CASE STUDY: SOCIAL ENGINEERING ATTACK
A REPORT

Submitted by

SHRISTY SINGH(RA2111030010140)

Under the Guidance of

Dr. Deepika D
Assistant Professor

DEPARTMENT OF NETWORKING AND COMMUNICATIONS

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE ENGINEERING
with specialization in Cyber Security

SCHOOL OF COMPUTING
COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR - 603203

MAY 2024

DEPARTMENT OF NETWORKING AND COMMUNICATIONS
SCHOOL OF COMPUTING
College of Engineering and Technology
SRM Institute of Science and Technology

CASE STUDY ON "SOCIAL ENGINEERING ATTACK"

EVEN Semester (2023-2024)

Course Code & Course Name: 18CSE386T – Penetration Testing and Vulnerability Assessment

Year & Semester : III/VI

Report Title : Ethical hacking using penetration testing tools

Course Faculty **:** Dr. Deepika D

Student Name : (RA2111030010140) SHRISTY SINGH

Evaluation:

S.No	Parameter	Marks
1	Problem Investigation & Methodology Used	/5
2	Tool used for investigation	/5
3	Demo of investigation	/5
4	Uploaded in GitHub?	/5
5	Viva	/5
6	Report	/5
	Total	**/30**

Date :

Staff Name :

Signature :

CASE STUDY ON **“SOCIAL ENGINEERING ATTACK”**

INTRODUCTION:

In the dynamic landscape of cybersecurity, where technology fortifies defenses and adversaries continuously innovate their attack vectors, social engineering remains a potent and persistent threat.

Social engineering, a psychological manipulation technique, exploits human instincts and tendencies to bypass technical safeguards, gaining unauthorized access to sensitive information, systems, or physical spaces. The objective of this is to analyze the effectiveness of social engineering attacks within the context of penetration testing, elucidating vulnerabilities, and proposing remedial measures to fortify organizational security posture.

SCOPE:

1.Human Element: Social engineering attacks primarily target the human element within an organization, exploiting psychological vulnerabilities rather than technical weaknesses.

2.Multifaceted Techniques: Social engineering encompasses a wide array of techniques, including phishing, pretexting, baiting, tailgating, and spear-phishing, each leveraging different aspects of human behavior and interaction.

3.Cross-Platform Vulnerabilities: Social engineering attacks can target various communication channels, including email, phone calls, social media, and in-person interactions, highlighting the need for a multi-dimensional defense strategy.

4.Impact Beyond Technology: While social engineering attacks often lead to unauthorized access to systems or data, they can also result in financial loss, reputational damage, regulatory non-compliance, and compromise of physical security.

OBJECTIVE:

1.Information Gathering: Social engineering attacks often involve reconnaissance activities to gather information about targeted individuals, organizations, or systems, enabling attackers to craft convincing pretexts and tailor their tactics accordingly.

2.Exploitation of Trust: By exploiting human trust and authority dynamics, social engineering attacks aim to establish rapport with targeted individuals, thereby increasing the likelihood of compliance with malicious requests or actions.

3.Evasion of Technical Controls: Social engineering attacks seek to circumvent technical security controls, such as firewalls, intrusion detection systems, and encryption, by targeting the weakest link in the security chain—the human element.

4.Psychological Manipulation: Social engineering attacks leverage psychological manipulation techniques, such as fear, urgency, curiosity, and social compliance, to elicit desired behaviors from targeted individuals, often without their awareness.

5.Payload Delivery: In addition to obtaining sensitive information or access credentials, social engineering attacks may also involve the delivery of malware, ransomware, or other malicious payloads to compromise systems or facilitate further exploitation.

6.Persistence and Adaptation: Social engineering attackers are adept at adapting their tactics and techniques to circumvent evolving security measures, making it imperative for organizations to remain vigilant and continually update their defense strategies.

TOOL USED AND APPLICATION TO PERFORM:

Social engineering toolkit is a free and open-source tool which is used for social engineering attacks like phishing, sending SMS, faking phone, etc. It is a free tool that comes with Kali Linux, or we can download and install it directly from Github. The Social Engineering Toolkit is designed and developed by a programmer named Dave Kennedy. Security researchers and penetration testers use this tool to check cybersecurity issues in systems all over the world. The goal of the social engineering toolkit is to perform attacking techniques on their machines. This toolkit also includes website vector attacks and custom vector attacks, which allow us to clone any website, perform phishing attacks.

