Abstract

In the dynamic and ever-evolving landscape of information technology, the need for robust cybersecurity practices and tools is more critical than ever. Organizations and individuals face an increasing array of threats, ranging from network vulnerabilities to web application weaknesses and social engineering attacks. Ethical hackers and penetration testers play a crucial role in identifying and mitigating these vulnerabilities to protect sensitive data and infrastructure. However, penetration testers and ethical hackers often grapple with the challenge of managing and accessing a diverse set of cybersecurity tools, each catering to different aspects of testing and assessment.

Hence we propose a toolkit i.e CyberSec ProSuite that facilitates information gathering, vulnerability scanning, exploitation, and various other critical cybersecurity tools, all under a single, unified interface.CyberSec ProSuite is an all-in-one toolkit designed to empower penetration testers and ethical hackers with a wide range of essential tools and resources for assessing and securing applications, networks, websites, and more. This versatile toolkit offers a streamlined approach to ethical hacking and penetration testing, allowing professionals to efficiently uncover vulnerabilities and ensure the resilience of their digital assets.

Table of Content

Table of Figures

CHAPTER 1: INTRODUCTION

Introduction

CyberSec ProSuite is a comprehensive all-in-one toolkit designed to cater to the needs of cybersecurity professionals, ethical hackers, and security enthusiasts alike. This cutting-edge toolkit brings together a carefully curated selection of the most frequently used tools in the hacking process, creating a one-stop solution for those seeking to understand, assess, and secure digital systems and networks. With an intuitive and user-friendly interface, CyberSec ProSuite simplifies the complexities of cybersecurity, allowing both novices and experts to harness its power effectively. It regularly updates its arsenal to stay ahead of evolving cyber threats, ensuring users have access to the latest techniques and vulnerabilities for ethical hacking, penetration testing, and vulnerability assessment. CyberSec ProSuite is the go-to resource for anyone looking to bolster their cybersecurity skills and fortify their digital defenses in an interconnected world.

CyberSec ProSuite is an all-in-one toolkit designed to empower penetration testers and ethical hackers with a wide range of essential tools and resources for assessing and securing applications, networks, websites, and more. This versatile toolkit offers a streamlined approach to ethical hacking and penetration testing, allowing professionals to efficiently uncover vulnerabilities and ensure the resilience of their digital assets.

1.1 Motivation behind project

In an era where digital interconnectedness is integral to daily life, the importance of safeguarding digital assets and networks against malicious actors cannot be overstated. CyberSec ProSuite presents itself as a pivotal resource, offering the means to both understand and fortify digital defenses. Moreover, ethical hacking, penetration testing, and vulnerability assessment are crucial components of proactive cybersecurity, yet the responsible use of these tools requires careful examination and guidance.

This study is driven by the desire to not only harness the full potential of CyberSec ProSuite but also to explore its ethical dimensions, its adaptability to emerging technologies, and its efficacy across diverse network environments. By delving into these aspects, we seek to bolster cybersecurity practices and contribute to the ongoing battle against cyber threats in an increasingly digital world.

1.2 Problem Statement

The problem statement at the core of CyberSec ProSuite, an all-in-one toolkit housing commonly used hacking tools, arises from the escalating cybersecurity challenges in today's interconnected world. As digital systems and networks become more intricate and integral to our lives, the threat landscape continually evolves. In this context, CyberSec ProSuite offers a powerful resource for ethical hackers and cybersecurity professionals. However, several pressing issues demand attention.

Firstly, the ethical implications of utilizing hacking tools must be examined rigorously. The potential for misuse and illegal activities necessitates a comprehensive understanding of responsible and lawful use, requiring ethical guidelines and frameworks.

Secondly, the toolkit's adaptability is paramount. The rapidly changing nature of cyber threats demands constant updates and enhancements to ensure CyberSec ProSuite remains a relevant and effective tool for identifying vulnerabilities and safeguarding digital assets.

Lastly, accessibility and usability are pivotal for ensuring the toolkit's widespread adoption and utility. To empower both seasoned experts and newcomers in the field of cybersecurity, the interface must be user-friendly, and comprehensive documentation should be readily available.

Addressing these issues is essential to fully harnessing the capabilities of CyberSec ProSuite, promoting ethical hacking practices, and fortifying our digital defenses in an era where cyber threats are ever-present and increasingly sophisticated.

1.3 Objectives

- In an era where information flows ceaselessly and critical systems rely on interconnected networks, the need for a robust cybersecurity framework has never been more pronounced.
- With cyber threats evolving in sophistication and frequency, the role of penetration testers and ethical hackers in identifying and mitigating vulnerabilities has become indispensable.
- The objective of CyberSec Prosuite is to provide a comprehensive and user- friendly toolkit to cater to the needs of penetration testers and ethical hackers.
- The all-in-one arsenal brings together a wide array of essential resources under a unified

interface, promising to revolutionize the practice of ethical hacking and penetration testing.

- By offering a diverse set of tools spanning from information gathering to threat intelligence integration,
- CyberSec ProSuite seeks to streamline workflows, enhance efficiency, and contribute to the resilience of modern digital ecosystems.

1.4 Conclusion

In this chapter, we've provided a brief overview of our project. We've explained why we're doing it and outlined our main goals. This information sets the stage for the rest of our project. As we move forward, we'll build upon what we've discussed here, making sure we stay on track with our original vision and objectives. We're excited about the journey ahead and the opportunity to tackle the challenges and opportunities our project presents. The work we've done in this chapter demonstrates our dedication, and we can't wait to see how our project develops in the upcoming chapters.

CHAPTER 2: REVIEW OF LITERATURE

2.1 Review of Literature

These research papers aim to simplify the work of penetration testers and ethical hackers by consolidating a wide array of tools under one user-friendly interface. They also provide insights into the strengths and limitations of existing tools and suggest areas for future research.

"Penetration Testing Active Reconnaissance Phase- Optimized Port Scanning With Nmap Tool": According to our observations and analysis the authors proposed a scan strategy that illustrates how penetration testers should deal with large volumes of traffic and to avoid any type of traffic restriction. They also have analyzed that if the active scan phase starts without any proper strategy it affects the bandwidth as well as scan task time [1].

"Automation of Cyber-Reconnaissance A Java-based Open Source Tool for Information Gathering": In this paper authors have proposed a system which is a Java-based tool that helps in locating and saving organization specific data.It also provides the possibility of implementing network-based passive information gathering that reduces traffic within the internal network like passive OS fingerprinting to enumerate OSs in use [2].

“Self Port Scanning Tool: Providing a More Secure Computing Environment Through the Use of Proactive Port Scanning”: In this paper authors have introduced an assessment method which uses the nmap software to scan ports, that is developed to aid System Administrators (SAs) with analysis of open ports on their systems [3].

"Embedded Port Scanner (EPSS)System Using Linux and Single Board Computer": In this paper authors have proposed an approach to develop a software which performs port scan using half-open and UDP technique. The software can be executed on a Linux based Single Board Computer (SBC) which runs TS-Linux 2.4.23 kernel [4].

" A Case Study on Web Application Vulnerability Scanning Tools": In this paper authors have performed a comparative analysis between various types of information gathering tools like Nessus,Acunetix-Web Vulnerability Scanner and OWASP Zed Attack Proxy (ZAP) in order to find pros, cons and effectiveness of each tool [5].

" Large Scale Port Scanning Through Tor Using Parallel Nmap Scans to Scan Large Portions of the IPv4 Range": This paper focuses on effective port scanning while maintaining anonymity using Tor. It maximizes the range of scanning by using a third-party data source to target specific areas of interest in the IPv4 range and then scanning those areas anonymously with parallelized scanners as an effective way to anonymously collect internet scan data [6].

“Research and Design on Web Application Vulnerability Scanning Service”: In this paper authors have discussed about the open source Web application vulnerability scanners and by comparing various scanners, they selected (W3af) Web Application Attack and Audit Framework for Web interface package, and designed an audit module that increased the Clickjacking vulnerability scan in HTML5 [7].

“Analysis of Freeware Hacking Toolkit”: This paper mainly focuses on analyzing the security posture of various freeware computer security tools. A virtual computer network environment was also set up to demonstrate how some computer security tools can be exploited for malicious purposes [8].

“Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools”: In this paper the authors have performed MITM attack and ARP spoofing to demonstrate that computer networks are still vulnerable to dangerous attacks even today whether they use HTTPS or HTTP [9].

“ECR(Encryption with Cover Text and Reordering) based Text Steganography”: In this paper the authors have proposed a new approach for text-based steganography that uses simple Ex-Or Operation for enciphering the secret message and reordering the text as per 8-bit random key [10].

“Analysis and Classification of SQL Injection Vulnerabilities and Attacks on Web Applications”: In this paper authors have performed all types of SQL injection attacks on various banking applications, Blog and shopping websites in order to find potential vulnerabilities and prepared a report summarizing all the key points to strengthen the security posture of these websites [11].

“Research on SQL injection vulnerability attack model”: In this paper authors have proposed a model that contains all types of SQL injection tools that can be used to find SQL injection vulnerabilities. It works faster than traditional models and it is more efficient, concise and comprehensive [12].

2.2 Comparative analysis table

Sr.no	Paper Title	Paper Findings	Technology Used
1	Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool	According to our observations and analysis the authors [1] proposed a scan strategy that illustrates how penetration testers should deal with large volumes of traffic and to avoid any type of traffic restriction. They also have analyzed that if the active scan phase starts without any proper strategy it affect the bandwidth as well as scan task time.	Nmap tool
2	Automation of Cyber-Reconnaissance A Java-based Open Source Tool for Information Gathering	In this paper [2] authors have proposed a system which is a Java-based tool that helps in locating and saving organization specific data.It also provides the possibility of implementing network-based passive information gathering that reduces traffic within the internal network like passive OS fingerprinting to enumerate OSs in use.	Automation of Open source reconnaissance tools
3	Self Port Scanning Tool: Providing a More Secure Computing Environment Through the Use of Proactive Port Scanning	In this paper [3] authors have introduced an assessment method which uses the nmap software to scan ports, that is developed to aid System Administrators (SAs) with analysis of open ports on their systems.	Nmap tool for self port scanning
4	Embedded Port Scanner (EPSS)System Using Linux and Single Board Computer	In this paper [4] authors have proposed an approach to develop a software which performs port scan using half-open and UDP technique. The software can be executed on a Linux based Single Board Computer (SBC) which runs TS-Linux 2.4.23 kernel	Embedded port scanning using linux

5	A Case Study on Web Application Vulnerability Scanning Tools	In this paper [5] authors have performed a comparative analysis between various types of information gathering tools like Nessus,Acunetix-Web Vulnerability Scanner and OWASP Zed Attack Proxy (ZAP) in order to find pros, cons and effectiveness of each tool.	OWASP ZAP, Nessus, Acunetix
6	Large Scale Port Scanning Through Tor Using Parallel Nmap Scans to Scan Large Portions of the IPv4 Range	This paper [6] focuses on effective port scanning while maintaining anonymity using Tor. It maximizes the range of scanning by using a third-party data source to target specific areas of interest in the IPv4 range and then scanning those areas anonymously with parallelized scanners as an effective way to anonymously collect internet scan data.	Nmap, Tor
7	Research and Design on Web Application Vulnerability Scanning Service	In this paper [7] authors have discussed about the open source Web application vulnerability scanners and by comparing various scanners, they selected (W3af) Web Application Attack and Audit Framework for Web interface package, and designed an audit module that increased the Clickjacking vulnerability scan in HTML5.	HTML5, W3af
8	Analysis of Freeware Hacking Toolkit	This paper [8] mainly focuses on analyzing the security posture of various freeware computer security tools. A virtual computer network environment was also set up to demonstrate how some computer security tools can be exploited for malicious purposes.	hashcat, Nmap, Johntheripper
9	Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools	In this paper [9] the authors have performed MITM attack and ARP spoofing to demonstrate that computer networks are still vulnerable to dangerous attacks even today whether they use HTTPS or HTTP.	Bettercap, Ettercap
10	ECR(Encryption with Cover Text and Reordering) based Text Steganography	In this paper [10] the authors have proposed a new approach for text-based steganography that uses simple Ex-Or Operation for enciphering the secret message and reordering the text as per 8-bit random key.	ECR based Steganography

11	Analysis and Classification of SQL Injection Vulnerabilities and Attacks on Web Applications	In this paper [11] authors have performed all types of SQL injection attacks on various banking applications, Blog and shopping websites in order to find potential vulnerabilities and prepared a report summarizing all the key points to strengthen the security posture of these websites.	SQLmap, Burp
12	Research on SQL injection vulnerability attack model	In this paper [12] authors have proposed a model that contains all types of SQL injection tools that can be used to find SQL injection vulnerabilities. It works faster than traditional models and it is more efficient, concise and comprehensive.	SQLmap, PortSwigger

2.3 Conclusion

In conclusion, the review of literature has provided invaluable insights into the challenges and opportunities within the field. It has emphasized the importance of responsible hacking practices, adherence to ethical guidelines, and compliance with legal regulations. Furthermore, the literature review has informed our project's objectives, guiding our efforts to create a unified and accessible toolkit that addresses the needs of penetration testers and ethical hackers.

