

Mass Mail Email Attack using SET

A PROJECT REPORT

Submitted by

Divija Agrawal [Reg No: RA2111030010251]

Muskan Maheshwari [Reg No: RA2111029010025]

Harshil Chedda [Reg No: RA2111029010004]

Under the Guidance of

Dr. Sowmiya. B

Assistant Professor, Department of Computing Technologies *in*

partial fulfillment of the requirements for the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING



DEPARTMENT OF COMPUTING TECHNOLOGIES

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR– 603 203

NOV 2023



SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR–603 203

BONAFIDE CERTIFICATE

Certified that 18CSE412J (Offensive Security) project report titled “**Mass Mail Email Attack using SET**” is the bonafide work of **Divija Agrawal [Reg No: RA2111030010251]**, **Muskan Maheshwari [Reg No: RA2111029010025]**, **Harshil Chedda [Reg No: RA2111029010004]** who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported here in does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion for this or any other candidate.

SIGNATURE

Dr. Sowmiya. B
Assistant Professor
Department of Computing Technologies
Institute of Science and Technology

SIGNATURE

Dr. M. PUSHPALATHA
HEAD OF THE DEPARTMENT
Department of Computing Technologies
SRM Institute of Science and Technology SRM



Department of Computing Technologies
**SRM Institute of Science and Technology Own
Work Declaration Form**

Degree/Course : B. Tech in Computer Science and Engineering

Student Names : **Divija Agrawal, Muskan Maheshwari, Harshil Chedda**

Registration Number : **RA2111030010251, RA2111029010025, RA2111029010004**

Title of Work : **Mass Mail Email Attack using SET**

I/We here by certify that this assessment compiles with the University's Rules and Regulations relating to Academic misconduct and plagiarism, as listed in the University Website, Regulations, and the Education Committee guidelines.

I / We confirm that all the work contained in this assessment is our own except where indicated, and that we have met the following conditions:

- ☐ Clearly references / listed all sources as appropriate
- ☐ Referenced and put in inverted commas all quoted text (from books, web, etc.)
- ☐ Given the sources of all pictures, data, etc. that are not my own.
- ☐ Not made any use of the report(s) or essay(s) of any other student(s) either past or present
- ☐ Acknowledged in appropriate places any help that I have received from others (e.g., fellow students, technicians, statisticians, external sources)
- ☐ Compiled with any other plagiarism criteria specified in the Course hand book / University website

I understand that any false claim for this work will be penalized in accordance with the University policies and regulations.

DECLARATION:

I am aware of and understand the University's policy on Academic misconduct and plagiarism and I certify that this assessment is my / our own work, except where indicated by referring, and that I have followed the good academic practices noted above.

Student 1 Signature:

Student 2 Signature:

Student 2 Signature:

Date:

If you are working in a group, please write your registration numbers and sign with the date for every student in your group.

TABLE OF CONTENTS

| S. No. | Title | Page No. |
|---------------|------------------------------------|-----------------|
| 1. | Abstract | 1 |
| 2. | Introduction | 2 |
| 3. | Background | 3 |
| 4. | Social-Engineering Toolkit | 4 |
| 5. | Types of SET attacks in Kali Linux | 5 |
| 6. | How to use SET | 6 |
| 7. | Steps to perform Mass Mail Attack | 7 - 9 |
| 8. | Conclusion | 10 |
| 9. | References | 11 |

ABSTRACT

This project explores the application of the Social-Engineer Toolkit (SET) in the context of mass mailing simulations for educational and testing purposes. The study aims to assess the effectiveness of mass mailing as a social engineering technique and to analyze its implications for cybersecurity awareness and defense mechanisms.

The research methodology involves the ethical use of SET to simulate mass mailing campaigns, replicating common social engineering tactics such as phishing emails. The study examines the responses of targeted individuals within a controlled environment, focusing on factors such as click-through rates, user awareness, and potential vulnerabilities.

Key objectives include:

1. **Effectiveness Assessment:** Evaluate the success rate of mass mailing simulations in terms of user engagement and susceptibility to social engineering attacks.
2. **User Awareness:** Analyze the impact of mass mailing simulations on user awareness and ability to identify phishing attempts.
3. **Security Implications:** Investigate potential security vulnerabilities or risks introduced by mass mailing simulations and explore mitigation strategies.