Features of Social Engineering Toolkit:

- Social Engineering Toolkit is **free** and **open source.**
- Social Engineering Toolkit is portable, which means we can quickly switch attack vectors.
- Social Engineering Toolkit supports integration with third-party modules.
- Social Engineering Toolkit is a **multi-platform** tool; we can run it in **Windows, Linux,** and **Unix.**
- Social Engineering Toolkit contains access to the **Fast-Track Penetration Testing platform.**
- Social Engineering Toolkit offers various attack vectors like **Website Attacks, Infection Media Generator, Website Attacks,** etc.

Application used could be web application which is examining the security of web applications and online platforms, including the susceptibility to social engineering attacks such as clickjacking, cross-site scripting (XSS), and social engineering-based authentication bypass.

TOOL INSTALLATION PROCEDURE:

In latest versions of Kali Linux Social Engineering toolkit is an inbuilt software .

In order to install SET in Kali follow the following steps:

1.System Requirements:

Ensure that your system meets the minimum requirements for running SET. Generally, any modern Linux distribution should suffice. You'll need Python installed on your system, as SET is written in Python.

2.Clone the SET Repository:

Open a terminal window on your Linux system. Clone the SET repository from GitHub using Git. Run the following command:

git clone https://github.com/trustedsec/social-engineer-toolkit.git

3.Navigate to the SET Directory:

Change your current directory to the SET directory that you just cloned. Use the 'cd' command to navigate:

cd social-engineer-toolkit

4.Install Dependencies:

SET requires various dependencies to function correctly. You can install them using the setup.py script provided:

sudo python setup.py install

5. Start SET:

After the installation process completes successfully, you can start the Social-Engineer Toolkit by running the setoolkit command in the terminal:

sudo setoolkit

6. Follow the On-Screen Instructions:

Once SET launches, you'll be presented with a menu of options. Follow the on-screen instructions to navigate through the different modules and features of SET. You can explore various attack vectors, such as phishing, credential harvesting, payload generation, and more**.**

7. Update SET (Optional):

It's a good practice to regularly update SET to ensure you have the latest features and security patches. You can update SET by navigating to the SET directory and running:

git pull This command will pull all the latest versions.

STEPS OF ETHICAL HACKING THAT COULD BE PERFORMED ON SOCIAL ENGINEERING ATTACK:

Ethical hacking, including social engineering attacks, follows a structured approach to ensure responsible and effective testing while minimizing potential harm.

1. Information Gathering:

Gather information about the target organization, its employees, infrastructure, and security measures. Utilize open-source intelligence (OSINT) techniques to collect publicly available information from sources such as social media, company websites, online forums, and public records.

2. Reconnaissance:

Conduct reconnaissance to identify potential attack vectors and vulnerabilities within the target organization. Analyze the gathered information to determine the most effective social engineering tactics and targets.

3.Scanning and enumeration:

Create a plausible pretext or scenario to establish trust and credibility with the target individual or organization. Craft a convincing story or persona that aligns with the pretext, such as posing as an IT support technician, vendor representative, or trusted colleague.

4.Gaining access/Exploitation:

Gaining access or exploitation is approached with the utmost caution and adherence to legal and ethical boundaries. Identifying vulnerabilities , Exploitation frameworks , Payload Deployment are done in the step gaining access / exploitation . Exploit human trust and vulnerabilities to elicit the desired response from the target individuals, such as clicking on malicious links, downloading attachments, or disclosing sensitive information.

