***BUILDING A CUSTOMIZED OPENSOURCE (OS)***

***WITH CYBERSECURITY FRAMEWORK***

**M. Kowshik** **Mr. E.R. Ramesh**

M.Sc CFIS, Center of Excellence in Digital Forensics,

Department of Computer Science and Engineering, Perungudi, Chennai-600089

Dr. M.G.R Educational and Research Institute,

Maduravoyal, Chennai-600 095.

**Ms. Sarika Jain Dr. S. Geetha**

Center of Excellence in Digital Forensics, Head of the Department

Perungudi, Chennai-600089 Department of Computer Science and engineering,

Dr. M.G.R Educational and Research Institute,

Maduravoyal, Chennai-600 095.

*Abstract*— Open-Source Knowledge, frequently alluded to as OSINT, can mean numerous things to numerous individuals. Authoritatively, it is characterized as any knowledge delivered from openly accessible data that is gathered, took advantage of, and dispersed sooner rather than later to an suitable crowd to address a particular knowledge prerequisite OSINT search procedures don't have any significant bearing just to sites. There are some free programs that computerize the pursuit and assortment of information. Utilizing of OSINT, you can go way more profound and challenge what we typically comprehend as the openly accessible information. That is the reason call it reconnaissance obtaining. With the goal that the client must mindful of openly data spillage. So our fundamental thought process of this undertaking is we will construct an OSINT machine without any preparation utilizing a proxmox server modify the portion renditions, virtual box VM climate and taking Linux appropriation So this custom OSINT os adjusted from the buscador operating system and some more... presently it's not accessible for security purposes so we are overhauling a portion of these highlights of the instruments from the old ones. The fundamental objective of OSINT os is client should realize about his data is spilled or not. The client needs a fundamental information on PC and virtualization ideas so the operating system will to guide the method involved with utilizing instruments it will be straightforwardness to use as basic

*Keywords- OS, OSINT, Internet Relay Chat , GNU's Not Unix, WEE chat;*

# **Introduction**

This undertaking is fundamentally centered around the typical client and new to OSINT expert so our project utilizes an OSINT (Open Source Insight) structure for this operating system customization process. So this custom OSINT os adjusted from the buscador operating system and some more... implanted instruments currently it's not accessible for security purposes so we are overhauling a portion of these elements of the instruments from the old ones. Past operating system doesn't conceal plainly the instruments that have utilized and some of them not redesigned and it will cause like bogus positive reports. We making into straightforwardness to utilize and we making a local area like a kali Linux engineer we give the operating system to use in a low arrangement specs framework. We attempting to carry out the update script for this situation the client utilizing another kind of Linux then the client can essentially run up the content to change entire framework into an OSINT reason and it will eliminate some of undesirable pre-stacked applications.

Open-Source Knowledge, frequently alluded to as OSINT, can mean numerous things to numerous individuals. Formally, it is characterized as any insight created from freely accessible data that is gathered, took advantage of, and scattered on time to anfitting crowd to address a particular insight prerequisite OSINT search methods don't matter just to sites. There are some free programs that mechanize the hunt and assortment of information. Utilizing of OSINT, you can go way more profound and challenge what we normally comprehend as the freely accessible information. That is the reason call it reconnaissance obtaining. With the goal that the client must mindful of openly data spillage. So our primary rationale of this undertaking is we will construct an OSINT machine without any preparation utilizing a proxmox server redo the piece forms, virtualbox VM climate and taking Linux appropriation So this custom OSINT os adjusted from the buscador operating system and some more... presently it's not accessible for security purposes so we are redesigning a portion of these highlights of the instruments from the old ones.. The client needs an essential information on PC and virtualization ideas so the operating system will to guide the method involved with utilizing devices it will be simplicity to use as basic.

**WHAT IS OSINT**

OSINT (Open-Source Insight) is the assortment and investigating data that is accumulated from public or open sources. It's one of the data gathering strategy in entrance testing field These open sources can be something as basic as a Google search or looking through online entertainment like Facebook, Instagram or LinkedIn. You will be stunned by how much information there is streaming out there openly (or efficiently) you can accumulate on people or organizations. Generally focused on (or semi-designated) assaults start with some sort of OSINT information gathering. Open-source data is accessible to everybody. That implies it can likewise be utilized for odious purposes by danger entertainers and foe bunches similarly as effectively as it is gotten to by network safety experts or the knowledge local area. One of the most well-known reasons cybercriminals influence OSINT is for social designing purposes. They will frequently accumulate individual data of potential casualties by means of virtual entertainment profiles or other internet-based movement to make a profile of the person that can then be utilized to modify phishing assaults. OSINT can likewise be utilized for discovery avoidance, for example by auditing freely uncovered insight, danger entertainers know where associations might set up safeguard lines and search for substitute strategies for assaults.