CHAPTER 3 PROPOSED SYSTEM

3.1Problem Statement

The problem we're addressing with CyberSec ProSuite is all about the growing importance of cybersecurity in our digital world. As technology advances, so do the ways that bad actors can use it to harm others. We needed a solution to help people understand and defend against these threats. One problem is that hacking, when done maliciously, can cause a lot of harm. So, we wanted to create a toolkit that teaches people about hacking but also emphasizes doing it responsibly and legally. It's important to use these skills for good, like finding and fixing vulnerabilities in systems. Another issue is that hacking can be really complicated, and finding the right tools can be a hassle. So, we decided to put all the essential hacking tools in one place – that's CyberSec ProSuite. It's like having a complete toolbox for cybersecurity, making it easier for both beginners and experts. Lastly, the digital world changes rapidly, and new threats emerge all the time. We needed to create a toolkit that stays up-to-date with the latest challenges. This way, CyberSec ProSuite can always help users identify and address new cyber problems effectively.

The problem that the "CyberSec ProSuite" project aims to address is the lack of a consolidated, user-friendly toolkit that provides penetration testers and ethical hackers with a comprehensive suite of tools to streamline their testing and assessment processes. This toolkit should facilitate information gathering, vulnerability scanning, exploitation, and various other critical cybersecurity tasks, all under a single, unified interface.

The key issues this project seeks to resolve include:

1. **Tool Integration:** Currently, professionals often need to juggle multiple tools, each with its own interface and setup process. This leads to inefficiencies in workflow and increased learning curves.
2. **Resource Accessibility:** Many cybersecurity tools are scattered across the internet or require specific installations. This hampers accessibility and hinders quick response to security assessments and testing requirements.
3. **Comprehensiveness:** As new threats emerge and cybersecurity standards evolve, it's challenging for professionals to keep up with the ever-expanding list of tools and technologies.
4. **User-Friendly Interface:** Existing tools often vary in terms of usability and user interface design, making it difficult for both newcomers and experienced professionals to work efficiently.

3.2 Block Diagram

The below Figure 3.1 Shows how blocks i.e components are connected to different modules of toolkit and how the process appears to involve user interaction, data processing, output generation, and decision points. Let's break down the components of the figure 3.1 block diagram of CyberSec ProSuite:

User Selects Operation: This is where the user initiates the process by selecting a specific operation or task to be executed.

Operation Executed: Once the user selects an operation, it is executed as indicated.

User Interaction (Gui Or Cli): Depending on the user's preference, they interact with the system using either a Graphical User Interface (GUI) or Command Line Interface (CLI).

Data Preprocessing, Toolkit Execution, Database Access: Data preprocessing is performed as part of the operation, which may involve cleaning, transformation, or manipulation of data. This likely represents the use of specialized tools or software to perform a specific task or operation. Access to a database may be required to retrieve or store data needed for the operation.

Output Generation, Report Creation, User Feedback: After processing the data, the system generates some form of output. This step involves creating reports or documents based on the processed data. The user is given an opportunity to provide feedback or input at this point.

User Decision (Continue Operation Or Exit): Based on the user's feedback or decision, they can choose to continue with the operation or exit the process.

The block diagram is shown below:

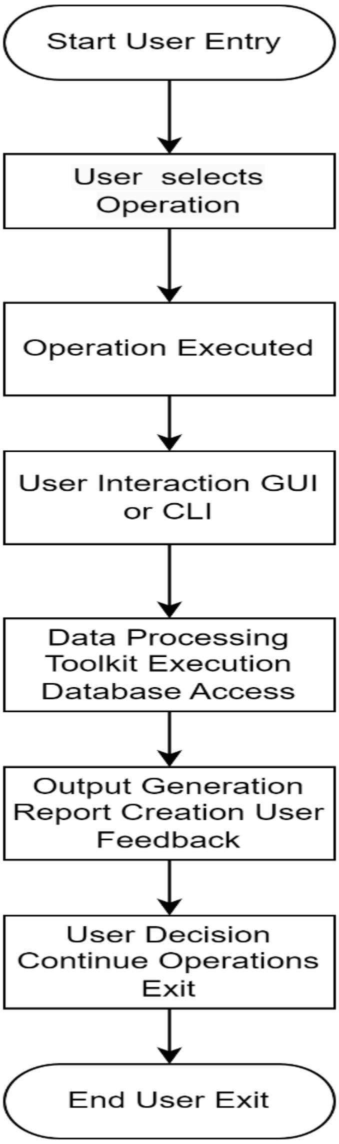

Start User Entry
User selects Operation
Operation Executed
User Interaction GUI or CLI
Data Processing Toolkit Execution Database Access
Output Generation Report Creation User Feedback
User Decision Continue Operations Exit
End User Exit

Figure 3.1 Block Diagram of CyberSec ProSuite

The above block diagram consists of several interconnected components, each representing a significant module or functionality within the system.

3.3 Architectural Design

This simplified architecture diagram illustrates the high-level components of CyberSec ProSuite, including the user interface, backend API, and data repositories. In practice, the architecture might be more complex, with additional layers, security features, and scalability considerations based on your project's specific requirements.

The figure 3.2 outlines how these layers and components interact to create a robust and efficient cybersecurity toolkit.

The Architecture Design is shown below:

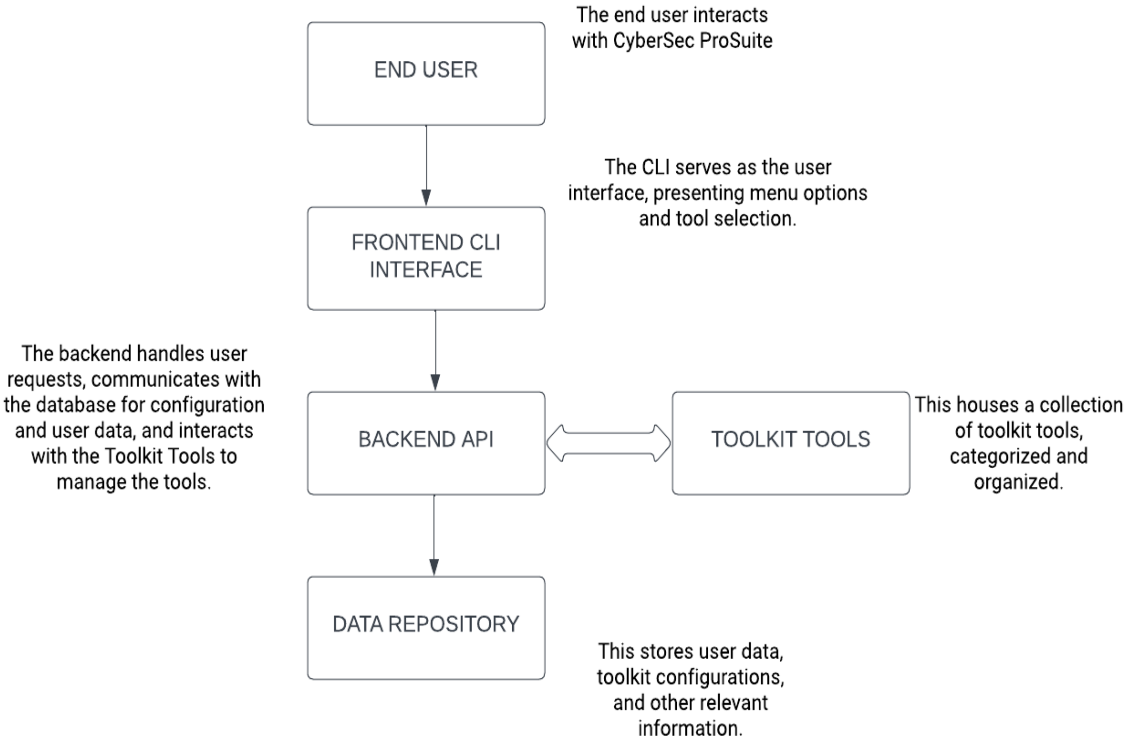

END USER
The end user interacts with CyberSec ProSuite
FRONTEND CLI INTERFACE
The CLI serves as the user interface, presenting menu options and tool selection.
The backend handles user requests, communicates with the database for configuration and user data, and interacts with the Toolkit Tools to manage the tools.
BACKEND API
TOOLKIT TOOLS
This houses a collection of toolkit tools, categorized and organized.
DATA REPOSITORY
This stores user data, toolkit configurations, and other relevant information.

Figure 3.2 Architectural Diagram of CyberSec ProSuite

3.4 ER Diagram

An Entity Relationship Diagram (ER Diagram) pictorially explains the relationship between entities to be stored in a database. Fundamentally, the ER Diagram is a structural design of the database. It acts as a framework created with specialized symbols for the purpose of defining the relationship between the database entities.