5.Maintaining Access and Persistence:

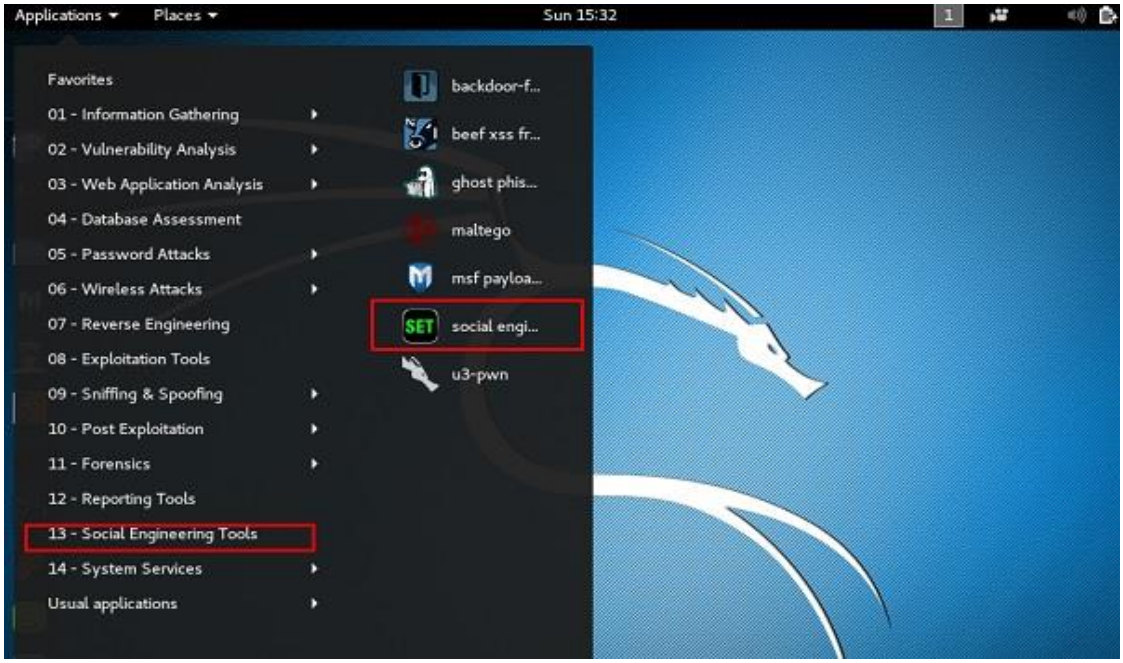
After successful exploitation, maintain persistence within the target environment to gather additional information, escalate privileges, or conduct further attacks. Document the results of the social engineering attack, including any compromised credentials, sensitive data obtained, and lessons learned for future engagements.

6.Clearing Tracks:

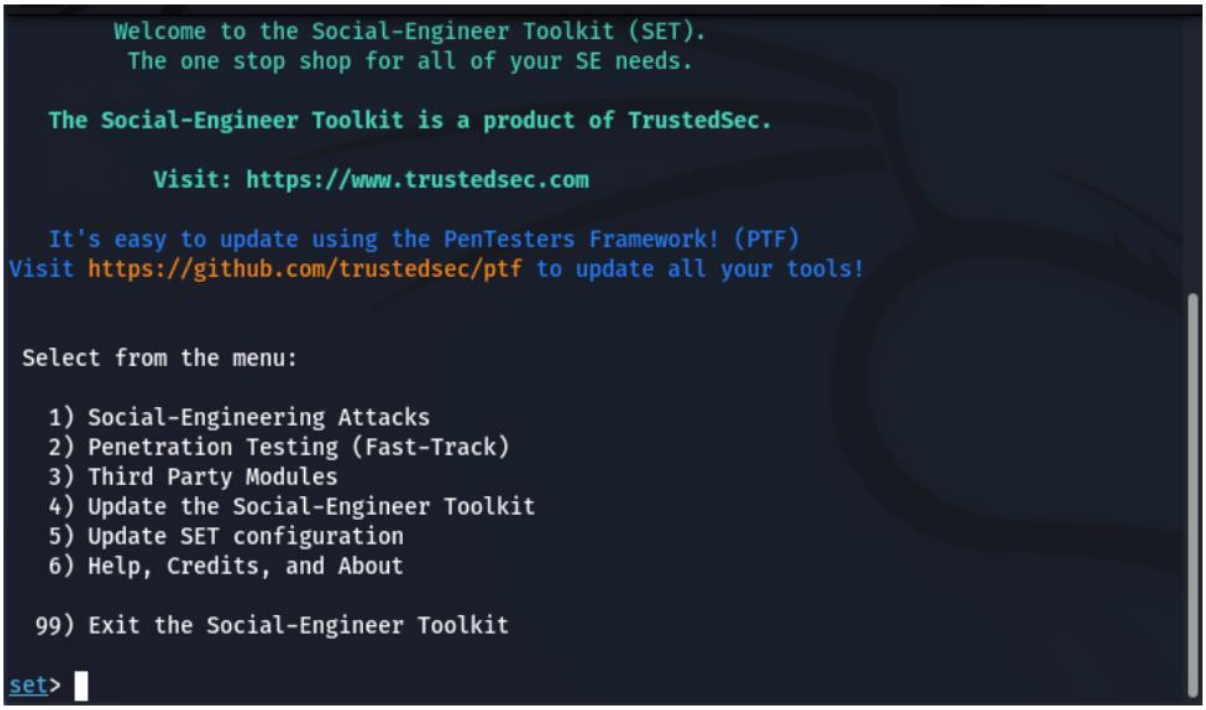
In ethical hacking, clearing tracks after conducting a social engineering attack is crucial to maintain confidentiality, integrity, and legal compliance. Logging and Documentation , Reversibility , Data Sanitization , Covering Tracks , Restoration of original state are some of the clearing tracks done in social engineering attack.

