Report entitled “**DART | DATA ANALYSIS FOR RED TEAMER**” done by me under the guidance of **Dr. A. SIVASANGARI, M.E.,Ph.D** is submitted in partial fulfillment of the requirements for the award of a Bachelor of Technology degree in Information Technology.

DATE: 10/05/2023

PLACE: Chennai



SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA UNIVERSITY OF SCIENCE AND TECHNOLOGY** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph. D, Dean**, School of Computing, **Dr.R.SUBASHINI M.E., Ph.D.**, Head of the Department of Information Technology for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. A.SIVASANGARI M.E., Ph.D.**, for her valuable guidance, suggestions, and constant encouragement paved the way for the successful completion of my phase-1 project work.

I wish to express my thanks to all the Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project.

ABSTRACT

Information Gathering and Enumeration / Scanning place a vital role in Ethical Hacking/Penetration Testing. The more they enumerate the more they get access to the enumeration part of penetration testing is a little bit time-consuming because of using multiple tools, several scripts, and comprehensive strategies in single scripts so it is unified. It works very exceedingly fast. The result will be more precise and accurate when using comprehensive scripts. Data Analysis for Red Teamer is a CLI-based Pentesting Tool, which is only supported in Linux (Debian) Operating System. It will give proper results and valuable data is important to test. This is applicable in the field of security professions and pen testers. It will cover a big range of audiences in security aspects DART helps Penetration Testers / Red Teamers to enumerate information in various technologies like Networking, Web applications, Open Source Intelligence (OSINT), and Cryptography. It uses the utility of security tools like Nmap, Nmap Scripting Engine (NSE), Whois-lookup, OSINT framework, Hash-Identifier, Hashcat, John the Ripper, and API. DART helps Penetration Testers / Red Teamer to navigate quickly and uses the full potential of the listed tool with a single comprehensive script. Data Analysis for Red Teamer uses the efficacy of Nmap (Network Mapper) for Network Enumeration. Nmap is while performing penetration testing. Open source Linux command-line program nmap is used to search open ports, detect the vulnerability, host detection, and operating system. Web Enumeration is a bit tougher than host discovery. It uses a particular methodology to uncover everything about a target web service. The open-source paradigm emphasised the collection of information using free programs. various public platforms, or resources. Another absolute necessity to safeguarding data in communications systems is cryptographic protocols. Cryptography diagnoses the hash type, and hash crack and encrypts the hash passwords.

TABLE OF CONTENTS		
Chapter no	TITLE	Page No
	ABSTRACT	v
	LIST OF FIGURES	vii
	LIST OF ABBREVIATIONS	viii
1	INTRODUCTION	9
	1.1 What is data Analysis	9
	1.2 What is cyber security	9
	1.3 Enumeration	10
2	LITERATURE SURVEY	11
	2.1 Inferences from the literature survey	14
3	REQUIREMENT ANALYSIS	15
	3.1 Software requirements	15
	3.2 VM Ware	15
	3.3 Kali Linux	15
	3.4 Metasploitable	16
	3.5 Visual Studio Code	17
	3.6 Python3	18
	3.7 Bash	18
4	DESCRIPTION OF THE PROPOSED SYSTEM	19
	4.1 Selected Methodology or proposed model	19
	4.2 System Architecture for the proposed system	29
	4.3 Description of Software for Implementation and Testing Plan of the Proposed System	30
	4.4 Project Implement plan	30
5	IMPLEMENTATION	31
	5.1 Commands involved in the tool	31
6	RESULT AND DISCUSSIONS	34
7	CONCLUSION	35
	7,1 Conclusion	35
	7.2 Future Scope	35
	REFERENCES	36
	APPENDIX	38
	A. SOURCE CODE	38
	B. SCREENSHOTS	49
	C. RESEARCH PAPER	56

LIST OF FIGURES

FIGURE NO.	FIGURE NAME	PAGE NO.
3.1	VM Ware	15
3.2	Kali Linux in VM ware	16
3.3	Metasploitable	17
3.4	Visual Studio Code	17
3.5	Logo of Bash	18
4.1	Techniques of Network Enumeration	20
4.1	Working of Nmap	21
4.2	Nmap detected the service version	21
4.3	OS detects the Mac address, type, etc	22
4.5	Rules and Scripts of NSE	24
4.6	Display ISP's on the map	26
5.1	Confirms the folder and path	31
5.2	List the tools using various technologies	31
5.3	Network Enumeration	32
5.4	A basic operation in Web Enumeration	32
5.5	Beginning process of prefix with phone number	33
5.6	SHA256 Hash Generator	33

LIST OF ABBREVIATIONS

ABBREVIATIONS	EXPANSIONS
OS	Operating System
CLI	Command Line Interface
GUI	Graphical Line Interface
BASH	Bourne Again shell
NSE	Nmap Scripting Engine
TLD	Top Level Domain
NMAP	Network Mapper
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
IP	Internet Protocol

CHAPTER 1

INTRODUCTION

1.1 What is Data analysis

Data Analysis is the process to focuses on scanning and examining network traffic data, with the intention of prohibiting or rapidly diagnosticate spiteful tasks. Data analysis helps particular companies make sense of data. Data analysts consistently analyze primary data for penetration and tendency. They use numerous tools and approaches to help organizations make decisions and achieve. Red teaming is the practice of testing the security of an organization's systems by imitating a spiteful actor and managing secure systems or data. A red team can be an extrinsically compressed group of penetration testers or a team within your own organization. Red teamers provide a way for companies to test their defenses in (nearly) real-world conditions. By allowing red teams to conduct attacks without warning, enterprises can see how their existing security practices work in response to emerging threats.

The software application, router, web service, as well as online version, be tested using only a method called pen testing to identify and exploit frailty Penetration testing is mandatory, isolated from appraising security, to also evaluate the efficacy of protection systems and security approaches. Each sort of desktop application, and device, including software, requires a security audit. and architecture. A process that looks at a network, piece of technology, or internet that can find its defects, as well as gaps, is characterized as vulnerability analysis.

1.2 What is cyber security

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as Information Technology Security, Ethical Hacking It is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. It is otherwise known as Computer Security or Information Technology security. There are Five stages in Cybersecurity. They are,

- Information Gathering
- Enumeration /Scanning
- Vulnerability Assessment

- **Reporting**

Information Gathering and Enumeration play a vital role in Cybersecurity

A defense of networks and machines against mandatory disclosure, corruption, **or** destruction of their equipment, programming, or metadata, along with the distortion or manipulation of amenities they provide, is regarded as ethical hacking, occasionally referred to as security in the field of information technology. It is sometimes described as data security measures as well as information assurance. Cybersecurity is broken down into five categories. Getting data, Penetration testing, Security Testing, Trying to exploit, and Disclosure **is** just a few of these activities. DART, however, only addresses the initial three cybersecurity levels.

As is appropriate, network security has grown to be among the top priorities in the modern world, including both individual users and programmers. The predominant aim of this system is to discover the operating system, host detection, scan open ports and detect vulnerabilities. Then it gives protection to secure the web-based system as well as illustrates every aspect of the program's features Next, the OSINT framework will outcome gather information about an individual or organization. After using Cryptography is an essential appliance for securing information in the computer, and it will examine the hash type and encrypts the hash passwords.

1.3 Enumeration

The enumeration in cyber security is extracting a system's valid usernames, machine names, share names, directory names, and other information. It is a key component of ethical hacking and Penetration Testing, as it can provide attackers with a wealth of information that can be used to exploit vulnerabilities. Enumeration can be used to find security vulnerabilities within systems and networks. By conducting an enumeration scan, you can see what ports are open on devices, which ones have access to specific services, and what type of information is being transmitted. This information can then be used to exploit weaknesses and gain unauthorized access. Enumeration is also called as Information Gathering Phase which is the first phase. It establishes an active connection to the system at this point and launches directed queries to learn more about the target. Enumeration is very important to programmers, as it poses significant challenges to the security of any system. Secure programming is emerging as an important concept because of enumeration.

CHAPTER 2

LITERATURE SURVEY

In 2016, Jai Narayan Goell et al, and BM Mehtre² et al. demonstrated how to use the Vulnerability assessment mechanism in its entirety as well as highlighting how it may be leveraged like a threat detection tool. A User acceptance testing enzyme's whole duration has been covered. Researchers have compiled a list of the world's top User acceptance testing programs, including gnu and widely viable, alongside details about the best ways to utilize tools as well as which virtual machines they are interchangeable with. Such techniques can just be extremely helpful for appraisal and just use during the Vulnerability assessment cycle. Experts have decided that there is a need to employ Highlights the characteristics more frequently.

In 2017, Sangeeta Nagpure. Sonal Kurkure Webpage security is aided by a risk evaluation including security testing for web-based- based applications. Pen testing, as well as security testing, are two distinct sorts of security tools. This would be required to carry out two independent jobs, and sometimes with odd results, within an identical space. Assessments and intrusion detection systems for whichever corporation's competent in operating in the security environment. Considering the weaknesses, either a conventional or automated exposure test is feasible. Those who evaluated a variety of known issues within Online apps concurrently with security audits using fully accessible as well as paid Internet assault methods.

In 2016 Prashant S. Shinde¹ et al, and Shrikant B. Ardhapurkar² et al has proposed the Study of Information security Through Scanning and Threat Intelligence which the variety of methods being used risk assessments and vulnerability scanning are fully described (VAPT). Pay careful attention to awareness regarding cyber security as well as the significance of keeping an organization sheltered. Those who reach the conclusion that there exists a different kind of VAPT tools, and that since vulnerabilities continue to develop, the ability to adequately should indeed be modified to explore security flaws while also becoming more versatile such that attack pattern signatures could be decided to add.

In 2018, Hasan, Ashikali, Meva, and Divyakant, has proposed Security testing on secure web applications which uses fundamental security of web applications through the methodology of potential vulnerabilities and functional testing (VAPT). So several cognitive as well as operational weaknesses might affect software applications Vulnerabilities can happen due to

poor programming or an outdated system. VAPT process is specific access to secure the logical and extensive technical vulnerability.

In 2018, Dr. SurenderJangra, Dr. Pankaj Kumar Verma, and A Survey on Assessment of Vulnerability and Network Security by Penetration Testing approached this paper and The system security and scientific method for performing complex protection as well as its analysis were described. Also, it explored the frequently utilized techniques and tools for accumulating data and assessing weaknesses. Eventually, vulnerability scanning paradigms are examined in order to detect security flaws so that fixes can be developed to replace holes and enhance the protection of the system, intranet, or apps. A methodology is a combination of particular values, operations, and output values. It directs everyone on how to get to the outcome from input data. The phases of penetration testing: Establishing a goal,

In 2019, S.M. Zia Ur Rashid has proposed Identifying and Avoiding Mysterious Dns server Conquest Potential Threats Schema describing that perhaps just using a registry of domain names is a critical component both of internet safety and the web applications utilized. The confidentiality and functionality of its web addresses are completely the responsibility of such nameservers. Nevertheless, there is an opportunity to seize over all the subdomains from the external agencies as a result of delays in sample authentication and Whois configuration issues. Such articles layout just the consequences of the issue on the company and provide a comprehensive review of subdomain invasion.

In 2019. Goutam, Vijay, has suggested Online Safety is Improved by Risk Assessments and Ethical Hacking Applications that focus on web application security. Security care when this comes to organizations, and structures, including the financial services sector. The banking system is more influenced by these problems. To check the security of the web application. The organization executes penetration testing which points out the web application security and attack actions. The structure will be mapped out which will deliver more safety to such websites.

In 2020, R. Pandey, V. Jyothinda, and U. K. Chopra Network penetration as well as contingency planning: The deployable approach Integration highlights the significance and scalability of electronic objects to growing hazard analysis. It suggests employing a supervised infrastructure to perform testing and get real results. Using evaluation methods, the Pic Microcontroller 3b+

must have been utilized to examine, analyze the absorbency, and evaluate support and knowledge flaws.

In 2021, Amey Kanunje, and Sourabh Mahale, has suggested Penetration Testing and Vulnerability Assessment which describes organizations that no longer have privately operated data and display the client's individual details among the security holes that could have been repaired. On a Penetration test, they identify this problem early as an attacker, and they advise how to fix them and eliminate eventuality vulnerability.

In 2021. Tae Hyun Kim et.al has approached Using Domain names to deliver global authentication and authorization to consumers in a quick and effective way is described in a survey of domain name system vulnerabilities and assaults. Nevertheless, the Domain name was first created lacking encryption, thus the data is not secure. We provide an outline of DNS issues, DNS assaults, and sometimes even security measures. For the goal of protecting against the assaults that are introduced and assessed, strikes were segmented in-depth by strategy. Its collection's key discovery is the introduction of a weakness. a vulnerability

In 2021, A. S. B. Singh, Y. Yusof, and Y. Nathan has proposed EAGLE: GUI-Based Penetration Testing Tool for Scanning and Enumeration is a Visual interface application that has been initiated made facilitate the process for even novice security researchers to still do screening as well as quantification. As a corollary, the modification of something like a broad range of parameters used mostly by high-level- level programming languages is eliminated. It is simple to navigate and comprehend the scan facts thanks to the equipment-appropriate outcome presenting and sharpening plugin.

In 2022, C. DeCusatis, P. Peko, J. Irving, M. Teacher, C. Laibach, and J. Hodge, Accessibility towards conducting security audits to distant medical services using inexpensive, fully accessible methods but rather open standards intellectual prowess has now been recommended and assessed inside A Framework for Open Source Intelligence Penetration Testing of Virtual Health Care Services. A creative-level manual testing approach for behavioral health care is offered. Considering feasibility for multiple approaches, which list prevalent weaknesses as well as recommended techniques

In 2022. J K Periasamy, Dakinisiwari V, and Tapasya K has proposed Assessjet – Internet Fuzzing and Contingency Planning that assist there in the detection of errors in apps and websites. This is primarily consistent only with risk evaluation of online sites that utilizes user information Security Vulnerabilities can be explored by utilizing proper scanning tools on the back end. This method generates a wide range of reports that covers the disparate security menacing a website

2.1 INFERENCES FROM LITERATURE SURVEY

- In the enumeration environment of the network and web where testing is just a click away, good enumeration is essential for finding open ports, detecting the host, and operating the system.
- Keep factors of network enumeration are extracting network range and mapping the network.
- Domain name system is essential for web service and is responsible for the safety and functionality of the domain names

CHAPTER 3

REQUIREMENT ANALYSIS

3.1 SOFTWARE REQUIREMENTS :

- VMware (Virtualization)
- Kali Linux (Main Operating System)
- Metasploitable (Vulnerable Machine)
- Visual Studio Code (Text Editor)
- Python3
- Bash

3.2 VMware

- VMware is a software that enables users with virtualization
- It is a virtual machine software from VMWare.
- It enables multiple copies of the same operating system, or there can be several different operating systems that can run simultaneously on the same
- VMWare's virtualization technology one would be able to run another machine within another physical machine and perform all tasks.
- Hypervisor abstracts the software from PC's hardware and thus creates and manages the virtual machines



Fig 3.1 VM ware

3.3 Kali Linux

- Kali Linux is a Debian-based Linux distribution.
- Kali Linux is a specially designed OS for network analysts, Penetration testers.

- It is completely free and open source. So you can use it for free and even contribute for its development.
- That is easily accessible and offered for free to information security experts and enthusiasts.
- Supported Platform of the Metasploitable a vulnerable machine for developing and executing security exploits.