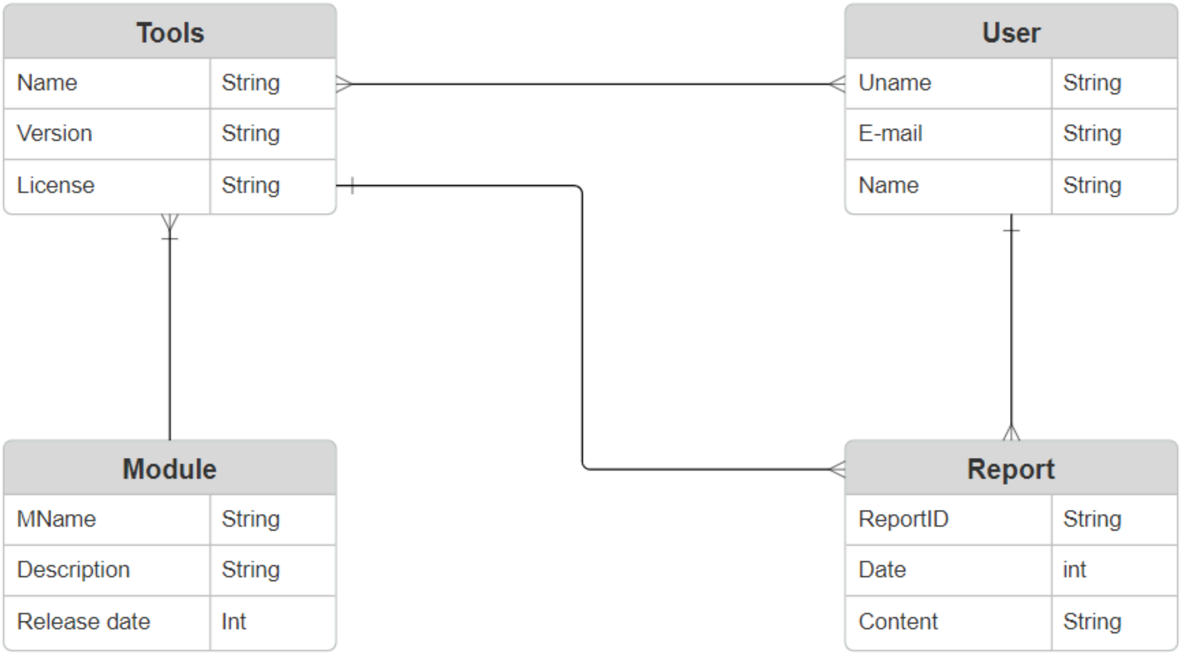


Figure 3.3 ER Diagram of CyberSec ProSuite

3.5 Methodology / Algorithm

The methodology or the Algorithm of CyberSec Prosuite is as follows:

1. **Start Security Testing:** Initialize the security testing process.
2. **User Selects Testing Type:** Prompt the user to choose the type of security testing they wish to conduct (e.g., web application, network, mobile, etc.).
3. **Understand Objectives:** Define the objectives and scope of the security test, including what is to be tested and the goals of the assessment.
4. **Plan Test:** Create a detailed test plan that outlines Target assets (e.g., specific applications, network segments), Required resources, including personnel and tools, Specific testing methodologies and approaches.
5. **Configure Toolkit:** Set up CyberSec ProSuite with the user's customized selection of security tools and configurations, ensuring the toolkit is ready for testing.

6. **Execute Test:** Initiate the security testing process, following the plan created in the previous step. Execute selected security tools and tests on the target assets. Continuously monitor the progress of tests.
7. **Analyze Test Results:** Analyze the results generated by the security tools. Identify vulnerabilities, weaknesses, and potential threats in the tested systems.
8. **Report Generation:** Create a comprehensive security assessment report that includes:Detailed findings, including vulnerabilities and their severity,Supportive evidence, such as logs and screenshots.
9. **End Methodology:** Complete the security testing methodology.

3.6 Conclusion

In conclusion, the "CyberSec ProSuite" represents a comprehensive and powerful solution to address the ever-growing challenges in the field of cybersecurity. With its diverse range of features and capabilities, it offers organizations and individuals an effective means to protect their digital assets, detect vulnerabilities, and respond to cyber threats in a proactive and efficient manner.

CHAPTER 4: SOFTWARE & HARDWARE REQUIREMENTS

4.1 Software Requirements

- **Operating System:** Linux:The software requirement specifies the use of the Linux operating system. Linux is a popular choice for this project due to its robust security features, open-source nature, and extensive support for various cybersecurity tools. It provides a stable and flexible environment for running the toolkit.
- **Front End:** Python: For the front end of the application, Python is the chosen programming language. Python is well-suited for creating user interfaces and managing user interactions. Its simplicity and readability make it a valuable choice for developing the graphical aspects of the "CyberSec ProSuite" toolkit.
- **Backend:** Python, Bash: The backend of the application is powered by both Python and Bash scripting. Python's versatility and Bash's strength in shell scripting complement each other. Python is used for core backend logic, while Bash is utilized for tasks such as system interactions and script execution. This combination provides a robust foundation for the toolkit's functionality.
- **Tool:** VSCode: Visual Studio Code (VSCode) is the selected Integrated Development Environment (IDE) for this project. VSCode is a widely-used and efficient code editor known for its ease of use and extensive support for Python development. It offers features such as code debugging and syntax highlighting, enhancing the development process.

4.2 Hardware Requirements

- **Intel I3 7th Gen 4GB RAM:** The recommended hardware configuration for running the "CyberSec ProSuite" project includes an Intel Core i3 7th generation processor paired with 4GB of RAM. This configuration ensures smooth and efficient performance of the toolkit. It provides sufficient processing power and memory to handle various cybersecurity tasks effectively.
- **Minimum Hardware Requirement:** Pentium 3 166 MHz and 128MB RAM or Higher: The minimum hardware requirement specifies the least powerful system that can run the toolkit. It includes a Pentium 3 processor with a clock speed of 166 MHz and a minimum of 128MB of RAM. This minimal requirement allows the toolkit to function on older or less capable hardware while ensuring accessibility to a broader user base.

CHAPTER 5: DESIGN AND IMPLEMENTATION

5.1 Data Flow Diagram

5.1.1 DFD level-0

The DFD Level 0 diagram provides a structured overview of how users interact with the "CyberSec ProSuite" system, the execution of cybersecurity tools, data management, updates, compliance enforcement, and accessibility considerations. It serves as a foundational diagram for understanding the major components and data flows within your project.

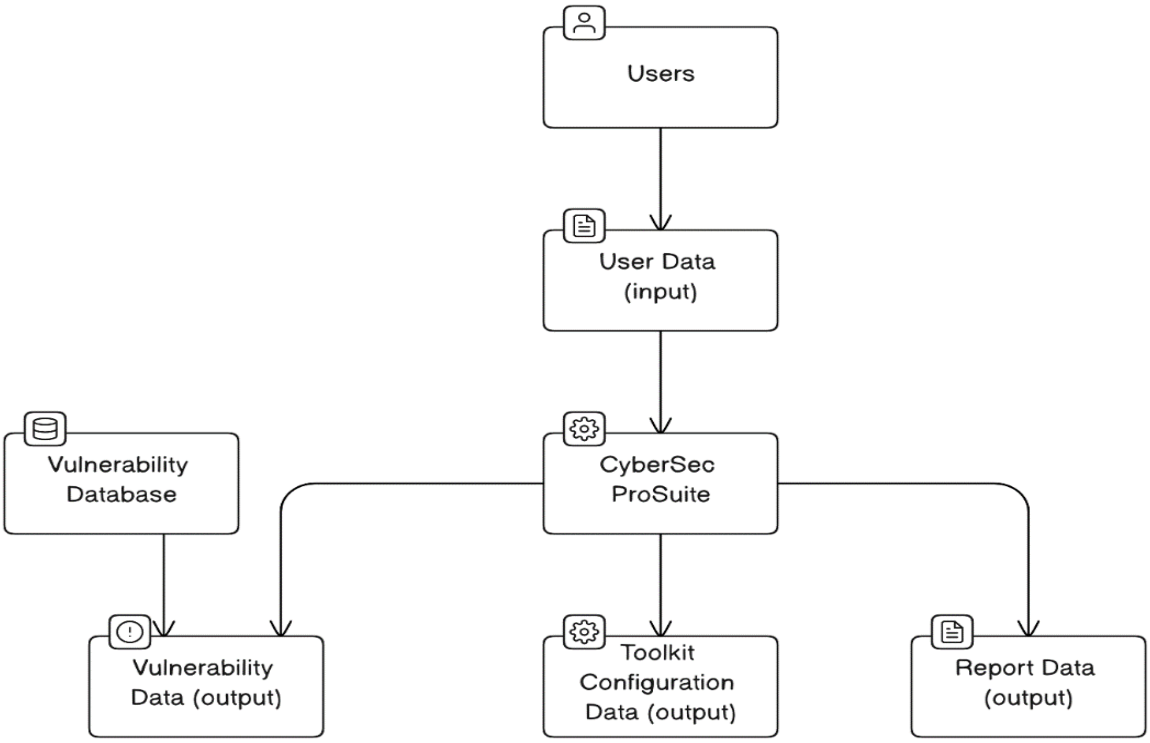


Figure 5.1 DFD LEVEL 0

5.1.2 DFD level-1

The below figure 3.5 DFD Level 1 diagram provides a detailed breakdown of sub processes within the major processes, highlighting the intricacies of user interaction, tool execution, data management, updates, compliance enforcement, and accessibility considerations within your "CyberSec ProSuite" project. This level of detail offers valuable insights into the inner workings of the system and is crucial for guiding further system design and implementation efforts.

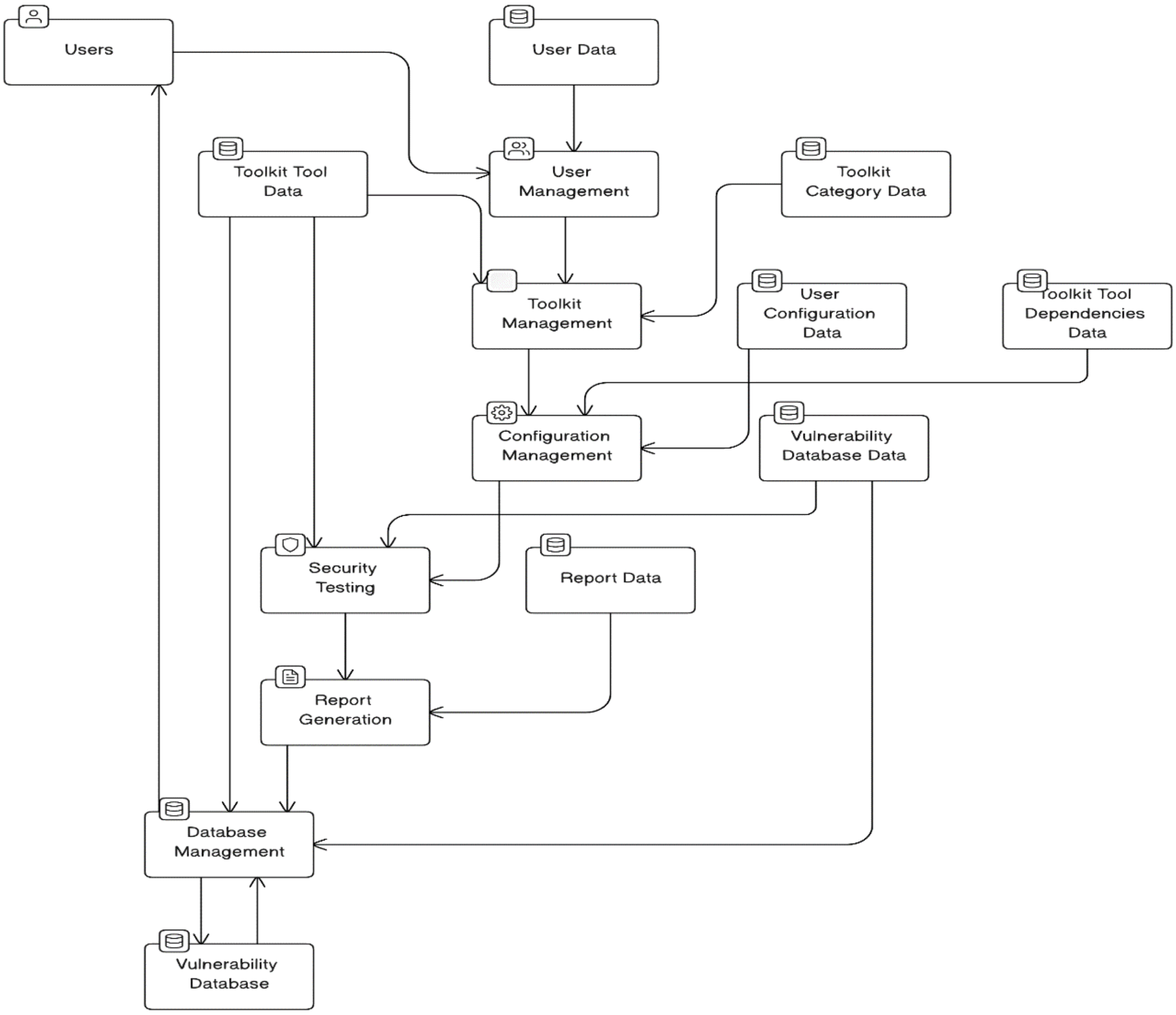


Figure 5.2 DFD LEVEL 1

5.1.3 Activity Diagram

The Activity Diagram for "CyberSec ProSuite" visually outlines the key activities and their flow within the system. It offers a clear representation of how users interact with the toolkit, execute tools, manage data, handle compliance, and ensure accessibility.