One more typical procedure utilized by programmers is Google hacking, which is additionally now and then alluded to as research dorking. Google hacking includes utilizing Google's web crawler and applications to run exceptionally unambiguous order look through that will distinguish framework weaknesses or delicate data. For instance, a cybercriminal can execute a record look for reports that contain the expression "delicate however unclassified data." They can use devices to check for any misconfigurations or security holes in a site's code. While there is a colossal measure of openly accessible data that can be utilized by online protection experts, the sheer volume of OSINT information which is scattered across various sources — can make it hard for security groups to remove key data of interest. Also, it is critical that the high-esteem, applicable data accumulated through OSINT movement is then incorporated with network safety devices and frameworks.

The OSINT structure is a procedure that incorporates information, processes, strategies, devices and methods to assist the security with joining distinguish data about a foe or their activities rapidly and precisely.

An OSINT system can be utilized to:

* Lay out the computerized impression of a known danger
* Accumulate all accessibility knowledge about an enemy's movement, interests, strategies, inspiration and propensities
* Arrange information by source, instrument, technique or objective
* Recognize chances to improve the current security act through framework suggestions

# **Literature survey**

Open-source operating systems are free and can be customized by anyone. They are popular because they offer users greater control over their systems and are more secure than proprietary operating systems. Popular open-source operating systems include Linux, FreeBSD, OpenBSD, and NetBSD. In recent years, several customized open-source operating systems have been developed for specific cybersecurity applications, such as the Kali Linux operating system for penetration testing and the Tails operating system for anonymous browsing.

Customized Open-Source Operating Systems with Cybersecurity Frameworks:

Several customized open-source operating systems have been developed with cybersecurity frameworks. These operating systems provide a pre-configured environment for cybersecurity professionals to perform their tasks. For example, the BlackArch Linux operating system is a customized open-source operating system with more than 2,000 pre-installed tools for penetration testing and cybersecurity analysis. The ArchStrike operating system is another customized open-source operating system based on Arch Linux that is specifically designed for cybersecurity professionals.

The importance of OSINT has increased significantly in recent years, as it helps organizations to identify and mitigate potential threats. Mark OS is a customized open-source operating system built specifically for OSINT activities. This literature survey provides an overview of the existing and proposed contents of Mark OS. Mark OS is based on the Buscador operating system, which is an OSINT-focused Linux distribution. The contents of TL OSINT OS, buscador OS include pre-installed tools and software that are essential for OSINT activities.

One of the key tools included in Mark OS is Maltego, which is a data-mining tool used for gathering and analysing information. Maltego is a popular OSINT tool that allows users to gather information about a target from various sources, including social media, online databases, and search engines. Maltego also allows users to visualize the relationships between different pieces of information, which can help them to identify potential connections and patterns. Another important tool included in Mark OS is Recon-ng, which is a reconnaissance framework used for information gathering. Recon-ng allows users to gather information about a target through a variety of sources, including social media, search engines, and online databases. The tool also includes a module system that allows users to extend its functionality. Mark OS also includes theHarvester, which is a tool used for email harvesting. theHarvester can be used to gather email addresses and other information about a target from various sources, including search engines and social media platforms. This tool is useful for conducting phishing campaigns or other types of social engineering attacks. Another tool included in Mark OS is Shodan, which is a search engine used for finding internet-connected devices. Shodan can be used to identify vulnerable devices on the internet, such as servers or routers, that could be exploited by attackers. This tool is often used by cybersecurity professionals to identify potential vulnerabilities in their own networks.