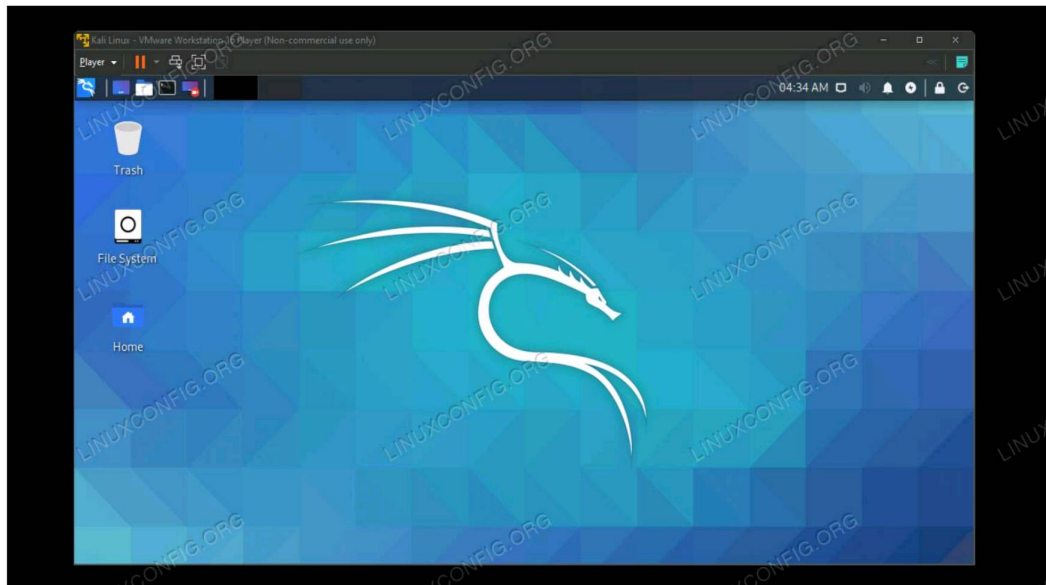


Fig 3.2 Kali Linux in VMware

3.4 Metasploitable:

- Metasploitable is a Vulnerable Machine.
- It is an open-source penetration testing and development platform.
- It provides to exploitation of a variety of applications, operating systems, and platforms. The main compone of Metasploits the module.
- It is easy to use Metasploit while conducting a large network penetration test. Metasploit conducts automated tests on all systems in order to exploit the vulnerability.
- Metasploit allows a clean exit from the target system it has compromised.
- There are six total module in Metasploitable are,
 - Exploits
 - Payload
 - Auxillary
 - Nops
 - Posts
 - Encoders

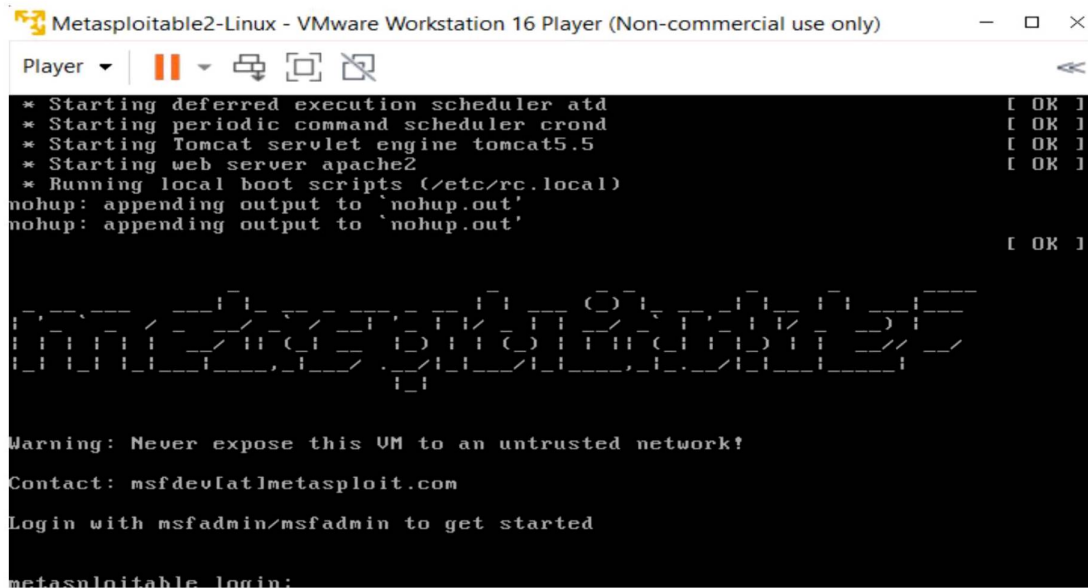


Fig 3.3 Metasploitable

3.5 Visual Studio Code

- Visual Studio Code, also commonly referred to as VS Code, is a source-code editor made by Microsoft with the Electron Framework, for Windows, Linux and macOS.
- Features include support for debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git.
- Users can change the theme, keyboard shortcuts, preferences, and install extensions that add additional functionality.
- In the Stack Overflow 2021 Developer Survey, Visual Studio Code was ranked the most popular developer environment tool among 82,000 respondents, with 70% reporting that they use it.

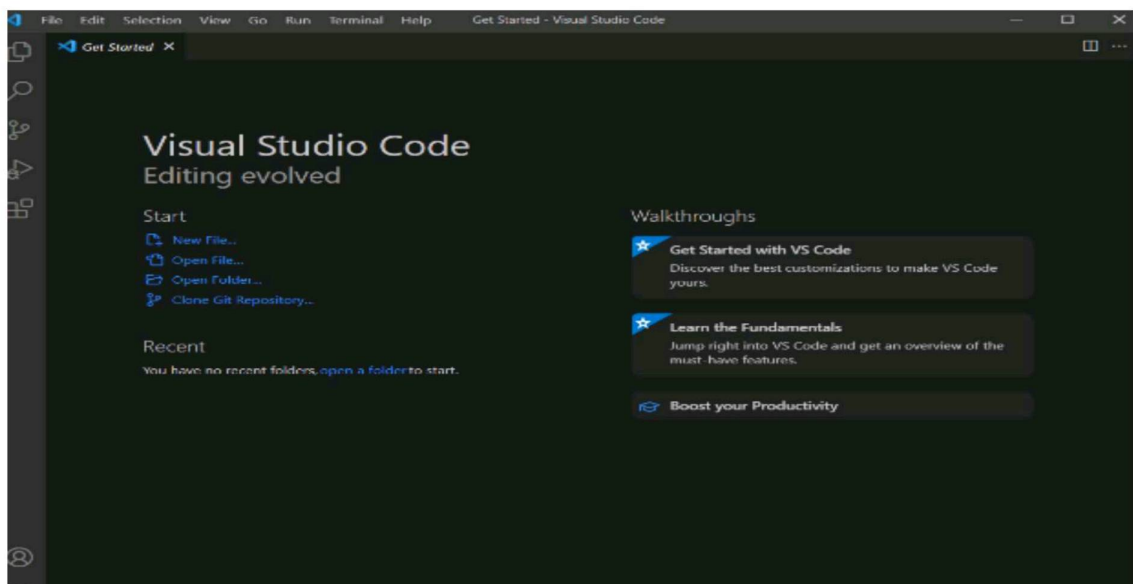


Fig 3.4 Visual Studio Code

3.6 Python3

- Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation.
- Python is dynamically-typed and garbage-collected.
- It supports multiple programming paradigms, including structured (particularly procedural), object-oriented and functional programming.
- It is often described as a "batteries included" language due to its comprehensive standard library.

3.7 Bash

- **BASH (BOURNE AGAIN SHELL)** is a shell program. SHELL Is the command interpreter for the Operating System.
- It is a command line language for UNIX-based Operating Systems. It allows you to control the computer like a developer
- It is a command language that allows us to work with the file on the computer in a way that's more efficient and powerful than a **Graphical User Interface (GUI)**
- It provides functional improvements over Bourne Shell for both programming and interactive use
- To save the file with the extension of **.sh**



Fig 3.5 Logo of Bash

CHAPTER 4

DESCRIPTION OF THE PROPOSED SYSTEM

4.1 SELECTED METHODOLOGY OR PROPOSED MODEL

Information is collected from a designated host or network through the method of network enumeration. We can utilize it to discover hosts, analyze open ports, as well as find security holes in computer systems. A component of "ethical hacking" for network security is networked scanning. Network enumeration may be carried out by certain penetration tests in an attempt to safeguard a software system. For network enumeration, choose any one tool, and then it asks you to type the IP address of the vulnerable machine. Once you completed typing of IP Address and then press enter it will give the result like the state of the port, vulnerability, operating system, services, how many ports are closed, and at last, it will display how long it takes for collecting that information

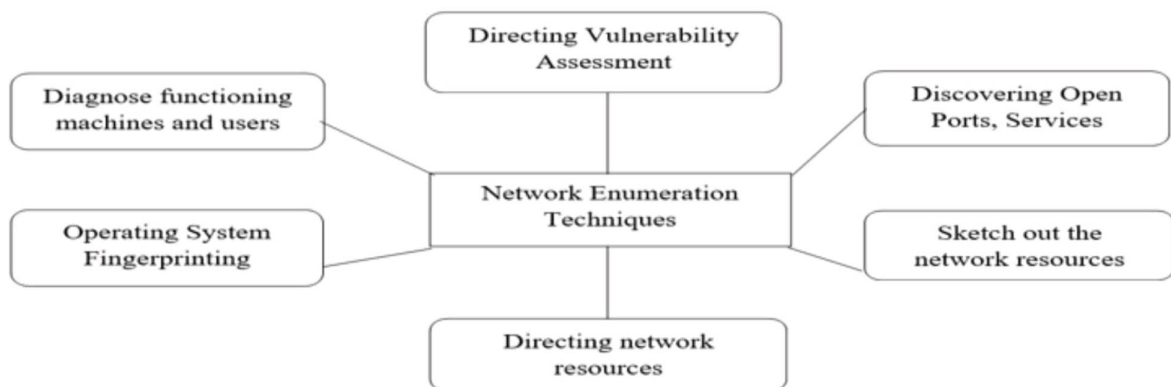


Fig 4.1 Techniques of Network Enumeration

Network Enumeration contains

- i)Nmap Comprehensive (all)
- ii)Nmap Service Version Detection
- iii)Nmap OS Detection
- vi)Nmap Live Host Detection
- v)Nmap Scripting Engine (NSE)

Nmap (Network Mapper) It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities. Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing. During security auditing and

vulnerability scanning, you can use Nmap to attack systems using existing scripts from the Nmap Scripting Engine

Nmap is a useful tool for network scanning and auditing purposes.

- It can search for hosts connected to the Network.
- It can search for free ports on the target host.
- It detects all services running on the host with the help of operating system.
- It also detects any flaws or potential vulnerabilities in networked system.

Advantages of NMAP:

- Nmap is open-source and **free** to use.
- It is used for auditing network systems as it can detect new servers.
- It will search for **subdomain** and Domain Name System.
- With the help of Nmap Scripting Engine (NSE), interaction can be made with the target host.
- It determines the nature of the service in the host and performs whether the host is a mail service or a web server:

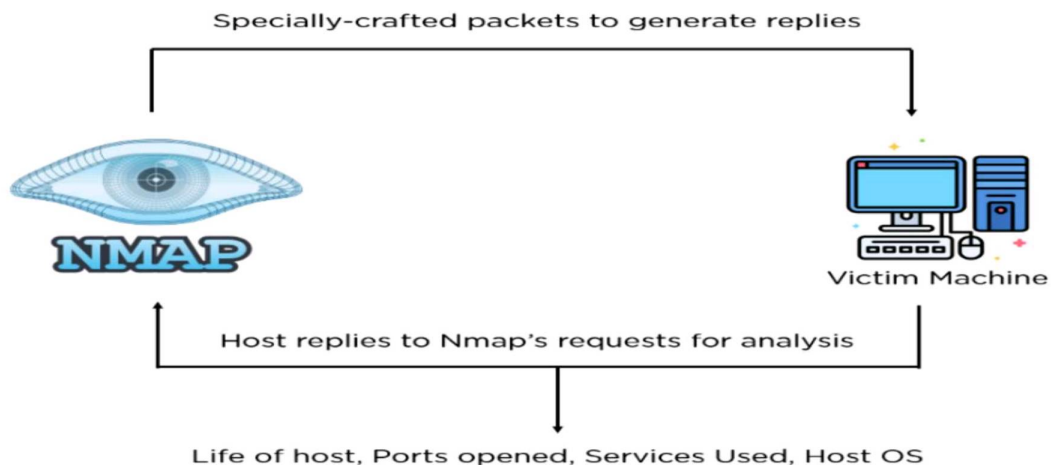


Fig 4.2 Working of Nmap

The nmap-service-probes database contains probes for querying various services and matching expressions to recognize and parse responses. Nmap might tell you that ports 25/tcp, 80/tcp, and 53/tcp are open. Nmap would report that those ports probably correspond to a mail server (SMTP), web server (HTTP), and name server (DNS) respectively. This lookup is usually accurate—the vast majority of daemons listening on TCP port 25 are, in fact, mail servers.

Version detection uses a variety of probes, located in the nmap-service-probes file, to solicit responses from the services and applications. Interrogating network services on remote devices to determine application name and version number. The exact version of a service is highly valuable for people looking for security vulnerabilities or monitoring their networks for any unauthorized Nmap queries the target host with the probe information and analyzes the response, comparing it against known responses for a variety of services, applications, and versions. Nmap tries to determine the following parameter are

- Service Protocol
- Application Name
- Version Number
- Hostname
- Device Type
- Operating System family

Both databases help Nmap first to detect the service behind the port such as ssh or http. Second, Nmap will try to find the software providing the service (such as OpenSSH for ssh or Nginx or Apache for http) and the specific version number.

```

IP >> 192.168.1.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-17 03:54 EDT
Nmap scan report for 192.168.1.6 (192.168.1.6)
Host is up (0.00026s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:55:C4:56 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.26 seconds
0

```

Fig 4.3 Nmap detected the service version

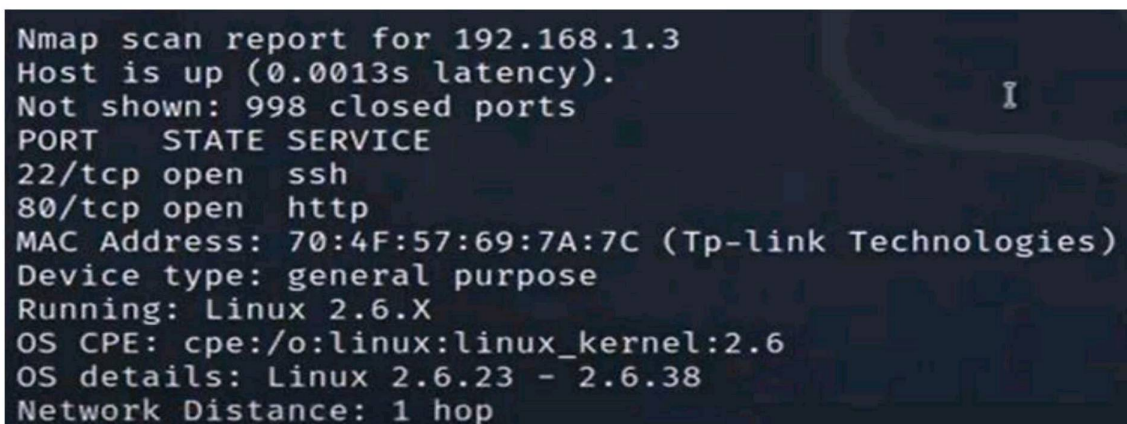
In the above picture this time Nmap detected openSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) behind port 22, Postfix behind port 25, and Apache httpd 2.2,8 ((Ubuntu) DAV/2) behind ports 80.

High speed, parallel operation via non-blocking sockets and a probe/match definition grammar designed for efficient yet powerful implementation. Determines the application name and version number where available—not just the service protocol. It will support both TCP and UDP Protocols.

To detect the operating system of a device, Nmap sends TCP and UDP packets to a port and analyzes its response. Operating System detection is also called fingerprinting. OS detection is far more effective if at least one open and one closed TCP port are found. We should know about the five separate probes being performed to determine the OS. There are five separate probes being performed. Each probe may consist of one or more packets. The response to each packet by the target system helps to determine the OS type

The five different probes are.:

- Sequence Generation
- ICMP Echo
- TCP Explicit Congestion Notification
- TCP
- UDP



```
Nmap scan report for 192.168.1.3
Host is up (0.0013s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 70:4F:57:69:7A:7C (Tp-link Technologies)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.23 - 2.6.38
Network Distance: 1 hop
```

Fig 4.4 OS detects Mac address, Device type et..

Live host detection is very important for pentester and ethical hacking. We are going to use Nmap in Kali Linux to scan the network for live hosts. Host discovery in Nmap is the process of gathering information about the host in the respective network. Host discovery is also known as ping scan. Nmap uses options like ping or built-in script to look after ports, services, and running servers on respective IPs using TCP and UDP. This may lead to further enumeration. Nmap uses the -sP flag for ping scanning. This form of scan is very advantageous for enumerating the host in a system. Nmap utilizing Transmission Control

Protocol and User Datagram Protocol, observes cloud services, applications, and connections leveraging embedded resources via probe or perhaps a constructed script. This may steer to further enumeration.

