

KAEZEL

A Social Engineering Framework



By:

Umair Fazal (SAP:23317)

Zeeshan Karim (SAP: 26219)

Supervised by: Dr. Jawaid Iqbal Jadoon

Faculty of Computing

Riphah International University, Islamabad

Fall 2024

A Dissertation Submitted To

Faculty of Computing,

Riphah International University, Islamabad

As a Partial Fulfillment of the Requirement for the Award of

the Degree of

Bachelors of Science in Cyber Security

Date: 15th November, 2024

Final Approval

This is to certify that we have read the report submitted by *Umair Fazal (23317) and Zeeshan Karim (26219)*, for the partial fulfillment of the requirements for the degree of the Bachelors of Science in Cyber Security (BSCY). It is our judgment that this report is of sufficient standard to warrant its acceptance by Riphah International University, Islamabad for the degree of Bachelors of Science in Cyber Security (BSCY).

Committee:

1

Dr. Jawaaid Iqbal Jadoon (Supervisor)

(Head of Cyber Security Department)

2

Dr. Musharraf Ahmed
(Head of Department/chairman)

Declaration

We hereby declare that this document “**KAEZEL (A SOCIAL ENGINEERING FRAMEWORK)**” neither as a whole nor as a part has been copied out from any source. It is further declared that we have done this project with the accompanying report entirely on the basis of our personal efforts, under the proficient guidance of our teachers, especially our supervisor **Dr. Jawaid Iqbal Jadoon**. If any part of the system is proved to be copied out from any source or found to be reproduction of any project from anywhere else, we shall stand by the consequences.

Umair Fazal

SAP: 23317

Zeeshan Karim

SAP: 26219

Dedication

This Project is especially dedicated to our Parents, whose heartwarming support, love, and appreciation has brought us to this day of fulfillment in our journey. A special thanks and appreciation to our esteemed supervisor Sir Dr. Jawaid Iqbal Jadoon, whose commitment and dedication to us and our success have been of immense help and value. We would like to express our deepest gratitude to all the faculty members and supporting staff. Without them this project would not have been successful. Their teaching methodology, dedication, and moral support were all the way supporting, helping us to grasp our foundational skills in the field of Cyber Security.

Acknowledgement

First of all, we are obliged to Allah Almighty the Merciful, the Beneficent and the source of all Knowledge, for granting us the courage and knowledge to complete this Project.

We would like to Appreciate the efforts and moral support of our respected Supervisor Sir Dr. Jawaid Iqbal Jadoon for his continuous appreciation, support and valuable guidance throughout the competition of this Project.

We would also like to express our deepest gratitude to all the teachers, Faculty members, and Supporting staff whose commitment and dedication for teaching has brought us to this day of completion in our journey. Their foundational knowledge and skills have been of immense value to us which led us to improve our knowledge and skills throughout the degree.

Umair Fazal

SAP: 23317

Zeeshan Karim

SAP: 26219

Abstract

The advancement and sophistication in potential threats in cyber industry, specifically social engineering attacks, demands advanced tools and frameworks to be incorporated for the effectiveness of Security assessments. This project constructs an effective social engineering framework that provides six major tools that incorporate features like phishing, mass mailing, exploitation through QR-code and hijacking the webcam for simulation of real-world scenarios and real time social engineering attacks. All these tools are intended to provide an effective security assessment within organizations on social engineering. The main objective of this framework is to provide a versatile and robust system for security professionals to facilitate their operation and assess the vulnerabilities of organizations along with providing training and awareness on social engineering by eliciting real time attacks on individuals. Dedicated stakeholders for this framework could be Organizations, cyber security professionals, educational institutions and Government agencies etc. The framework intends to provide an effective mechanism to encounter social engineering threats and improve security and defense mechanisms in organization.

1 Table of Contents

1	Chapter 1: Introduction	2
1.1	Introduction.....	2
1.1.1	Background	2
1.1.2	Existing Systems	2
1.1.3	Kaezel (A Social Engineering Framework)	3
1.1.3.1	Phisher.....	3
1.1.3.2	Camphisher	4
1.1.3.3	QR-Attack	4
1.1.3.4	URL-Mask	4
1.1.3.5	Find User.....	4
1.1.3.6	Kaezal_X.....	5
1.2	Opportunity and Stakeholders.....	5
1.2.1	Opportunities.....	5
1.2.1.1	Execution of real time attack	5
1.2.1.2	Awareness Campaign and trainings.....	5
1.2.1.3	Enhanced security policies.....	5
1.2.1.4	Integration in other frameworks.....	6
1.2.2	Stakeholders	6
1.2.2.1	Cyber Security teams and professionals	6
1.2.2.2	Educational Institutions	6
1.2.2.3	IT professionals.....	6
1.2.2.4	Government agencies.....	6
1.2.2.5	Private IT companies and consultants.....	6
1.3	Motivation and Challenges	7

1.3.1	Motivation.....	7
1.3.1.1	Advancements and social engineering.....	7
1.3.1.2	Enhancement of existing framework	7
1.3.1.3	Aid Security teams.....	7
1.3.2	Challenges.....	7
1.3.2.1	legal Consent.....	7
1.3.2.2	Performing attacks without causing harms	8
1.3.2.3	Advancement in potential threats.....	8
1.3.2.4	Data privacy and security.....	8
1.3.2.5	Technical complications	8
1.4	Significance of study.....	8
1.4.1	Effective security awareness.....	9
1.4.2	Security Assessments.....	9
1.4.3	Educational and ethical simulation	9
1.5	Goals and Objectives	9
1.5.1	Goals.	9
1.5.2	Objectives	10
1.5.2.1	simulating real attack	10
1.5.2.2	Effectiveness of security evaluation	10
1.5.2.3	Reinforce Pentesters for better operations	10
1.5.2.4	Effective security training.....	10
1.5.2.5	Ethical and legal requirements.....	10
1.6	Scope of project	11
1.6.1	Target Audience.....	11
1.6.2	Tool integration.....	11

1.6.3	Scalability and flexibility	11
1.6.4	Security and ethical compliance	11
1.7	Summary	12
2	Chapter 2: Literature Review	14
2.1	Introduction.....	14
2.2	Literature review	14
2.2.1	Browser Exploitation Framework (BeEF)	14
2.2.2	Social Engineering toolkit (SET).....	15
2.2.3	king phisher.....	15
2.2.4	Metasploit	16
2.2.5	Gophisher.....	16
2.2.6	Maltego	17
2.3	Comparative analysis:	17
2.4	Research gaps.....	18
2.4.1	Lack of comprehensive and real time social engineering simulations	18
2.4.2	Limited focus on training and awareness.....	19
2.4.3	Scalability and customization	19
2.5	Problem statement.....	19
2.6	Summary	20
3	Chapter 3: Requirement engineering.....	22
3.1	Introduction.....	22
3.2	Functional requirements.....	22
3.2.1	Phisher tool	22
3.2.2	Camphisher Tool.....	22
3.2.3	QR-attack tool.....	23

3.2.4	URL-mask tool.....	23
3.2.5	FindUser tool	23
3.2.6	Kaezal_X tool:	23
3.3	Non-Functional Requirements	23
3.3.1	Performance	23
3.3.2	Usability	24
3.3.3	Reliability.....	24
3.3.4	Security	24
3.3.5	Compatibility	24
3.4	Design diagrams.....	24
3.4.1	Data flow diagram.....	25
3.4.2	Use Case diagram	25
3.5	Hardware and Software requirements.....	26
3.5.1	Hardware requirements	26
3.5.1.1	Processor	26
3.5.1.2	Memory	26
3.5.1.3	Storage	27
3.5.1.4	Network Interface	27
3.5.2	Software requirements	27
3.5.2.1	Operating system	27
3.5.2.2	Python runtime environment.....	27
3.5.2.3	Tunneling Services.....	27
3.5.2.4	Webserver Software.....	27
3.6	Threat scenarios	27
3.6.1	Scenario 1: widespread of Phishing attacks.....	27

3.6.2	Scenario 2: Exploitation through QR-code.....	28
3.6.3	Scenario 3: URL-masking.....	28
3.7	Threat modeling Techniques.....	28
3.8	Threat Resistance Model.....	30
3.8.1	Awareness Training	30
3.8.2	Simulated attacks	30
3.8.3	Access control.....	30
3.8.4	Monitoring and logging	30
3.9	Summary	30
4	Proposed solution.....	33
4.1	Introduction.....	33
4.2	Proposed model.....	33
4.3	Data Collection methods.....	34
4.3.1	User interactions	34
4.3.2	Network logs.....	34
4.3.3	Survey Responses	34
4.3.4	Threat intelligence reports	34
4.4	Data pre-processing	34
4.4.1	Outlier removal	35
4.4.2	Classification.....	35
4.4.3	filtering.....	35
4.4.4	Prioritization	35
4.5	Evaluation matrices.....	35
4.5.1	Engagement and interaction rate.....	36
4.5.2	Realism and Robustness	36

4.5.3	Error analysis and adaptation rate	36
4.5.4	Improvement in awareness	36
4.6	Summary	36
5	Chapter 5: Implementation.....	39
5.1	Security property testing	39
5.1.1	Confidentiality	39
5.1.2	Integrity	39
5.1.3	Availability	40
5.1.4	Realism of simulations.....	40
5.2	System setup	40
5.2.1	Environment configuration	40
5.2.1.1	Operating System.....	40
5.2.1.2	Python	40
5.2.1.3	Tunneling Services.....	41
5.2.1.4	Webserver Software.....	41
5.2.1.5	Processor	41
5.2.1.6	Memory	41
5.2.1.7	Storage	41
5.2.1.8	Network Interface	41
5.3	System Integration	41
5.3.1	Components integration	41
5.3.2	API integration.....	42
5.3.3	Log management and storage setup	42
5.4	Test cases	42
5.4.1	Functionality test case.....	42