Ethical considerations and legal compliance are paramount throughout the research, with explicit permissions obtained for any simulated activities. The findings of this study aim to contribute valuable insights into the realm of cybersecurity education, assisting in the development of effective defense strategies against social engineering threats.

INTRODUCTION

In an era dominated by digital communication, the prevalence of cyber threats continues to pose significant challenges to individuals and organizations. Among these threats, social engineering remains a potent vector, exploiting human psychology to compromise information security. Mass mailing, as a form of social engineering through phishing, represents a pervasive method employed by attackers to deceive users and gain unauthorized access to sensitive information.

This project investigates the landscape of mass mailing within the context of ethical hacking and security testing, utilizing the Social-Engineer Toolkit (SET) as a controlled environment for simulations. The primary objectives are to assess the effectiveness of mass mailing as a social engineering technique, evaluate its impact on user awareness, and analyze the security implications associated with such simulated attacks.



Background

In the contemporary digital landscape, the advent of interconnected systems and widespread reliance on electronic communication has ushered in new challenges for information security. Among the myriad tactics employed by malicious actors, social engineering stands out as a persistent and evolving threat. Social engineering techniques exploit human psychology, manipulating individuals into divulging sensitive information or performing actions that compromise security.

Phishing, a subset of social engineering, involves the use of deceptive messages, often in the form of emails, to trick recipients into revealing confidential information. Mass mailing, as a specific category of phishing, amplifies the impact of these attacks by targeting a large number of individuals simultaneously. Attackers leverage social engineering tactics to craft convincing messages that mimic legitimate communication, exploiting trust to elicit responses.

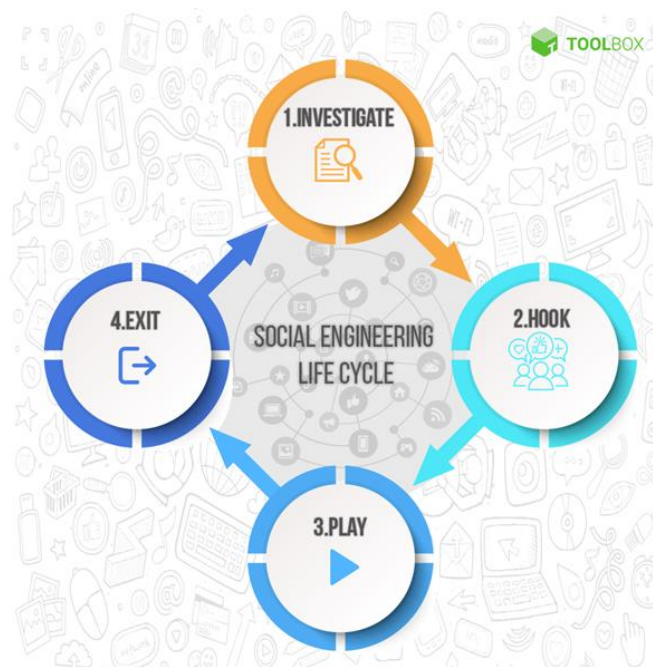
The evolution of mass mailing attacks has been fueled by the increasing sophistication of malicious actors. Cybercriminals employ techniques such as email spoofing, domain impersonation, and the use of malicious attachments or links to deceive users. These attacks not only compromise personal and organizational data but also undermine user confidence in online communication platforms.

In response to the escalating threat landscape, ethical hacking and penetration testing have emerged as critical components of cybersecurity strategies. Ethical hackers seek to understand and replicate the tactics employed by malicious actors in controlled environments, aiming to identify vulnerabilities and strengthen defenses.

Social-Engineer Toolkit (SET):

The Social-Engineer Toolkit (SET) represents a crucial tool in the arsenal of ethical hackers and security professionals. Developed as an open-source framework in Python, SET facilitates the simulation of social engineering attacks in a controlled and ethical manner. Its features include the creation of realistic phishing scenarios, credential harvesting simulations, and the generation of malicious payloads.

As the digital arms race between security professionals and cyber adversaries continues, understanding the intricacies of mass mailing attacks becomes paramount. This research leverages the capabilities of SET to conduct simulated mass mailing campaigns, shedding light on the effectiveness of these attacks, the level of user awareness, and the potential security implications.