The **Nmap Scripting Engine (NSE)** is an incredibly powerful addition to Nmap, extending functionality quite considerably. NSE. It's the ability to let users write and share their own scripts, so you're not limited to relying on the Nmap default NSE scripts. Nmap offers a variety of types of scans in order to scan a host for its open services. Used to identify services on a host, the operating system running on the host NSE scripts are great for drafting proof-of-concept code since the modules are written in Lua, a simple yet powerful language. NSE scripts must be coded in Lua language. It allows us to quickly program any task we have in mind with the help of the available NSE libraries. Its flexible syntax is easy to learn. API permits its Port scanning tool to take into account arguments specifying designate believable processes to be used during measurement. Browsers of the Command - line can write or distribute codes thanks to that too. it elevates Server well above typical fast and easy inspections into an even more automated, intricate one, including in space

- ❖ Needed to handle specific tasks that cannot be done easily in Nmap in C++.
- ❖ Motivations for using Lua.
- ❖ NSE uses Lua to allow scripts to run against a host in parallel.
- ❖ Scripts use bindings to Nmap libraries for performance and access to networking facilities.
- ❖ It helps us to find the vulnerable, state, port, services, references, etc...

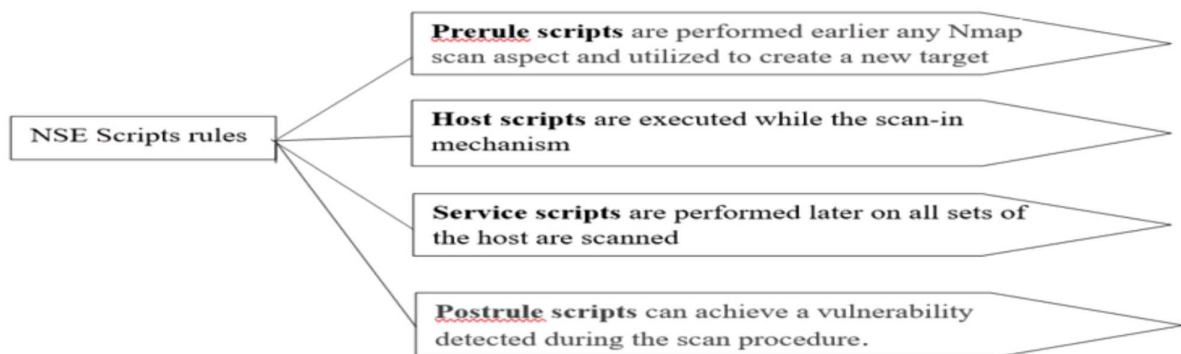


Fig 4.5 Rule and Scripts of NSE

Web Enumeration is used to discover resources in that website and web server, it helps us to find the machine name, username, admins and scripts, etc. It is a technique used for gathering information about the targeted website or domain or server It is used to identify

vulnerable URL domain information, subdomain information, and vulnerable directories. It is useful to report after finding vulnerable directories and subdomains to the respected person to develop it. Web enumeration involves discovering resources that the web server is using, as well as the underlying technology that the web server is running on. This information can help you choose more effective vectors to use in an attack, as well as exploit vulnerabilities in specific versions of web server software. A web domain is the URL or address of a webpage that replaces the Internet Protocol (IP) address. Learn about the definition of web domain, top-level domain (TLD), the purpose/explanation of web domains, and domain name syntax

Web Enumeration Contains

- i) Web Domain Information
- ii) Web Directory Enumeration
- iii) Web Subdomain Enumeration

A domain name is a string that identifies a realm of administrative autonomy, authority, or control within the Internet. Domain names are used in various networking contexts and for application-specific naming and addressing purposes. In general, a domain name identifies a network domain or an Internet Protocol (IP) resource, such as a personal computer used to access the Internet, or a server computer. Domain names are often used to identify services provided through the Internet, such as websites and email services. As of 2017, 330.6 million domain names had been registered. Domain names are formed by the rules and procedures of the Domain Name System (DNS). Any name registered in the DNS is a domain name. Domain names are organized in subordinate levels (subdomains) of the DNS root domain, which is nameless. The first level set of domain names is top-level domains (TLDs).

A web directory is a website that owns a listing of links to another website each of which is connected to an ordinary title and given a systematic method to discover websites. It is a data collection of websites organized in such a method that they ease navigation. These links to web labels are categorized according to particular criteria, such as alphabetical order. This assists users search for info in an individual way. A web directory builds it simple to discover websites by topic because a quest is beneficial in identifying internet sites utilizing vocabulary (plus if it's a visual google product, pictures, recording, etc.). Online portals provide a collection of hyperlinks that are organized to make navigation easier. A search query is provided by plenty of article directories thus individuals can conduct searches but instead browse the database. The following Figure 9 describes the directory enumeration

Web Subdomain Enumeration is the process of identifying all subdomains for a given domain. This can be useful for a variety of purposes, such as identifying potential targets for an

attack, or simply for organizational purposes. A subdomain is a second-level domain that is part of a larger domain. Organizations can use subdomain enumeration for a variety of purposes, such as inventorying their owned domains, or identifying which domains are being used for which purposes. This can be helpful in organizational security efforts, as it can help identify potential weak points that may need to be addressed. It is also really helpful to find old, deprecated, and potentially vulnerable applications hosted on subdomains of which no one still knows why they exist or who maintains them.

The term "open data intellectual ability" (OSINT) refers to instruments that make it possible the collection of publicly available or online data. Open-source data mining systems' main goal is to learn more. regarding individuals/organizations. Intelligence investigators and analysts support open-source information to improve their grasp of the menacing environment and assist secure organizations and individuals from well-known peril inside their IT surroundings. Skillset, cognitive prowess, and soft skills are all part of Open - source qualities. OSINT can be used to secure the network in different ways there are Detecting possible menaces, Performing risk assessment, and Surveillance of common platforms. OSINT frequently includes using modern analytical techniques, such as NLP and ML, to evoke penetration and intelligence from huge volumes of information.

OSINT includes

- i) Number Info
- ii) Trace the Global IP address

In the exploration of open-source intelligence, mobile numbers are crucial. Each and everyone has a phone, which is intimately related to their lives and contains extremely crucial information about them. To learn more about the phone number of the topic, use Number Info's OSINT to learn about the line type, carrier, target local format, target international format, prefix, location, and other pertinent details. The number itself contains some information, such as the nation, city, and occasionally the carrier, however, it is probable to bring out the additional data using a public platform. It can identify other details about the target that may be attached to the phone number, it's easy to identify the weakest link and attack the target using whatever information that's dug up. The data can be used to detect whether a phone number is a throwaway VoIP number used to hide the owner's identity or a cell phone belonging to a real person.

An Internet user should be able to openly access a worldwide IP address. An IP address with a local scope cannot be routed to the Internet. This implies that even while your device won't be able to access the Internet if it has a local-scope address, you will still be able to use

campus network resources. Uniquely assigned IP addresses to devices connected to the Internet. In the case of the address on the Internet, it is always necessary for communication over the Internet. If you look up a global IP address, “Internet Service Provider (ISP)” refers to a company that provides access to the Internet to both personal and business customers. ISPs may also provide other services, including email services, domain registration, web hosting, and browser packages. An ISP may also be referred to as an information service provider, a storage service provider, an internet network service provider (INSP), or any combination of these three based on the services offered by the company. you can discover the name of the nation, the region, the city, the time zone, and the Internet Service Provider (ISP). It immediately displays the ISP's location on Google Maps.

```

kali@kali: ~/Desktop/email2phonenumber
kali@kali: ~/Desktop/email2phonenumber/105x25
kali@kali:~/Desktop/email2phonenumber$ python3 email2phonenumber.py -h
usage: email2phonenumber.py [-h] {scrape,generate,bruteforce} ...

An OSINT tool to find phone numbers associated to email addresses

positional arguments:
  {scrape,generate,bruteforce}
  scrape                scrape online services for phone number digits
  generate              generate all valid phone numbers based on NANPA's public records
  bruteforce            bruteforce using online services to find the phone number

optional arguments:
  -h, --help            show this help message and exit
kali@kali:~/Desktop/email2phonenumber$

```

Fig4.6 Displays ISPs on the map

Cryptography is the study of securing communications from outside observers. take the original message, or plaintext, and converts it into ciphertext, which is not understandable. The key allows the user to decrypt the message, thus ensuring on they can read the message. The strength of the randomness of encryption_is also studied, which makes it harder for anyone to guess the key or input of the algorithm. Cryptography is how we can achieve more secure and robust connections to elevate our privacy. Advancements in cryptography make it harder to break encryptions so that encrypted files, folders, or network connections are only accessible to authorized users. Besides converting data together into a secured configuration, raw data can be protected via encryption. Manuscript correspondence has already been shielded against fraudulent reading through the implementation of cryptography since the beginning of recorded history. Crypto encodes messages and data to prevent anyone other than the destination node from seeing, interpreting, or processing it. In the modern era, encoding is used to safeguard metadata. A goal of this computational science field is to organize details in a manner that only permits users can perceive.

Cryptography includes

- i) Hash Identifier
- ii) Hash Cracking-< John The Ripper >
- iii) Hash Cracking-<Hashcat >

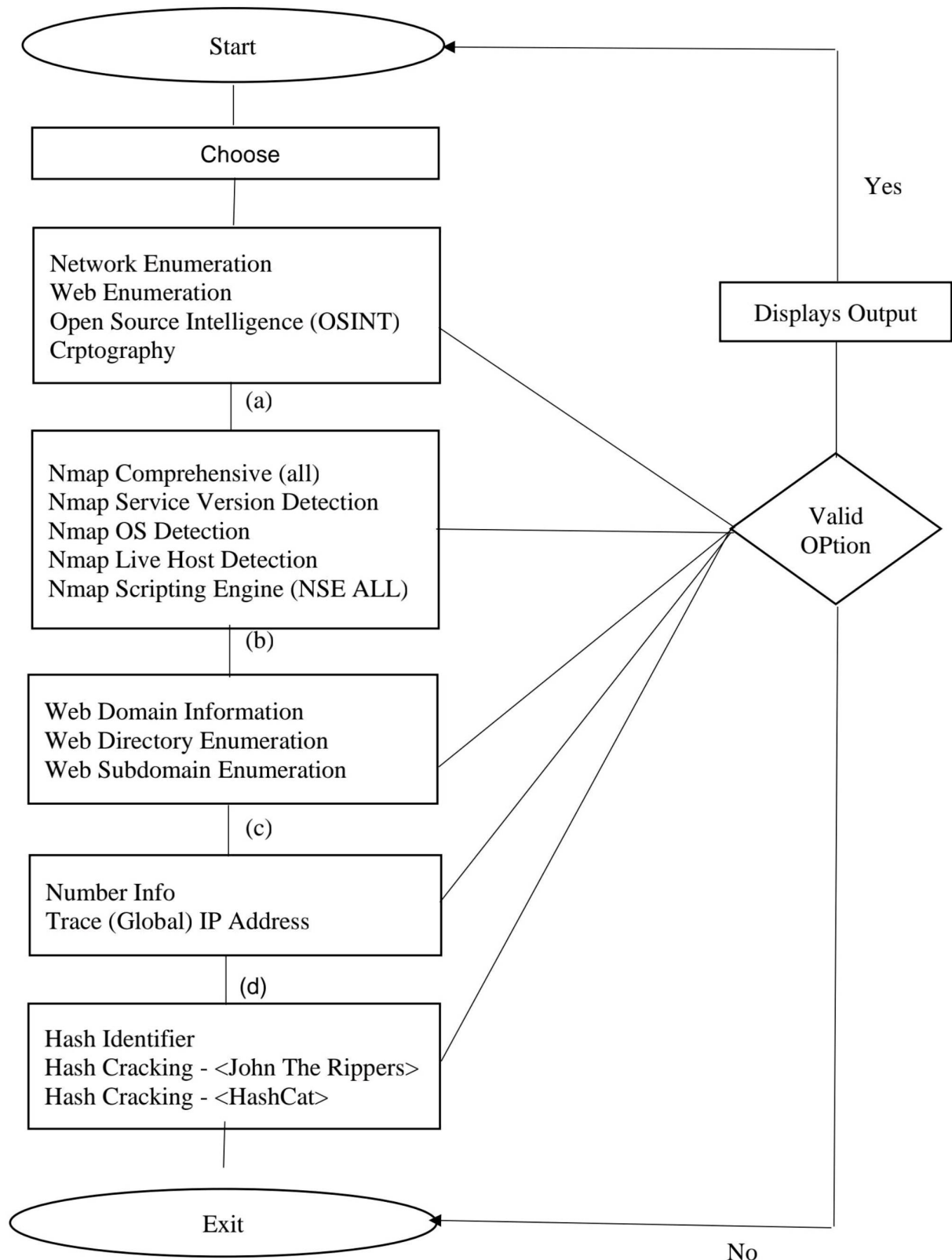
Hash-identifier is also helpful for identifying which hashing algorithm is being used to provide a checksum value for a download. And it can be used to determine what program a hashed file or value may belong to, such as an SQL database or another vendor-specific format. A hashing function turns the readable passwords into jumbled up messes of letters and numbers that should not be able to be reverse-engineered. Software that can distinguish between the various hashing algorithms used to secure data, particularly passwords. Data exchange between integrated data management systems is done using the encryption method of hashing. The hashing identifier in Eloqua can be used to practice and recognize two different types of hashes in order to exchange phone numbers and email addresses in an unidentified fashion. The capability provides hashed versions of the recent contact field information and allows you to map these details to other systems without providing any Personal Identifiable Information (PII). The performance uses SHA256 hashes to peculiar identify contacts. The following Figure 13 describes the discovery of hash to protect the data.

The tool for breaking passwords John The Ripper can recognize the majority of password hash types and offers a user-friendly command-line interface. Some of the key features of the tool include offering multiple modes to speed up password cracking, automatically detecting the hashing algorithm used by the encrypted passwords, and the ease of running and configuring the tool making it a password cracking tool of choice for novices and professionals alike. John the Ripper is a password cracker that works offline. In other words, it searches collected data for passwords without getting in touch with the target. Due to the fact that the method is often performed locally, on the attacker's workstation, this prevents the production of suspicious traffic. Although its primary application is to decrypt password hashes, John may also be used to decrypt encrypted private keys, secured archive files, and many other kinds of data.

Hashcat is a well-known and efficacious passcode cracker that is used by penetration testers, system administrators, perpetrators, and intelligence agencies. The hashcat seems to be a multi-threading functionality that allows you to set the numerous threads and prioritize execution. Password cracking differs from assuming a site username and password, which typically allows only one limited set of assumptions before holding the account. Rather, anyone who has managed to gain access to a computer system containing encryption keys

("hashes") will often attempt to break those hash values in order to retrieve the passwords. Hashcat is a particularly fast, efficient, and versatile hacking tool that assists brute-force attacks by conducting them with hash values of passwords that the tool is guessing or applying. When used for benign purposes, such as in penetration testing one's own infrastructure, it can reveal compromised or easy to guess credentials. Penetration testers on engagement will frequently find themselves cracking stolen password hashes to move laterally inside a network, or to escalate privileges to an admin user. Since penetration testers work to find security holes on purpose, under contract, so that their customer can improve their security, this is also a perfectly legitimate use case.

4.2 SYSTEM ARCHITECTURE FOR THE PROPOSED SYSTEM



4.3 DESCRIPTION OF SOFTWARE FOR IMPLEMENTATION AND TESTING PLAN OF THE PROPOSED SYSTEM

- ❖ Python3 is a computer programming language that is frequently used to create applications and websites, automate procedures, and analyze data.
- ❖ Python3 is not specialized for any particular issue and may be employed to develop a wide range of diverse programming.
- ❖ Python supports modules and packages, which encourages program modularity and code reuse.
- ❖ Python also has a number of libraries that enable coders to write programs for data analysis
- ❖ It is fully extensible as well as works well with other libraries and this language is perfectly suited to develop your tool.
- ❖ Its adaptability and complete novice-friendliness have elevated its position at the top of the list of languages for programming in practice nowadays.

4.4 PROJECT MANAGEMENT PLAN

- Dart helps to find the proper result and the valuable data is important to test
- The tool is made up of Python3 and bash script, it allows you to control the computer like a developer.
- This helps to give accuracy and precision and reduces the time
- It a very little time-consuming owing to the employment of numerous tools, and scripts, including thorough techniques in one script in order to ensure that it is unified.
- As the project is developed of various technologies built in single scripts to make time intensive so it is integrated
- It moves concerning quickly and conveniently employs all of the mentioned tools to their fullest extent utilizing only a single all-encompassing script.

CHAPTER 5

IMPLEMENTATION

5.1 COMMANDS INVOLVED IN THE TOOL

This tool supports Pentester / Red Teamer to enumerate information in disparate technologies like Networking, Web Applications, Open Source Intelligence, and Cryptography. Install the VMware player, Metasploitable and Kali Linux. Then Import the Kali Linux and Metasploitable to the VMware player, Once it is imported then do the configuration to get that in the working process.