5.4.2	Usability test case	43
5.5	Results and discussions	43
5.5.1	Functionality tests	44
5.5.1.1	Phishing simulation tool (Phisher).....	44
5.5.1.2	Camera Phishing tool (Camphish)	44
5.5.2	Usability test	44
5.5.2.1	User Interface (UI)	44
5.6	Development Practices and Standards:	45
5.6.1	Coding Standards:	45
5.6.2	Security Practices:	45
5.6.3	Version control:	45
5.6.4	Testing:	45
5.6.5	Ethical Standards:	45
5.7	Summary:	46
6	Conclusion and Outlook	48
6.1	Introduction.....	48
6.2	Achievements and Improvements	48
6.2.1	Effective social engineering tools.....	48
6.2.2	Educational applicability	48
6.2.3	Scalability and Flexibility	49
6.2.4	Ethical considerations	49
6.3	Critical review.....	49
6.3.1	Realism and Evasion.....	49
6.3.2	Security Concerns	49
6.3.3	Compatibility issues.....	50

6.4	Future recommendations and outlook.....	50
6.4.1	Advanced evasion techniques	50
6.4.2	Integration of Artificial Intelligence	50
6.4.3	Enhanced reporting and analysis	50
6.5	Summary	50
7	References	52

Table of Figures

Figure 1.1 Kaezal Interface	3
Figure 2.1 Social Engineering Toolkit (SET)	15
Figure 2.2 King Phisher Tool.....	16
Figure 2.3 Maltego.....	17
Figure 3.1Data Flow Diagram	25
Figure 3.2 Use Case diagram Kaezal	26

List of Tables

Table 2.1 Comparative analysis.....	17
Table 3.1 STRIDE model for threat modeling.....	29

Chapter 1:

Introduction

1 Chapter 1: Introduction

This chapter will entail a brief background of social engineering, the introduction, Existing frameworks and will provide a detailed description of our work in the realm of social engineering. Furthermore, this section will entail the stakeholders, goals and objectives along with the challenges and motivation faced during the development of this project.

1.1 Introduction

This section will delve into the introduction and elaborates key features, background and the tools that are being integrated in this project.

1.1.1 Background

In the realm of Cyber Security, Social Engineering poses a great challenge and a significant threat to those who are vulnerable. Instead of technical flaws and vulnerabilities, social engineering leverages human psychology to manipulate their minds to exploit and breach their security systems. Social engineering uses multiple techniques involving Phishing, Spoofing, Smishing, Scareware and pretexting etc. to manipulate humans which leads to the compromise of their sensitive information and Exploitation of their systems.

1.1.2 Existing Systems

These Social engineering tactics are being encountered by professionals who leverage multiple Social Engineering frameworks to spread awareness, find vulnerabilities and organize campaigns and educational programs to eradicate the threat that is being imposed on the individuals every day. Some of the frameworks are mentioned below.

- Social Engineering Toolkit (SET)
- Browser Exploitation Framework (BeEF)
- KingPhisher
- Metasploit
- Gophish
- Maltego

1.1.3 Kaezel (A Social Engineering Framework)

To encounter the challenges and growing needs of an effective system, we have developed a Social Engineering framework that leverages multiple social engineering techniques to simulate the attacks to scrutinize vulnerabilities, spread awareness and Education of Social Engineering threats and its impacts. Our system has integrated Six tools which are responsible for simulating Social Engineering in an effective way. The system is compatible with Linux Systems and furthermore the system will provide a friendly GUI Interface in the next phases of development as it further proceeds.

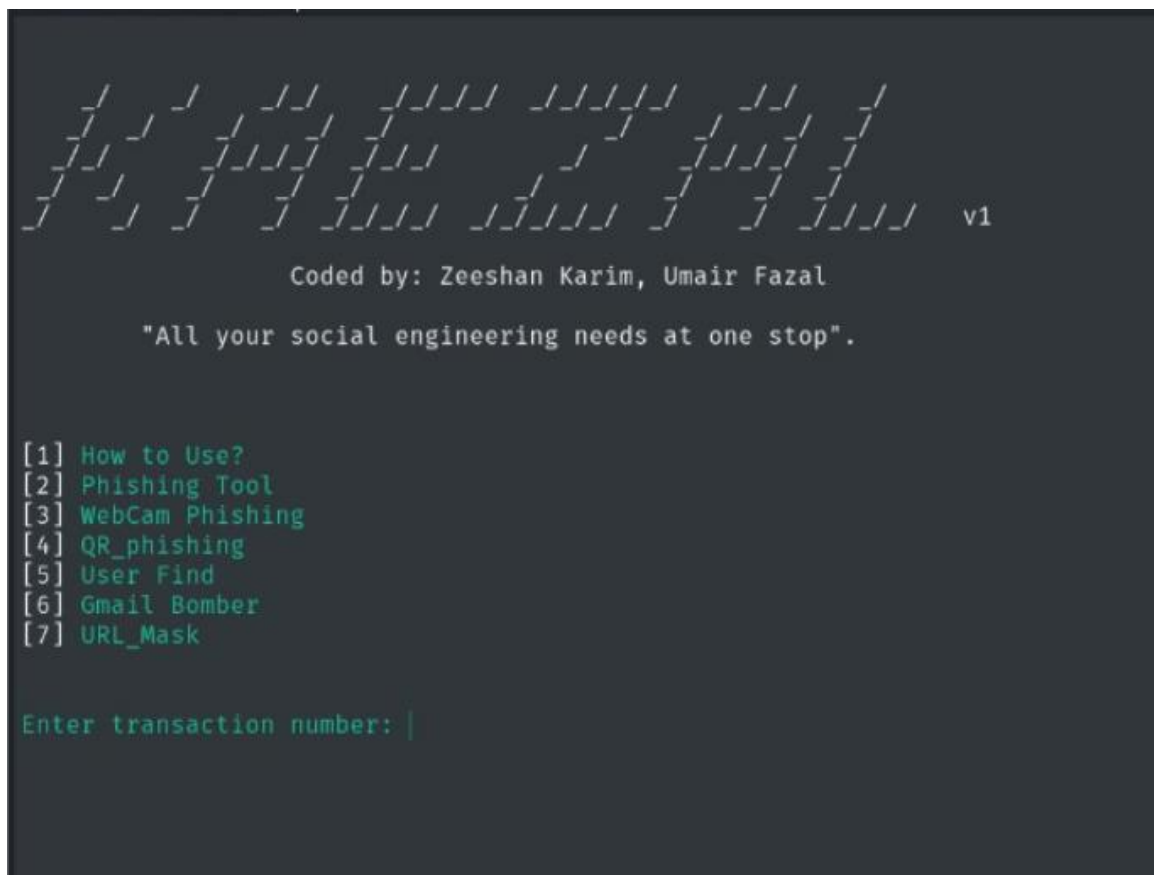
The image shows a terminal window with a dark background. At the top, there is a logo made of white and green characters that looks like a stylized 'K' or a series of slanted lines. To the right of the logo is the text 'v1'. Below the logo, it says 'Coded by: Zeeshan Karim, Umair Fazal'. Underneath that is a quote: '"All your social engineering needs at one stop".'. Then there is a list of menu items, each preceded by a number in brackets: [1] How to Use?, [2] Phishing Tool, [3] WebCam Phishing, [4] QR_phishing, [5] User Find, [6] Gmail Bomber, and [7] URL_Mask. At the bottom, there is a prompt 'Enter transaction number: ' followed by a vertical bar cursor.

Figure 1.1 Kaezel Interface

The tools integrated in our framework are following:

1.1.3.1 Phisher

This tool uses the Phishing technique to perform Social Engineering on the Victim to gain credentials. This tool firstly creates a local web server (PHP) that is responsible for hosting

the phishing webpage which is exposed to the internet using some service like Cloudflare, ngrok and LocalXpose. When the victim is exposed to this page it gains all the credentials entered by the victim on this page. This way it harvests the credentials to scrutinize this vulnerability using Phishing techniques.

1.1.3.2 Camphisher

This page also leverages the Phishing technique. This tool directs the victim to a legitimate looking webpage which requests for webcam permission. Upon permission this webpage starts capturing images of the victim's webpage and sends it to the attacker. In this way it simulates a phishing attack depicting the threat of granting access of resources to untrusted sources.

1.1.3.3 QR-Attack

This tool leverages the phishing through QR code. The tool generates a QR- code which upon scanning redirects the victim to a fake webpage which requests for credentials. and upon entering the credentials it sends it to the attacker resulting in exposure of sensitive credentials. This Tools simulates the Phishing attack through QR code which highlights the threat of scanning unknown codes from unauthentic sources.

1.1.3.4 URL-Mask

The tool disguises Phishing links to appear as trustworthy and authentic and more like a legitimate URL. This makes the victim engage to the given requests exposing sensitive information and credentials. This leverages the masking of malicious URLs to increase the effectiveness of social engineering.

1.1.3.5 Find User

This tool leverages the IP to collect and gather open-source information relevant to the IP address, providing the information about the user that is being associated with the IP Source. This conduct of information gathering provides the initial information for targeting a victim through Social Engineering.

1.1.3.6 Kaezal_X

Kaezal_X is specifically designed to simulate advanced social engineering attacks that target user trust and curiosity. By injecting malicious payloads into common files that users typically do not suspect, this tool helps organizations assess how vulnerable their systems are to such attacks. Additionally, it can be used for training employees to recognize suspicious files and protect their devices from such threats.

1.2 Opportunity and Stakeholders

This section will describe all the opportunities and stakeholder involved with the framework.

1.2.1 Opportunities

The opportunities that this project will bring to the industry involve:

1.2.1.1 Execution of real time attack

This tool gives the opportunity to pentesters and red teams to simulate real time social engineering scenarios and threats to identify vulnerabilities and victims that could become suspect to any attacker. By carrying out this strategy organization's abilities are being assessed to counter any social engineering attacks in future.

1.2.1.2 Awareness Campaign and trainings

By leveraging this tool organizations could enhance their security by performing real time social engineering attacks which will give the employees a basic understanding and awareness of such attacks and how to respond to them. This strategy could significantly lessen the risks of potential threats in future.

1.2.1.3 Enhanced security policies

The understanding developed after using this tool and collecting all the responses of individuals and organizations. The security teams could identify potential vulnerabilities and weaknesses and implement some effective policies that would significantly lessen the risk of threats.