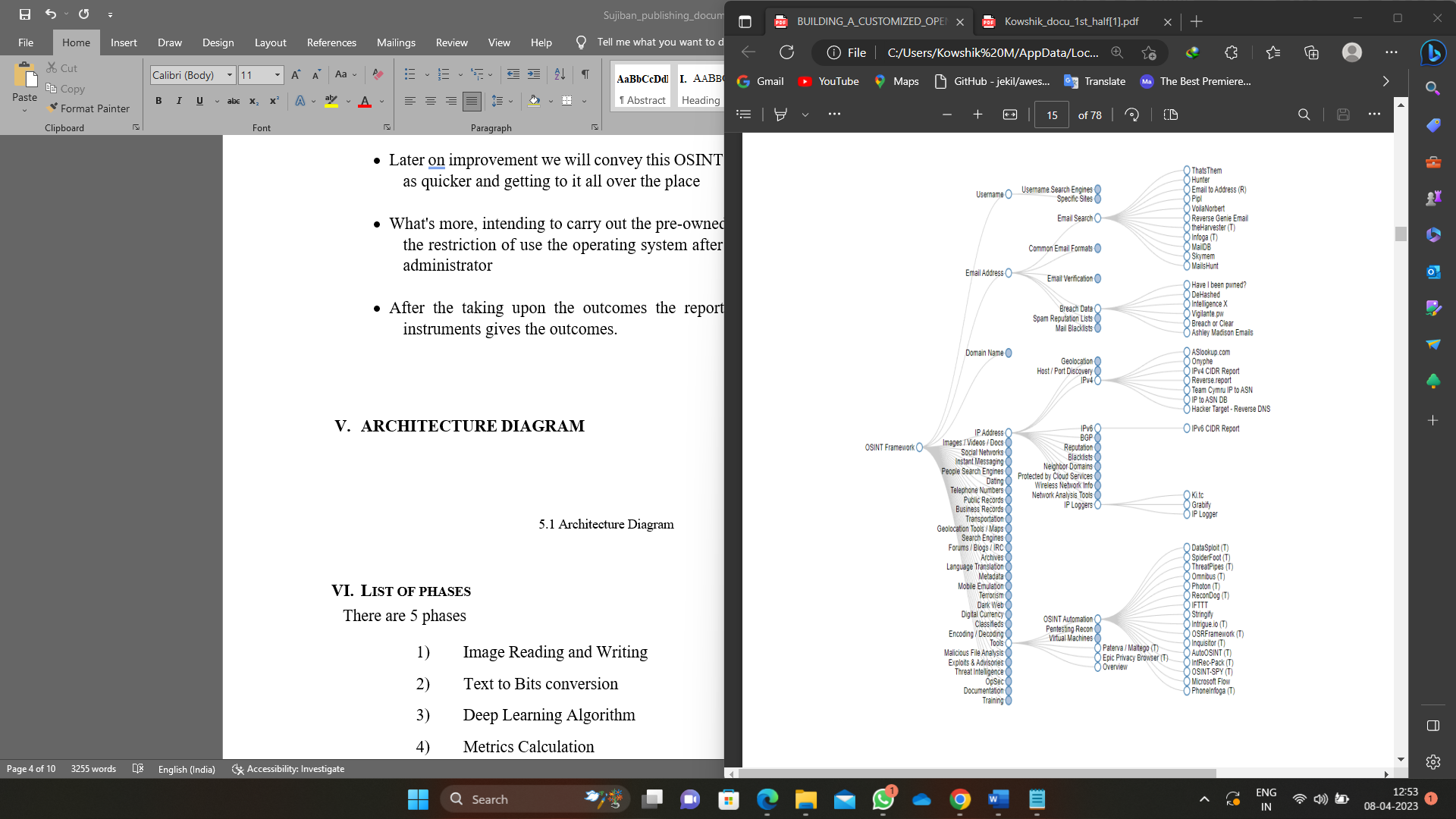
# **Existing system**

* In this current of this operating system by and large the altered apparatuses are there in the pre-assemble structure
* This permits the adaptability of utilizing it anyplace you approach a PC, whether or not or not you have your own gadget with you. we can just download it and use it all over
* Some distro of this OSINT os is light weight
* The OSINT expert individual practice to carry out an examination then it will supportive to utilize this OSINT os
* Once in a while it will help for the leveling up abilities so a portion of the renditions are doing a CTF (catch the flag) machines moreover