First, you open the VMware then boot the Kali Linux and Metasploitable simultaneously. Once that opens type the password to get into the Kali Linux but for Metasploitable you have to log in and find the IP address for Metasploitable. The IP address of the vulnerable machine is very crucial because it will travel through the Network Enumeration tools. Then again back to the Kali Linux to open the terminal. In that terminal type the command that command will confirm the path or folder and whether we use the right folder or not.

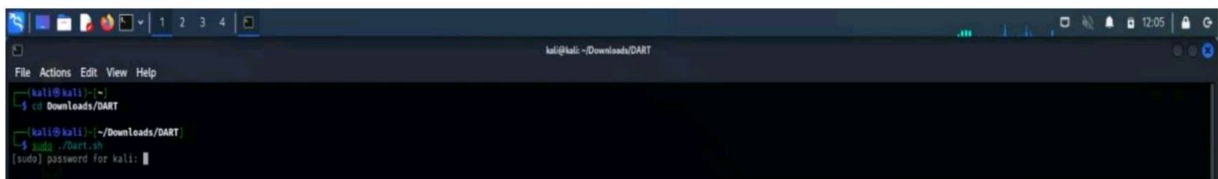


Fig 5.1 confirm the folder and path

Once it has been done it will pop up a sudo password for Kali, type the correct password then only it will allow you to proceed further. Again type the command ls it will list the tools or technologies and the technologies it will display the available service or tool as well as choose the available service.

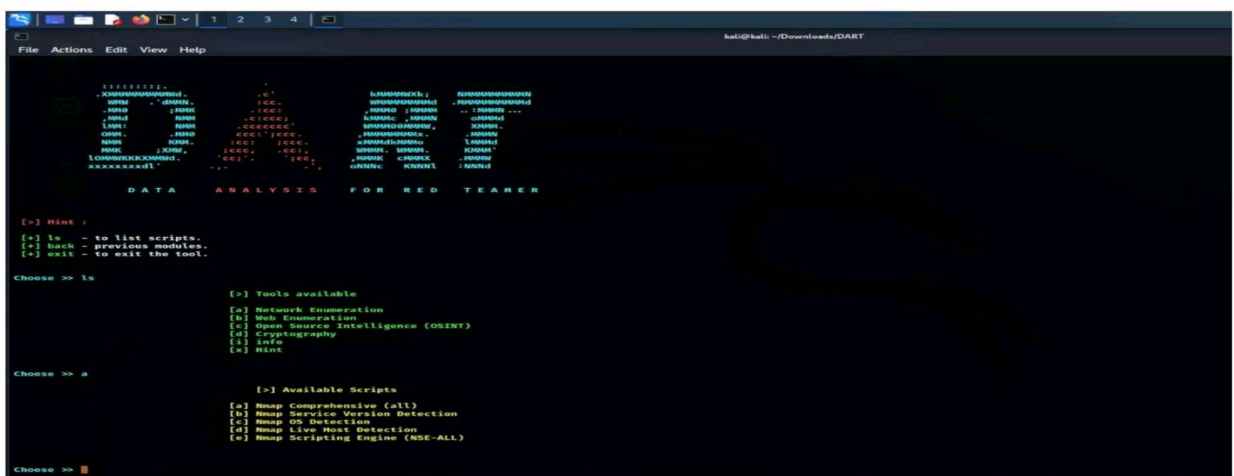


Fig 5.2 List the tools using various technologies

Further, the process is a little bit quite difference because here we using various

technologies in a single script to make the process will consume less time for testing. This tool will support disparate technologies that are Network Enumeration, Web Enumeration, Open Source Intelligence, and Cryptography

For Network Enumeration, once choose an available service or tool it will pop up an IP address here type the vulnerable machine IP address which we already took it out at the begging of the process. This Vulnerable machine will travel through the process of testing held on Network Enumeration and typing the IP address is done once means it will display the output like open ports, service, protocol, vulnerabilities, etc... this process is the same for four services except for Live host detection because there we have type full IP address like 192.168.91.129/24.

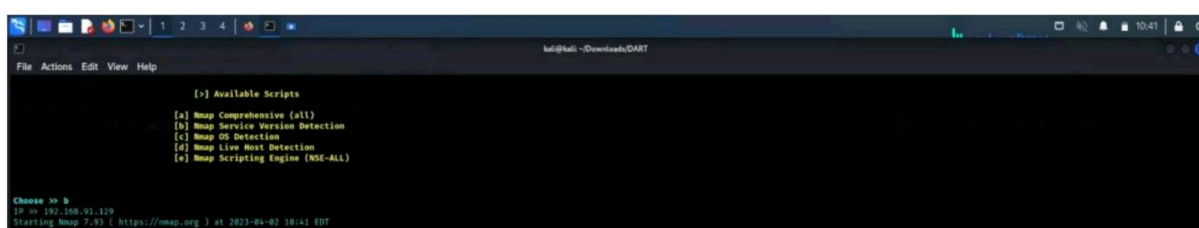


Fig 5.3 Network Enumeration

For Web Enumeration, again choose a service in the web enumeration. Once that has been done then the main operating system will pop up the domain. on that, you have to type the domain names like google.com, twitter.com, tryhackme.com, etc. Then once the typing command process over means it will dis[plays genuine outcomes. Here, the previous operation is kept on repeating for the next two services there is no changes in the process.

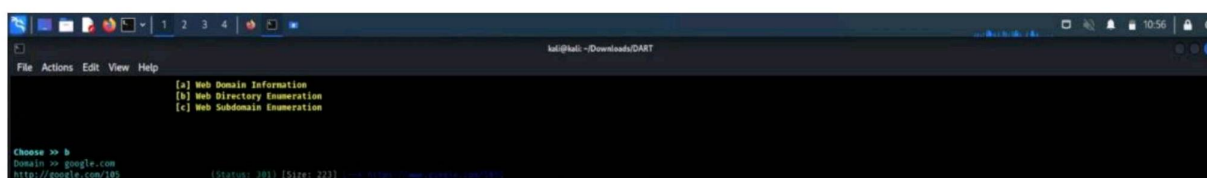


Fig 5.4 A Basic operation in Web Enumeration

In this Open Source Intelligence technology, we use two different services so both the procedure of the operation is different. First, the technology deal with Number info here chose the service it will, as usual, pop up a command like a phone number with a prefix. That prefix is important to discover the country, code, location, etc. In the same technology next, we saw the Trace Global IP address here also it will pop up a command global IP then open Firefox in the main operating system where you type my global IP in the search box. It will display the global IP. Once you have done the procedure it will display outcomes and directly locate to Google map.

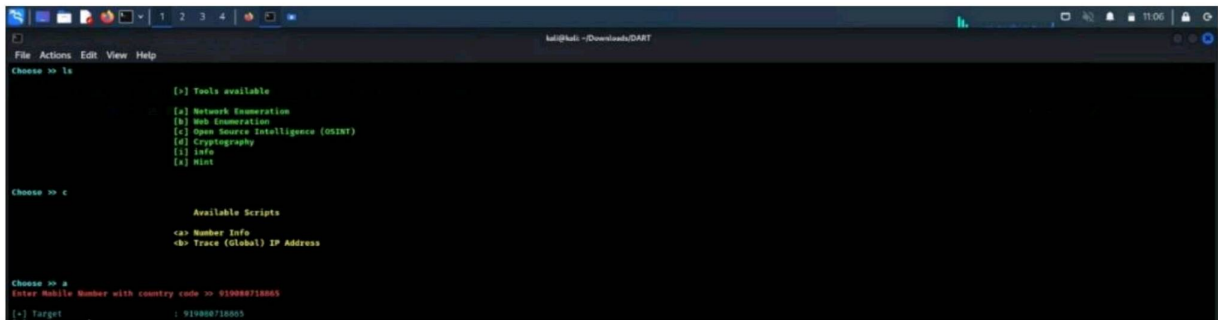


Fig 5.5 Beginning process of prefix with phone number

In Cryptography technology, this technology deals with three hashing services. These three hashing activities are completely different. First, it deals with Hash Identifier, as usual, chose the service it will pop up a hash for that you have to go to Google and search for the SHA256 generator. In that generator, generate the hash with normal words like football, cricket, toy, etc. Once you generated the hash copy the hash as well as paste that to the popped-up position then it will display the output. Next John The Ripper, previously we generated the hash is crucial for this and the next one which is Hashcat. For John The Ripper it will pop up a hash type for that we take the hash type from Has Identifier there it has rawSHA-256 which is the hash type for John The Ripper. It will generate the output quickly. Then for Hashcat it will pop up a hash number take the hash number from the Hash Identifier copy and paste the hash number at the popped-up place as usual it will generate output rapidly.

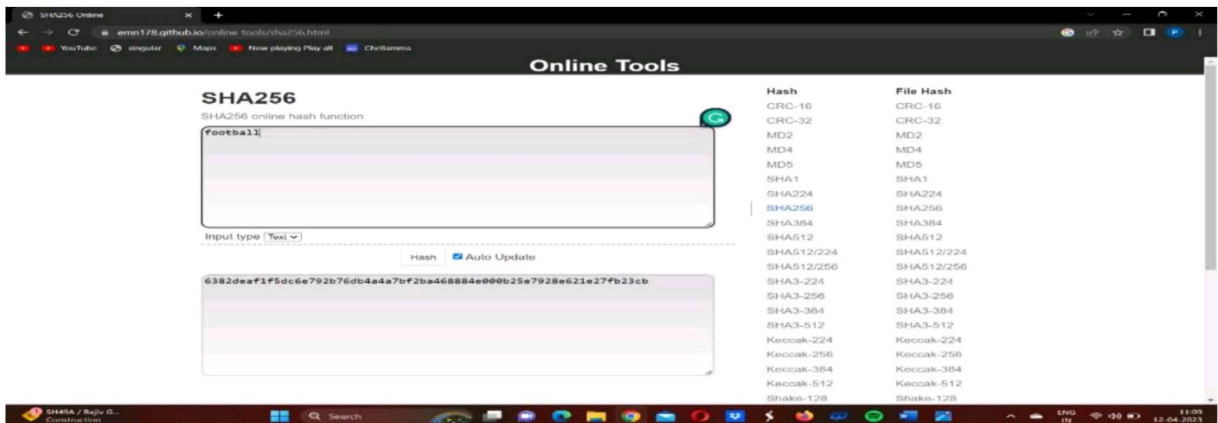


Fig 5.6 SHA256 Hash Generator

CHAPTER 6

RESULT AND DISCUSSIONS

The testing results should include a detailed analysis of the vulnerabilities discovered. It is the predominant and also most important distinction between pen tests and vulnerability assessments. The vulnerabilities discovered must always be reported accurately to the organization so that essential modifications can be made to repair the weakness throughout their processes. As comprehensive scripts are used, the outcome will become more detailed, accurate, and precise. This should produce high accuracy, as well as beneficial data is essential for testing. Also, it provides security for the web-based application as well as shows all of the application's detailed information. Following that, the Open source structure would also obtain data on a specific person or organization. Even when using Cryptography, which is an effective mechanism for safeguarding data stored on a computer, which will start examining a hash variety and authenticate the hash credentials.

CHAPTER 7

CONCLUSION

7.1 CONCLUSION

Everything is going online on the internet as a result of the ongoing digital revolution, and as we all know, the web is not an extremely secure protocol. As a result, precautions must be taken to protect the authenticity as well as the secrecy of the info. To expand reports of information security, cyber threats, as well as information leakage, researchers should ensure the security of our vital information. A vulnerability assessment is a complete and accurate method for detecting security vulnerabilities. This study provides crucial details about the stage as well as the significance of the testing process. System testing is divided into three stages: information gathering, scanning, and frailty evaluation. Each of the aforementioned phases can be done automatically utilizing Nmap and other tools.

7.2 FUTURE SCOPE

In the future. According to a technical report, the open source intelligence (OSINT) market will develop at a significant rate between 2020 and 2026. The increase in the availability of open-source data, as well as rising cyber risks, is expected to assist future growth. Analysts predict that perhaps the huge amount of information dissemination will have a critical effect on the market performance from 2020 to 2026. During the forecast period, the market will be assisted by increased accessibility to public information and advancements in technology. Over the course of time. OSINT would be developed to take the entire details of an individual person which will gather utilizing extraneous APIs, Google Eavesdropping, phone books, and also web crawlers, collect appropriate data such as nation, quick response code, as well as transmission OSINT efficient process,

MERITS:

- This tool is very safe and secure.
- It will give the proper outcomes and valuable data is important to test.
- This tool will be generated the result will be more precise and accurate because of using comprehensive scripts.
- Little bit time-consuming because developed with several scripts to build it as a single tool for discovering loopholes and vulnerabilities in an organization.

REFERENCES

- [1] Goel, Jai & Mehtre, Babu. (2016). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science*. 57. 710-715. 10.1016/j.procs.2015.07.458.
- [2] S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 2017, pp. 1-6, doi: 10.1109/ICCUBEA.2017.8463920.
- [3] Prashant S. Shinde; Shrikant B. Ardhapurkar. (2016). Cybersecurity analysis using vulnerability assessment and penetration testing. 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave) (IEEE Conference Publications), 1-5, DOI:10.1109/STARTUP. 2016.7583912.
- [4] Hasan, Ashikali and Meva, Divyakant, Web Application Safety by Penetration Testing (2018). *International Journal of Advanced Studies of Scientific Research*, Volume 3, Issue 9, 2018, Available at SSRN:
- [5] SurenderJangra, Pankaj Kumar Verma ,“A Survey on Vulnerability Assessment & Penetration Testing for Secure Communication.” *2018 3rd International Conference on Trends in Electronics and Informatics (ICOEI)* (2019): 320-325.
- [6] S.M.Z.U. Rashid, M. I. Kamrul and A. Islam, "Understanding the Security Threats of Esoteric Subdomain Takeover and Prevention Scheme," 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox'sBazar, Bangladesh, 2019, pp. 1-4, doi: 10.1109/ECACE.2019.8679122.
- [7] Goutam, Arvind & Tiwari, Vijay. (2019). Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application. 601-605. 10.1109/ISCON47742.2019.9036175.
- [8] R. Pandey, V. Jyothindar and U. K. Chopra, "Vulnerability Assessment and Penetration Testing: A portable solution Implementation," 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), Bhimtal, India, 2020, pp. 398-402, doi: 10.1109/CICN49253.2020.9242640.
- [9] AmeyKanunje, Sourabh Mahale, Niraj Khare and Pratik Daund, “Penetration Testing and Vulnerability Assessment”, 2021. 2320-9364, ISSN (Print): 2320-9356
- [10] Tae, Hyun & Kim, Douglas & Reeves,. (2021). A survey of domain name system vulnerabilities and attacks. 1. 34-60.
- [11] A. S. B. Singh, Y. Yusof and Y. Nathan, "EAGLE: GUI-Based Penetration Testing Tool for Scanning and Enumeration," 2021 14th International Conference on Developments in e Systems Engineering (DeSE), 2021, pp. 97-101, doi: 10.1109/DeSE54285.2021.9719338.

- [12] C. DeCusatis, P. Peko, J. Irving, M. Teache, C. Laibach and J. Hodge, "A Framework for Open Source Intelligence Penetration Testing of Virtual Health Care Systems," 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2022, pp. 0760-0764, doi: 10.1109/CCWC54503.2022.9720785.
- [13] J. K. Periasamy, D. V and T. K, "AssessJet - Penetration testing and Vulnerability Assessment for Websites," 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), 2022, pp. 1-4, doi: 10.1109/IC3IoT53935.2022.9767928.