1.2.1.4 Integration in other frameworks

Cyber security teams and professionals could leverage this tool by integrating its functionalities in their existing systems which will allow them to carry out their security tasks and assessments more effectively.

1.2.2 Stakeholders

The Stakeholders that could be influenced and will be benefited with this toolkit involves:

1.2.2.1 Cyber Security teams and professionals

The cyber security team members that include penetration testers, analysts, red teams and social engineering experts could leverage this tool to perform real time attacks to find vulnerabilities, suspect victims and enhance security of systems.

1.2.2.2 Educational Institutions

Individuals in academic programs that are associated with cyber security, information security and social engineering research and training whether they are researchers, teachers or students could take advantage of this tool in their academics for enhancing their understanding in the field of their relevant interests.

1.2.2.3 IT professionals

Developers and system engineers could leverage this tool by integrating it into other systems where needed to enhance the features of their existing systems.

1.2.2.4 Government agencies

The Security agencies, law enforcement and other state sensitive agencies could take some good advantage of this tool to enhance their security and eradicate potential social engineering threats within the organization.

1.2.2.5 Private IT companies and consultants

Some software houses and IT companies could leverage this tool by providing social engineering services and consultancy to enhance security of their clients and provide awareness trainings and programs

1.3 Motivation and Challenges

This section will provide the key motivations and highlights the challenges occurred in the development of this toolkit.

1.3.1 Motivation

The motivation factors for the development of this tool involves:

1.3.1.1 Advancements and social engineering

With the advancement of the IT industry and technology the potential threats and ranges of attacks are also rising. For this reason, a significant advancement in the field of cybersecurity is needed which will provide advanced strategies and attacks to assess the vulnerabilities and security of organizations.

1.3.1.2 Enhancement of existing framework

While there are many effective tools available in the market, a gap exists which could be covered by providing advanced strategies, new features and user friendliness of the system are some aspects that were kept in view.

1.3.1.3 Aid Security teams

Penetration testers and red teams need robust and advanced systems and tools every day to tackle rising threats. For this reason, a need for an advancement in the field of social engineering is needed which could leverage new tactics and strategies to enhance the effectiveness of simulating new and advanced social engineering attempts.

1.3.2 Challenges

The challenges that we might encounter with the advent of this framework are following:

1.3.2.1 legal Consent

While developing such kinds of tools an ethical consent is needed for its use. It should be kept in view that such tools are being operated in a safe environment with legal and ethical considerations for legitimate use and not for some unethical purpose.

1.3.2.2 Performing attacks without causing harms

While using these tools the security teams should ensure that the performance of realistic attacks doesn't cause potential harm or any loss to data or sensitive information. A backup plan should be in consideration every time while using these tools.

1.3.2.3 Advancement in potential threats

As we know the attackers are active every time progressing each day to harm individuals. It should be considered that such tools need upgradation and advancement with passage of time to enhance effectiveness and efficiency of the system to provide better security assessment.

1.3.2.4 Data privacy and security

While performing attacks, captured data and sensitive information must be well managed, kept confidential and not be leaked or mismanaged. The protection of the data is a significant challenge for social engineering tools and frameworks.

1.3.2.5 Technical complications

Such frameworks require technical expertise and practical knowledge to maintain and integrate the features accordingly. while developing such a tool, a user-friendly feature must be incorporated for the ease of access and usage for every user.

1.4 Significance of study

This project plays an important role in the field of Cyber security, specifically in the awareness and defense of social engineering. In today's world with the advancement of technology, human mind and their vulnerabilities have been considered the most exploited aspect for the compromise of organizational digital security. The project aims to provide a platform for simulating real world scenarios and social engineering attacks as a training program for spreading awareness and training individuals for any social engineering attack that may occur in future.

The importance of the study lies in following aspects:

1.4.1 Effective security awareness

Kaezal provides a platform where employees would be exposed to real world scenarios and simulated attacks such as multiple exploitation and phishing attacks. These attacks will train and spread awareness within employees of organization, this will result in mitigating any potential threat that may occur in future.

1.4.2 Security Assessments

The toolkit provides security teams to identify potential threat and vulnerabilities within organization by taking a look into analysis and reports. This will let the organization to maintain their security by enhancing their security programs, awareness and other security policies to reduce the exposure of company's assets to a potential threat.

1.4.3 Educational and ethical simulation

This toolkit provides an ethical and secure environment to learn from social engineering attacks. This attention leads academia and educational institutes to utilize this tool for educational purposes, and for developing new security policies without exposing any sensitive information.

1.5 Goals and Objectives

This section describes the goals and objective of the framework detailing the specific outcomes it aims to achieve

1.5.1 Goals.

The major aim and goal for the development of this project is to deliver an enhanced mechanism and security framework for performing advanced social engineering attacks to simulate realistic scenarios for the assessment of organizations and firms to find potential vulnerabilities and gaps of improvement. By incorporating such frameworks organizations could enhance their security by upgrading their policies and maintain security at their best.

1.5.2 Objectives

The objectives of the framework will provide a clear overview of the tool's purpose. The main objectives involve:

1.5.2.1 simulating real attack

The objective of this framework is to provide the feature of performing real-time scenarios and attacks for assessing potential vulnerabilities and spreading awareness by providing hands-on experience to the victims about social engineering and its potential threats.

1.5.2.2 Effectiveness of security evaluation

By providing such features as provided in our framework, the effectiveness of security assessment could be enhanced to provide better evaluation of the security and the potential threats that could be imposed on the organization.

1.5.2.3 Reinforce Pentesters for better operations

One of the objectives of this framework is to provide the security professionals a robust and effective system to perform better with advanced tools and features to upgrade the performance of their assessments and operations.

1.5.2.4 Effective security training

By providing such tools an objective of providing a facility of security training and running campaigns on social engineering could be incorporated within organizations. this includes the simulation of real-world scenarios on employees and teaching them how to counter situations.

1.5.2.5 Ethical and legal requirements

The objective of this tool is to provide a system which is bound to perform with ethical and legal considerations. The frameworks must incorporate the feature of consent approval before testing.

1.6 Scope of project

This toolkit is designed to deal with the advancements in cyber attacks and social engineering threats and to provide a defense mechanism against these potential threats within organizations. The scope of the project incorporates implementation development of a toolkit that would be integrated with multiple social engineering tools that would be capable of simulating real world social engineering scenarios. These tools will provide organization to assess their security posture and identify any potential vulnerabilities.

Key features within the scope of this project include:

1.6.1 Target Audience

The target audience for this toolkit will be banks, administrations, IT industries, security professional and other agencies where the data sensitivity is a major aspect and are subjected to provide a strict security posture for the organization. The framework would also be beneficial for academia and educational institution for Cyber Security trainings and research purposes.

1.6.2 Tool integration

The toolkit integrates six major tools for performing major social engineering attacks like phishing, webcam access, phishing through links, QR code and other media elements. These tools will simulate multiple social engineering attacks in a controlled environment. Functional features

1.6.3 Scalability and flexibility

The project has the feature of being scalable, this will allow the toolkit for the addition of new tools and tactics for social engineering and OSINT features in future for advancements. The toolkit will also be able to be compatible with other platforms and integrate with other security frameworks to make its efficiency better with time.

1.6.4 Security and ethical compliance

As the toolkit is dealing with sensitive information and data, toolkit adheres to strict ethical guidelines and compliance of standards to maintain security of the sensitive data/ the toolkit

is dedicated only for training and education purposes and within a controlled environment, to avoid any misuse or misconduct of the tools.

1.7 Summary

The developed social engineering framework intends to encounter social engineering in the advancement of technologies. Social engineering is a potential threat that is being imposed in organizations and most of them get victimized. Assuming the potential gaps in the industry we have incorporated such a framework which provides advanced social engineering tools and features which intends to provide enhanced security assessments, social engineering training and awareness, a platform for professionals for better operations and for research and academic purposes. The framework has incorporated six major tools which are Phisher, Kaezal_x, URL-Mask, FindUser, QR-attack and Camphisher. The framework is versatile and robust on its own and can be integrated with other systems and provides key features like user friendly interface, ease of access and usability, scalability and robustness.

Chapter 2:

Literature Review

2 Chapter 2: Literature Review

In this chapter we would be discussing the literature review of the already existing Frameworks. We would take a look at the existing systems like BeEF, SET, Maltego Etc. We would discuss their compatibility, features and other important aspects in the realm of Cyber Security.

2.1 Introduction

In the world of Cyber Security Social Engineering has always been a critical threat to the industries and organizations along with the general public. People who are vulnerable to Social Engineering attacks are manipulated easily leading to the disclosure of critical and confidential information. Various Social Engineering frameworks and toolkits have been developed for malicious as well as awareness and educational purposes for red teaming and pentesting. This literature review will elaborate all the key aspects and features of the currently existing systems that are publicly available on some platform.

2.2 Literature review

The contemporary systems that we are going to discuss in this literature review that provide social engineering features are following:

- **BeEF**
- **SET**
- **King Phisher**
- **Metasploit**
- **Gophish**
- **Maltego**

2.2.1 Browser Exploitation Framework (BeEF)

This framework is an open-source web-based framework that leverages the vulnerabilities of Web Browser to exploit an individual on the web. This framework leverages the client side specifically to look for vulnerabilities. attackers manipulate individuals into

interacting with links that are malicious leading them towards compromise of data and system.

2.2.2 Social Engineering toolkit (SET)

This is an open-source framework used for social engineering purposes. It has various attack tactics and strategies that make a social engineering attack successful. Pentesters and ethical hackers perform some real attacks to find vulnerabilities within organizations to mitigate the risk of disclosure of any sensitive information or system exploitation.