SCREENSHOTS OF IMPLEMENTING SOCIAL ENGINEERING ATTACK:

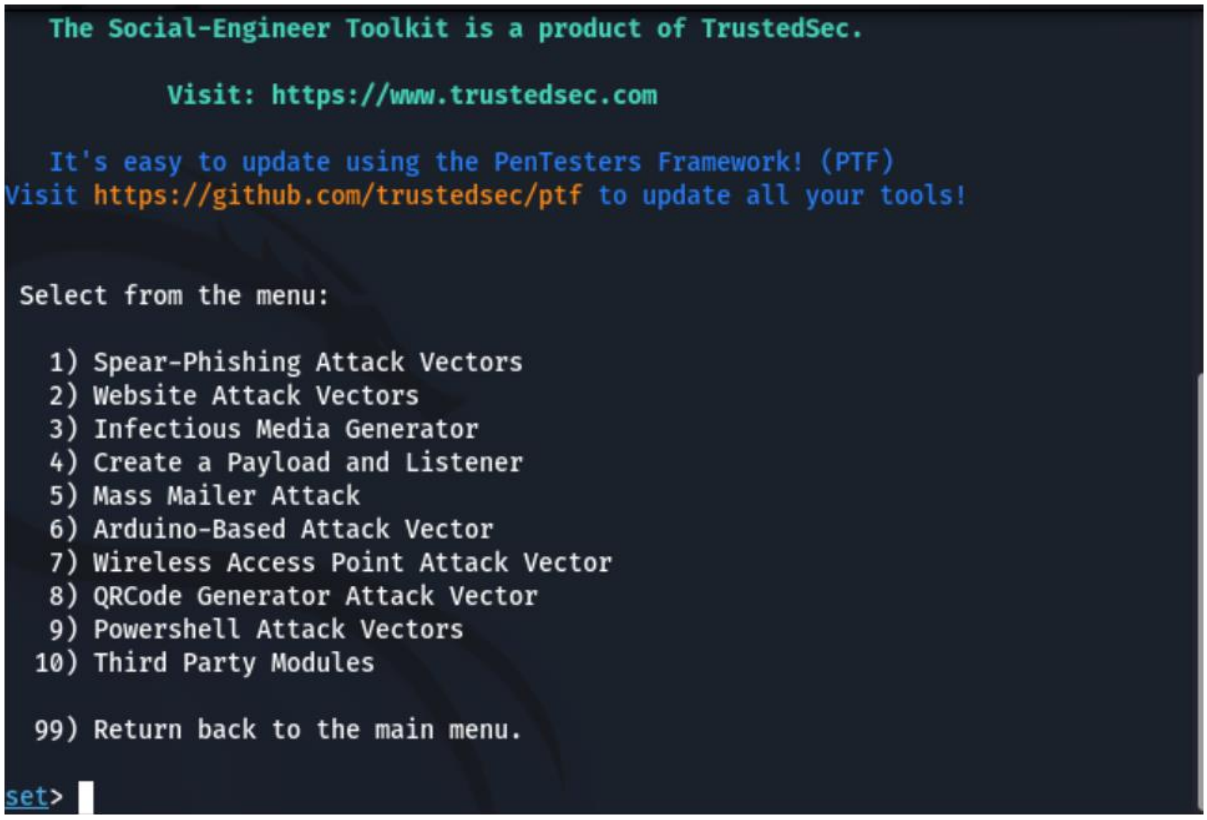
Step 1: Open Kali Linux



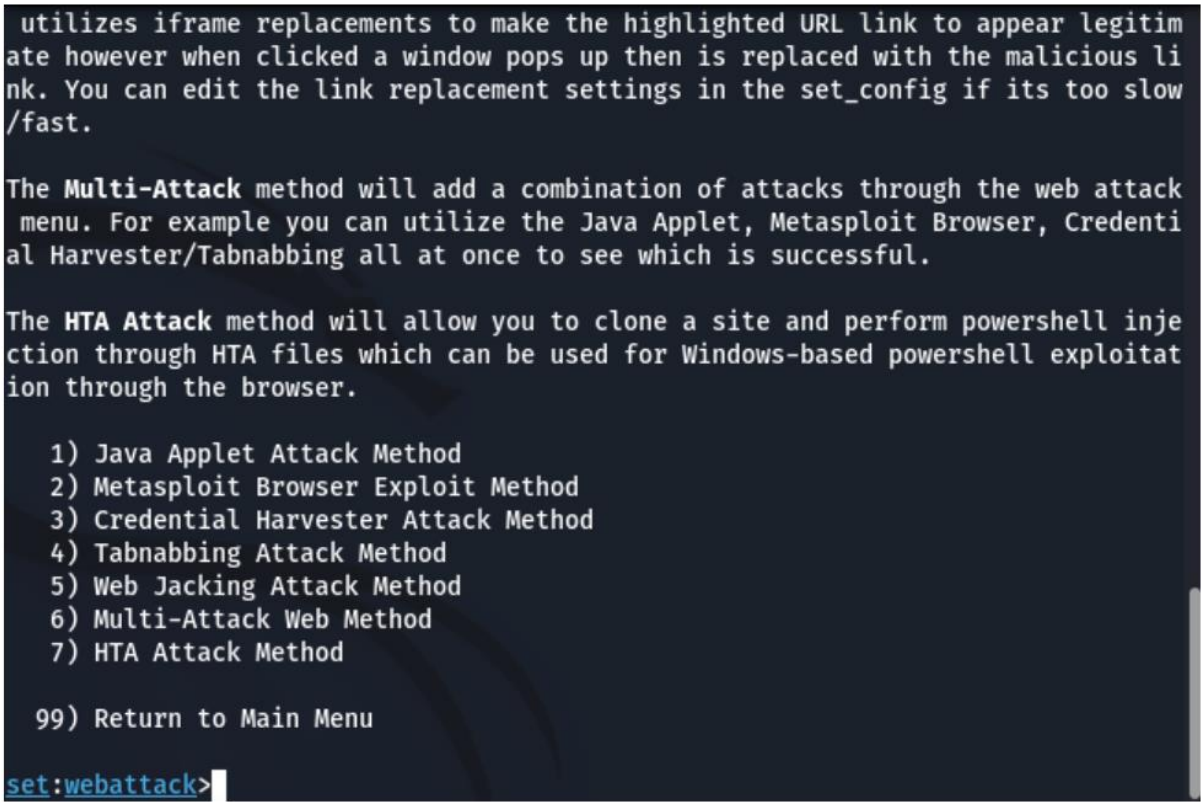
Step 2: Select the first option “Social Engineering Attacks”.



Step 3: Now select the second option “Website Attack Vectors”.