TYPES OF SET ATTACKS IN KALI LINUX

The Social-Engineer Toolkit (SET) is often used in the Kali Linux operating system for ethical hacking and penetration testing purposes. Below are some specific SET attacks that can be performed in Kali Linux:

1. Social Engineering Attacks:

- Credential Harvester Attack: Clones a website and captures login credentials.
- Site Cloner Attack: Clones a website without capturing credentials, useful for delivering other payloads.
- Spear Phishing Attack: Customizes phishing emails for targeted individuals or organizations.

2. Metasploit Integration:

- Web Attack: Metasploit Browser Exploit: Integrates with Metasploit to launch browser-based exploits against a target.

3. Java Applet Attack:

- Java Applet Attack: Uses a malicious Java applet to exploit vulnerabilities in the Java Runtime Environment.

4. Wireless Attacks:

- Wireless Access Point Attack: Creates a rogue wireless access point to entice users to connect.

5. Infectious Media Generator:

- Infectious Media Generator: Creates USB drives or other removable media with malicious payloads.

6. Malicious File Attacks:

- Create a Payload and Listener: Generates various types of malicious payloads, including executables or documents.

7. Teensy USB HID Attack:

- Teensy USB HID Attack: Uses a Teensy USB device to emulate a human interface device, enabling automated keystroke injections.

To use SET in Kali Linux:

1. Open a terminal in Kali Linux.
2. Type “**setoolkit**” to launch the Social-Engineer Toolkit.
3. Follow the on-screen menu to choose and execute the desired attack.

MOST COMMON SOCIAL ENGINEERING ATTACKS



Main features:

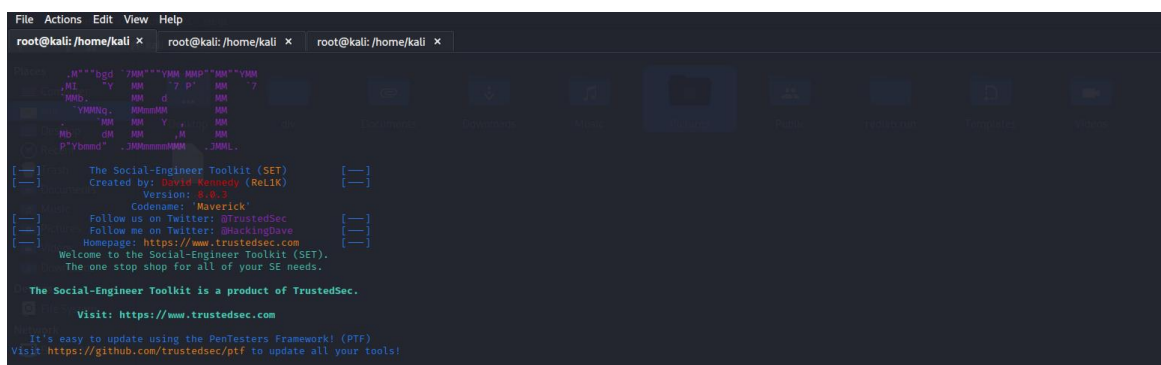
- Multi-platform: It can run on Linux, Unix and Windows.
- Supports integration with third party modules.
- Allows multiple tweaks from the configuration menu.
- Includes access to the Fast-Track Penetration Testing platform
- Social engineering attack options such as Spear-Phishing Attacks, Website Attacks, Infection Media Generator, Mass Mailing, Arduino-Based Attack, QRCode Attacks, Powershell Attack Vectors, and much more.

Steps to do to Mass mail email attack using SET –

open the root terminal and type:

setoolkit

And SET opens Up



```
File Actions Edit View Help
root@kali: /home/kali x root@kali: /home/kali x root@kali: /home/kali x

[---]
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 3.8.3 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
[---] Welcome to the Social-Engineer Toolkit (SET). [---]
[---] The one stop shop for all of your SE needs. [---]
[---]
[---] The Social-Engineer Toolkit is a product of TrustedSec. [---]
[---] Visit: https://www.trustedsec.com [---]
[---]
[---] It's easy to update using the PenTesters Framework! (PTF) [---]
[---] Visit https://github.com/trustedsec/ptf to update all your tools! [---]
```