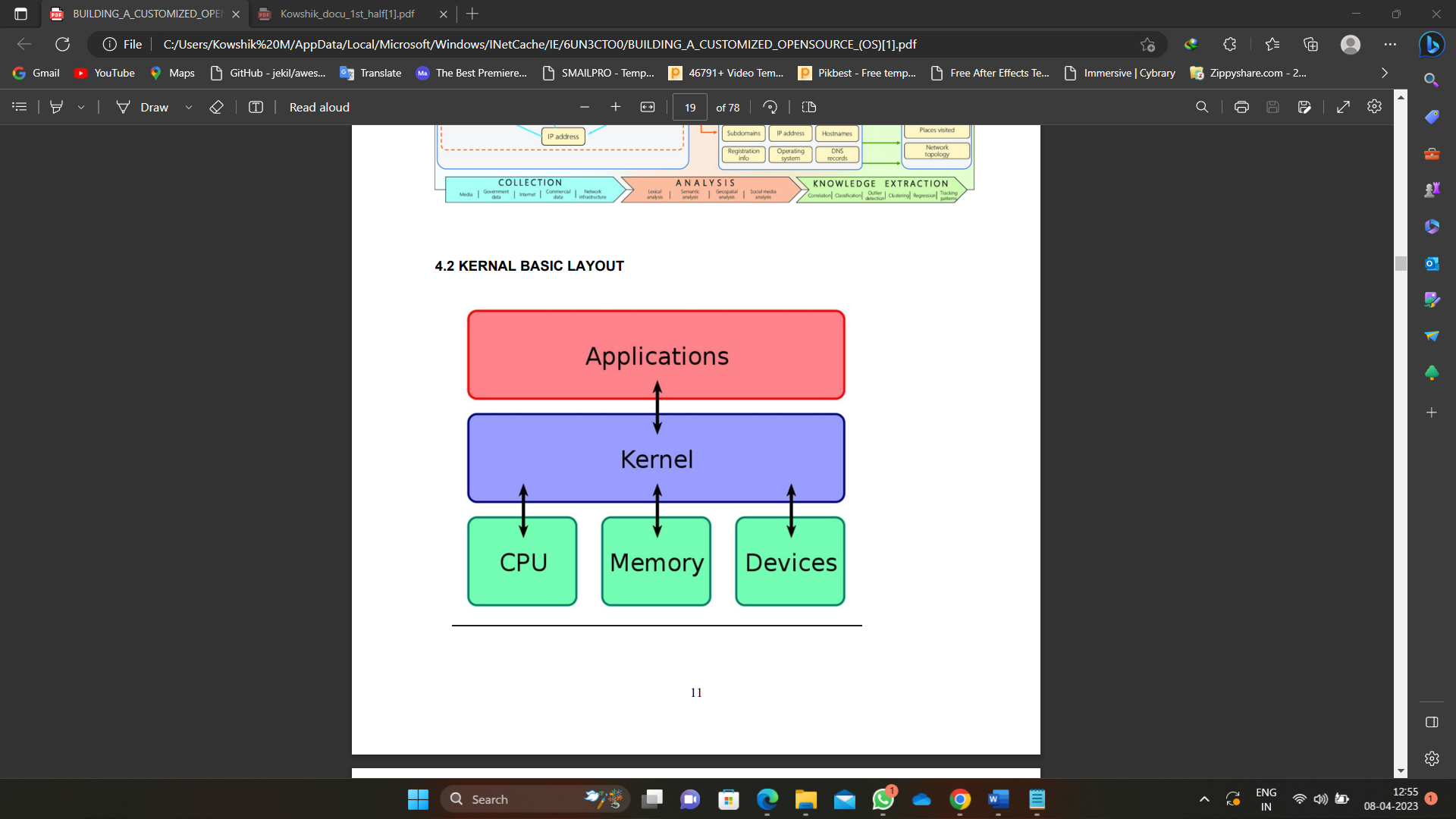
# **proposing system**

* We will improve this operating system into a less complex approach to getting to it like a single tick of establishment over to switch around into the OSINT operating system
* Contrasting with the more seasoned form we are redesigning every single device on the off chance that not works we attempt to overhaul into the elective instruments
* In more seasoned renditions a large number of the device's outcomes accompanies for the most part a bogus positive one and some of them are not in fresher one possibility getting a misleading report will be kept away from we will redesign nearly everything
* Later on upgrade we will convey this OSINT os into the cloud stage to carry out examination as much as quicker and getting to it all over
* After the taking upon the outcomes the reports are produced consequently after the effective of each apparatuses gives the outcomes
* Later on improvement we will convey this OSINT os into the cloud stage to carry out examination as much as quicker and getting to it all over the place
* What's more, intending to carry out the pre-owned admittance cutoff points to cloud occasion and confine the restriction of use the operating system after that should be change the secret word by root client of administrator
* After the taking upon the outcomes the reports are created consequently after the fruitful of each instruments gives the outcomes.