APPENDIX

A. SOURCE CODE

```
from NmapComp import nmapcomp
from NmapServ import nmapportserv
from NmapLiveHost import livehost
from NmapOs import nmapos
from NmapNSE import nmapnse
```

```
#Color
```

```
grey  = "\033[1;37m"
```

```
red   = "\033[1;31m"
```

```
green = "\033[1;32m"
```

```
yellow = "\033[1;33m"
```

```
cyan  = "\033[1;96m"
```

```
purple = "\033[1;35m"
```

```
def networkenum():
```

```
from Dart import main_menu
```

```
print(yellow + ""
```

```
[>] Available Scripts
```

```
[a] Nmap Comprehensive (all)
```

```
[b] Nmap Service Version Detection
```

```
[c] Nmap OS Detection
```

```
[d] Nmap Live Host Detection
```

```
[e] Nmap Scripting Engine (NSE-ALL)
```

```

"""
inp = (input(cyan + "Choose >> "))

if (inp == 'a'):
    nmapcomp()

elif (inp == 'b'):
    nmapportserv()

elif (inp == 'c'):
    nmapos()

elif (inp == 'd'):
    livehost()

elif (inp == 'e'):
    nmapnse()

elif (inp == 'back'):
    main_menu()

elif (inp == 'exit'):
    exit()

elif (inp == 'x'):
    print(red + "Hint :")

    print(green + "ls " + grey + " - to list scripts.")

    print(green + "back " + grey + " - previous modules.")

    print(green + "exit " + grey + "- to exit the tool.")

elif (inp == 'ls'):
    print(green + """

[>] Available Scripts

```

- [a] Nmap Comprehensive (all)
- [b] Nmap Service Version Detection
- [c] Nmap OS Detection
- [d] Nmap Live Host Detection
- [e] Nmap Scripting Engine (NSE-ALL)

""")

else:

print(red + "Enter an valid option")

while True:

networkenum()

if __name__ == "__main__":

networkenum()

#Nmap Comprehensive scan

import os

#Color

grey = "\033[1;37m"

red = "\033[1;31m"

green = "\033[1;32m"

yellow = "\033[1;33m"

cyan= "\033[0;96m"

purple="\033[0;35m"

def nmapcomp():

```
IP = input(cyan+"IP >> ")
print(os.system("nmap -sV -n -v -Pn -p- -T4 " + IP + " -A --open"))
```

```
if __name__=="__main__":
```

```
nmapcomp()
```

```
#Nmap Service Detection
```

```
import os
```

```
#Color
```

```
grey = "\033[1;37m"
```

```
red = "\033[1;31m"
```

```
green = "\033[1;32m"
```

```
yellow = "\033[1;33m"
```

```
cyan= "\033[0;96m"
```

```
purple="\033[0;35m"
```

```
def nmapportserv():
```

```
IP = input(cyan+"IP >> ")
```

```
print(os.system("nmap -sV -Pn --min-rate 300 " + IP))
```

```
if __name__=="__main__":
```

```
nmapportserv()
```

```
#Nmap OS scan
```

```
import os
```



```

#Color

grey = "\033[1;37m"

red = "\033[1;31m"

green = "\033[1;32m"

yellow = "\033[1;33m"

cyan= "\033[0;96m"

purple="\033[0;35m"


def nmapos():

IP = input(cyan+"IP >> ")

print(os.system("sudo nmap -O -T 5 " + IP))


if __name__=="__main__":

nmapos()

#print(os.system("nmap -A -T 5 " + IP))


#Nmap Live Host

import os

#Color

grey =  "\033[1;37m"

red  =  "\033[1;31m"

green =  "\033[1;32m"

yellow =  "\033[1;33m"

cyan  =  "\033[0;96m"

purple =  "\033[0;35m"

```

```

def livehost():

IP = input(cyan+"IP/CIDR >> ")

print(os.system("nmap -sP " + IP + " | grep -o 192.168.*.*"))


if __name__=="__main__":

livehost()

#Nmap NSE


import os


#Color

grey = "\033[1;37m"

red = "\033[1;31m"

green = "\033[1;32m"

yellow = "\033[1;33m"

cyan= "\033[0;96m"

purple="\033[0;35m"


def nmapnse():

IP = input(cyan+"IP >> ")

print(os.system("nmap --script=vuln "+ IP ))

if __name__=="__main__":

nmapnse()

from WebDomainInfo import webdomaininfo

from WebDirEnum import webdirenum

```

```
from WebSubdomainEnum import websubdomainenum
```

```
# Color
```

```
#Color
```

```
grey  = "\033[1;37m"
```

```
red   = "\033[1;31m"
```

```
green = "\033[1;32m"
```

```
yellow = "\033[1;33m"
```

```
cyan  = "\033[1;96m"
```

```
purple = "\033[1;35m"
```

```
def webenum():
```

```
from Dart import main_menu
```

```
print(yellow + """
```

```
[>] Available Scripts
```

```
[a] Web Domain Information
```

```
[b] Web Directory Enumeration
```

```
[c] Web Subdomain Enumeration
```

```
""")
```

```
inp = (input(cyan + "Choose >> "))
```

```
if (inp == 'a'):
```

```
webdomaininfo()
```

```
elif (inp == 'b'):
```

```
webdirenum()
```

```
elif (inp == 'c'):
```

```
websubdomainenum()
```

```
elif (inp == "back"):
```

```
main_menu()
```

```
elif (inp == 'exit'):
```

```
exit()
```

```
elif (inp == 'ls'):
```

```
print(green + ""
```

```
[>] Available Scripts
```

```
[a] Web Domain Information
```

```
[b] Web Directory Enumeration
```

```
[c] Web Subdomain Enumeration
```

```
""")
```

```
elif (inp == 'x'):
```

```
print(red + "Hint :")
```

```
print(green + "ls " + grey + " - to list scripts.")
```

```
print(green + "back " + grey + " - previous modules.")
```

```
print(green + "exit " + grey + "- to exit the tool.")
```

```
else:
```

```
print(red + "Enter an valid option")
```

```
while True:
```



```
webenum()
```

```
if __name__ == "__main__":
```

```
webenum()
```

```
import os
```

```
#Color
```

```
grey = "\033[1;37m"
```

```
red = "\033[1;31m"
```

```
green = "\033[1;32m"
```

```
yellow = "\033[1;33m"
```

```
cyan= "\033[0;96m"
```

```
purple="\033[0;35m"
```

```
def webdomaininfo():
```

```
domain = input(cyan+"Domain >> ")
```

```
print(os.system("whois " + domain))
```

```
if __name__=="__main__":
```

```
webdomaininfo()
```

```
#Hydra Web Enum
```

```
import os
```

```
#Color
```

```
grey = "\033[1;37m"
```

```
red = "\033[1;31m"
```

```
green = "\033[1;32m"
```

```
yellow = "\033[1;33m"
```

```
cyan= "\033[0;96m"
```

```
purple="\033[0;35m"
```

```
def webdirenum():
```

```
domain = input(cyan+"Domain >> ")
```

```
print(os.system("sudo gobuster dir -e -u " + domain + " -w /usr/share/wordlists/dirb/big.txt -t 40 -q"))
```

```
if __name__=="__main__":
```

```
webdirenum()
```

```
# Web sub domain enum
```

```
import os
```

```
#Color
```

```
grey = "\033[1;37m"
```

```
red = "\033[1;31m"
```

```
green = "\033[1;32m"
```

```
yellow = "\033[1;33m"
```

```
cyan = "\033[0;96m"
```

```
purple = "\033[0;35m"
```

```
def websubdomainenum():
```

```
domain = input(cyan+"Domain >> ")
```

```
print(os.system("sudo assetfinder -subs-only " + domain))
```

```
if __name__=="__main__":
```

```
websubdomainenum()
```

```
from OsintNumberInfo import osintnumberinfo
```

```
from OsintTraceIP import osinttraceip
```

```
#Color
```

```
grey = "\033[1;37m"
```

```
red = "\033[1;31m"
```

```
green = "\033[1;32m"
```

```
yellow = "\033[1;33m"
```

```
cyan = "\033[1;96m"
```

```
purple = "\033[1;35m"
```

```
def osint():
```

```
from Dart import main_menu
```

```
print(yellow + """
```

```
Available Scripts
```

```
<a> Number Info
```

```
<b> Trace (Global) IP Address
```

```
""")
```

```
inp = (input(cyan + "Choose >> "))
```

```
if (inp == 'a'):
```

```
osintnumberinfo()
```

```
elif (inp == 'b'):
```

```
osinttraceip()
```

```
kali@kali: ~/Downloads/DART
```

```
File Actions Edit View Help
```

```

      :~::~~::~~::
,XMMMMMMMMMMMMMMd.
NMNM .'.dNMN.
.MMO ;MMK
.NMd NMN
LNM: NMN
OMM. .MMO
NMN NMN
NMK !XMM.
LOMMKKKKMMMd.
XXXXXXXXd'

      .c'
      :cc.
      :ccc.
      .c:ccc;
      .cccccc'
      ccc:'ccc.
      :ccc :ccc.
      :ccc. :cci.
      'cc'.' 'jce.

kMMMMCKk;
MMMMMMMMMMd
.MMO ;MMMN
kMMMc ;MMMN
MMMMMMMMMMN,
MMMMMMMMMK.
.MMdMMMo
MMMM. MMN.
MMMc cMMMX
oNNMc KMMNL

MMMMMMMMMMMN
.. :MMMN ...
oMMMd
XMNM.
.MNMN
LMMD
KMMA'
.MMO
.MMO
:MNMd

DATA ANALYSIS FOR RED TEAMER

```

```
[>] Hint :
```

```
[+] ls - to list scripts.
[+] back - previous modules.
[+] exit - to exit the tool.
```

```
Choose >> ls
```

```
[>] Tools available
```

```
[a] Network Enumeration
[b] Web Enumeration
[c] Open Source Intelligence (OSINT)
[d] Cryptography
[i] info
[x] Hint
```

```
Choose >> a
```

```
[>] Available Scripts
```

```
[a] Nmap Comprehensive (all)
[b] Nmap Service Version Detection
[c] Nmap OS Detection
[d] Nmap Live Host Detection
[e] Nmap Scripting Engine (NSE-ALL)
```

```
Choose >>
```