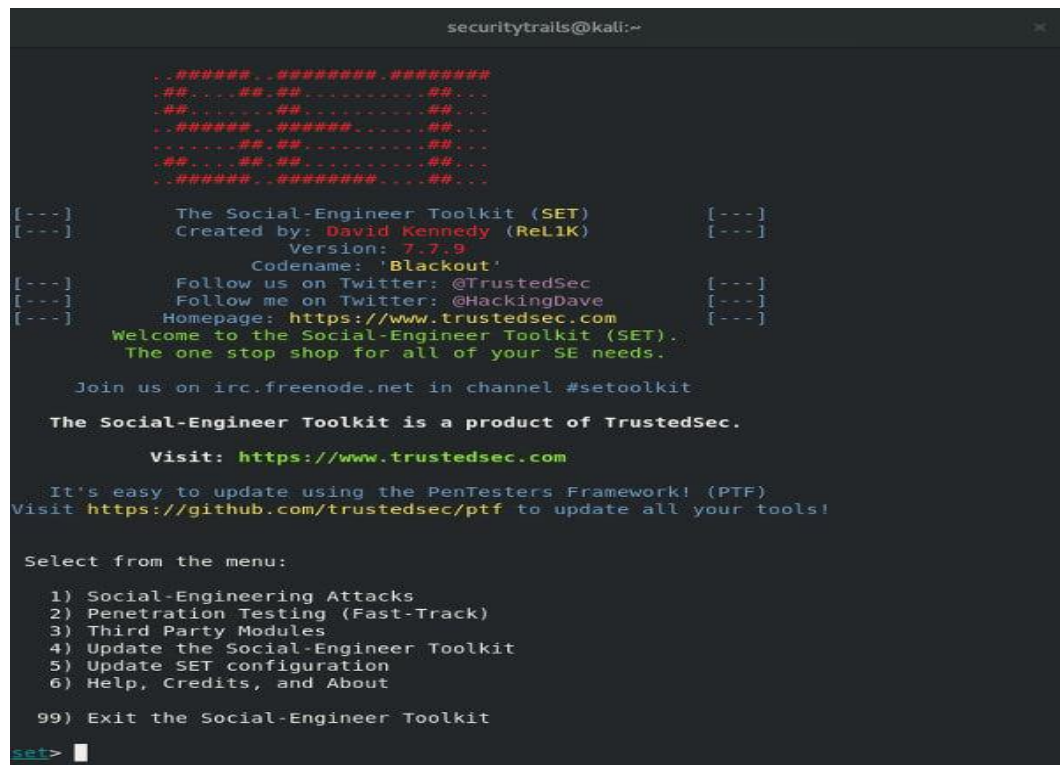
A screenshot of a terminal window titled 'securitytrails@kali:~'. The terminal displays the Social-Engineer Toolkit (SET) version 7.7.9 interface. At the top, there is a decorative ASCII art banner. Below it, the text reads: 'The Social-Engineer Toolkit (SET)', 'Created by: David Kennedy (ReL1k)', 'Version: 7.7.9', 'Codename: 'Blackout''. It then provides social media links for Twitter (@TrustedSec and @HackingDave) and a homepage URL (https://www.trustedsec.com). A welcome message follows: 'Welcome to the Social-Engineer Toolkit (SET). The one stop shop for all of your SE needs.' Below this, it says 'Join us on irc.freenode.net in channel #setoolkit' and 'The Social-Engineer Toolkit is a product of TrustedSec.' It also provides a link to visit 'https://www.trustedsec.com'. A note mentions updating using the PenTesters Framework! (PTF) with a link to 'https://github.com/trustedsec/ptf'. A menu is presented with options: '1) Social-Engineering Attacks', '2) Penetration Testing (Fast-Track)', '3) Third Party Modules', '4) Update the Social-Engineer Toolkit', '5) Update SET configuration', '6) Help, Credits, and About', and '99) Exit the Social-Engineer Toolkit'. The prompt 'set>' is visible at the bottom left.

Figure 2.1 Social Engineering Toolkit (SET)

2.2.3 king phisher

King Phisher is an open-source tool which provides the feature of performing some real-world phishing attacks to find vulnerabilities and loop holes on the systems. The tool is aimed at spreading awareness and education to eradicate the chances of social engineering exploitation. It is used mainly by the penetration testing teams to improve the security infrastructure of organizations. Key features include harvesting of credentials, phishing email generation, Reporting etc.

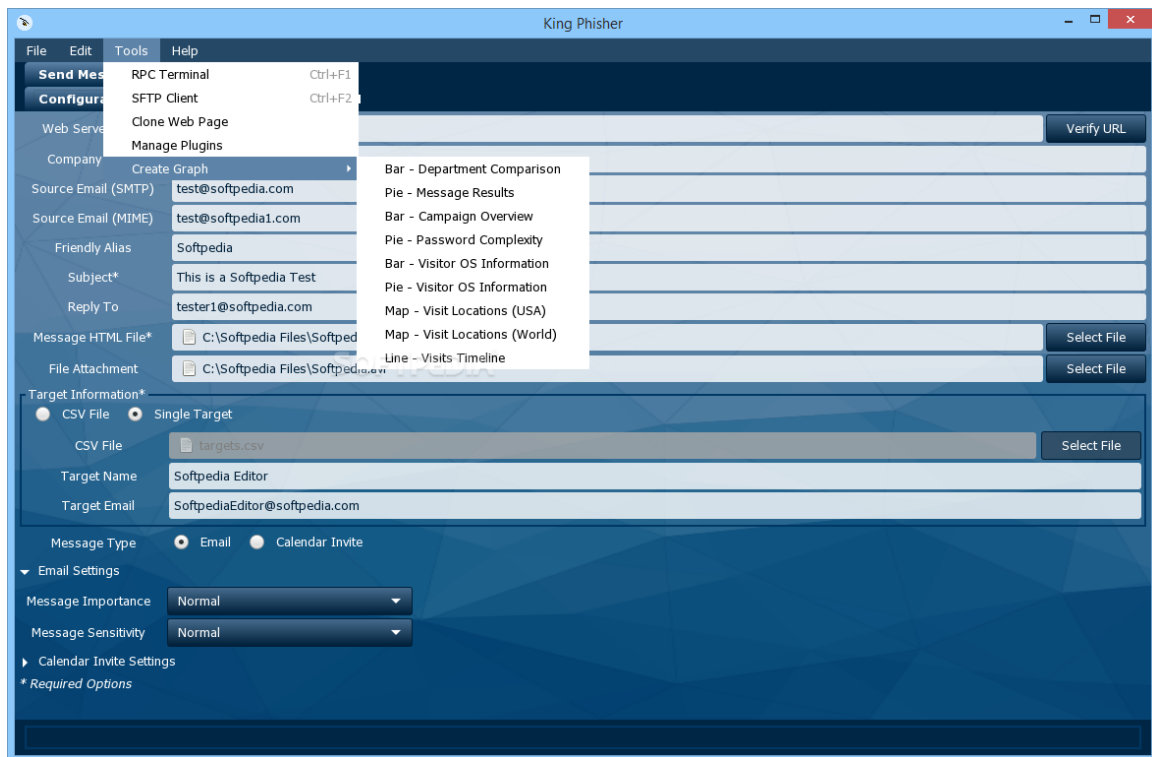


Figure 2.2 King Phisher Tool

2.2.4 Metasploit

Metasploit is an advanced and an open-Source Framework developed for the use of penetration testing. The aim of this framework is to provide the testers a comprehensive set of attacks and exploitation framework to perform real world attacks, imposing threats and finding loopholes by leveraging systems Vulnerabilities. It is widely used by pentesters to enhance the securities of organizations by implementing security assessments and exploitations to inspect vulnerabilities.

2.2.5 Gophisher

Gophisher is an open-source tool which is leveraged by Penetration Testers for managing and conducting of campaigns related to phishing and Social Engineering as an awareness and training programs amongst organizations. It provides cross-platform compatibility with a user-friendly interface to manage and organize phishing campaigns efficiently.

2.2.6 Maltego

Maltego is an open-source platform which provides the features of Open-Source intelligence and data mining for analysis of links, reconnaissance and information gathering across platforms. It provides insights on mapping entity relationships from various sources and integrates with databases to collect data from open sources.

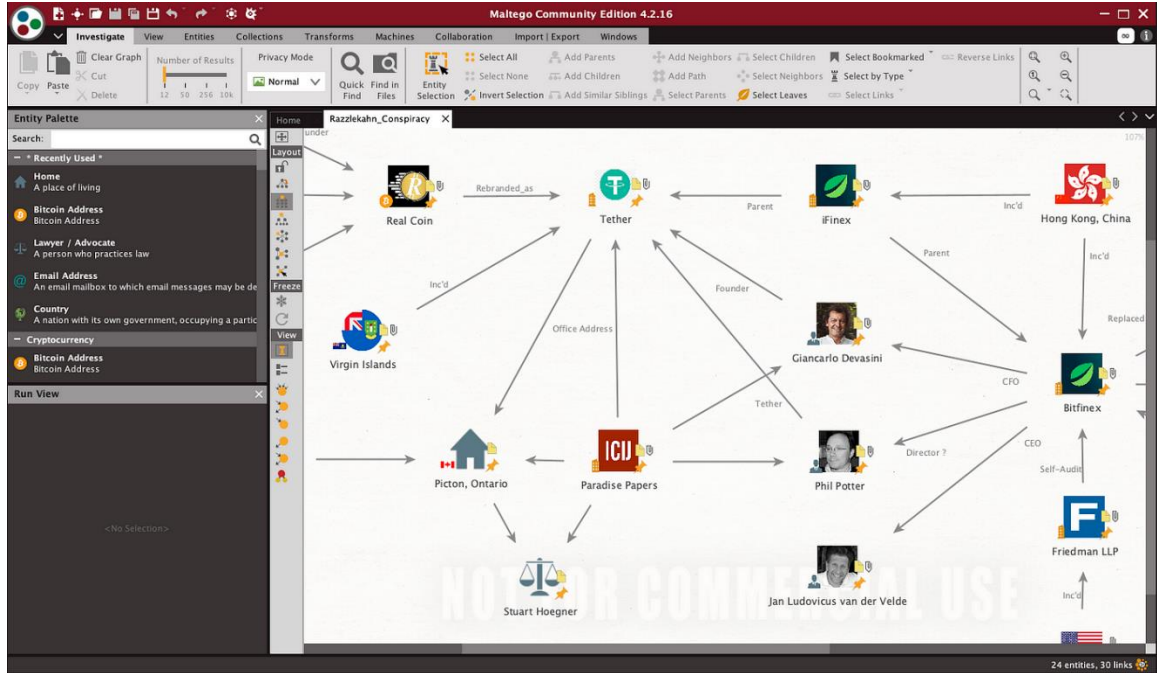


Figure 2.3 Maltego

2.3 Comparative analysis:

The following table will provide a critical comparative analysis of our toolkit against other advance and established frameworks. This analysis will examine each framework across its critical features.