# **ARCHITECTURE DIAGRAM**



5.1 Architecture Diagram



5.2 Architecture Diagram

# **List of Modules**

In the application, the following modules are implemented.

1. Update Process Automation
2. Chatting Services
3. Framework
4. Email Osint
5. Anonymous Chatting Service

## **Update Process Automation**

Bash is a popular shell used in Linux and other Unix-based operating systems. It provides a powerful and flexible command-line interface for users to interact with the operating system.

* Command line interface: Bash provides a command-line interface for users to run commands and perform various tasks.
* Command history: Bash maintains a history of previously run commands, allowing users to easily recall and reuse them.
* Command completion: Bash provides command completion features, making it easier to type commands and reducing the risk of typos.
* Environment variables: Bash provides a way to set and use environment variables, which are used to store information that can be used by scripts and other programs.
* Scripting: Bash provides a scripting language that can be used to automate tasks and perform complex operations.

## **Chatting Services**

IRC (Internet Relay Chat) is a system of virtual chat rooms that allow users to communicate with one another in real-time over the internet. It was one of the first online communication systems and is still widely used today, especially in the opensource communities for anonymous and gaming communities.

Here are the key components of an IRC service:

Server: The IRC server is the backbone of the IRC network. It is responsible for managing the communication between clients, storing messages, and maintaining channels and user information.

Client: An IRC client is a software program that allows a user to connect to an IRC server and participate in chat rooms. There are many different types of IRC clients available, ranging from simple text-based clients to more advanced graphical clients.

Channel: A channel is a virtual room within an IRC network where users can communicate with one another. Users can join and leave channels as they please, and channels can be configured with different modes, such as password protection or moderation.

Nicknames: A nickname is a unique identifier that a user chooses to represent themselves within an IRC network. Nicknames are used to identify users in channels and to direct messages to specific users.

Commands: IRC uses a set of commands that allow users to perform actions such as joining and leaving channels, sending messages, setting user modes, and querying server information. These commands are entered into the client and sent to the server for processing.

Scripting: Many IRC clients provide support for scripting, which allows users to automate tasks or add custom functionality to their client. Scripting can be done in a variety of programming languages, including Perl, Python, and Ruby.

Here are some of the main modules that make up an IRC service using of freenode server:

IRC Server: The server component of an IRC service provides the central hub for communication and acts as the intermediary between IRC clients. The server is responsible for routing messages between clients and maintaining the state of the network and its channels.

IRC Client: An IRC client is a software application that allows users to connect to an IRC server and participate in chat rooms. Clients typically provide a graphical user interface (GUI) for sending and receiving messages, managing channels, and other tasks.

Protocol: IRC uses a simple text-based protocol for communication between clients and servers. The protocol defines the syntax and semantics for messages exchanged between clients and servers, including commands for joining and leaving channels, sending messages, and more.

Channel Management: An IRC service typically includes support for managing channels, including creating new channels, inviting users to channels, and moderating channel conversations.

User Management: An IRC service typically includes support for managing users, including registering nicknames, authenticating users, and managing user privileges and access.

Network Services: The Freenode network incorporates a scope of administrations to help clients and networks, including an electronic point of interaction for interfacing with the organization, a help channel (#freenode), and instruments for overseeing channels and clients

## **Framework**

Maltego: Maltego is a data mining and intelligence gathering software used for open-source intelligence (OSINT) and digital forensics investigations, to gather, analyse, and visualize information about a specific target in a graph-like format.

Recon-ng: Web reconnaissance framework for gathering and organizing information about a target from various open-source sources, designed to be used for security research and investigations.

## **Email OSINT**

THE HARVESTER: is a reconnaissance tool used for gathering email addresses, subdomains, and hostnames of a target, from various public sources like search engines, PGP key servers, and others, for security research and investigation purposes.

EMAIL HARVESTER: An email harvester is a tool used to collect and gather email addresses from various sources such as websites, social media platforms, and other publicly available databases, for the purpose of marketing or spamming.

HOLEHE: Holehe is a tool used for security research and reconnaissance, to identify the username across multiple websites and services, and gather information about a target, such as their email addresses, real names, and other public information.