49

```
File Actions Edit View Help

[>] Available Scripts

[a] Nmap Comprehensive (all)
[b] Nmap Service Version Detection
[c] Nmap OS Detection
[d] Nmap Live Host Detection
[e] Nmap Scripting Engine (NSE-ALL)

Choose >> b
IP >> 192.168.91.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-02 10:41 EDT
Nmap scan report for 192.168.91.129
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.0 - 4.0 (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0 - 4.0 (workgroup: WORKGROUP)
112/tcp   open  exec         netkit-rsh rshcd
113/tcp   open  login        OpenBSD or Solaris rlogind
114/tcp   open  tcpwrapped
1899/tcp  open  java-rmi     GNU Classpath gmicregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
1122/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-Jubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8080/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:0C:29:61:C6:C7 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.14 seconds
0

[>] Available Scripts

[a] Nmap Comprehensive (all)
[b] Nmap Service Version Detection
```

```
File Actions Edit View Help

[>] Available Scripts

[a] Nmap Comprehensive (all)
[b] Nmap Service Version Detection
[c] Nmap OS Detection
[d] Nmap Live Host Detection
[e] Nmap Scripting Engine (NSE-ALL)

Choose >> c
IP >> 192.168.91.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-02 10:43 EDT
Nmap scan report for 192.168.91.129
Host is up (0.0000s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
112/tcp   open  exec
113/tcp   open  login
114/tcp   open  shell
1899/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:0C:29:61:C6:C7 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.06 seconds
0
```



```
File Actions Edit View Help
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.9854814545
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Redacted for Privacy
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
Registrant Street: Kalkofnsvegur 2
Registrant City: Reykjavik
Registrant State/Province: Capital Region
Registrant Postal Code: 101
Registrant Country: IS
Registrant Phone: +354.4212434
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: a70a4ff6d25041a48378997194f9e834.protect@withheldforprivacy.com
Registry Admin ID:
Admin Name: Redacted for Privacy
Admin Organization: Privacy service provided by Withheld for Privacy ehf
Admin Street: Kalkofnsvegur 2
Admin City: Reykjavik
Admin State/Province: Capital Region
Admin Postal Code: 101
Admin Country: IS
Admin Phone: +354.4212434
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: a70a4ff6d25041a48378997194f9e834.protect@withheldforprivacy.com
Registry Tech ID:
Tech Name: Redacted for Privacy
Tech Organization: Privacy service provided by Withheld for Privacy ehf
Tech Street: Kalkofnsvegur 2
Tech City: Reykjavik
Tech State/Province: Capital Region
Tech Postal Code: 101
Tech Country: IS
Tech Phone: +354.4212434
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: a70a4ff6d25041a48378997194f9e834.protect@withheldforprivacy.com
Name Server: kip.ns.cloudflare.com
Name Server: una.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-04-01T16:32:05.372 <<<
For more information on Whois status codes, please visit https://icann.org/epp
0
```

```
File Actions Edit View Help

[a] Web Domain Information
[b] Web Directory Enumeration
[c] Web Subdomain Enumeration

Choose >> b
Domain >> google.com
http://google.com/105 (Status: 301) [Size: 223] --> https://www.google.com/105/
http://google.com/104 (Status: 301) [Size: 223] --> https://www.google.com/104/
http://google.com/2001 (Status: 301) [Size: 224] --> https://www.google.com/2001/
http://google.com/2002 (Status: 301) [Size: 224] --> https://www.google.com/2002/
http://google.com/2003 (Status: 301) [Size: 224] --> https://www.google.com/2003/
http://google.com/2004 (Status: 301) [Size: 224] --> https://www.google.com/2004/
http://google.com/2005 (Status: 301) [Size: 224] --> https://www.google.com/2005/
http://google.com/2006 (Status: 301) [Size: 224] --> https://www.google.com/2006/
http://google.com/2008 (Status: 301) [Size: 224] --> https://www.google.com/2008/
http://google.com/2007 (Status: 301) [Size: 224] --> https://www.google.com/2007/
http://google.com/2009 (Status: 301) [Size: 224] --> https://www.google.com/2009/
http://google.com/2010 (Status: 301) [Size: 224] --> https://www.google.com/2010/
http://google.com/2012 (Status: 301) [Size: 224] --> https://www.google.com/2012/
http://google.com/2011 (Status: 301) [Size: 224] --> https://www.google.com/2011/
http://google.com/2013 (Status: 301) [Size: 224] --> https://www.google.com/2013/
http://google.com/2015 (Status: 301) [Size: 224] --> https://www.google.com/2015/
http://google.com/2014 (Status: 301) [Size: 224] --> https://www.google.com/2014/
http://google.com/2016 (Status: 301) [Size: 224] --> https://www.google.com/2016/
http://google.com/2017 (Status: 301) [Size: 224] --> https://www.google.com/2017/
http://google.com/2019 (Status: 301) [Size: 224] --> https://www.google.com/2019/
http://google.com/2018 (Status: 301) [Size: 224] --> https://www.google.com/2018/
http://google.com/2020 (Status: 301) [Size: 224] --> https://www.google.com/2020/
http://google.com/410 (Status: 301) [Size: 223] --> https://www.google.com/410/
http://google.com/318 (Status: 301) [Size: 223] --> https://www.google.com/318/
http://google.com/A (Status: 301) [Size: 221] --> https://www.google.com/A
http://google.com/Research (Status: 301) [Size: 220] --> https://www.google.com/Research
http://google.com/a (Status: 301) [Size: 221] --> https://www.google.com/a
http://google.com/about (Status: 301) [Size: 225] --> https://www.google.com/about
http://google.com/accessibility (Status: 301) [Size: 233] --> https://www.google.com/accessibility
http://google.com/account (Status: 301) [Size: 227] --> https://www.google.com/account
http://google.com/adwords (Status: 301) [Size: 210] --> https://www.google.com/adwords
http://google.com/action (Status: 301) [Size: 225] --> https://www.google.com/action
http://google.com/activity (Status: 301) [Size: 0] --> https://google.com/activity
http://google.com/adurl (Status: 301) [Size: 210] --> https://www.google.com/adurl
http://google.com/admanager (Status: 301) [Size: 0] --> https://www.google.com/admanager
http://google.com/adresses (Status: 301) [Size: 228] --> https://www.google.com/adresses
http://google.com/ads (Status: 301) [Size: 223] --> https://www.google.com/ads
http://google.com/advertise (Status: 301) [Size: 220] --> https://www.google.com/advertise
http://google.com/advertisers (Status: 301) [Size: 231] --> https://www.google.com/advertisers
http://google.com/advertising (Status: 301) [Size: 231] --> https://www.google.com/advertising
http://google.com/adviser (Status: 301) [Size: 227] --> https://www.google.com/adviser
http://google.com/advisor (Status: 301) [Size: 227] --> https://www.google.com/advisor
http://google.com/adview (Status: 301) [Size: 225] --> https://www.google.com/adview
```

```
File Actions Edit View Help

Choose >> c
Domain >> facebook.com
www.facebook.com
facebook.com
edge-iglite-p42-shv-01-seal.facebook.com
livestream-edgetee-ws-upload-staging-shv-01-seal.facebook.com
edge-z-p4-shv-01-viel.facebook.com
edge-mqtt-p4-shv-01-seal.facebook.com
edgeray-turn-msgr-shv-01-mbal.facebook.com
edge-iglite-p42-shv-01-hbel.facebook.com
edge-fwdproxy-2-bgp-01-jnbl.facebook.com
edge-fwdproxy-5-bgp-01-mbal.facebook.com
experiment-dns-science-1200.facebook.com
edge-c2p-shv-01-mbal.facebook.com
edge-dgw-mini-shv-01-mad1.facebook.com
edgeray-turn-msgr-shv-01-viel.facebook.com
dowproxy-mobile-shv-01-gual.facebook.com
edge-fwdproxy-4-bgp-01-hbel.facebook.com
edge-fwdproxy-1-bgp-01-seal.facebook.com
oculus.cldr.facebook.com
edge-stun-shv-01-gual.facebook.com
edge-msgr-latest-shv-01-seal.facebook.com
edge-stun-shv-01-seal.facebook.com
edge-fblite-tcp-p1-shv-01-viel.facebook.com
edge-rtp-relay-40000-shv-01-hbel.facebook.com
edge-rtp-relay-40000-shv-01-mad1.facebook.com
star-mini.cldr.facebook.com
edge-fwdproxy-2-bgp-01-mbal.facebook.com
edge-iglite-p3-shv-01-gual.facebook.com
lirt-upi-shv-01-viel.facebook.com
whatsapp-chatd-igd-p4-shv-01-seal.facebook.com
edge-fwdproxy-3-bgp-01-mbal.facebook.com
edge-iglite-p1-shv-01-viel.facebook.com
edge-latest-shv-01-mad1.facebook.com
edge-extern-shv-01-jnbl.facebook.com
oculus-verts-shv-01-mbal.facebook.com
edge-extern-shv-01-mad1.facebook.com
edge-msgr-latest-shv-01-hbel.facebook.com
synthetic-e2e-elborod-sli-shv-01-gual.facebook.com
edge-atlas-shv-01-jnbl.facebook.com
headers-shv-00-rpm0.facebook.com
edge-stun-shv-01-viel.facebook.com
secure-edge-latest-shv-01-mad1.facebook.com
edgeray-turn-msgr-shv-01-seal.facebook.com
edge-onevc-sip-shv-01-hbel.facebook.com
edge-mqtt-p4-shv-01-hbel.facebook.com
edge-fwdproxy-2-bgp-01-mad1.facebook.com
edge-mqtt-p4-shv-01-gual.facebook.com
edge-z-p4-shv-01-mad1.facebook.com
edgeray-turn-msgr-shv-01-gual.facebook.com
secure-edge-latest-shv-01-hbel.facebook.com
wit-edge-shv-01-mbal.facebook.com
```

```
File Actions Edit View Help

Choose >> ls

[+] Tools available
    [a] Network Enumeration
    [b] Web Enumeration
    [c] Open Source Intelligence (OSINT)
    [d] Cryptography
    [i] Info
    [x] Hint

Choose >> c

Available Scripts
    <a> Number Info
    <b> Trace (Global) IP Address

Choose >> a
Enter Mobile Number with country code >> 919080718865

[-] Target : 919080718865
[-] Target Local Format : 09080718865
[-] Target International Format : +919080718865
[-] Prefix : +91
[-] Carrier : Reliance Jio Infocomm Ltd (RJIL)
[-] Code : IN
[-] Location : Tamil Nadu
[-] Country : India (Republic of)

Available Scripts
    <a> Number Info
    <b> Trace (Global) IP Address

Choose >> a
Enter Mobile Number with country code >> 6581669100

[-] Target : 6581669100
[-] Target Local Format : 81669100
[-] Target International Format : +6581669100
[-] Prefix : +65
[-] Carrier : StarHub Mobile Pte Ltd
[-] Code : SG
[-] Location : 
[-] Country : Singapore (Republic of)
```



```
File Actions Edit View Help

[>] Available Scripts

[a] Hash Identifier
[b] Hash Cracking - <John The Ripper>
[c] Hash Cracking - <HashCat>

Choose >> a
HASH >> e3b0c44298fc1c149afbf4c8996fb92427ae41e4649d933ca495991b7852b855
SHA-256 [JTR: raw-sha256]
GOST R 34.11-94 [JTR: gost]
SHA3-256 [JTR: dynamic_388]
Keccak-256 [JTR: raw-keccak-256]
Snefru-256 [JTR: snefru-256]
RIPEMD-256 [JTR: dynamic_148]
Haval-256 (3 rounds) [JTR: haval-256-3]
Haval-256 (4 rounds) [JTR: dynamic_298]
Haval-256 (5 rounds) [JTR: dynamic_388]
GOST CryptoPro S-Box [JTR: gost]
Skein-256 [JTR: skein-256]
Skein-512(256)
Ventrilo
sha256($pass.$salt) [JTR: sha256] [JTR: dynamic_81]
sha256($salt.$pass) [JTR: sha256] [JTR: dynamic_81]
sha256(unicode($pass), $salt) [JTR: sha256]
sha256($salt, unicode($pass)) [JTR: sha256]
HMAC-SHA256 (key = $pass) [JTR: hmac] [JTR: hmac-sha256]
HMAC-SHA256 (key = $salt) [JTR: hmac] [JTR: hmac-sha256]
sha256(sha256($pass)) [JTR: dynamic_81]
sha256(sha256_raw($pass)) [JTR: dynamic_84]
sha256(sha256($pass), $salt) [JTR: sha256] [JTR: dynamic_85]
sha256($salt, sha256($pass)) [JTR: sha256] [JTR: dynamic_86]
sha256($salt, sha256_raw($pass)) [JTR: sha256]
sha256(sha256($salt), sha256($pass)) [JTR: dynamic_87]
sha256(sha256($pass), sha256($pass)) [JTR: dynamic_88]
PANAMA [JTR: dynamic_328]
BLAKE2-256
MD6-256
Cisco Type 7
BigCrypt [JTR: bigcrypt]
Umbraco HMAC-SHA1 [JTR: umbraco]

[>] Available Scripts

[a] Hash Identifier
[b] Hash Cracking - <John The Ripper>
[c] Hash Cracking - <HashCat>

Choose >>
```

```
File Actions Edit View Help

sha256($salt.$pass) [JTR: sha256] [JTR: dynamic_81]
sha256(unicode($pass), $salt) [JTR: sha256]
sha256($salt, unicode($pass)) [JTR: sha256]
HMAC-SHA256 (key = $pass) [JTR: hmac] [JTR: hmac-sha256]
HMAC-SHA256 (key = $salt) [JTR: hmac] [JTR: hmac-sha256]
sha256(sha256($pass)) [JTR: dynamic_81]
sha256(sha256_raw($pass)) [JTR: dynamic_84]
sha256(sha256($pass), $salt) [JTR: sha256] [JTR: dynamic_85]
sha256($salt, sha256($pass)) [JTR: sha256] [JTR: dynamic_86]
sha256($salt, sha256_raw($pass)) [JTR: sha256]
sha256(sha256($salt), sha256($pass)) [JTR: dynamic_87]
sha256(sha256($pass), sha256($pass)) [JTR: dynamic_88]
PANAMA [JTR: dynamic_328]
BLAKE2-256
MD6-256
Cisco Type 7
BigCrypt [JTR: bigcrypt]
Umbraco HMAC-SHA1 [JTR: umbraco]

[>] Available Scripts

[a] Hash Identifier
[b] Hash Cracking - <John The Ripper>
[c] Hash Cracking - <HashCat>

Choose >> b
HASH >> 6eb99958d834c612dda35d8aa998f7214e554d35ea6829d8138a8a674941d9
HASH TYPE>> raw-sha256
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-SHA256 [SHA256 128/128 ANK 4x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password123 (?)
2g 0:00:00:02 DONE (2023-03-28 14:03) 0.7874g/s 5646Kp/s 5672Kc/s (454579) ..*/Vamos!
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.

[>] Available Scripts

[a] Hash Identifier
[b] Hash Cracking - <John The Ripper>
[c] Hash Cracking - <HashCat>

Choose >>
```



```

kali@kali:~/Downloads/DART
File Actions Edit View Help

sha256($salt.unicode($pass)) [JtR: 1400]
HMAC-SHA256 (key = $pass) [JtR: 1400] [JtR: hmac-sha256]
HMAC-SHA256 (key = $salt) [JtR: 1400] [JtR: hmac-sha256]
sha256($sha256($pass)) [JtR: dynamic_63]
sha256($sha256_raw($pass)) [JtR: 1400] [JtR: dynamic_64]
sha256($sha256($pass).$salt) [JtR: 1400] [JtR: dynamic_65]
sha256($salt.sha256($pass)) [JtR: 1400] [JtR: dynamic_66]
sha256($salt.sha256_raw($pass)) [JtR: 1400] [JtR: dynamic_67]
sha256($sha256($salt).sha256($pass)) [JtR: dynamic_68]
sha256($sha256($pass).sha256($pass)) [JtR: dynamic_69]
PANAMA [JtR: dynamic_100]
BLAKE2-256
MD6-256
Cisco Type 7
BigCrypt [JtR: bigcrypt]
Umbraco HMAC-SHA1 [JtR: 1400]
0

[>] Available Scripts

[a] Hash Identifier
[b] Hash Cracking - <John The Ripper>
[c] Hash Cracking - <HashCat>

Choose >> c
HASH >> 6382deaf1f5dc0e792b76db4aa7bf2ba468884e00b25e7928e61e27fb23cb
HASH NUMBER >> 1400
0
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.0-debian Linux, None+Asserts, RELoc, LLVM 13.0.1, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

+ Device #1: pthread-intel(R) Core(TM) i3-1005G1 CPU @ 1.20GHz, 1337/2739 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

hashfile 'hash.txt' on line 2 (bdefef...a0d208c790ae7ae17ecfc3cbacbf): Token length exception
hashfile 'hash.txt' on line 3 (bdefef...a0d208c790ae7ae17ecfc3cbacbf): Token length exception
hashfile 'hash.txt' on line 4 (01d78cde2365535e0933baae48a9abc2): Token length exception
hashfile 'hash.txt' on line 5 (01d78cde2365535e0933baae48a9abc2): Token length exception
hashfile 'hash.txt' on line 6 (01d78cde2365535e0933baae48a9abc2): Token length exception
hashfile 'hash.txt' on line 8 (d4d38dc098f00b204a9000998cfc8427e): Token length exception
hashfile 'hash.txt' on line 9 (sha256): Token length exception

+ Token length exception: 7/13 hashes
This error happens if the wrong hash type is specified, if the hashes are
malformed, or if input is otherwise not as expected (for example, if the
--username option is used but no username is present)

Hashes: 6 digests; 4 unique digests, 1 unique salts

```

```

kali@kali:~/Downloads/DART
File Actions Edit View Help

INFO: Removed 3 hashes found as potfile entries.

Host memory required for this attack: 0 MB

Dictionary cache hit:
+ Filename...: rockyou.txt
+ Passwords...: 14344385
+ Bytes.....: 139921507
+ Keyspace...: 14344385

Cracking performance lower than expected?

+ Append -D to the commandline.
This lowers the maximum supported password/salt length (usually down to 32).

+ Append -w 1 to the commandline.
This can cause your screen to lag.

+ Append -S to the commandline.
This has a drastic speed impact but can be better for specific attacks.
Typical scenarios are a small wordlist but a large ruleset.

+ Update your backend API runtime / driver the right way:
https://hashcat.net/faq/wrongdriver

+ Create more work items to make use of your parallelization power:
https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 1400 (SHA2-256)
Hash.Target....: hash.txt
Time-Started...: Sun Apr 2 11:16:59 2023 (25 secs)
Time-Elapsed...: Sun Apr 2 11:17:24 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 584.5 kH/s (0.57ms) @ Accel:256 Loops: Thr:1 Vec:8
Recovered.....: 3/4 (75.00%) Digests (total), 0/4 (0.00%) Digests (new)
Progress.....: 14344385/14344385 (100.00%)
Rejected.....: 0/14344385 (0.00%)
Restore.Point...: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: $HEX[206b7269737465566e16e6e65] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1...: Util: 48%

Started: Sun Apr 2 11:16:56 2023

```

C. RESEARCH PAPER

Priyadharshani B
UG Scholar
Department of IT
Sathyabama Institute of Science
and Technology Chennai, India
priyatamil0502@gmail.com

Kalaivani M
UG Scholar
Department of IT
Sathyabama Institute of Science
and Technology Chennai, India
kalaimutuganathan980@gmail.com

Sivasangari A
Associate Professor
Department of IT
Sathyabama Institute of Science
and Technology Chennai, India
sivasangarikavya@gmail.com

Abstract—

Information Gathering and Enumeration / Scanning place a vital role in Ethical Hacking/Penetration Testing. The more they enumerate the more they get access to the enumeration part of penetration testing is a little bit time-consuming because of using multiple tools, several scripts, and comprehensive strategies in single scripts so it is unified. It works very exceedingly fast. The result will be more precise and accurate when using comprehensive scripts. Data Analysis for Red Teamer is a CLI-based Pentesting Tool, which is only supported in Linux (Debian) Operating System. It will give proper results and valuable data is important to test. This is applicable in the field of security professions and pen testers. It will cover a big range of audiences in security aspects DART helps Penetration Testers / Red Teamers to enumerate information in various technologies like Networking, Web applications, Open Source Intelligence (OSINT), and Cryptography. It uses the utility of security tools like Nmap, Nmap Scripting Engine (NSE), Whois lookup, OSINT framework, Hash-Identifier, Hashcat, John the Ripper, and APL. DART helps Penetration Testers / Red Teamer to navigate quickly and uses the full potential of the listed tool with a single comprehensive script. Data Analysis for Red Teamer uses the efficacy of Nmap (Network Mapper) for Network Enumeration. Nmap is while performing penetration testing. Open source Linux command-line program nmap is used to search open ports, detect the vulnerability, host detection, and operating system. Web Enumeration is a bit tougher than host discovery. It uses a particular methodology to uncover everything about a target web service. The open-source paradigm emphasized the collection of information using free programs, various public platforms, or resources. Another absolute necessity to safeguarding data in communications systems is cryptographic protocols. Cryptography diagnoses the hash type, and hash crack and encrypts the hash passwords.

Keywords— Penetration Testing, Nmap, Network Security, Web Application Penetration Testing, Vulnerability Assessment, Hash Tracking, OSINT

I. INTRODUCTION

Data Analysis is the process to focuses on scanning and examining network traffic data, with the intention of prohibiting or rapidly diagnosticate spiteful tasks. Data analysis helps particular companies make sense of data. Data analysts consistently analyze primary data for penetration and tendency. They use numerous tools and approaches to help organizations make decisions and achieve. Red teaming is the practice of testing the security of an organization's systems by unitating a spiteful actor and managing secure systems or data. A red team can be an extrinsically

compressed group of penetration testers or a team within your own organization.

The software application, router, web service, as well as online version, be tested using only a method called pen testing to identify and exploit frailty. Penetration testing is mandatory, isolated from appraising security, to also evaluate the efficacy of protection systems and security approaches. Each sort of desktop application, and device, including software, requires a security audit, and architecture. A process that looks at a network, piece of technology, or internet that can find its defects, as well as gaps, is characterized as vulnerability analysis.

Cybersecurity is indeed the discipline for protecting sensitive data plus highly essential assets against online threats. A defense of networks and machines against mandatory disclosure, corruption, or destruction of their equipment, programming, or metadata, along with the distortion or manipulation of amenities they provide, is regarded as ethical hacking, occasionally referred to as security in the field of information technology. It is sometimes described as data security measures as well as information assurance. Cybersecurity is broken down into five categories. Getting data, Penetration testing, Security Testing, Trying to exploit, and Disclosure is just a few of these activities. DART, however, only addresses the initial three cybersecurity levels.

As is appropriate, network security has grown to be among the top priorities in the modern world, including both individual users and programmers. The predominant aim of this system is to discover the operating system, host detection, scan open ports and detect vulnerabilities. Then it gives protection to secure the web-based system as well as illustrates every aspect of the program's features. Next, the OSINT framework will outcome gather information about an individual or organization. After using Cryptography is an essential appliance for securing information in the computer, and it will examine the hash type and encrypts the hash passwords.

2. RELATED WORK

In 2016, Jai Narayan Goel¹ et al. and BM Mehre² et al. demonstrated how to use the Vulnerability assessment mechanism in its entirety as well as highlighting how it may be leveraged like a threat detection tool. A User acceptance testing enzyme's whole duration has been covered. Researchers have compiled a list of the world's top User acceptance testing programs, including gnu and widely viable, alongside details about the best ways to utilize tools as well as which virtual machines they are interchangeable with. Such techniques can just be extremely helpful for appraisal and just use during the Vulnerability assessment cycle. Experts have decided that there is a need to employ Highlights the characteristics more frequently.