Table 2.1 Comparative analysis

Framework	Technology	Feature & attacks	Compatible Platform	Usage	Scalability
BeEf	Browser based	Social Engineering attacks, Browser Exploitation	Linux	Examining User/Client-side vulnerabilities	Moderate

SET	Python-Open Source	Phishing, Web Cloning, SMS Spoofing	Linux Windows MacOS	Red Teaming, Penetration Testing, Security Training	High
KingPhisher	Python-Open Source	Campaigns, Phishing Email generation,	Linux	Performing real world phishing attacks	High
Metasploit	Ruby- Open Source	Exploitation , Payload generation,	Cross-Platform	Exploitation, Payload Creation, Post Exploitation	High
Gophish	Open Source, Cross-Platform	Phishing, Reporting, Campaigns	Linux Windows MacOS	Simulating Phishing attacks, Training, Awareness	High
Maltego	OSINT	Data Mining, Link analysis, Geospatial Mapping	Cross-Platform	Information Gathering, Data examination	High

2.4 Research gaps

The following aspects have been considered while finding research gaps against the toolkit Kaezal.

2.4.1 Lack of comprehensive and real time social engineering simulations

There exist many tools where they detect and mitigate certain vulnerabilities and find technical security loops, there is a significant gap in tools that provides real time and encompassing simulation of social engineering attacks. Lots of tools performs and offers single attack vectors for these assessments. Kaezal aims to fill this gap by providing six major tools which provide multiple attacks vectors which could simulate real world scenarios on individuals to identify potential threats and assess them.

2.4.2 Limited focus on training and awareness

While there exists tool which focuses on identifying potential threats and vulnerabilities, those tools are mainly designed to be used by professional and ethical hackers, this potentially examines the security infrastructures of course, but they lack the feature of training and awareness of non-technical users. As social engineering is usually associated with exploitation of humans by manipulating them there is critical need of such infrastructure that should educate and train individuals by performing real time simulations of attacks on them. Kaezal reduces this gap by providing these features and offers security assessment along with training for individuals on how to identify and respond to social engineering attacks

2.4.3 Scalability and customization

Many tools and frameworks lack flexibility and customization and focuses on limited features, thus limiting their effectiveness for large scale usage. As with the advancements there is a need of such framework which could be adaptable to incorporate new features and wide variety of use cases according to requirements. Kaezal provides aims to reduce this gap by providing scalability and flexibility allowing the framework for the addition of new features and tactics in future.

2.5 Problem statement

In today's digital era where technologies are getting more advance every day, organizations face a potential threat from social engineering attacks, where the intruders try to exploit the company's assets by manipulating their employees and use their sensitive information to gain unauthorized access breaching their security defenses.

There is a need of such platform where individuals could be trained against these social engineering threats, and make them identify their potential vulnerabilities which may expose company's assets and breach their security architecture.

Kaezal holds the ability to reduce this gap by providing an infrastructure that is integrated with such tools that could simulate real world scenario for social engineering attacks which will help the organizations to assess and analyze their potential vulnerabilities and threats.

The companies could train and make their policies strict against these examinations to make a more strict and resilient security infrastructure.

2.6 Summary

This literature review provides an insight on the current existing systems in the realm of Cyber Security. These frameworks utilize human psychology and human centric approach for finding vulnerabilities, finding loopholes, and gathering personal information. Leveraging these features, these frameworks provide awareness and training against social engineering attacks, providing education to incorporate defense mechanisms against intruders and attackers.

Most of these Frameworks are open source and compatible across multiple platforms, providing the organizations to utilize them for enhancing their security and organize campaigns against social engineering attacks. Nevertheless, a slight gap still exists in providing ease of access, effectiveness and new attack vectors across the network providing researchers for a gap in the industry.

Chapter 3:

Requirement engineering

3 Chapter 3: Requirement engineering

This chapter delves into the phase of requirement engineering which were applied while developing this toolkit for social engineering. The chapter focuses on the discussion of relevant problem scenarios, the functional and non-functional requirements

3.1 Introduction

This chapter will discuss the phases of requirement engineering by focusing on the problem scenarios first which lead us to gather the relevant and much needed requirements in the first place. The problem scenarios elucidate all the functional and nonfunctional requirements and all the features that should be incorporated within the framework. Then all the details which are relevant to its functional requirements are entailed which must be incorporated to fulfill the features and need for the system. Proceeding next, we will discuss the non-functional requirements which are relevant to this system like usability, scalability and other considerations. The phase of requirement engineering is as important as the development of the system itself as it depicts all the roles and responsibilities of the system and ensures that the system works as it was intended to work effectively.

3.2 Functional requirements

This section explains all the functional requirements that are considered to be necessary to develop this framework.

3.2.1 Phisher tool

- The creation of a local web server is mandatory for hosting the phishing webpage.
- The credentials and information entered by the victim must be stored or captured by the tool.
- Exposure of web server to the internet is mandatory.

3.2.2 Camphisher Tool

- The website to which the victim would be redirected must look legitimate.
- Upon redirection to the webpage, the tool must request for access to the webcam.

- It should capture the images upon access and transit them to attacker's side.

3.2.3 QR-attack tool

- Generation of QR code
- The victim must be redirecting to a phishing webpage when the code is scanned.
- The tool must capture the credentials and information upon entry.

3.2.4 URL-mask tool

- The tool must need to generate a URL that is being masked for distribution
- the link should be redirecting the user to the correct webpage that is intended.

3.2.5 FindUser tool

- The intended information must be collected about the required IP address.
- The tool should fetch data from the databases and OSINT tools.
- Present data in a user-friendly way to understand it easily.

3.2.6 Kaezal_X tool:

- The tool must be able to embed a backdoor into different kind of media file like pdf, jpg, png etc without altering appearance of the file.
- When the target opens the file, the backdoor must trigger and grant system access.
- Must operate in stealth mode to avoid user detection.

3.3 Non-Functional Requirements

This section briefs the non-functional requirements of the framework.

3.3.1 Performance

- The tools should have a good response time for every action.
- The tools should be able to manage multiple requests and users without performance decline.
- The toolkit should be able to accommodate further tools and features in future ensuring scalability.

3.3.2 Usability

- The toolkit should incorporate a friendly GUI user interface.
- The Complexity should be lessened as compared to conventional command line interfaces which need technical expertise.
- The tool should provide user manual and documentation for help and understanding of the framework.

3.3.3 Reliability

- The tool should be available to legitimate users and provide maximum uptime without delay.
- The tool should handle errors effectively and should provide error messages upon occurrence.

3.3.4 Security

- The collected data like credentials and other sensitive information should be well managed and provide a secure mechanism without losing it or getting compromised to illegitimate users.
- The tool should contain logs and timestamps for audit and accountability.
- The access should be role based so everyone could not interact with sensitive information.

3.3.5 Compatibility

- The tool should be compatible with every major platform and operating system like Linux systems, macOS and windows etc.

3.4 Design diagrams

This section will illustrate diagrams and use cases which will demonstrate operation and usage of the framework.

3.4.1 Data flow diagram

The data flow diagram of the toolkit will illustrate the process of interaction among two entities. The DFD will represent how the data flow from one setup towards other entity for simulation of an attack resulting in harvesting credentials or an unauthorized access.

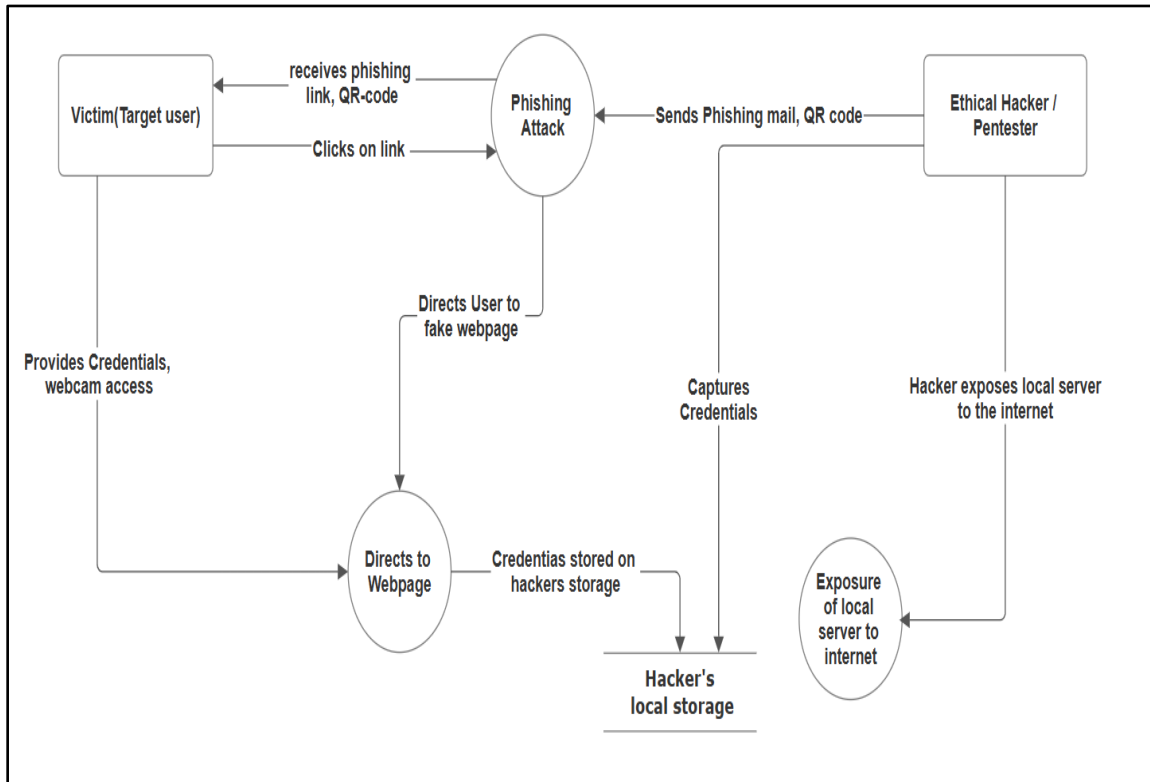


Figure 3.1 Data Flow Diagram

3.4.2 Use Case diagram

The use case diagram of this framework provides an overview of interaction between two main entities of this framework. A hacker/ Pentester simulates social engineering attacks while the victim interacts by clicking the link and providing access gain or credentials. The use case diagram has been illustrated below.