This Activity Diagram serves as a roadmap of activities within the "CyberSec ProSuite" system, guiding the user journey from interaction to tool execution, data management, compliance checks, and accessibility considerations. It visually represents the flow of activities, helping stakeholders understand the system's functionality and user interactions.

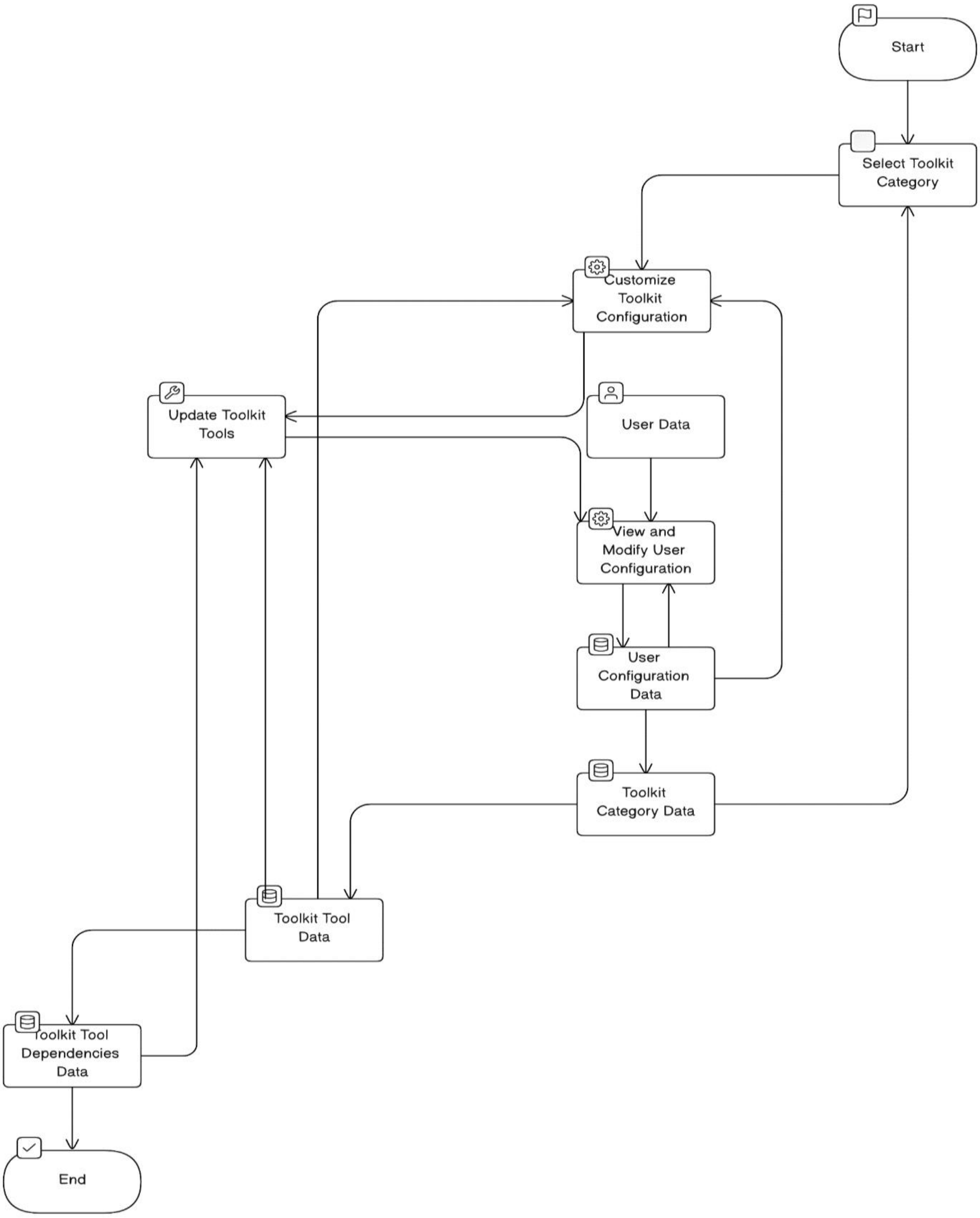


Figure 5.3 Activity Diagram

5.1.4 Use Case Diagram

The Use Case Diagram provides a clear visual representation of how users (actors) interact with the "CyberSec ProSuite" system through different use cases. Fig 3.7 illustrates the key functionalities of the toolkit, including tool selection, configuration, report generation, compliance checks, and accessibility considerations. This diagram serves as a valuable tool for understanding the system's use cases and user interactions.

The below image shows a diagrammatic representation of the workflow of our project.

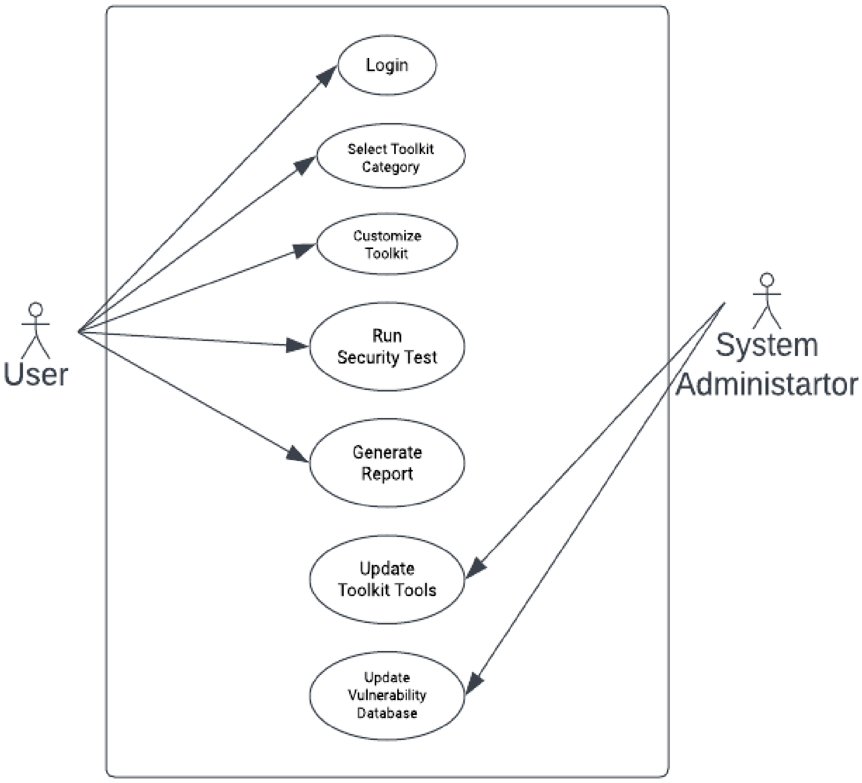


Figure 5..4 Use case diagram of CyberSec ProSuite

5.1.5 Sequence Diagram

The below figure 5.5 is the sequence diagram of CyberSec ProSuite in the toolkit there are 3 participants as follows.

Participant: User, Toolkit, Module.

The working is as follows:

I. User interacts with CyberSec proSuite and Selects a tool from the UI.

II. CyberSec proSuite sends operation requests to the Module and Loads the Tool.

III. Module Executes the Tool and sends the output of each request to the CyberSecProsuite.

IV. CyberSec ProSuite Display Tool Output or Report the User.

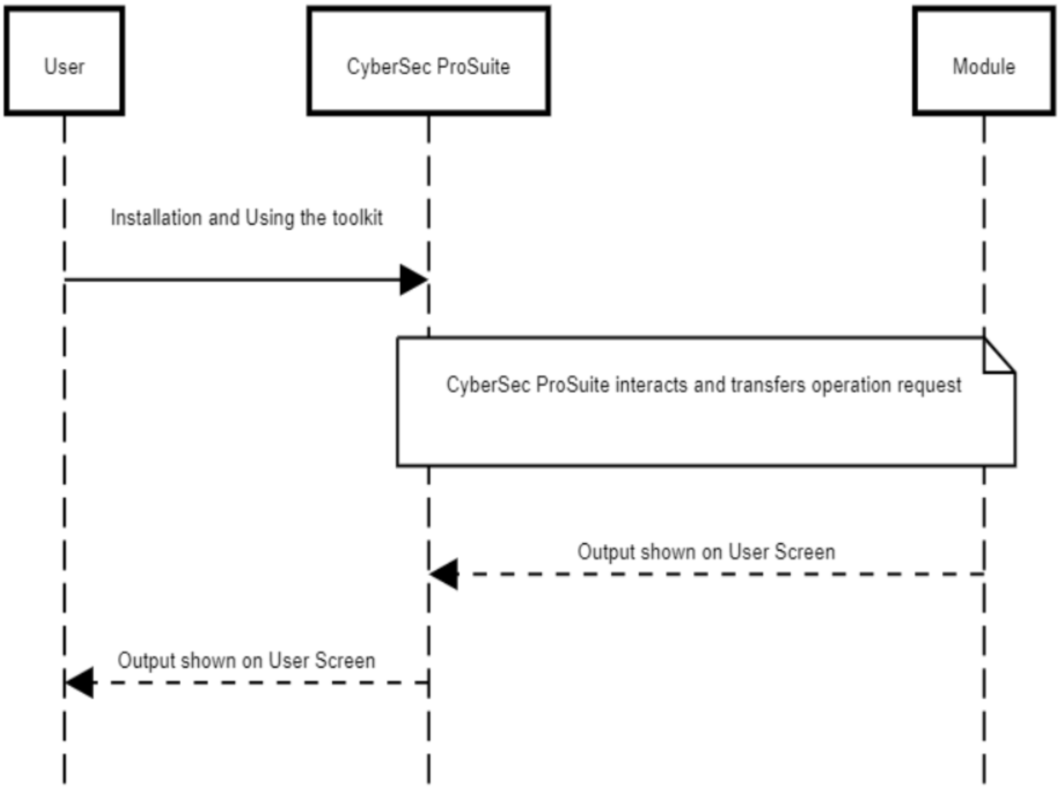
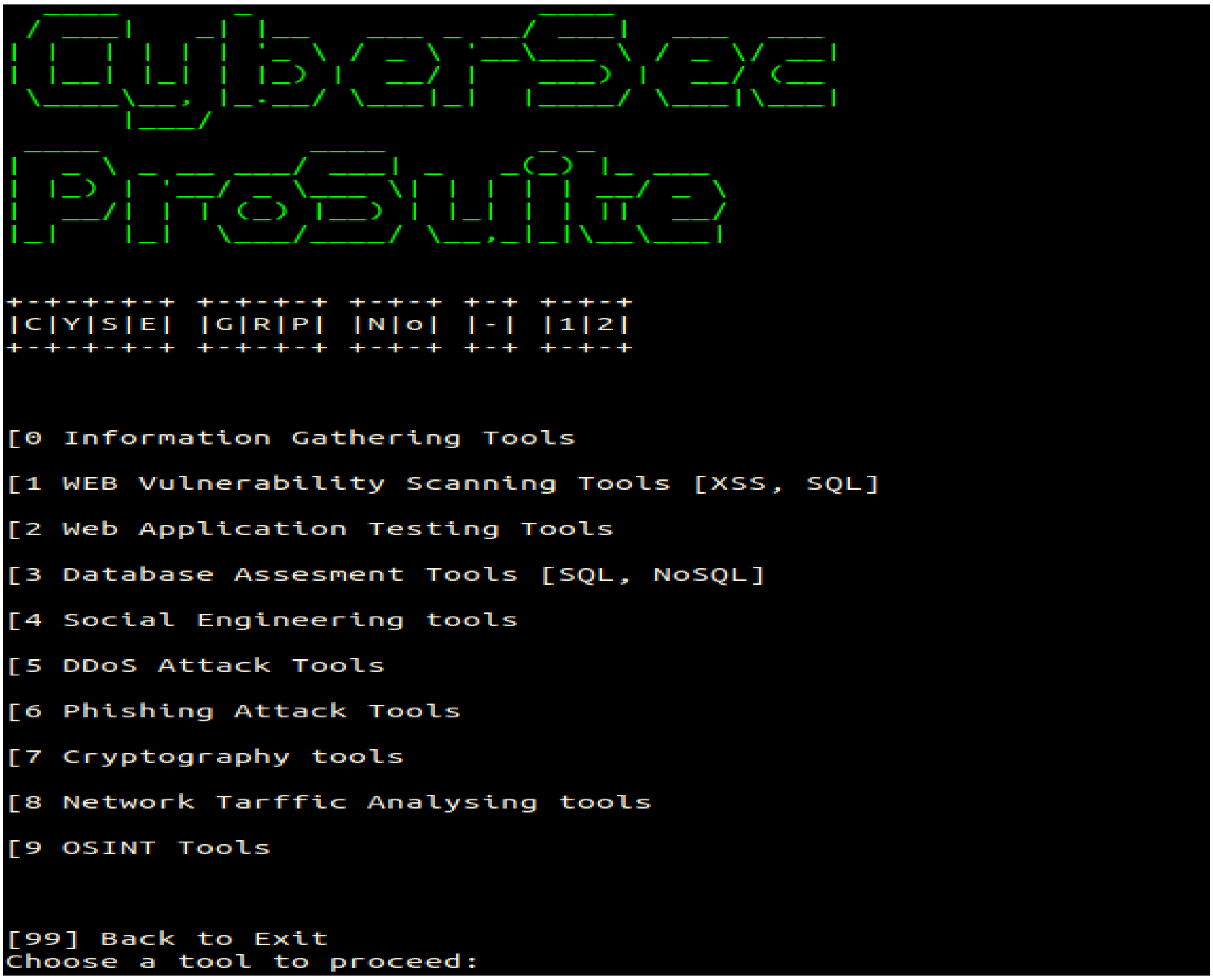

User
CyberSec ProSuite
Module
Installation and Using the toolkit
CyberSec ProSuite interacts and transfers operation request
Output shown on User Screen
Output shown on User Screen

Figure 5.5 Sequence diagram of CyberSec ProSuite

5.2 Implementation

5.2.1 Command line Interface of CyberSec ProSuite

Command line interface is designed using python programming language as shown in below fig 5.6. Various tools tools that are used in ethical hacking process ranging from Reconnaissance to Post attack tools are integrated in the CyberSec ProSuite.These Tools include Nmap,Web Recon and RED hawk for reconnaissance, XSS Scanner and SQLmap for web vulnerability testing,Skipfish, Hackbox, MainCoon and ParamSpider for web application testing and many more.The below figure 5.6 is User interface of the tool. Once the toolkit is Installed into the system user can navigate through each and every module of tools by using the Keypad for e.g Select"1" to open Web vulnerability assessment tools or "0" to open the module of information gathering tools and so on. To exit the tool type "99" in the command prompt and enter. To Select the operation that a user wants to perform enter the number assigned to the left side of each tool in the menu as shown in the diagram below. After installing the toolkit into the system one can start the process of ethical hacking.

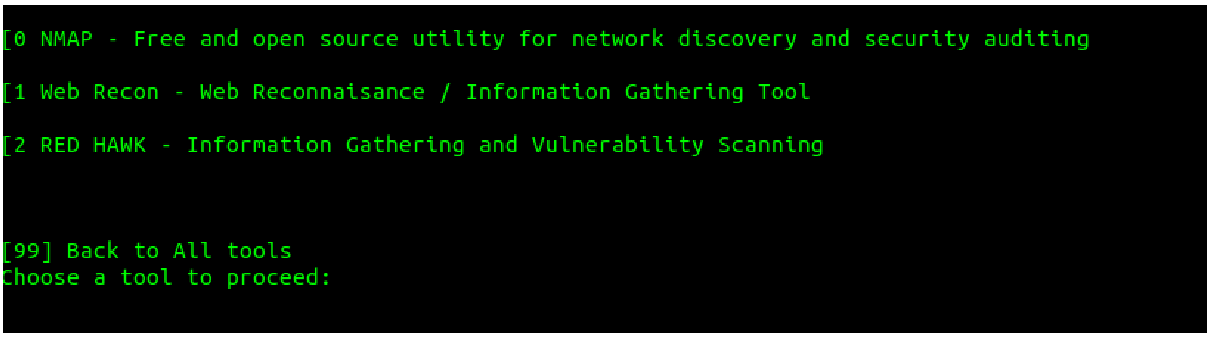


```
  ____      _               ____
 / ___|   _| |__   ___ _ __/ ___|  ___  ___
| |  | | | | '_ \ / _ \ '__\___ \ / _ \/ __|
| |__| |_| | |_) |  __/ |   ___) |  __/ (__
 \____\__, |_.__/ \___|_|  |____/ \___|\___|
      |___/
 ____            ____        _ _
|  _ \ _ __ ___ / ___| _   _(_) |_ ___
| |_) | '__/ _ \\___ \| | | | | __/ _ \
|  __/| | | (_) |___) | |_| | | ||  __/
|_|   |_|  \___/|____/ \__,_|_|\__\___|


+-+-+-+-+ +-+-+-+ +-+-+ +-+ +-+-+
|C|Y|S|E| |G|R|P| |N|o| |-| |1|2|
+-+-+-+-+ +-+-+-+ +-+-+ +-+ +-+-+


[0 Information Gathering Tools

[1 WEB Vulnerability Scanning Tools [XSS, SQL]

[2 Web Application Testing Tools

[3 Database Assesment Tools [SQL, NoSQL]

[4 Social Engineering tools

[5 DDoS Attack Tools

[6 Phishing Attack Tools

[7 Cryptography tools

[8 Network Tarffic Analysing tools

[9 OSINT Tools


[99] Back to Exit
Choose a tool to proceed:
```

Figure 5.6 Command line Interface of CyberSec ProSuite

5.2.1 Information gathering and Application Testing Tools

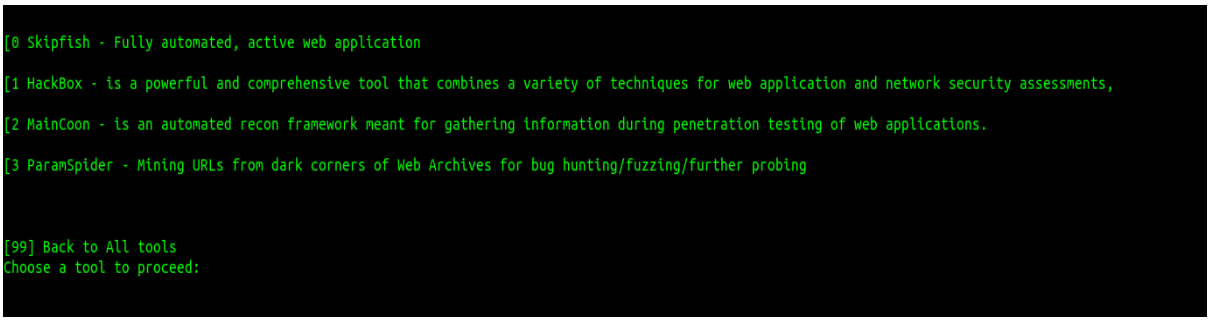
For the purpose of information gathering the tools like Nmap, Web Recon and red hawk are integrated into the system and for Web Application testing There are tools like SQL Map, Skip Fish, XSS Scanner that are integrated into the CyberSec ProSuite as shown in fig 5.7 and fig 5.8 below.Once the toolkit is Installed into the system user can navigate through each and every module of tools by using the Keypad for e.g Select"1" to open Web vulnerability assessment tools or "0" to open the module of information gathering tools and so on. To exit the tool type "99" in the command prompt and enter.



```
[0 NMAP - Free and open source utility for network discovery and security auditing

[1 Web Recon - Web Reconnaisance / Information Gathering Tool

[2 RED HAWK - Information Gathering and Vulnerability Scanning


[99] Back to All tools
Choose a tool to proceed:
```

Figure 5.7 Information Gathering Tools

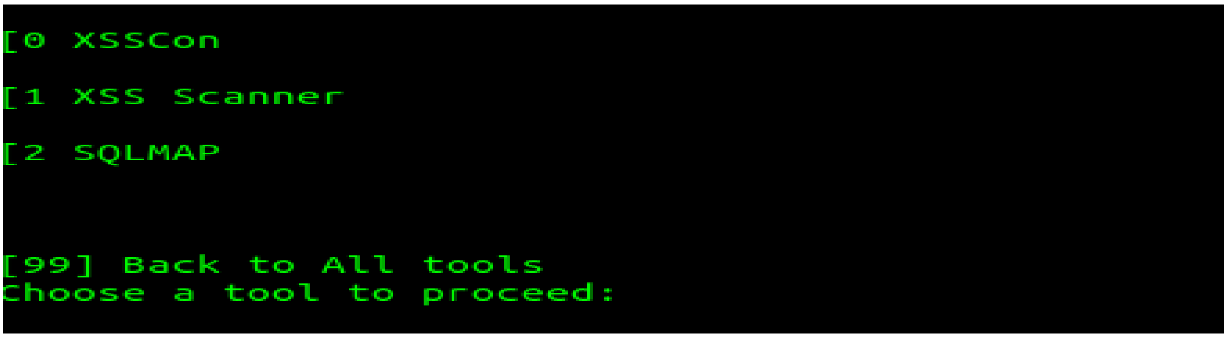
The fig 5.8 below is the module where all of modern Web application testing tools are integrated.Once the toolkit is Installed into the system user can navigate through each and every module of tools by using the Keypad



```
[0 Skipfish - Fully automated, active web application

[1 HackBox - is a powerful and comprehensive tool that combines a variety of techniques for web application and network security assessments,

[2 MainCoon - is an automated recon framework meant for gathering information during penetration testing of web applications.

[3 ParamSpider - Mining URLs from dark corners of Web Archives for bug hunting/fuzzing/further probing


[99] Back to All tools
Choose a tool to proceed:
```