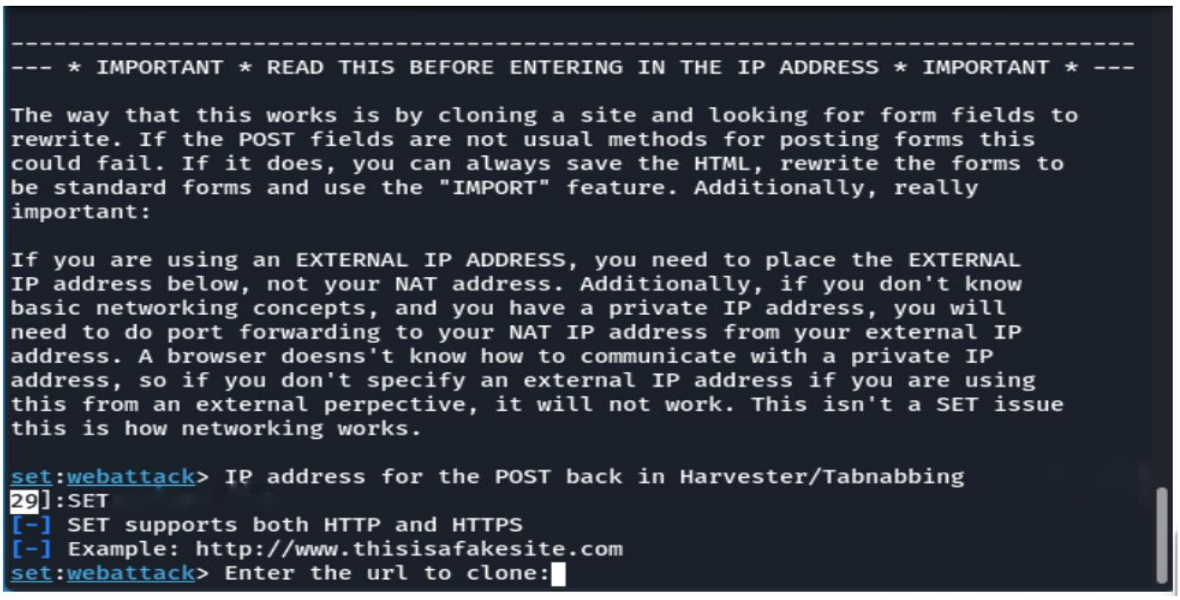


Step 4: Then, select the third option, “Credential Harvester Attack Method”.



Step 5: At last, “Select Site Cloner”.

Step 6: Now enter your localhost IP address and press Enter Button.



Step 7: Now enter any URL that you want to clone

```
set:webattack> Enter the url to clone:www.facebook.com/login.php/

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are av
ailable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Step 8: After that, your localhost IP will clone the site that you have entered to clone. Now you can send your IP address after converting it into any link to grab the information of any victim. Once it is done their username and password can be hacked.

```
The best way to use this attack is if username and password form fields are avai
lable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
[redacted] - - [14/Jul/2022 12:44:21] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2849
PARAM: lsd=AVp3NET1AWg
PARAM: display=
PARAM: isprivate=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgndim=eyJ3IjoxOTIwLCJoIjoxMDgwLCJhdyI6MTkyMCwiYWgiOjEwNTEsImMiOjI0fQ==
PARAM: lgnrnd=001415_1eXa
PARAM: lgnjs=1657782862
POSSIBLE USERNAME FIELD FOUND: email=hello+user
POSSIBLE PASSWORD FIELD FOUND: pass=this+is+my+password
PARAM: prefill_contact_point=
PARAM: prefill_source=
```

CONCLUSION:

In conclusion, the social engineering toolkit attack assessment revealed critical vulnerabilities and implications for the organization's security posture. Successful execution of social engineering tactics underscored the need for enhanced defenses and awareness. Key lessons include insights into human behaviour and organizational weaknesses. Recommendations include bolstering security awareness training, policy enforcement, and technical controls. Mitigation strategies encompass layered defenses, monitoring, and continuous improvement. Collaboration and proactive measures are essential for defending against evolving threats. Moving forward, implementing remediation measures, ongoing monitoring, and evaluation are crucial to enhancing resilience and readiness against social engineering attacks.

REFERENCES:

TrustedSec's GitHub Repository: The official repository for the Social-Engineer Toolkit maintained by TrustedSec, the organization behind SET. It provides access to the latest source code, documentation, and updates.

- Repository Link: https://github.com/trustedsec/social-engineer-toolkit

- Documentation Link: https://github.com/trustedsec/social-engineer-toolkit/wiki

- The Social-Engineer Toolkit: An Ethical Hacker's Guide to Social Engineering Assessments" by Christopher Hadnagy

- "Penetration Testing: A Hands-On Introduction to Hacking" by Georgia Weidman