Select Social Engineering Attacks, Option 1

Option 1 : Social-Engineering Attacks



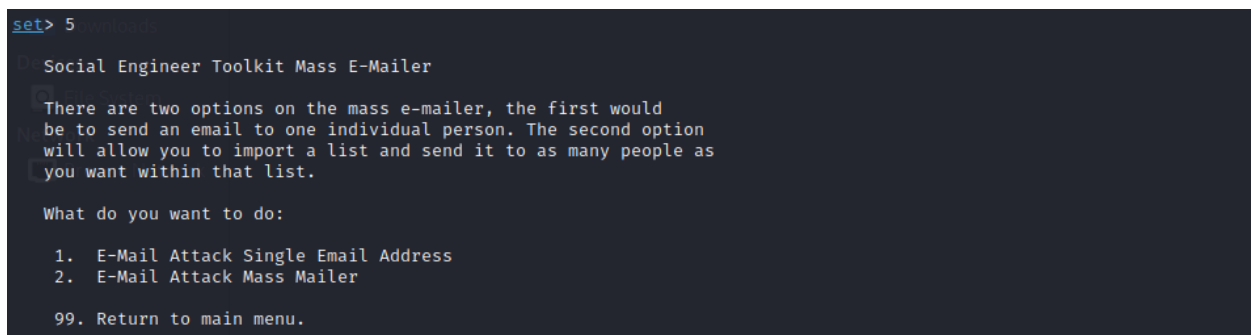
```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.
```

Now as we need to do a mass email attack, select option 5.

Option 5 : Mass Mailer Attack



```
set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.
```

Option 2 : Email Attack Mass Mailer

```
set:mailer>2
```

The mass emailer will allow you to send emails to multiple individuals in a list. The format is simple, it will email based off of a line. So it should look like the following:

```
john.doe@ihazemail.com  
jane.doe@ihazemail.com  
wayne.doe@ihazemail.com
```

This will continue through until it reaches the end of the file. You will need to specify where the file is, for example if its in the SET folder, just specify filename.txt (or whatever it is). If its somewhere on the filesystem, enter the full path, for example /home/relik/ihazemails.txt

Now you need to define the path to the email list. For us, this is **gmaillist.txt**. Just add the file-name with the path.

The easiest way is to drag and drop the gmaillist.txt file into the terminal.

```
set:phishing> Path to the file to import into SET:/home/kali/gmaillist.txt
```

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

Enter the Gmail address you want the mass attack sent from. The email address and password must be correct.

Next, enter the name that you want the email recipients to see in their Inbox. This is the name that will flash first in front of your victim. Pay specific attention to this field, as this where the actual social engineering takes place. *This could be "Admin" in case of a spear-phish attack.*

Now the SET will ask you to enter the password for the email account.

After entering the password, you have the option to specify this message as high priority. Sometimes this may be effective, but it could also make the victim suspicious, so we suggest using this option only when it suits your needs.

Now SET will ask you to enter the subject of the email .

Enter the subject of the email

Now the SET will ask you if you want the body of the message to be HTML or Plain Text .(P for plain text or H for html)

Enter the body text

Enter the body of the email here ..

```
set:phishing>1
set:phishing> Your gmail email address:phiser410@gmail.com
set:phishing> The FROM NAME the user will see:Hacker
Email password:
set:phishing> Flag this message/s as high priority? [yes/no]:n
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:mass mail
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:Mass mail attack using set
Next line of the body: test
Next line of the body: END
[*] SET has finished sending the emails
```

This is how hackers perform mass email attack.

Conclusion

In summary, the use of the Social-Engineer Toolkit (SET) for simulating mass mail campaigns reveals the potency of mass mailing attacks in manipulating user behavior. The toolkit's versatility and customization features highlight the ease with which attackers can deceive users, emphasizing the need for robust cybersecurity education. Ethical use of SET underscores its value as a controlled environment for security professionals, contributing to ongoing efforts in developing effective defense strategies. This research provides insights into the evolving landscape of social engineering threats, emphasizing ethical considerations, legal compliance, and the continuous pursuit of knowledge for securing digital environments.

References

1. <https://www.social-engineer.org>.
2. <https://www.kali.org/tools/set/>
3. <https://www.youtube.com/watch?v=l5V4tDqidlw>