Figure 5.8 Web Application Testing Tools

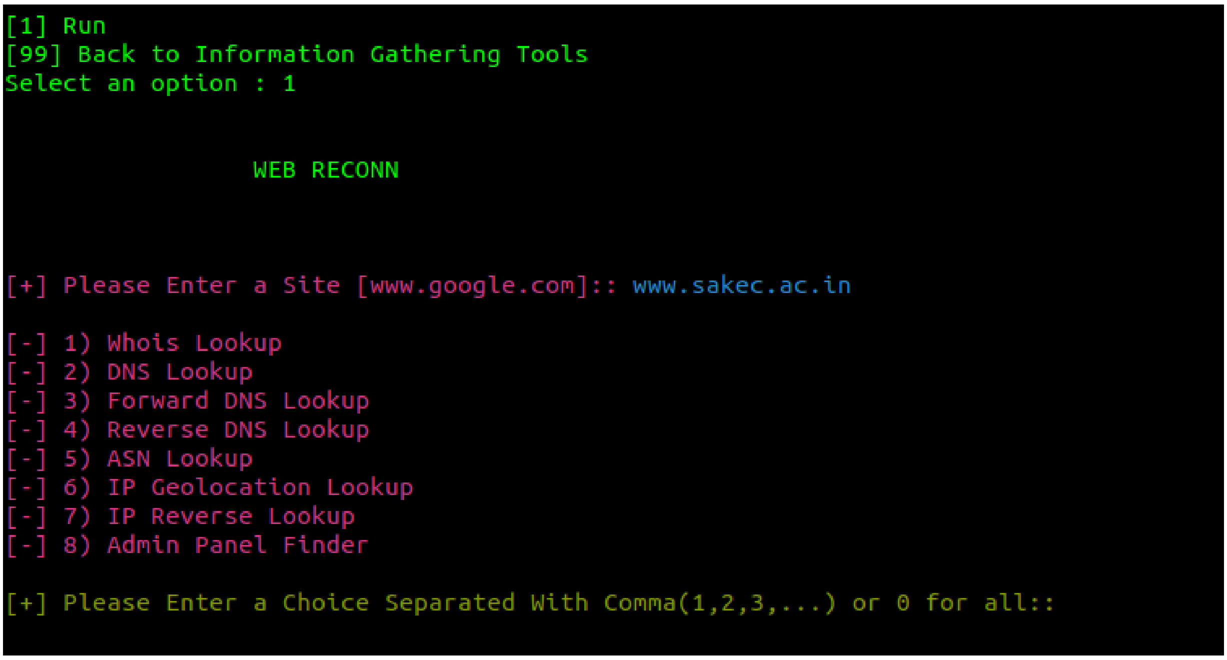
The fig 5.9 is the CLI interface of web vulnerability testing tool as shown below.Once the toolkit is Installed into the system user can navigate through each and every module of tools by using the Keypad and start searching for vulnerabilities.



```
[0 XSSCon

[1 XSS Scanner

[2 SQLMAP


[99] Back to All tools
Choose a tool to proceed:
```

Figure 5.9 Web Vulnerability Testing Tools

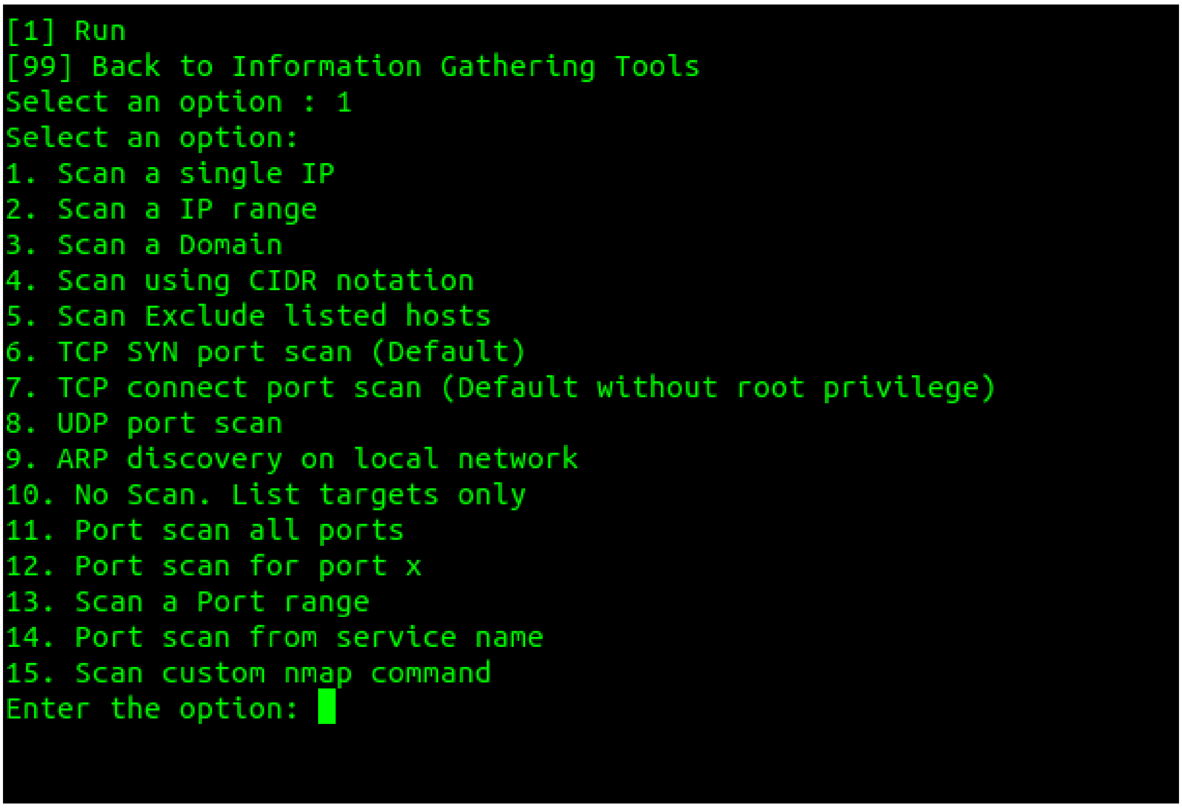
The below fig 5.8 shows the features through which various types of lookups can be performed on the targeted website. The lookup includes WHOis lookup, DNS lookup, ASN lookup and IP reverse lookup. The user can navigate through each and every module of tools by using the different keys.



```
[1] Run
[99] Back to Information Gathering Tools
Select an option : 1


                 WEB RECONN



[+] Please Enter a Site [www.google.com]:: www.sakec.ac.in

[-] 1) Whois Lookup
[-] 2) DNS Lookup
[-] 3) Forward DNS Lookup
[-] 4) Reverse DNS Lookup
[-] 5) ASN Lookup
[-] 6) IP Geolocation Lookup
[-] 7) IP Reverse Lookup
[-] 8) Admin Panel Finder

[+] Please Enter a Choice Separated With Comma(1,2,3,...) or 0 for all::
```

Figure 5.10 Web Recon Output

The Fig 5.10 shows the multiple types of options of Nmap ranging from IP Scan to various types of port scanning techniques. The Nmap tool has in-built commands and features for reconnaissance purposes which serves as a valuable asset for ethical hackers and security professionals.

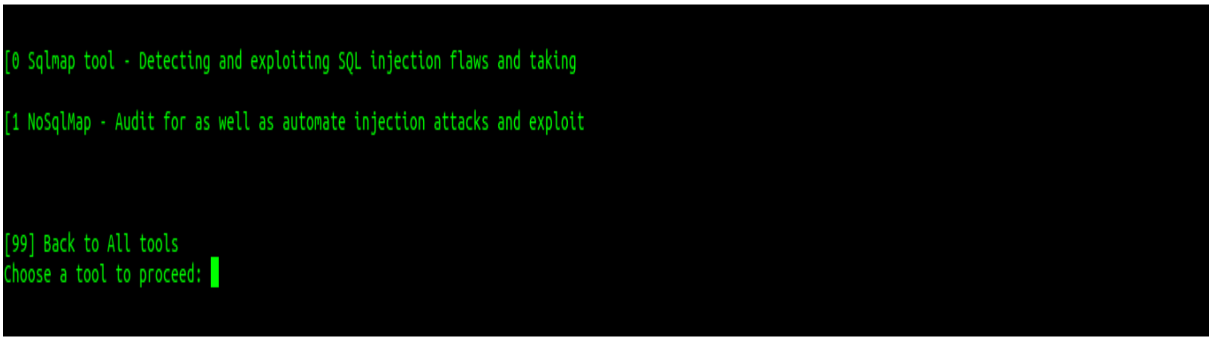


```
[1] Run
[99] Back to Information Gathering Tools
Select an option : 1
Select an option:
1. Scan a single IP
2. Scan a IP range
3. Scan a Domain
4. Scan using CIDR notation
5. Scan Exclude listed hosts
6. TCP SYN port scan (Default)
7. TCP connect port scan (Default without root privilege)
8. UDP port scan
9. ARP discovery on local network
10. No Scan. List targets only
11. Port scan all ports
12. Port scan for port x
13. Scan a Port range
14. Port scan from service name
15. Scan custom nmap command
Enter the option: 
```

Figure 5.10 Range of Options in Nmap

5.2.2 Database Assessment and DoS Attack Tools

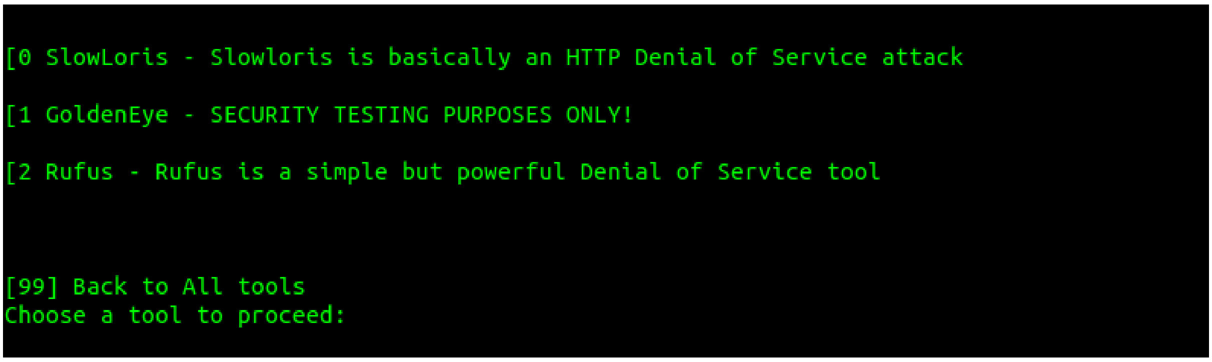
The tools that are integrated into the system for the purpose to perform Database exploitation and Denial of service attacks are SQLmap Tool,NoSqlMap and SlowLoris, GoldenEye, Rufus respectively as shown in fig 5.11 and fig 5.12. Once the CyberSec ProSuite is installed into the system all the tools will be automatically downloaded into the environment there is no need to install each and every tool manually. The below figure also contains output generated by these tools.



```
[0 Sqlmap tool - Detecting and exploiting SQL injection flaws and taking

[1 NoSqlMap - Audit for as well as automate injection attacks and exploit



[99] Back to All tools
Choose a tool to proceed:
```