In 2017, Sangeeta Nagpure, Sonal Kurkure Webpage security is aided by a risk evaluation including security testing for web-based, based applications. Pen testing, as well as security testing, are two distinct sorts of security tools. This would be required to carry out two independent jobs, and sometimes with odd results, within an identical space. Assessments and intrusion detection systems for whichever corporation's competent in operating in the security environment. Considering the weaknesses, either a conventional or automated exposure test is feasible. Those who evaluated a variety of known issues within Online apps concurrently with security audits using fully accessible as well as paid Internet assault methods.

In 2016 Prashant S. Shinde¹ et al, and Shrikant B. Ardhapurkar² et al has proposed the Study of Information security Through Scanning and Threat Intelligence which the variety of methods being used risk assessments and vulnerability scanning are fully described (VAPT). Pay careful attention to awareness regarding cyber security as well as the significance of keeping an organization sheltered. Those who reach the conclusion that there exists a different kind of VAPT tools, and that since vulnerabilities continue to develop, the ability to adequately should indeed be modified to explore security flaws while also becoming more versatile such that attack pattern signatures could be decided to add.

In 2018, Hasan, Ashikah, Meva, and Divyakant, has proposed Security testing on secure web applications which uses fundamental security of web applications through the methodology of potential vulnerabilities and functional testing (VAPT). So several cognitive as well as operational weaknesses might affect software applications Vulnerabilities can happen due to poor programming or an outdated system. VAPT process is specific access to secure the logical and extensive technical vulnerability.

In 2018, Dr. SurenderJangra, Dr. Pankaj Kumar Verma, and A Survey on Assessment of Vulnerability and Network Security by Penetration Testing approached this paper and The system security and scientific method for performing complex protection as well as its analysis were described. Also, it explored the frequently utilized techniques and tools for accumulating data and assessing weaknesses. Eventually, vulnerability scanning paradigms are examined in order to detect security flaws so that fixes can be developed to replace holes and enhance the protection of the system, intranet, or apps. A methodology is a combination of particular values, operations, and output values. It directs everyone on how to get to the outcome from input data. The phases of penetration testing: Establishing a goal,

In 2019, S.M. Zia Ur Rashid has proposed Identifying and Avoiding Mysterious Dns server Conquest Potential Threats Schema describing that perhaps just using a registry of domain names is a critical component both of internet safety and the web applications utilized. The confidentiality and functionality of its web addresses are completely the responsibility of such nameservers. Nevertheless, there is an opportunity to seize over all the subdomains from the external agencies as a result of delays in sample authentication and Whois configuration issues. Such articles layout just the consequences of the issue on the company and provide a comprehensive review of subdomain invasion.

In 2019, Goutam, Vijay, has suggested Online Safety is Improved by Risk Assessments and Ethical Hacking Applications that focus on web application security. Security care when this comes to organizations, and structures, including the financial services sector. The banking system is more influenced by these problems. To check the security of the web application. The organization executes penetration testing which points out the web

application security and attack actions. The structure will be mapped out which will deliver more safety to such websites.

In 2020, R. Pandey, V. Jyothinda, and U. K. Chopra Network penetration as well as contingency planning: The deployable approach Integration highlights the significance and scalability of electronic objects to growing hazard analysis. It suggests employing a supervised infrastructure to perform testing and get real results. Using evaluation methods, the Pic Microcontroller 3b1 must have been utilized to examine, analyze the absorptency, and evaluate support and knowledge flaws.

In 2021, AmeyKamunje, and Sourabh Mahale, has suggested Penetration Testing and Vulnerability Assessment which describes organizations that no longer have privately operated data and display the client's individual details among the security holes that could have been repaired. On a Penetration test, they identify this problem early as an attacker, and they advise how to fix them and eliminate eventually vulnerability.

In 2021, Tae Hyun Kim et al has approached Using Domain names to deliver global authentication and authorization to consumers in a quick and effective way is described in a survey of domain name system vulnerabilities and assaults. Nevertheless, the Domain name was first created lacking encryption, thus the data is not secure. We provide an outline of DNS issues, DNS assaults, and sometimes even security measures. For the goal of protecting against the assaults that are introduced and assessed, strikes were segmented in-depth by strategy. Its collection's key discovery is the introduction of a weakness, a vulnerability

In 2021, A. S. B. Singh, Y. Yusof, and Y. Nathan has proposed EAGLE: GUI-Based Penetration Testing Tool for Scanning and Enumeration is a Visual interface application that has been initiated made facilitate the process for even novice security researchers to still do screening as well as quantification. As a corollary, the modification of something like a broad range of parameters used mostly by high level level programming languages is eliminated. It is simple to navigate and comprehend the scan facts thanks to the equipment-appropriate outcome presenting and sharpening plugin.

In 2022,C. DeCusatis, P. Peko, J. Irving, M. Tencher, C. Laibach, and J. Hodge, Accessibility towards conducting security audits to distant medical services using inexpensive, fully accessible methods but rather open standards intellectual prowess has now been recommended and assessed inside A Framework for Open Source Intelligence Penetration Testing of Virtual Health Care Services. A creative-level manual testing approach for behavioral health care is offered. Considering feasibility for multiple approaches, which list prevalent weaknesses as well as recommended techniques.

In 2022, J K Perinsamy, Dakiniswari V, and Tapasya K has proposed Assessjet – Internet Fuzzing and Contingency Planning that assist there in the detection of errors in apps and websites. This is primarily consistent only with risk evaluation of online sites that utilizes user information Security Vulnerabilities can be explored by utilizing proper scanning tools on the hack end. This method generates a wide range of reports that covers the disparate security menacing a website

3. WORK PROPOSAL

In the proposed system, this system generates the result will be higher precise and accurate although using comprehensive scripts. This mechanism will produce proper results. It will provide genuine

outcomes and the valuable data is more essential. This tool supports Pentester / Red Teamer to enumerate information in disparate technologies like Networking, Web Applications, Open Source Intelligence, and Cryptography. The following Figure 1 describes about the architecture of the proposed system.

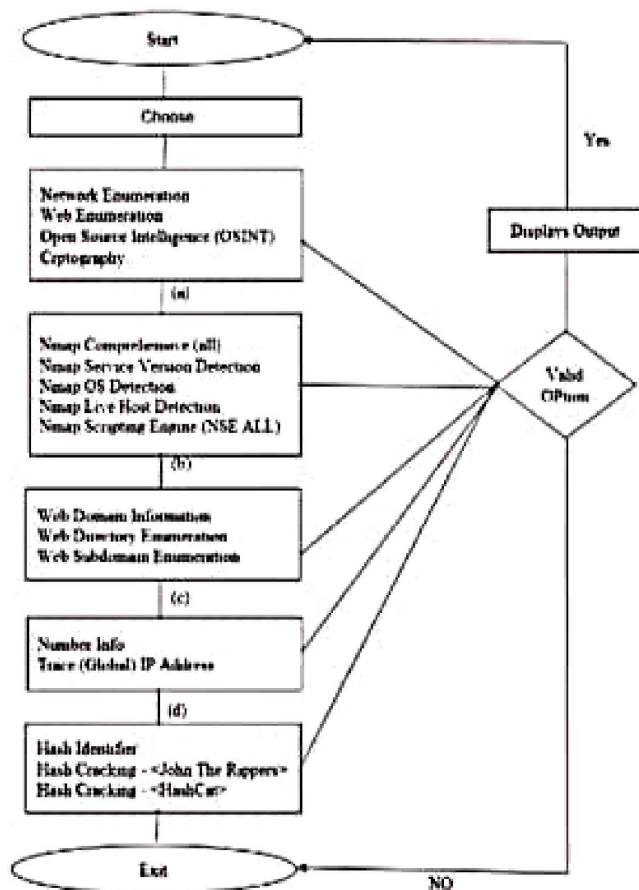


Fig 1 System Architecture of Proposed work

The proposed work of system architecture describes the process of Starting / Booting the Kali Linux (Main Operating System) and Metasploitable (Vulnerable Machine) by using VMware. Type the command ls will show the list of technologies. Then choose the technologies: Network Enumeration, Web Enumeration, Open-Source Intelligence (OSINT), and Cryptography. Once you choose to network, web, OSINT, and cryptography it will display the list of tools.

3.1 NETWORK ENUMERATION

Information is collected from a designated host or network through the method of network enumeration. We can utilize it to discover hosts, analyze open ports, as well as find security holes in computer systems. A component of "ethical hacking" for network security is networked scanning. Network enumeration may be carried out by certain penetration tests in an attempt to safeguard a software system. For network enumeration, choose any one tool, and then it asks you to type the IP address of the vulnerable machine. Once you completed typing of IP Address then press enter it will give the result like the state of the port, vulnerability, operating system, services, how many ports are closed, and at last, it will

display how long it takes for collecting that information. The following Figure 2 describe about the techniques in network enumeration

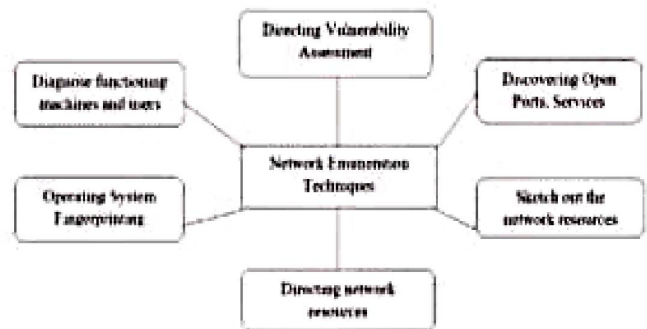


Fig 2 Techniques of Network Enumeration

Network Enumeration Contains

- a) Nmap Comprehensive (All)
- b) Nmap Service Version Detection
- c) Nmap OS Detection
- d) Nmap Live Host Detection
- e) Nmap Scripting Engine (NSE ALL)

3.1.1 NMAP COMPREHENSIVE (ALL)

Nmap is also known as Network Mapper. Network Internet address/port screening is done with the help of this fully accessible Debian control application functionality for the purpose of locating program installation. The manner it has indeed grown allows it to accurately measure equally wireless connections as well as isolated hosts. Nmap is a utility that not merely retrieves bandwidth utilization and yet also aids in detecting and preventing issues with the network. The CLI and GUI are both simple to utilize (GUI). Security experts might use Port scanning for verifying which objects were active on their internet, find open networks as well as services, and find existing vulnerabilities. Data collected upon this Linux kernel used by machines can also be found using Metasploit. When planning supplemental ways for software testing, it might provide precise details like Multiple operating systems. Working on Nmap is a three-step process which is Sending Requests, Receiving Replies, and Analyzing Responses. Nmap can perform some of the duties which are

- Finding connected machines on such a connection.
- Checking the network's available port numbers.
- Seeing routing paths and respective identification numbers on even a configuration.
- Spotting weaknesses in information assets

The following Figure 3 describes the comprehensive of nmap

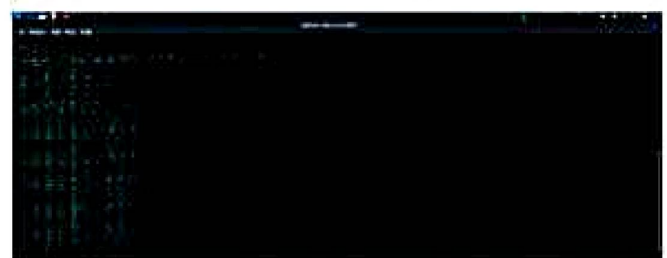


Fig 3 Nmap Comprehensive

3.1.2 NMAP SERVICE VERSION DETECTION

The database of Nmap-service probes contains queries to request various services as well as identical phrases to lead analysis

and analyze responses. According to Traceroute therapeutic effects, pins 25, 80, as well as 53 for Data transmissions all seem to be available. The vulnerability scanner is interested in asking about routes that might imitate domain controllers (DNS), application servers (HTTP), and default gateway (SMTP). This result seems to be typically quite reliable and valid because a huge majority of people who watch and listen to Tcp protocol 25 are actually carrier pigeon machines. The Target machine module consists of a mixture of queries that are used by version prediction to make requests for responses based on services and apps.

Querying internet providers on distant systems to discover the names as well as versions of the application. As users search for security flaws in the computer network, the specific version of a service is incredibly valuable. For every illegal mapping request, a targeted host investigates the parameters and answers. These issues have included the Transform Existing, Implementation Identifier, Unique Identifier, Subnet mask, Browser Type, as well as Virtual Machine Companions. Nmap listens for. Both databases help Nmap identify a service, including HTTP or SSH, that comes well after the port. Nmap then will make an attempt to establish its service-handling technology (including OpenSSH for ssh or Nginx or Apache for HTTP) and its specific sequence number. The following Figure 4 describes about the detection in services and version number.



Fig 4 Detection of services and version numbers

3.1.3 NMAP OS DETECTION

In Nmap OS detection, to discover the operating system of a tool, Nmap forwards scrutiny of Transmission Control Protocol together with User Datagram Protocol communications transmitted via the destination its response. The purpose of Linux Kernel Diagnostics (OSID) software is to traverse the internet but also determine the piece of software from each computer. The key component of data that can assist site managers in preventing security risks is the Kernel of each and every server just on a subnet, as well as those without predefined identities.

The term "fingerprinting" equally applies to operating system detection. OS identification is considerably effectual whenever at least two TCP ports—one active and one closed—are discovered. Users ought to be aware of the five extricate investigations, being accomplished to evaluate the OS. There are five extricate probes being executed. One or even more packets may also be present in each and every probe. All and every packets reply to the aimed system assists to identify the Operating System type. The following Figure 5 describes the probes in operating system.

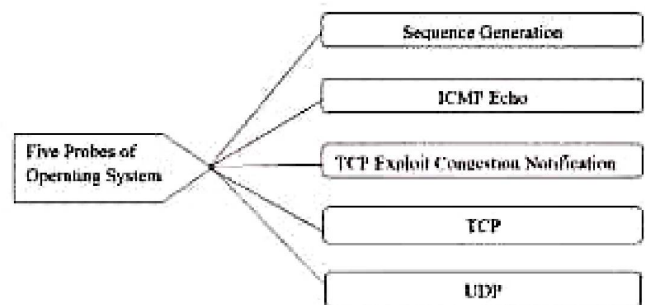


Fig 5 Probes of Operating System

3.1.4 NMAP LIVE HOST DETECTION

Live Host Detection is extremely essential for Information Security analysts and White Hat /Ethical Hacking. It makes it probable to scan an individual host or a massive network with thousands of hosts and identify pertinent information on it. We are referring to utilizing Nmap in Kali Linux to scrutinize the network for active hosts. Host detection is the sequence used mostly by Ip spoofing to obtain data on each and every server in a wireless router. The following Figure 6 describes the returned all the scanned and detected host



Fig 6 Nmap will return all scanned and detected host

Host detection is also known as ping scan. Nmap provides you with accurate info on all active IPs on your networks, and each IP can then be probed which allows the highest check of whether is used by an authorized or an unauthorized person.

Nmap uses the -sP flag for ping scanning. This form of scan is very advantageous for enumerating the host in a system. Nmap utilizing Transmission Control Protocol and User Datagram Protocol, observes cloud services, applications, and connections leveraging embedded resources via probe or perhaps a constructed script. This may steer to further enumeration.