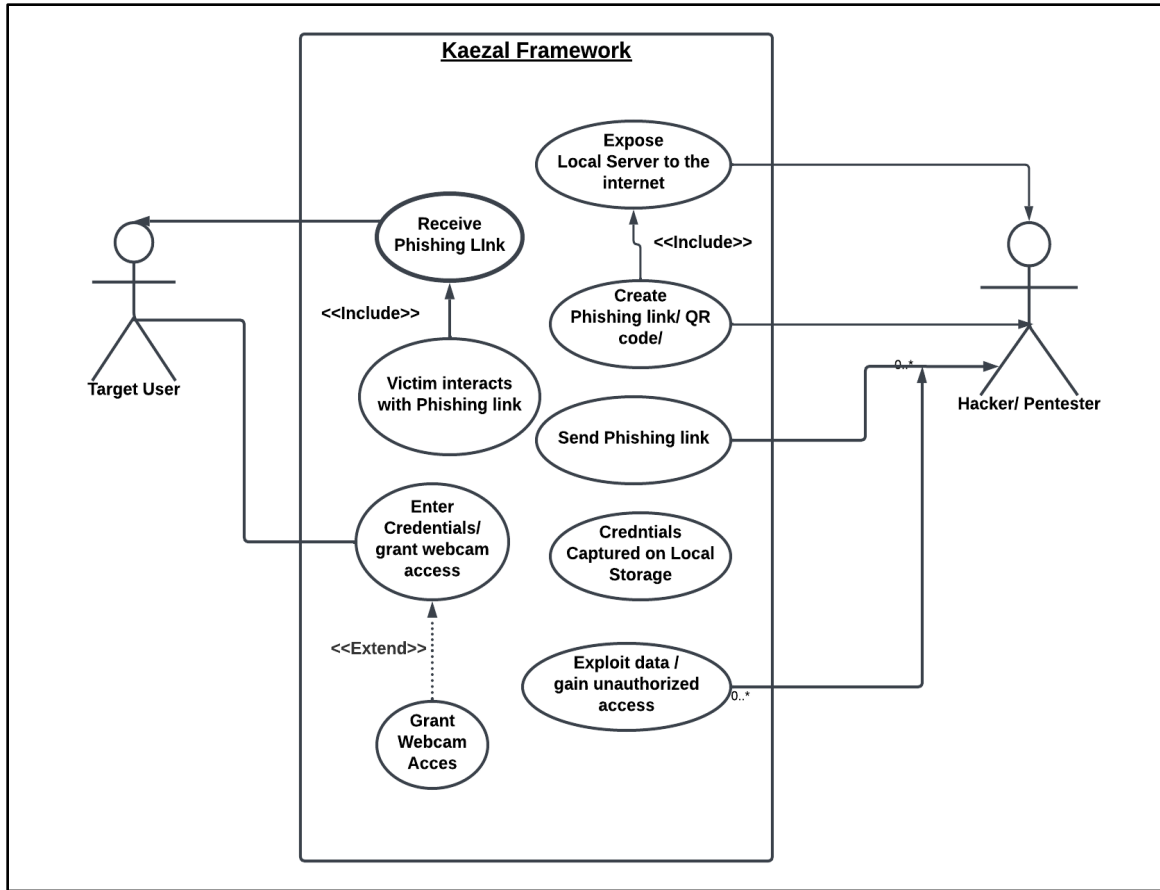


Figure 3.2 Use Case diagram Kaezal

3.5 Hardware and Software requirements

Following hardware and software requirements should be met to deploy the framework on any other system for smooth operation and efficient deployment.

3.5.1 Hardware requirements

3.5.1.1 Processor

A multi core processor, preferably intel i5 or equivalent to run the execution smoothly.

3.5.1.2 Memory

A minimum of 4 GB RAM should be required to operate the toolkit.

3.5.1.3 Storage

To install the toolkit, a minimum of 10 GB free disk space should be sufficient for installation of files, logs and other needs.

3.5.1.4 Network Interface

To ensure successful simulation of attacks, an ethernet or WIFI must be incorporated for internet access.

3.5.2 Software requirements

3.5.2.1 Operating system

The framework is compatible with Linux distributions such as Ubuntu, Kali or any other Linux distributary which supports the execution of security and network tools.

3.5.2.2 Python runtime environment

Python 3.0x should be pre-installed, as the framework's script could not run as they are built on python.

3.5.2.3 Tunneling Services

Services like Ngrok, Cloudflared or Serveo should be required to expose the local servers to the internet.

3.5.2.4 Webserver Software

Nginx or Apache should be required for hosting certain tools locally or remotely.

3.6 Threat scenarios

This section outlines the threat scenarios that our tool is capable of performing and organizations encounter them on daily basis with the advancement of technology.

3.6.1 Scenario 1: widespread of Phishing attacks

Organizations are frequently getting attacked these days by phishing attacks and employees get victimized by revealing sensitive information which involves PII, financial secrecy, confidential information etc. These victims fall for these attacks and get victimized even

though there are multiple security measures being put in place. The advent of such tools that would perform such realistic attacks and spread awareness could and educate them by giving them hands-on experience and training can enhance the organization's security measures.

3.6.2 Scenario 2: Exploitation through QR-code

With the advancement of technology, the security concerns are also getting critical every day. The use of QR codes nowadays for multiple purposes is being leveraged by the attackers. People scan QR codes everywhere at restaurants, at events and payments also. The attackers use these legitimate look-a-like QR codes to redirect the victim towards fake websites or web pages where the victim falls for his prey and shares sensitive information like credentials and compromises confidential data. Organizations need such a tool which incorporates such advanced social engineering tactics to educate their employees.

3.6.3 Scenario 3: URL-masking

The URL masking techniques are being leveraged by the attackers to create legitimate look alike links to manipulate individuals to click on them. These QR-codes most often lead to credential theft and in some cases malware injection or embedded payloads are often integrated into these codes which makes the threats more catastrophic. A need for a tool is there which depicts real time scenarios where a URL masking leads to such threats and educates the individuals.

3.7 Threat modeling Techniques

For this framework the STRIDE threat modeling technique is accurate and could be mapped with this framework for identifying potential threats to help incorporating defense mechanisms. The STRIDE model aligns accurately with such social engineering threats for which this framework has been developed. Mapping the STRIDE model with this framework can help to identify how each element of STRIDE aligns with the specific threats that Kaezal encounters.

The following table maps each element of STRIDE model with Kaezal framework

Table 3.1 STRIDE model for threat modeling

STRIDE category	Threat scenario	Kaezal Tool	Description
Spoofing	Phishing attacks	Phisher, QR-Code attack, URL mask, Camphisher	These tools simulate emails from spoofed identities, for educating and training individuals against Spoofing
Tampering	Altered QR-codes or URL containing malwares or payloads	QR-Attack, URL mask	Allows user to identify tampered URLs, QR-Code and malwares, helping them to identify and avoid such content in future.
Repudiation	Attackers deny unauthorized access	Phisher	Helping user to understand how audit trails could encounter repudiation
Information Disclosure	Phishing attacks, QR code attacks that may manipulate users to share sensitive information	Phisher, Camphisher, Backdoor injection, FindUser	Simulates such scenarios where users may potentially get exposed to sensitive information disclosure
Denial of Service (DoS)	Email flooding through phishing attacks	Phisher (for flooding emails)	Trains user to identify and report such emails to ensure availability of system
Elevation of Privilege	Social engineering attacks that may deceive users into providing unauthorized access	Phisher, QR-code attack	Educates individuals to stay aware about such attacks, which allows granting unauthorized access to the attacker

3.8 Threat Resistance Model

The best fit model that is compatible and is suitable for Kaezal's goal of simulation of real time attacks against social engineering attacks. This model comprises of multiple, overlapping layers of defense that aims to stop, detect and respond to potential threats. In the scenario of this toolkit this model may include.

3.8.1 Awareness Training

The primary layer, that aims to provide social engineering trainings to individuals about social engineering attacks so they could response to them in a careful way in future.

3.8.2 Simulated attacks

The attack simulation of this toolkit provides real-time scenarios to provide user awareness against social engineering attacks.

3.8.3 Access control

To prevent compromises multi factor authentication and strict user permission should be implemented incorporating a strict access control mechanism.

3.8.4 Monitoring and logging

Tracking and logging the login attempts and malicious links and other elements may prevent any potential harm if system is ever compromised.

3.9 Summary

This chapter provides a clear understanding on the development of this project, proceeding with discussion of functional and non-functional requirements that would be the foundation for the success of this project. The chapter begins with describing the problem scenarios to highlight the need for such a framework. Such scenarios focus our attention on developing such tools with simulation of best practices and assessment of social engineering. Proceeding further, the chapter entails the functional requirements that must should be incorporated for the effective and efficient development of such a framework. The non-functional requirements elucidate the necessary requirements that should be incorporated

for the efficiency of the system involving security, usability, scalability and performance etc. By detailing all these requirements, the chapter sets a fundamental ground for the development of the project.

Chapter 4:

Proposed Solution

4 Proposed solution

This chapter aims to provide the proposed solution for enhancing social engineering awareness and trainings and providing security assessments within organizations through this framework. The chapter will provide inn depth analysis of design approach, data preprocessing methods, data collection methods. Furthermore, the chapter will explain the tools and techniques that are incorporated within this framework for performing simulations of multiple attack vectors.