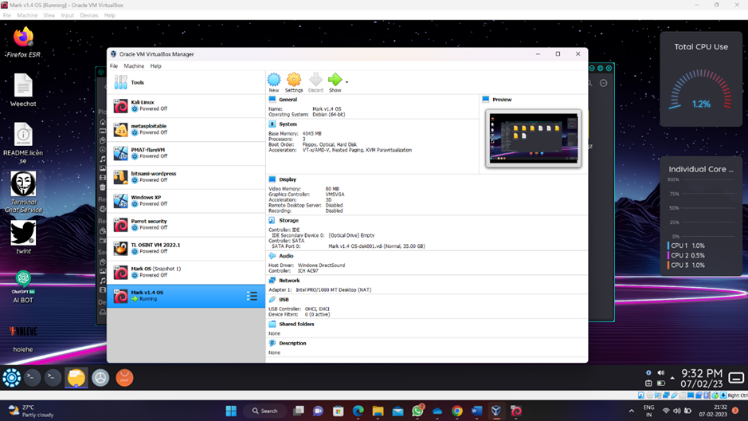
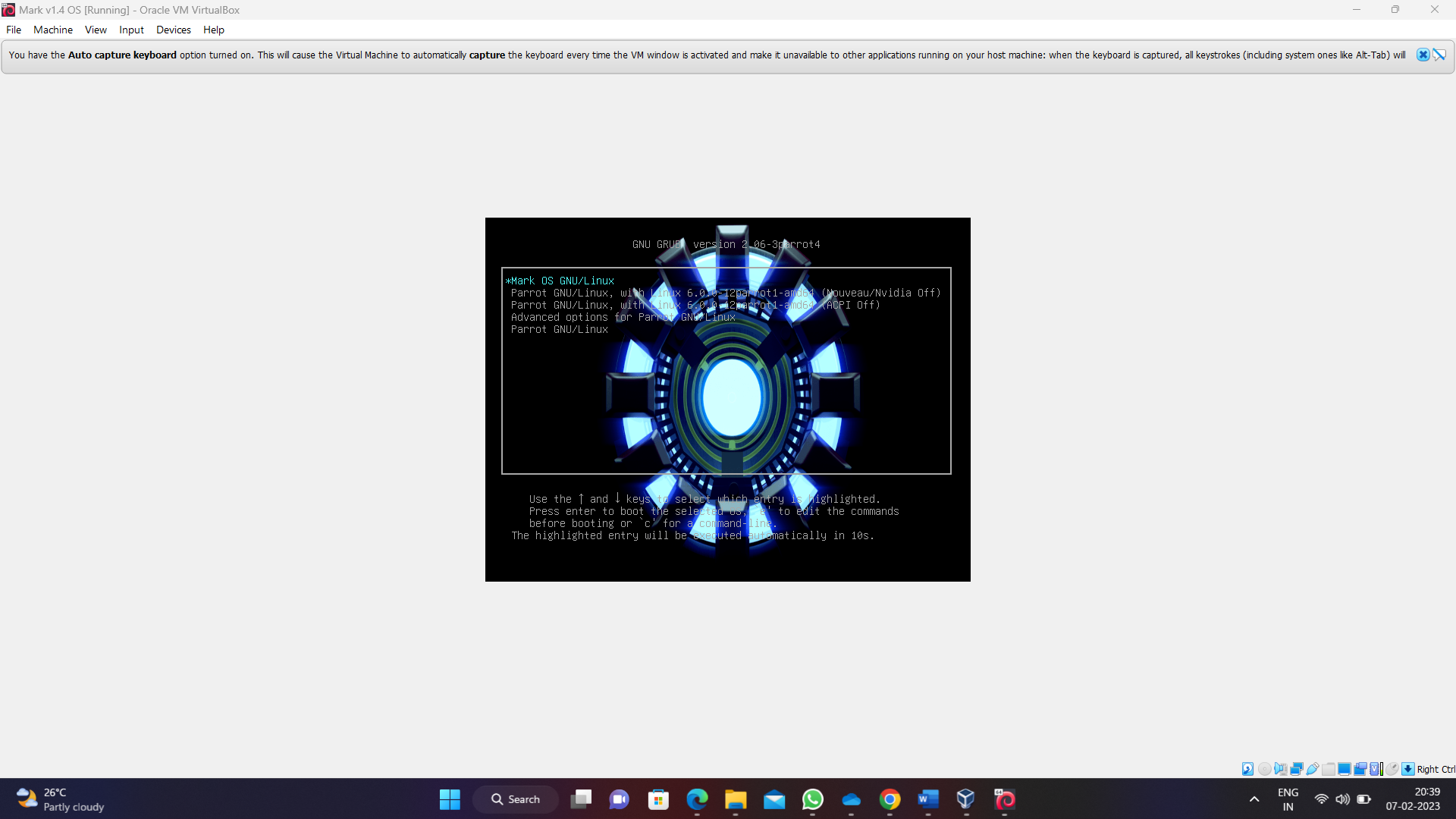
## **Anonymous Chatting Service**