3.1.5 NMAP SCRIPTING ENGINE (NSE ALL)

The programming framework of the network mapper is an extremely vigorous extension of Nmap, prolonging performance appreciably. NSE. It has the capability to permit users to produce and distribute their own scripts. To save a Nmap a Nmap Scripting Engine in the extension of nse. NSE is efficient in achieving a vast difference in inches. It can detect the devices on the system, scan for patulous ports, execute a whois query, and more. It can probe a network to detect a recently disclosed vulnerability. The rule activates causing the script to execute, and the active task in the script is achieved. This allows users to extend Nmap and make it more useful. NSE scripts are high for sketching proof of concept code since the programs are written in Lua, an effortless still strong language. NSE scripts must be coded in Lua language. It permits us to rapidly program all tasks and adaptable syntax is simple to attain. API permits its Port scanning tool to take into account arguments specifying designate believable processes to be used during measurement. Browsers of the Command - line can write or distribute codes thanks to that too. it elevates Server well above typical fast and easy inspections into an even more automated,

intricate one, including in space. The following Figure 7 describes about the rules and scripts of NSE

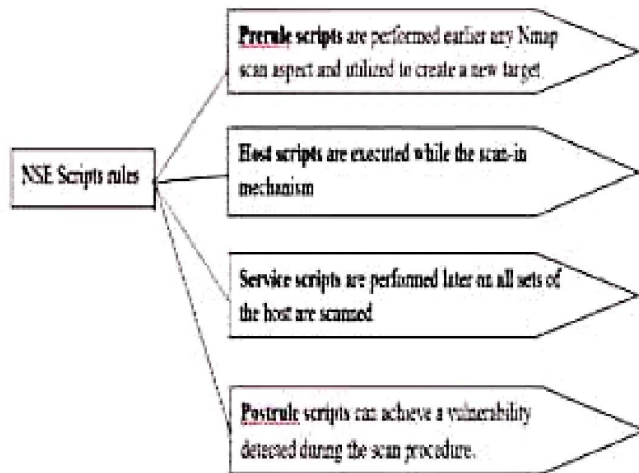


Fig 7 Rules and Scripts of Nmap Scripting Engine

3.2 WEB ENUMERATION

Web Enumeration is accustomed to exploring assets in that website and web server, it assists us to identify the machine name, username, admins and scripts, etc. It is an approach used to obtain data about the targeted domain, server, or website. It is familiar to find susceptible directories, risky subdomains, and weak domain data. It is beneficial to pass on later unearthing vulnerable directories and subdomains to the recognized individual to evolve it. The data can assist you to select more efficacious aims to apply in an assault, as well as use vulnerabilities in particular versions of web server software. For Web Enumeration, choose a tool, and then it asks you to type the domain name once you finish typing it will show the results like register domain ID, registry expiry date, domain status, creation date, updated date, terms of use, etc.

Web Enumeration contains

- Web Domain Information
- Web Directory Enumeration
- Web Subdomain Enumeration

3.2.1 WEB DOMAIN INFORMATION

The web address is a term or expression that defines an area of effective supervision, competence, or sovereignty upon that World wide web. During technical early diagnosis of location as well as in a multitude of other interconnected situations, domains are still used. A DNS server identifies potential a virtual network or alternatively, actual Internet Backbone (IP) assets, like the central server or a system used to access the site. Sites are extensively sometimes used to distinguish online service providers, such as web hosts and internet companies. Prior to 2017, 330.6 million web pages had been obtained. Both policies and procedures of the Domain Registration Organization dictate where names are issued (DNS). All names that are incorporated into the IP are considered domain names. Subdomains or register name's lower echelons. The following Figure 8 describes the information gathered on the domain of the web.

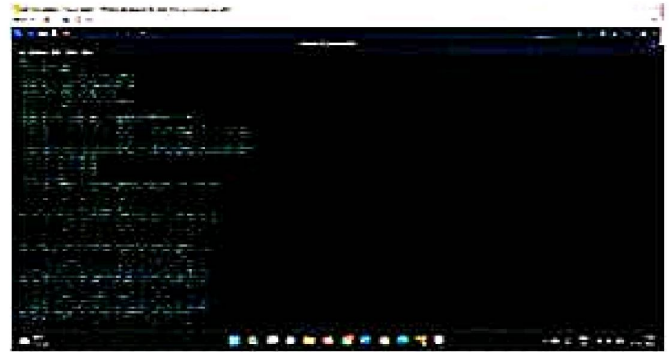


Fig 8 Information analyzed on the web domain

3.2.2 WEB DIRECTORY ENUMERATION

A web directory is a website that owns a listing of links to another website each of which is connected to an ordinary title and given a systematic method to discover websites. It is a data collection of websites organized in such a method that they ease navigation. These links to web labels are categorized according to particular criteria, such as alphabetical order. This assists users search for info in an individual way. A web directory builds it simple to discover websites by topic because a quest is beneficial in identifying internet sites utilizing vocabulary (plus if it's a visual google product, pictures, recording, etc.). Online portals provide a collection of hyperlinks that are organized to make navigation easier. A search query is provided by plenty of article directories thus individuals can conduct searches but instead browse the database. The following Figure 9 describes the directory enumeration.

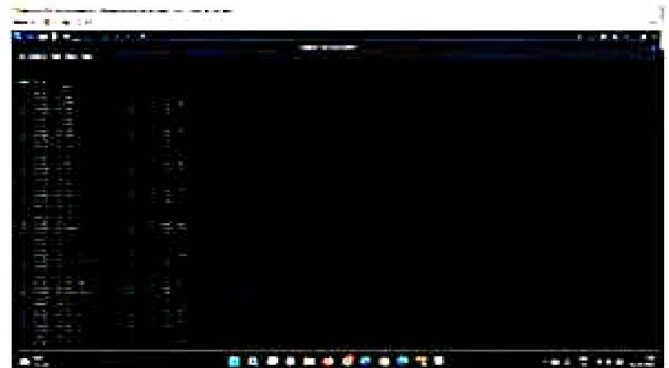


Fig 9 Enumeration in Directory

3.2.3 WEB SUBDOMAIN ENUMERATION

The repeating unit known as more than just a subcategory is just a section of something like a bigger name.. Subdomains can be accustomed to the disparateness of objects, such as hosting a blog; an e-commerce website, or even an entirely disparate website from the base domain. Subdomains are generally acclimated to separate various services or performances within an organization or Company. Subdomain enumeration is the mechanism of diagnosing each and every subdomain for a produced domain. This can be helpful for different kinds of goals, such as diagnosing the probable aim of an assault, or easily for authoritative purposes. Subdomain enumeration could assist to generate a range of protection assessments by disclosing domains/sub-domains of aimed companies and it enlarges the probability of discovering vulnerabilities or flaws. The following Figure 10 describes the scanning the whole details of the sub domain.

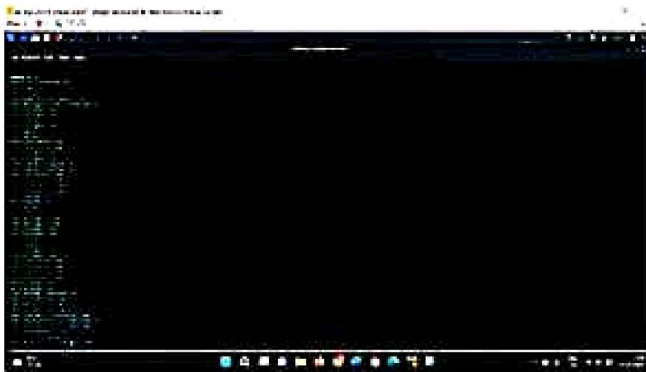


Fig 10 Scanning the details of the subdomain

3.3 OPEN SOURCE INTELLIGENCE (OSINT)

The term "open data intellectual ability" (OSINT) refers to instruments that make it possible the collection of publicly available or online data. Open-source data mining systems' main goal is to learn more, regarding individuals/organizations. Intelligence investigators and analysts support open-source information to improve their grasp of the menacing environment and assist secure organizations and individuals from well-known peril inside their IT surroundings. Skillset, cognitive prowess, and soft skills are all part of Open - source qualities. OSINT can be used to secure the network in different ways there are Detecting possible menaces, Performing risk assessment, and Surveillance of common platforms. OSINT frequently includes using modern analytical techniques, such as NLP and ML, to evoke penetration and intelligence from huge volumes of information.

OSINT contains

- a) Number Info
- b) Trace (Global) IP Address

3.3.1 NUMBER INFO

In the exploration of open-source intelligence, mobile numbers are crucial. Each and everyone has a phone, which is intimately related to their lives and contains extremely crucial information about them. To learn more about the phone number of the topic, use Number Info's OSINT to learn about the line type, carrier, target local format, target international format, prefix, location, and other pertinent details. The number itself contains some information, such as the nation, city, and occasionally the carrier, however, it is probable to bring out the additional data using a public platform. The following Figure 11 describes the piece of information with the help of a phone number.

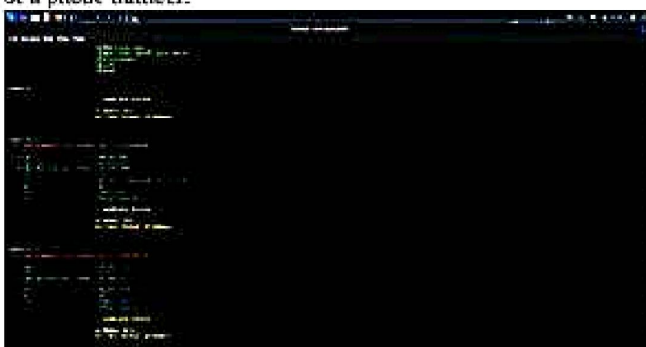


Fig 11 Taking a piece of information from a number

3.3.2 TRACE (GLOBAL) IP ADDRESS

An Internet user should be able to openly access a worldwide IP address. An IP address with a local scope cannot be routed to the Internet. This implies that even while your device won't be able to access the Internet if it has a local-scope address, you will still be able to use campus network resources. If you look up a global IP address, you can discover the name of the nation, the region, the city, the time zone, and the Internet Service Provider (ISP). It immediately displays the ISP's location on Google Maps. The following Figure 12 describes the ISP's on the map with help of global Ip

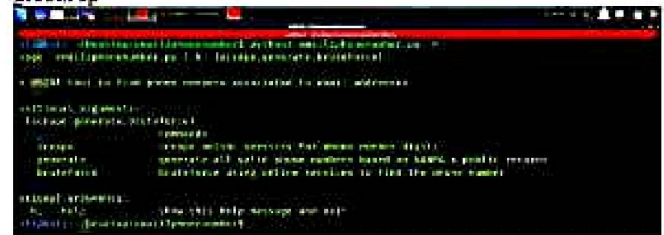


Fig 12 displays the ISP's on the map

3.4 CRYPTOGRAPHY

Besides converting data together into a secured configuration, raw data can be protected via encryption. Manuscript correspondence has already been shielded against fraudulent reading through the implementation of cryptography since the beginning of recorded history. Crypto encodes messages and data so prevent anyone other than the destination node from seeing, interpreting, or processing it. In the modern era, encoding is used to safeguard metadata. A goal of this computational science field is to organize details in a manner that only permit users can perceive

Cryptography contains

- a) Hash Identifier
- b) Hash Cracking - <John The Rippers>
- c) Hash Cracking - <Hashcat>

3.4.1 HASH IDENTIFIER

Software that can distinguish between the various hashing algorithms used to secure data, particularly passwords. Data exchange between integrated data management systems is done using the encryption method of hashing. The hashing identifier in Eloquent can be used to practice and recognize two different types of hashes in order to exchange phone numbers and email addresses in an unidentified fashion. The capability provides hashed versions of the recent contact field information and allows you to map these details in other systems without providing any Personal Identifiable Information (PII). The performance uses SHA256 hashes to peculiar identity contacts. The following Figure 13 describes the discovering of hash to protect the data



Fig 13 Identifying the hash to secure data

3.4.2 HASH CRACKING - <JOHN THE RIPPER>

The tool for breaking passwords John The Ripper can recognize the majority of password hash types and offers a user-friendly command-line interface. John the Ripper is a password cracker that works offline. In other words, it searches collected data for passwords without getting in touch with the target. Due to the fact that the method is often performed locally, on the attacker's workstation, this prevents the production of suspicious traffic. Although its primary application is to decrypt password hashes, John may also be used to decrypt encrypted private keys, secured archive files, and many other kinds of data.

3.4.3 HASH CRACKING - <HASHCAT>

Hashcat is a well known and efficacious passcode cracker that is used by penetration testers, system administrators, perpetrators, and intelligence agencies. The hashcat seems to be a multi-threading functionality that allows you to set the numerous threads and prioritize execution. Password cracking differs from assuming a site username and password, which typically allows only one limited set of assumptions before holding the account. Rather, anyone who has managed to gain access to a computer system containing encryption keys ("hashes") will often attempt to break those hash values in order to retrieve the passwords. The Following Figure 14 describes the hash code cracking with the help of hash and hash number



Fig 14 Cracking hash codes

4. RESULT AND DISCUSSION

The testing results should include a detailed analysis of the vulnerabilities discovered. It is the predominant and also most important distinction between pen tests and vulnerability assessments. The vulnerabilities discovered must always be reported accurately to the organization so that essential modifications can be made to repair the weakness throughout their processes. As comprehensive scripts are used, the outcome will become more detailed, accurate, and precise. This should produce high accuracy, as well as beneficial data is essential for testing. Also, it provides security for the web-based application as well as shows all of the application's detailed information. Following that, the Open source structure would also obtain data on a specific person or organization. Even when using Cryptography, which is an effective mechanism for safeguarding data stored on a computer, which will start examining a hash variety and authenticate the hash credentials.

5. PROSPECTIVE IMPROVEMENTS

In the future, According to a technical report, the open source intelligence (OSINT) market will develop at a significant rate between 2020 and 2026. The increase in the availability of open-source data, as well as rising cyber risks, is expected to assist future

growth. Analysts predict that perhaps the huge amount of information dissemination will have a critical effect on the market performance from 2020 to 2026. During the forecast period, the market will be assisted by increased accessibility to public information and advancements in technology. Over the course of time, OSINT would be developed to take the entire details of an individual person which will gather utilizing extraneous APIs, Google Eavesdropping, phone books, and also web crawlers, collect appropriate data such as nation, quick response code, as well as transmission OSINT efficient process.

6. CONCLUSION

Everything is going online on the internet as a result of the ongoing digital revolution, and as we all know, the web is not an extremely secure protocol. As a result, precautions must be taken to protect the authenticity as well as the secrecy of the info. To expand reports of information security, cyber threats, as well as information leakage, researchers should ensure the security of our vital information. A vulnerability assessment is a complete and accurate method for detecting security vulnerabilities. This study provides crucial details about the stage as well as the significance of the testing process. System testing is divided into three stages: information gathering, scanning, and frailty evaluation. Each of the aforementioned phases can be done automatically utilizing Nmap and other tools.

7. REFERENCES

- [1] Goel, Ja & Mehre, Babu. (2016). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science*, 57, 710-715. 10.1016/j.procs.2015.07.458.
- [2] S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," 2017 International Conference on Computing, Communication, Control and Automation (ICCCUBEA), Pune, India, 2017, pp. 1-6. doi: 10.1109/ICCCUBEA.2017.8463920.
- [3] Prashant S. Shinde; Shrikant B. Ardhapurkar. (2016). Cybersecurity analysis using vulnerability assessment and penetration testing. 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave) (IEEE Conference Publication), 1-5, DOI:10.1109/STARTUP.2016.7583912.
- [4] Hasan, Ashikali and Meva, Divyakant. Web Application Safety by Penetration Testing (2018). *International Journal of Advanced Studies of Scientific Research*, Volume 3, Issue 9, 2018, Available at SSRN.
- [5] SurenderJangra, Pankaj Kumar Verma, "A Survey on Vulnerability Assessment & Penetration Testing for Secure Communication" 2018 3rd International Conference on Trends in Electronics and Informatics (ICTEI) (2019): 320-325.
- [6] S.M.Z.U. Rashid, M. I. Kamrul and A. Islam, "Understanding the Security Threats of Esoteric Subdomain Takeover and Prevention Scheme," 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox'sBazar, Bangladesh, 2019, pp. 1-4. doi: 10.1109/ECCE.2019.8679122.
- [7] Goutam, Arvind & Tiwari, Vijay. (2019). Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application. 601-605. 10.1109/ISCON47742.2019.9036175.
- [8] R. Pandey, V. Jyothindar and U. K. Chopra, "Vulnerability Assessment and Penetration Testing: A portable solution Implementation," 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), Dhimal, India, 2020, pp. 398-402. doi: 10.1109/CICN49253.2020.9242640.

- [9] Amey Kamunje, Sourabh Mahale, Niraj Khare and Pratik Daund, "Penetration Testing and Vulnerability Assessment", 2021. 2320-9364, ISSN (Print): 2320-9356
- [10] Tae, Hyun & Kim, Douglas & Reeves,. (2021). A survey of domain name system vulnerabilities and attacks. 1. 34-60.
- [11] A. S. B. Singh, Y. Yusof and Y. Nathan, "EAGLE: GUI Based Penetration Testing Tool for Scanning and Enumeration," 2021 14th International Conference on Developments in e Systems Engineering (DeSE), 2021, pp. 97-101, doi: 10.1109/DeSE54285.2021.9719338.
- [12] C. DeCusatis, P. Peko, J. Irving, M. Teache, C. Laihach and J. Hodge, "A Framework for Open Source Intelligence Penetration Testing of Virtual Health Care Systems," 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2022, pp. 0760-0764, doi: 10.1109/CCWC54503.2022.9720785.
- [13] J. K. Periasamy, D. V and T. K., "AssessJet - Penetration testing and Vulnerability Assessment for Websites," 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), 2022, pp. 1-4, doi: 10.1109/IC3IoT153935.2022.9767928.