Figure 5.11 Database Assessment Tools

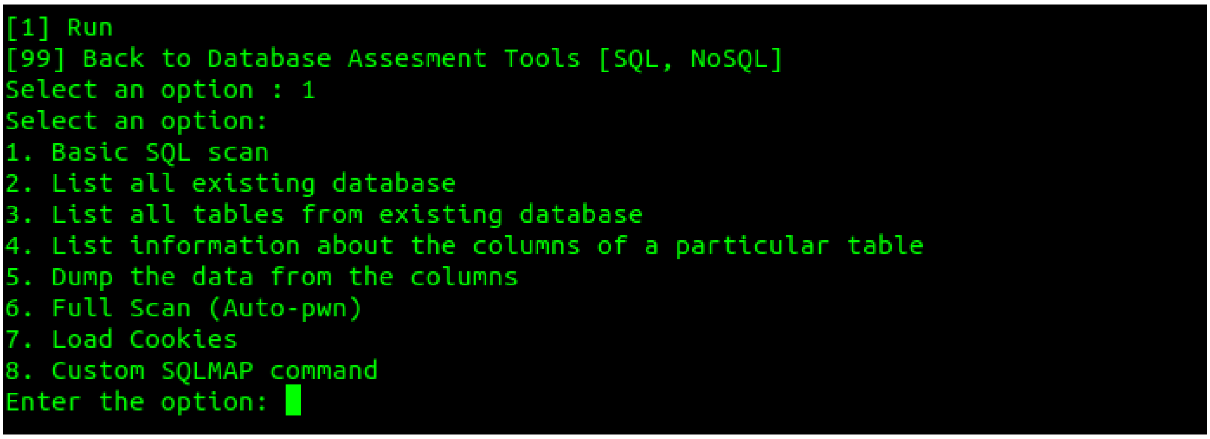
The tools that are integrated into the system for the purpose to perform Denial of Service attacks are SlowLoris, GoldenEye and Rufus as shown in fig 5.12. These are best Dos attack tools till this date and work efficiently while performing Denial of service and DDos attacks.



```
[0 SlowLoris - Slowloris is basically an HTTP Denial of Service attack

[1 GoldenEye - SECURITY TESTING PURPOSES ONLY!

[2 Rufus - Rufus is a simple but powerful Denial of Service tool



[99] Back to All tools
Choose a tool to proceed:
```

Figure 5.12 DoS Attacking Tools

Fig 5.13 shows the tool that is integrated into the system for the purpose of Database exploitation is SqlMap that has a wide range of features that work efficiently while finding vulnerabilities in the database of web applications that uses structured query language.

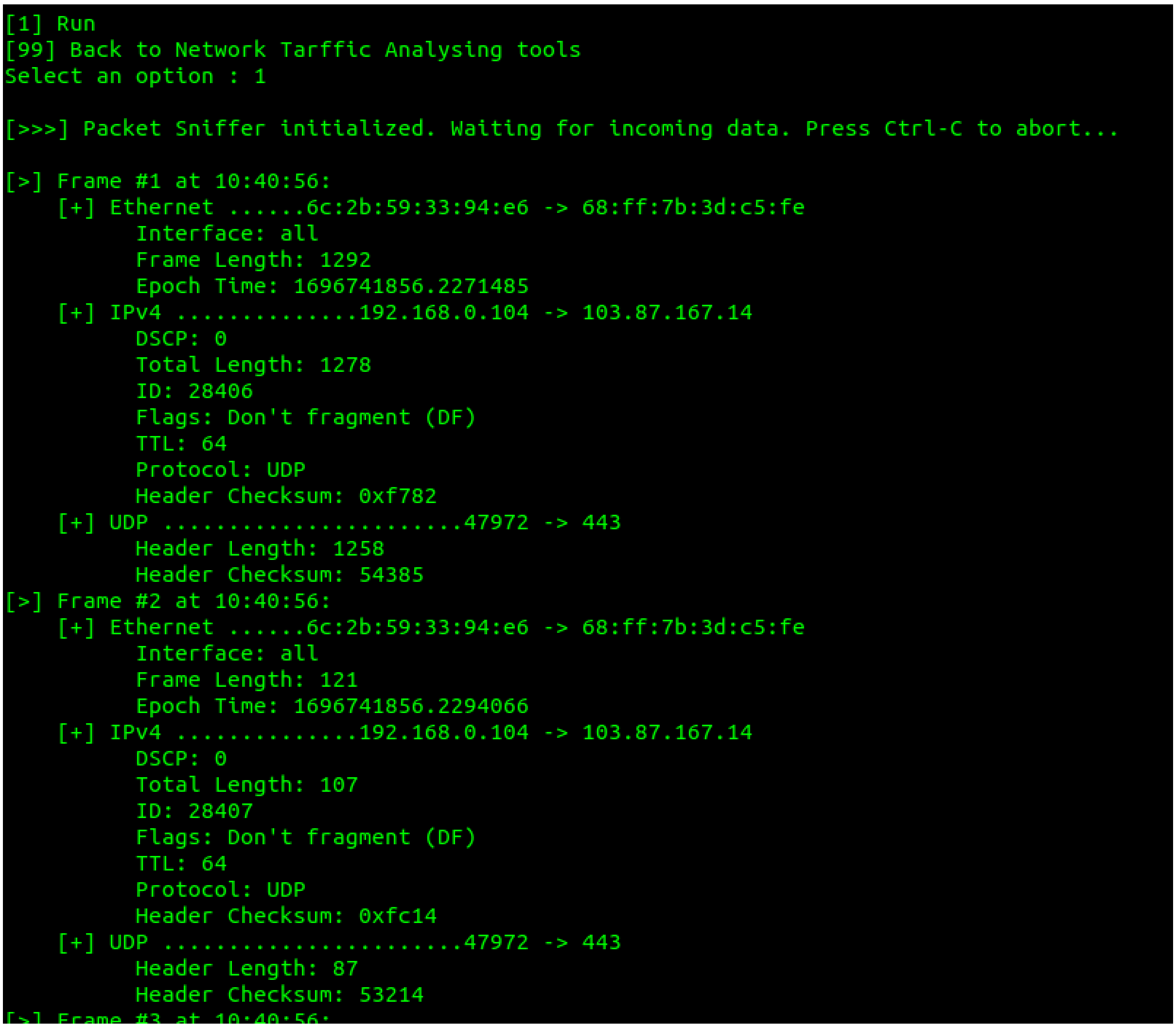


```
[1] Run
[99] Back to Database Assesment Tools [SQL, NoSQL]
Select an option : 1
Select an option:
1. Basic SQL scan
2. List all existing database
3. List all tables from existing database
4. List information about the columns of a particular table
5. Dump the data from the columns
6. Full Scan (Auto-pwn)
7. Load Cookies
8. Custom SQLMAP command
Enter the option:
```

Figure 5.13 Range of Options in SQL Map

5.2.3 Packet Sniffer

Packet sniffer in the toolkit enables network administrators to troubleshoot issues by inspecting data packets, aiding in the identification of network congestion, misconfigurations, and hardware faults. It plays a pivotal role in network security, detecting suspicious activities, unauthorized access attempts, and potential cyber threats. By scrutinizing protocols, it assists in debugging complex network interactions and optimizing performance, ensuring efficient bandwidth utilization.

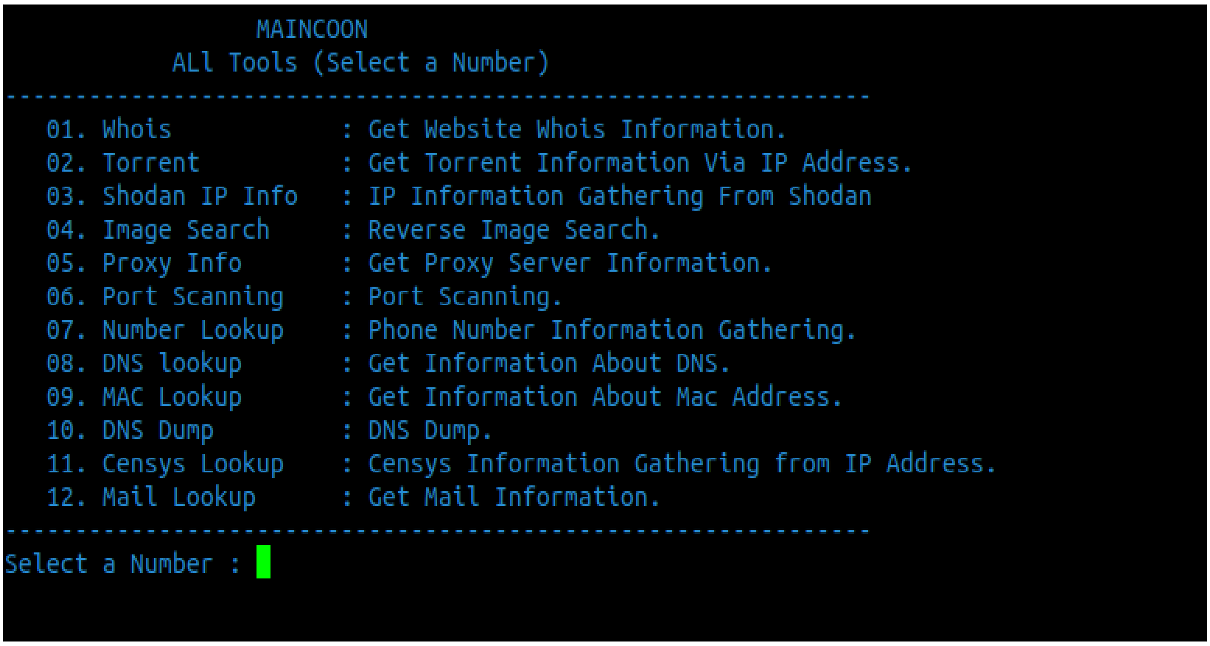


```
[1] Run
[99] Back to Network Tarffic Analysing tools
Select an option : 1

[>>>] Packet Sniffer initialized. Waiting for incoming data. Press Ctrl-C to abort...

[>] Frame #1 at 10:40:56:
    [+] Ethernet ......6c:2b:59:33:94:e6 -> 68:ff:7b:3d:c5:fe
          Interface: all
          Frame Length: 1292
          Epoch Time: 1696741856.2271485
    [+] IPv4 .............192.168.0.104 -> 103.87.167.14
          DSCP: 0
          Total Length: 1278
          ID: 28406
          Flags: Don't fragment (DF)
          TTL: 64
          Protocol: UDP
          Header Checksum: 0xf782
    [+] UDP ......................47972 -> 443
          Header Length: 1258
          Header Checksum: 54385
[>] Frame #2 at 10:40:56:
    [+] Ethernet ......6c:2b:59:33:94:e6 -> 68:ff:7b:3d:c5:fe
          Interface: all
          Frame Length: 121
          Epoch Time: 1696741856.2294066
    [+] IPv4 .............192.168.0.104 -> 103.87.167.14
          DSCP: 0
          Total Length: 107
          ID: 28407
          Flags: Don't fragment (DF)
          TTL: 64
          Protocol: UDP
          Header Checksum: 0xfc14
    [+] UDP ......................47972 -> 443
          Header Length: 87
          Header Checksum: 53214
[>] Frame #3 at 10:40:56:
```

Figure 5.14 Packet Sniffer

5.2.4 Web Vulnerability Testing Tool

MAINCOON is a powerful web application testing tool. It has a robust suite of features that allows cybersecurity professionals and quality assurance teams to conduct comprehensive security assessments and vulnerability scans on web applications. By simulating real-world attack scenarios, MAINCOON identifies and reports potential security weaknesses such as SQL injection, cross-site scripting (XSS), and other common vulnerabilities. This Tool streamlines the process of identifying and rectifying vulnerabilities, ultimately enhancing the overall security posture of web-based platforms.



```
                  MAINCOON
            ALl Tools (Select a Number)
--------------------------------------------------------------
   01. Whois            : Get Website Whois Information.
   02. Torrent          : Get Torrent Information Via IP Address.
   03. Shodan IP Info   : IP Information Gathering From Shodan
   04. Image Search     : Reverse Image Search.
   05. Proxy Info       : Get Proxy Server Information.
   06. Port Scanning    : Port Scanning.
   07. Number Lookup    : Phone Number Information Gathering.
   08. DNS lookup       : Get Information About DNS.
   09. MAC Lookup       : Get Information About Mac Address.
   10. DNS Dump         : DNS Dump.
   11. Censys Lookup    : Censys Information Gathering from IP Address.
   12. Mail Lookup      : Get Mail Information.
--------------------------------------------------------------
Select a Number : 
```

Figure 5.15 MAINCOON Web Application Testing Tool

5.3 Conclusion

In this chapter we have successfully integrated and tested various information gathering tools, Web Application testing tools, DOS attack tools, packet sniffers and vulnerability assessment tools .Once the toolkit is Installed into the system all of the above mentioned tools will be automatically loaded into the framework and it will be ready to use.