TERMINAL BASED CHAT (WEECHAT): Weechat is a free, fast, and light-weight terminal-based IRC client, used for chatting and communicating with people over the Internet, offering features like script ability, multiple protocols support, and a customizable interface, for efficient and flexible real-time communication. offering features like encryption, logging, and scripting, for use in technical and collaborative settings.

OPEN AI PROJECT (chatGPT): ChatGPT is a state-of-the-art language model developed by OpenAI, used for natural language processing tasks, such as text generation, translation, and conversation, providing a conversational interface for input and output, and demonstrating human like language understanding and response capabilities.

# **SCREEN SHOTS**

**7.1 Virtual Machine Configuration 7.2 Mark OS Custom Boot Menu**

 ****

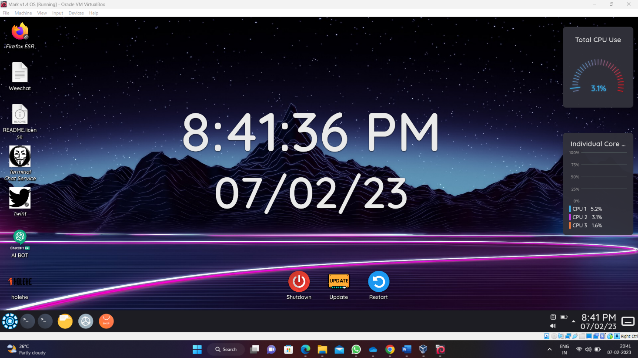
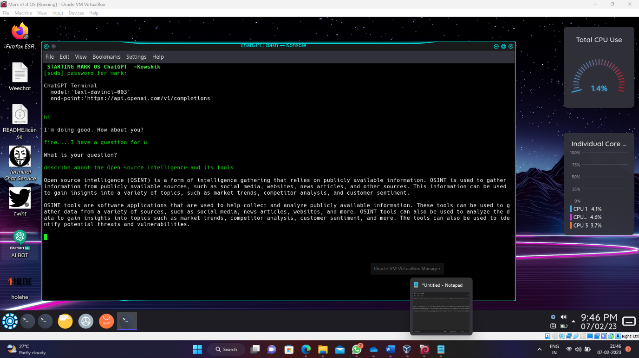
7.1 Virtual machine configuration 7.2 Mark OS custom Boot menu

**7.3 Mark OS Plymouth Custom Bootloader 7.4 Custom Login Panel Plugin**

## 

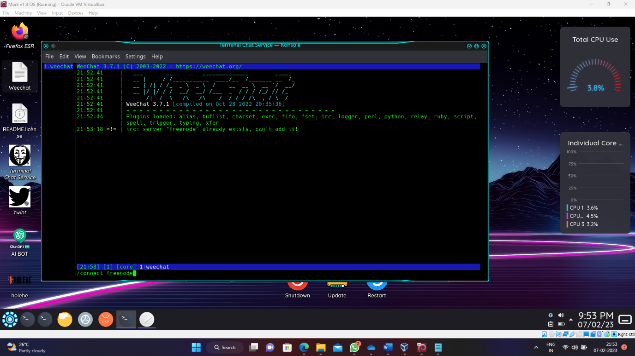
7.3 Mark OS Plymouth Custom Bootloader7.4 Custom Login Panel Plugin