4.1 Introduction

Social engineering attacks critically exploits organizations assets and sensitive data by exploiting human behaviors. The presence of highly effective security measures still couldn't resist the potential harms that are caused by manipulating human minds which has been proven a critical vulnerability in the realm of cyber security, especially social engineering. The Kaezal framework reduces this potential vulnerability by providing awareness and training through real time simulation of social engineering attacks. The framework aims to provide the organizations to analyze and assess their security posture and train their employees to adapt such technical knowledge which could help them recognize and help them resist such threats in future.

4.2 Proposed model

Kaezal framework is developed with a qualitative, experimental approach which aims to provide a real time simulation of common attack vectors of social engineering. This approach will help the individuals within organizations to understand attack vectors and its nature by getting expose to them in a controlled environment. By integrating some of the major and common social engineering tactics in the tools of this framework, the framework will provide a highly effective insights in assessing the potential threats and vulnerabilities in organization.

The project provides hands on training of employees with the capability of collecting insights and assessing security posture of organization through real time simulation of

social engineering attack vectors. These features provide a comprehensive training experience which will result in the betterment of organization's security infrastructure.

4.3 Data Collection methods

Data collection in this toolkit will be achieved by several sources:

4.3.1 User interactions

After simulation of real time attacks the responses of user interaction will be collected, helping the organization to assess the security future and identify potential threats. These interactions will be recorded to analyze behavioral patterns and identify the potential loop holes and knowledge gaps that could be used later to imply strict security policies.

4.3.2 Network logs

Within these simulation exercise network logs will be monitored to map behavioral patterns later to analyze the potential vulnerabilities leading to follow such attempts.

4.3.3 Survey Responses

Before and after training surveys will be conducted on user literacy, technical knowledge and effectiveness of training infrastructure and the improvements that are achieved in adapting and understanding knowledge of social engineering.

4.3.4 Threat intelligence reports

Prior reported incidents and threat intelligence reports within organizations and other industries could help provide accurate data to assess and refine the attack vectors and such simulations in future for this framework.

4.4 Data pre-processing

The following data pre-processing methodologies will help to enhance the effectiveness and accuracy of the system's functionality.

4.4.1 Outlier removal

While performing simulations it is necessary that the responses collected are accurate and accidental responses or unintended actions does not influence the effectiveness of the framework. For instance, an individual accidentally clicks a malicious link without interacting with the content or without giving any credentials upon demand, these actions may affect the analysis. Such anomalies need removal to make the insights of collecting responses more accurately.

4.4.2 Classification

Classification of user responses to a certain simulation and user response to it is a critical way of preprocessing the data. This analysis classifies the user's interaction to a specific simulation allowing the framework to saturate behaviors according to attack types. By classifying areas in such way, the framework could incorporate customization in such areas to address particular vulnerabilities and loop holes.

4.4.3 filtering

During the social engineering exercises, lots of data is generated including systems log and irrelevant network traffic. Filtering such irrelevant data which does not pertain to these exercises and creates disruption in analysis could help for an accurate analysis of collected data.

4.4.4 Prioritization

During these simulation exercises, it is critical to record frequently occurring interactions to prioritize the risk levels. By highlighting levels of risk, the framework could provide insights to help organizations to incorporate additional trainings and mitigate risk factors by strengthening their policies and security posture.

4.5 Evaluation matrices

There are several evaluation matrices that highlights the effectiveness and accuracy of the framework's usability and efficiency. These matrices include:

4.5.1 Engagement and interaction rate

This metric of evaluation will highlight the rate of user interaction through click rates and overall engagement with the threat scenarios. A high rate of engagement will show ability of simulations to capture user responses and providing effective learning. A low rate will typically indicate a need of betterment to the solution and enhancing the frameworks to make the simulations more relevant.

4.5.2 Realism and Robustness

The realism of the attack vectors will highlight how effective and accurately the simulations has been replicated according to real world social engineering attacks. The better replication of such scenarios to the real-world scenarios will lead the individual to be prepared for actual attacks in real time. Feedback of users and cyber security experts could evaluate the realism of these scenarios and attack vectors.

4.5.3 Error analysis and adaptation rate

This matric hunt the common errors and responses to a specific simulation that occurs more frequently. For instance, if a user frequently falls for a specific type of attack vector, the framework could be customized for a more behavior centric approach to incorporate more effective training in such areas to make the training more relevant and enhance the effectiveness of the framework.

4.5.4 Improvement in awareness

This matric evaluates the user literacy and efficiency of simulations by collecting pre and post qualitative survey. By analyzing these insights, the framework could incorporate more refine and effective shifts in the knowledge areas to adapt and continuously improve the training environment for users.

4.6 Summary

The proposed solution, this framework provides a realistic approach to identify and assess potential vulnerabilities and understand social engineering attacks. The framework aims to provide multiple tools for performing social engineering attack simulations in an ethical

and controlled manner, offering the organizations to assess their security posture and secure their sensitive information and assets through realistic trainings and analysis of potential vulnerabilities. Through effective data collection methods, pre processing and usage of advance tools and techniques, this framework illustrates its usability and significance in raising awareness and strengthening organizational security infrastructures.

Chapter 5:

Implementation

5 Chapter 5: Implementation

In the phase of Implementation of the KAEZAL Social Engineering Toolkit, the phase went through a structured and mutual way of fulfillment to ensure the effectiveness of all social engineering attacks and techniques. The toolkit's aim to provide a useful information and perception into discovered vulnerabilities that a social engineering technique may exploit providing a platform to analyze these insights in an ethical way. All the phases from development, deployment and reporting of this toolkit required strict dedication and implementation of technical skills for coding and deployment and management skills as well for other resources and project management.

In this phase we will elaborate the testing methodologies carried out to test the effectiveness of the framework, other methodologies acquired and all the strategies and processes that were used for the accomplishment of this Toolkit.

5.1 Security property testing

The kaezal framework went through several security measure to ensure it cover all essential security standards and protocols. Key security features include:

5.1.1 Confidentiality

To ensure the confidentiality of the sensitive data achieved upon interaction of the user during social engineering exercise. The information saves into hacker's machine in its local storage and to provide confidentiality the machine has utilized BitLocker Encryption. By encrypting, the BitLocker saves the data and protects it from the use of any unauthorized person. Even the storage device, if removed externally, the data will remain inaccessible to any outer source. This encryption will provide confidentiality to the sensitive data collected while simulating these attacks.

5.1.2 Integrity

Integrity tests will identify that the received data remains accurate and unaltered during performance of a social engineering attack and later. This test ensures that collected data and information remains in its actual state and remain unaltered.

5.1.3 Availability

The availability test ensures that the system remains available under different loads and multiple simulations. This test may include bombing victim with lots of mails or the simulation of attacks on multiple users at same time to ensure that the system remains responsive and prevents lagging and delays.

5.1.4 Realism of simulations

The objective of the toolkit is to provide the simulation of social engineering attacks in a controlled and ethical environment ensuring that the simulations are relevant and realistic, resulting in simulations of real time scenarios and mimicking actual social engineering attacks. Realism tests ensures that the tool is able to mimic such scenarios effectively, enhancing the effectiveness of the trainings.

5.2 System setup

This section describes the configuration specifications for the environment of the framework and essential functions.

5.2.1 Environment configuration

The environment configuration will elaborate the hardware and software and other necessary requirements needed for the configuration of this framework.

5.2.1.1 Operating System

Kaezal is optimized for Linux distributions such as Ubuntu, Kali, Parrot and other platforms which incorporates security tools. The framework could also be deployed on macOS and windows with some changes in future.

5.2.1.2 Python

Python 3.0 or newer should be installed on system to integrate the framework, as the scripts of this framework are written in python using libraries for automation, network operation etc.

5.2.1.3 Tunneling Services

Services like Ngrok, Cloudflared or Serveo should be required to expose the local servers to the internet.

5.2.1.4 Webserver Software

Nginx or Apache should be required for hosting certain tools locally or remotely.

5.2.1.5 Processor

A multi core processor, preferably intel i5 or equivalent to run the execution smoothly.

5.2.1.6 Memory

A minimum of 4 GB RAM should be required to operate the toolkit.

5.2.1.7 Storage

To install the toolkit, a minimum of 10 GB free disk space should be sufficient for installation of files, logs and other needs.

5.2.1.8 Network Interface

To ensure successful simulation of attacks, an ethernet or WIFI must be incorporated for internet access.

5.3 System Integration

This section describe how different tools and components are integrated within the framework, the APIs used and database management strategies utilized for development of this framework.

5.3.1 Components integration

Kaezal integrates various tools incorporating real world simulation of social engineering attacks on individuals in a controlled and an ethical manner. The different tools that are, Phisher, Camphish, QR code attack, FindUser, Kaezal_x, and URL mask, all these tools have been integrated in this framework in a unified structure. All these tools are centrally managed.

5.3.2 API integration

In kaezal's FindUser tool an API from a reputable lookup website has been used. This API helps the tool to retrieve the geolocation of any given IP address providing information like City, region and country or state details which could help the user to assess the data. This tool is specifically used to incorporate OSINT feature into our system. This geographical information adds valuable insights in collecting data of a target for social engineering purposes.

5.3.3 Log management and storage setup

Kaezal incorporates the hacker machine's local storage for dealing with the logs and any data collected during the simulations. The local storage has been encrypted by a BitLocker to ensure the security of the sensitive data stored on storage.

5.4 Test cases

This section details the test cases used to validate the systems functionality, security, usability and performance. These test cases follow a standard format.

5.4.1 Functionality test case

Test case ID: TC-F01

Objective: generation of realistic phishing emails intended to attack victim

Pre-conditions: The tool must be integrated and should be in operational state.

Test course:

1. Initiate the Kaezal framework.
2. Open the phisher tool.
3. Expose the local server to the internet using a web service.
4. Provide victim's email address for the simulation of attack.
5. Chose a sample fake webpage for the phishing email.
6. Send the Email.
7. Collect responses upon interaction.