CHAPTER 6: CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

The "CyberSec ProSuite" project represents a substantial advancement in the realm of cybersecurity solutions, offering a wide array of benefits and capabilities while not without its limitations. In this conclusion, we will explore the advantages and disadvantages of this innovative system.

Advantages:

- Many Helpful Tools: This project offers lots of tools to help keep your digital stuff safe. It can find vulnerabilities, protect your data, and more. That's a big plus.
- Easy to Use: They made it so anyone, even if you're not a tech whiz, can use it. You can click around with a mouse or type commands if you want.
- Super Secure: Your data will be locked up like Fort Knox. They use special tricks to make sure only the right people can access it.
- Keeps Up with the Times: It's like a digital superhero that can adapt to new challenges. It plays nice with other security tools, which is handy.
- Follows the Rules: If you've got rules to follow (like laws or company policies), this project helps you stay on the right side of those rules.

Disadvantages:

- User Interface Constraints: Limited Usability: CLIs are typically text-based and may lack the graphical features of a graphical user interface (GUI). This can limit the toolkit's user-friendliness, especially for those who are not CLI-savvy.
- Platform Compatibility: Cross-Platform Compatibility: Ensuring the toolkit works across different operating systems (Windows, Linux, macOS) can be complex, as command syntax and availability of certain tools may vary.
- Tool Integration: Tool Compatibility: Different tools may require specific dependencies, libraries, or runtime environments. Ensuring smooth integration of diverse tools within the CLI can be challenging.
- Updates and Maintenance: Tool Versioning: As tools frequently receive updates, maintaining compatibility and staying current with the latest versions can be time-consuming.

6.2 Future Scope

The future scope of the CyberSec ProSuite project lies in expanding its reach and usability by creating both a Command Line Interface (CLI) and a Graphical User Interface (GUI) version of the toolkit. This dual-interface approach will cater to a wider user base and enhance user-friendliness while retaining the power and comprehensiveness of the toolkit.

1. GUI Integration: Develop a Graphical User Interface (GUI) that complements the existing CLI version. This will make the toolkit accessible to users who are more comfortable with visual interfaces.
2. Cross-Platform Compatibility: Ensure that both the CLI and GUI versions are compatible with major operating systems (Windows, Linux, macOS), allowing users to choose their preferred interface.
3. User Profiles: Implement user profiles and preferences in the GUI to enable personalization, such as theme selection and tool arrangement, making the toolkit more user-centric.
4. Enhanced Usability: Design an intuitive and user-friendly GUI with features like drag-and-drop tool selection, real-time feedback, and interactive dashboards for monitoring tests.
5. Educational Resources: Offer educational resources within the GUI, such as tutorials, documentation, and links to relevant cybersecurity courses, to facilitate user learning and skill development.

CHAPTER 7: REFERENCES

[1]. M. Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan and Ata-ur-rehman, "Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool," 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 2019, pp. 1-6, doi: 10.1109/ICOMET.2019.8673520.

[2]. A. Roy, L. Mejia, P. Helling and A. Olmsted, "Automation of cyber-reconnaissance: A Java-based open source tool for information gathering," 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 2017, pp. 424-426, doi: 10.23919/ICITST.2017.8356437.

[3]. .J. E. Kocher and D. P. Gilliam, "Self port scanning tool: providing a more secure computing environment through the use of proactive port scanning," 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05), Linköping, Sweden, 2005, pp. 139-143, doi: 10.1109/WETICE.2005.51.

[4]. .N. Ahmed, Z. I. A. Khalib, R. B. Ahmed, W. M. Ghossoon, S. Sudin and S. Asi, "Embedded Port Scanner (EPSS) System using linux and Single Board Computer," 2008 International Conference on Electronic Design, Penang, Malaysia, 2008, pp. 1-5, doi: 10.1109/ICED.2008.4786717.

[5]. N. I. Daud, K. A. Abu Bakar and M. S. Md Hasan, "A case study on web application vulnerability scanning tools," 2014 Science and Information Conference, London, UK, 2014, pp. 595-600, doi: 10.1109/SAI.2014.6918247.

[6]. .R. R. Rohrmann, V. J. Ercolani and M. W. Patton, "Large scale port scanning through tor using parallel Nmap scans to scan large portions of the IPv4 range," 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 2017, pp. 185-187, doi: 10.1109/ISI.2017.8004906.

[7]. W. Qianqian and L. Xiangjun, "Research and design on Web application vulnerability scanning service," 2014 IEEE 5th International Conference on Software Engineering and Service Science, Beijing, China, 2014, pp. 671-674, doi: 10.1109/ICSESS.2014.6933657.

[8]. Udhayan, M. Muruga Prabu, V. Aravinda Krishnan and R. Anitha, "Reconnaissance Scan Detection Heuristics to disrupt the pre-attack information gathering," 2009 International Conference on Network and Service Security, Paris, France, 2009, pp. 1-5.

[9]. A. R. Chordiya, S. Majumder and A. Y. Javaid, "Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools," 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 2018, pp. 0438-0443.

[10]. S. Kataria, T. Kumar, K. Singh and M. S. Nehra, "ECR (encryption with cover text and reordering) based text steganography," 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013), Shimla, 2013, pp. 612-616, doi: 10.1109/ICIIP.2013.6707666.

[11]. C. Sharma and S. C. Jain, "Analysis and classification of SQL injection vulnerabilities and attacks on web applications," 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), Unnao, India, 2014, pp. 1-6, doi: 10.1109/ICAETR.2014.7012815.

[12]. G. Su, F. Wang and Q. Li, "Research on SQL Injection Vulnerability Attack model," 2018 5th IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), Nanjing, China, 2018, pp. 217-221, doi: 10.1109/CCIS.2018.8691148.

[13]. S. Alazmi and D. C. de Leon, "Customizing OWASP ZAP: A Proven Method for Detecting SQL Injection Vulnerabilities," 2023 IEEE 9th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), New York, NY, USA, 2023, pp. 102-106, doi: 10.1109/BigDataSecurity-HPSC-IDS58521.2023.00028.

[14]. N. Atikah, M. R. Ashila, D. R. Ignatius Moses Setiadi, E. H. Rachmawanto and C. A. Sari, "AES-RC4 Encryption Technique to Improve File Security," 2019 Fourth International Conference on Informatics and Computing (ICIC), Semarang, Indonesia, 2019, pp. 1-5, doi: 10.1109/ICIC47613.2019.8985825.

[15]. F. Schuckert, H. Langweg and B. Katt, "Systematic Generation of XSS and SQLi Vulnerabilities in PHP as Test Cases for Static Code Analysis," 2022 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Valencia, Spain, 2022, pp. 261-268, doi: 10.1109/ICSTW55395.2022.00053.

[16]. T. Aung and Z. T. T. Myint, "Effective Web Application Vulnerability Testing System Using Proposed XSS_SQL_Scanning_Algorithm," 2023 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 2023, pp. 189-193, doi: 10.1109/ICCA51723.2023.10181398.

[17]. .B. Zukran and M. M. Siraj, "Performance Comparison on SQL Injection and XSS Detection using Open Source Vulnerability Scanners," 2021 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 2021, pp. 61-65, doi: 10.1109/ICoDSA53588.2021.9617484.

[18]. Zulkarneev and A. Kozlov, "New Approaches of Multi-agent Vulnerability Scanning Process," 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 2021, pp. 0488-0490, doi: 10.1109/USBEREIT51232.2021.9455061.

[19]. G. Song et al., "Which Doors Are Open: Reinforcement Learning-based Internet-wide Port Scanning," 2023 IEEE/ACM 31st International Symposium on Quality of Service (IWQoS), Orlando, FL, USA, 2023, pp. 1-10, doi: 10.1109/IWQoS57198.2023.10188692.

[20]. F. Mohammed, N. A. A. Rahman, Y. Yusof and J. Juremi, "Automated Nmap Toolkit," 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC), Bhubaneswar, India, 2022, pp. 1-7, doi: 10.1109/ASSIC55218.2022.10088375.

[21]. H. Sharad Sonawane, S. Deshmukh, V. Joy and D. Hadsul, "Torsion: Web Reconnaissance using Open Source Intelligence," 2022 2nd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2022, pp. 1-4, doi: 10.1109/CONIT55038.2022.9848337.

[22]. Udhayan, M. Muruga Prabu, V. Aravinda Krishnan and R. Anitha, "Reconnaissance Scan Detection Heuristics to disrupt the pre-attack information gathering," 2009 International Conference on Network and Service Security, Paris, France, 2009, pp. 1-5.

[23]. Vinny Troia, "Automated Tools for Network Discovery," in Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques , Wiley, 2020, pp.83-117, doi: 10.1002/9781119541004.ch5.

[24]. F. Mohammed, N. A. A. Rahman, Y. Yusof and J. Juremi, "Automated Nmap Toolkit," 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC), Bhubaneswar, India, 2022, pp. 1-7, doi: 10.1109/ASSIC55218.2022.10088375.

[25]. T. Zhang and X. Guo, "Research on SQL Injection Vulnerabilities and Its Detection Methods," 2020 4th Annual International Conference on Data Science and Business Analytics (ICDSBA), Changsha, China, 2020, pp. 251-254, doi: 10.1109/ICDSBA51020.2020.00071.

CHAPTER 8: PUBLICATION

8.1Research Papers Published

1. Mohammad Saqib, Yatin Rathod, Dimple Rathore, Dr. Shwetambari Borade, “CyberSec ProSuite”, ICTACT Journal of Soft Computing, 2024.

8.2 Intellectual Property Rights-Copyright

1. Dairy Number: 9736/2024-CO/SW, Title of Work “CyberSec ProSuite”, March 2024, Computer Software Work by Mohammad Saqib, Dimple Rathore, Yatin Rathod & Dr.Shwetambari Borade

CHAPTER 8: ACKNOWLEDGEMENT

Acknowledgement

We take this opportunity to express our sincere thanks to our Guide, Dr.Shwetambari Borade, the faculty in the Department of Cyber Security in Shah and Anchor Kutchhi Engineering College for guiding us and suggesting regarding the line of work for our project “CyberSec ProSuite”. We would like to express our gratitude towards their constant encouragement, support and guidance throughout the progress.

Also, we would like to thank our Principal – Dr. Bhavesh Patel and Dr. Nilakshi Jain, Head of Cyber Security Department, for their help, support & guidance for this project.

We are also thankful to all Faculty members of our department for their help and guidance during completion of our project