**7.5 Mark Os Kde Plasma Interface 7.6 Terminal Based ChatGPT**

**** 

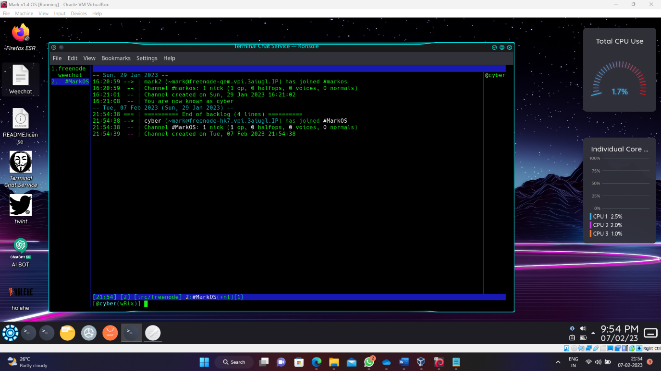
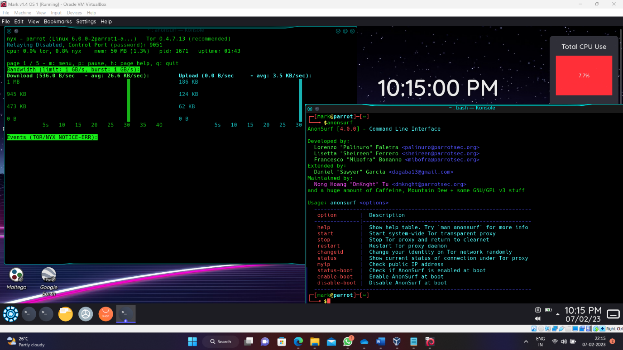
7.5 Mark OS kde Plasma Interface 7.6 Terminal Based ChatGPT

**7.7 WEEchat service 7.8 Freenode server (Anonymous Communication)**

** **

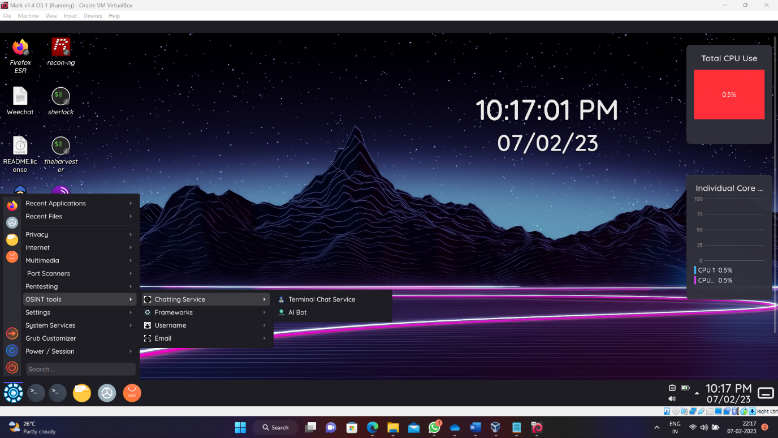
7.7 WEEchat Service 7.8 Freenode server

**7.9 Joining the MarkOS community 7.10 Anonsurf Working**

****  ****

7.9 Joining the Mark OS community 7.10 Anonsurf Working

**7.11 OSINT Tools In Launcher**

****

# **Conclusion**

OSINT based operating system would likely emphasize the importance of gathering information from publicly available sources to gain insights into various systems and networks. This information can be used to identify vulnerabilities, monitor trends, and support decision-making processes. OSINT tools and techniques provide a powerful way to collect data, but it's important to use them ethically and responsibly to avoid violating privacy and security policies. The OSINT operating system can be used for both defensive and offensive purposes, and it requires a strong understanding of the tools and techniques available as well as the ability to analyze and interpret the data collected.

It is essential to highlight the various tools and techniques used in OSINT, their advantages, and limitations. In the future of this project going to implement as the vulnerable machine to make practice it though and developing the mind map to work out the OSINT process. The significance of open-source data in today's information-driven world, and how it helps organizations and individuals to stay informed, proactive and secure. The importance of ethical and responsible use of OSINT and the need for legal compliance when collecting and using public data.

# **REFERENCE**

* Open-Source Intelligence Techniques: Resources for Searching and Analyzing Online Information: Author-Michael Bazzell Edition-9th, 8th 2021 ,2019
* <https://osintframework.com/>
* <https://www.exploit-db.com/google-hacking-database>
* <https://inteltechniques.com/buscador/>
* <https://www.tracelabs.org/>
* <https://null-byte.wonderhowto.com/how-to/use-buscador-osint-vm-for-conducting-online-investigations-0186611/>
* <https://christitus.com/choose-linux-distro/>
* Tanenbaum, A. S., & Bos, H. (2015). Modern Operating Systems (4th Edition). Pearson.
* "Linux Kernel Development" by Robert Love - This book provides an in-depth understanding of how the Linux kernel works, which is essential for building a custom operating system.
* "Operating System Concepts" by Abraham Silberschatz, Peter Baer Galvin, and Greg Gagne - This book covers the fundamental concepts of operating systems, including process management, memory management, and file systems.