Test case ID: TC-F02

Objective: to verify whether the phishing attempt grant access to webcam upon victim's approval.

Pre-conditions: The tool must be integrated and should be in operational state.

Test course:

1. Initiate the Kaezal framework.
2. Open the camphish tool.
3. Expose the local server to the internet using a web service.
4. Provide victim's email address for the simulation of attack.
5. Chose a sample fake webpage against the fake link.
6. Send the Email.
7. Collect responses upon granting access of webcam.

5.4.2 Usability test case

Test case ID: TC-U01

Objective: to check the usability and ease of access of the tool for administrator usage.

Pre-conditions: framework is operational and admin has logged in.

Test course:

1. Initiate the Kaezal framework.
2. Navigate through different sections of the framework.
3. Ensure each section provides clear instructions and are labeled correctly.

Expected result: the user interface should be clear and easily understandable and causing no error while navigating anywhere into framework.

5.5 Results and discussions

In this section we will present the result of the framework and discuss upon them in the aspect of Performance and usability tests that has been done. The tests aim to assess the overall efficiency of the system in simulating real time social engineering attacks ensuring user friendly interface.

5.5.1 Functionality tests

This section will elaborate the results and discussion on the performance tests carried out in testing phase.

5.5.1.1 Phishing simulation tool (Phisher)

Results: This attack simulated a real time social engineering attack by generating a fake email which seemed to be legitimate. The web pages were that were linked with the URLs were looking real to manipulate victims mind into putting their credentials.

Discussion: the features of this tool were critical in terms of creating real world scenarios for social engineering attacks. The tool has been effective in identifying the risks that an individual may encounter while receiving a mail.

5.5.1.2 Camera Phishing tool (Camphish)

Results: the camphish tool has been simulated accurately which manipulated the target victim in granting access to the web cam to capture their live movements and monitor them which is the primary objective of this social engineering attack.

Discussions: the tool has executed its functionality with accuracy. However, to make it more effective capturing live video of the webcam instead of capturing screen shots of the victim's actions after intervals would play a significant role in enhancing functionalities of this tool.

5.5.2 Usability test

This section will describe the results and discussion on the Usability tests carried out in testing phase.

5.5.2.1 User Interface (UI)

Results: the result indicate that the interface of this framework was fine and easily accessible. Each component of the interface in every section was clearly labeled, and navigation was easy. The user could easily simulate and perform any action on the tool without any complication.

Discussion: the test carried out illustrates the user interface to be friend and easily accessible to an individual having varying level of technical expertise. However, adding a demonstration of the usage to the framework's user manual could help in assisting further.

5.6 Development Practices and Standards:

To ensure and adapt best industry practices and maintaining industry standards each and every aspect of the project were kept highly maintained using proper coding standards and following all ethical considerations and guidelines. Following standards were met during the project development phases.

5.6.1 Coding Standards:

While developing the webpages and writing scripts for phishing and different techniques proper coding style and standards were followed throughout the project. Indentations, comments and all documentation were maintained properly at each step.

5.6.2 Security Practices:

Data Encryption and obfuscation was a challenging and must for the following tasks to ensure security and obfuscation of gathered confidential and sensitive data of the victim.

5.6.3 Version control:

Github was used to maintain and manage version which allowed us to maintain and keep record of changes and cohesion between members and supervisor.

5.6.4 Testing:

To identify any fault or issue unit tests were carried out throughout the development and its effectiveness and functionality were ensured to be carried out perfectly.

5.6.5 Ethical Standards:

This tool strictly adheres to ethical standards and is intended to use only for educational purposes and simulated environments to perform best ethical practice in industry.

5.7 Summary:

The success of this project is achieved through maintaining strict discipline during implementation of all the phases and ensuring mutual cohesion between members and supervisor. The members used agile practices and structured approach utilizing their expertise at their best where required. The implementation of this toolkit required effective technical skills and managerial skills to achieve its accomplishment. This toolkit is simulated in a Linux environment by leveraging Python, PHP, JavaScript and some web-based technologies to develop and perform multiple social engineering attacks efficiently. The tool integrated features like phishing, QR code attacks, backdoor generation and geolocation finding. This tool ensures the best practices to perform and identify potential social engineering threats. The tool ensures best ethical considerations to ensure its adaptability among cyber security industries and to be used for educational purposes.

Chapter 6:

Conclusion and Outlook

6 Conclusion and Outlook

6.1 Introduction

This chapter concludes and summarizes the development procedure and implementation strategies and over all accomplishment of this project. Furthermore, the chapter will discuss the key achievements, major contributions and any areas of improvement that needs to be considered. The chapter will also ponder upon the critical aspect of the project as well as providing future suggestions and recommendation for its enhancement. This chapter aims to provide an overall conclusion for the performance of this project and its part and significance that will enhance the future of cyber security learning and trainings in the industry and educational institutions providing an effective social engineering awareness.

6.2 Achievements and Improvements

This project has successfully developed and accomplished its main objectives of developing a social engineering toolkit. Some of the significant achievement of this project comprises:

6.2.1 Effective social engineering tools

The main objective of this toolkit was to develop such a robust platform which will perform social engineering attacks. This tool has successfully accomplished six major tools which cover social engineering tactics using phishing and other techniques like URL masking and backdoor generation. Furthermore, the toolkit also provides information using IP addresses to find geolocation. These tools provide a robust platform for the simulation of real word social engineering scenarios for educational and awareness purposes.

6.2.2 Educational applicability

The initial focus of this toolkit was to spread awareness and training of individuals by leveraging real world social engineering scenarios. This will enhance the capabilities of organization and enhance its security matters. The toolkit provides an effective platform

for this purpose by simulating real world social engineering scenarios in a controlled and ethical way.

6.2.3 Scalability and Flexibility

The toolkit was designed for enhancing its functionality and features providing scalability and flexibility in future. This allows the toolkit to add more features and set of tools to encounter challenges and evolving potential threats with the advancement of tech industry.

6.2.4 Ethical considerations

The project was intended to provide a toolkit which could be used legitimately and this toolkit has followed all ethical standards to ensure the ethical and legitimate use of this toolkit for educational and awareness purposes.

6.3 Critical review

While considering its key features and achievements that provides robustness of this system, this toolkit also has some areas that needs to be further worked upon to achieve further improvement.

6.3.1 Realism and Evasion

While the toolkit provides the best approach for simulating real world scenarios, some advanced techniques and evasion threats may have been missed out. For example, these days phishing techniques are getting more sophisticated, artificial intelligence has been a major challenge which leverages deep fake technologies to manipulate individuals.

6.3.2 Security Concerns

While this toolkit possesses strict security measures still the security concern is a major challenge for this toolkit itself because of its sensitive nature. The toolkit aims to collect and capture sensitive information of individuals which needs to be protected at all cost. The tool already has been well maintained and security features are up to the mark, but there remains a need of more sophisticated and advance access controls and audit logs for best accountability.

6.3.3 Compatibility issues

As of now the toolkit is compatible only for Linux, but there are other major platforms like macOS, windows and cloud-based environment for which its optimization is needed to ensure smoother functionality across multiple platforms.

6.4 Future recommendations and outlook

In future the toolkit may focus in developing in such areas which include:

6.4.1 Advanced evasion techniques

In future as the technology and the internet crime advances the toolkit should evolve itself with new tactics that incorporates advance phishing techniques and also consider AI as a potential threat for phishing attempts and provides more obfuscated phishing URL and web page designs should be more realistic and advance.

6.4.2 Integration of Artificial Intelligence

The toolkit should be added with more advance features incorporating AI and Machine learning algorithms to identify specific behaviors and creates user-based scenarios and simulate zero-day attacks for a suspected victim.

6.4.3 Enhanced reporting and analysis

The toolkit should provide an effective report and analysis upon simulation of any attempt on victim and should collect data for insights that could offer organizations to improve their security awareness and bring more advancement and training programs for individuals.

6.5 Summary

The Kaezal Social engineering toolkit attains a significant value in the field of Cyber Security and its education across platforms. The simulation of real-world social engineering attacks, organization could leverage to educate and make their employees aware and train for any potential threat and dangers of social engineering attacks which are critical and more common these days. While this tool has achieved its initial objective of

providing a social engineering tools, areas such as compatibility, security and other concerns needs improvement and more refinement. Furthermore, integration of artificial intelligence features and cloud compatibility and reporting of threats could improve this toolkit for the future and will make it relevant for upcoming challenges. This toolkit holds a potential to become a major resource against battling social engineering attacks in future.

7 References

- I. Sabih, Z. (n.d.). Learn Social Engineering from scratch. O'Reilly Online Learning. <https://www.oreilly.com/library/view/learn-social-engineering/9781789341584/>
- II. (PDF) Social Engineering Attack Framework. (n.d.). https://www.researchgate.net/publication/263588935_Social_Engineering_Attack_Framework
- III. Auditing Social Engineering: A practical approach. ISACA. (n.d.). <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/auditing-social-engineering-a-practical-approach>
- IV. Borges, E. (n.d.). Securitytrails | The Social Engineering Toolkit (SET) - securitytrails. www.securitytrails.com. <https://securitytrails.com/blog/the-social-engineering-toolkit>
- V. Dixit, R. (2023, June 21). Social Engineering Tools. Medium. <https://medium.com/@dixitra20/social-engineering-tools-427ce3787f97>
- VI. Ignitetch *Ignitetch/advphishing: This is advance phishing tool ! OTP phishing, GitHub*. Available at: <https://github.com/Ignitetch/AdvPhishing> (Accessed: 15 November 2024).
- VII. *Diagramming powered by intelligence* (no date) *Lucidchart*. Available at: https://www.lucidchart.com/pages/landing?utm_source=google (Accessed: 15 November 2024).
- VIII. <https://github.com/1RaY-1>
- IX. <https://github.com/adi1090x>

- X. <https://github.com/AliMilani>
- XI. <https://github.com/Ignitetch/AdvPhishing>
- XII. <https://github.com/MoisesTapia>
- XIII. <https://github.com/E343IO>
- XIV. <https://github.com/bdhackers009>
- XV. https://twitter.com/linux_choice