International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.017 ISSN: 2581-4621

Understanding Social Engineering Tactics and Their Impact on Cyber Attacks

[1]D Neeraja, [2]Mr.Edukondalu Simhadati,
[1]pg scholar,[2]Assistant Professor,
[1]Computer Networks and Information Security, [2]CSE department,
[1]duddyalaneeraja103@gmail.com , [2]sek780080@gmail.com
[1] G. Narayanamma Institute of Technology and Science, Hyderabad, Telangana, India.
[2]Shadan College of Engineering & Technology, Autonomous, Hyderabad, Telangana, India.

Abstract:
Cybercriminals employ social engineering to trick others into revealing confidential information, providing unauthorized access, or performing actions that undermine security. Social engineering employs human psychology and emotions to manipulate individuals into making bad choices, as opposed to conventional hacking, which relies on technical vulnerabilities. Phishing, pretexting, baiting, and tailgating are typical methods. Social engineering is perhaps the strongest and most destructive cyberattack method as it is based on exploiting trust, fear, curiosity, or urgency. There are a variety of social engineering attacks using different methods to trick users into defying security [12]. The most common types are: Rather than focusing on technological flaws in systems, these strategies all take advantage of human weaknesses, such as trust, fear, or urgency. The most crucial step in preventing social engineering attacks is being aware of these tactics. More than technological flaws, human behavior especially cognitive biases are the focus of social engineering including the psychological aspect of cyberattacks. Cybercriminals use deception, manipulation, and persuasion to gain illegal access to infrastructure or private data [13]. These assaults typically take advantage of feelings of haste, anxiety, greed, and trust.

Keywords: Social engineering, Phishing, Psychological manipulation, Cyberattacks.

1. Problem Statement:

Social engineering is a type of cyberattack that takes advantage of human psychology and emotional stimuli to trick people into revealing sensitive information, granting unauthorized access, or taking actions that undermine security. In spite of the progress made in technical defense, social engineering is one of the most successful and perilous types of cybercrime, and it tends to circumvent conventional security controls. The issue is the vulnerability of people to such attacks and hence the need to comprehend and counter the psychological factors that result in vulnerabilities[14]. The most prevalent categories are: Instead of targeting technology weaknesses in systems, all of these tactics use human vulnerabilities like trust, fear, or time pressure. The most important action to thwart social engineering attacks is being vigilant for these methods. Most of all technological weaknesses, cognitive biases human behavior is the subject of social engineering as well as the psychological factor of cyberattacks. Cybercrooks exploit the use of lies, manipulation, and influence to achieve illegal access to infrastructure or personal information [13]. Such attacks mostly exploit emotions of haste, anxiety, greed, and trust.

2. Objectives:

List and classify the various types of social engineering attacks, including baiting, tailgating, pretexting, and phishing.

Discuss the psychological tactics employed by cybercriminals to deceive their victims, including trust, fear, urgency, and curiosity.

Discuss the most recent measures for preventing social engineering attacks, such as technical defenses, awareness campaigns, and training.

Promote critical thinking and emotional intelligence to provide organizational and personal protection against social engineering attacks.

Discuss how effective the suggested solutions minimize the probability that social engineering attacks will succeed.

3. Literature survey

“Adolescents’ and social engineering: The role of psychometrics factors in determining vulnerability and designing interventions [1]”,

The increasing popularity of social media among teenagers, especially in Qatar, has contributed to a surge in social engineering attacks on this susceptible group. Research indicates that teenagers are more vulnerable to manipulation via the internet owing to psychological aspects like trust, curiosity, and a sense of need for social acceptance. The consequences of these attacks are usually negative and have included exposure to obscenity, blackmailing, and extortion. Research identifies the necessity to understand how psychometric dimensions interact with demographic factors in being able to predict susceptibility to these types of attacks. Furthermore, socio-technical measures, such as digital literacy schemes, have been shown to mitigate adolescent susceptibility to social engineering.

“The Need for Social Intelligence Training for Industrial Engineers”

Location: Makkah, Saudi Arabia. Social intelligence (SI) is becoming more and more important for industrial engineers as it helps them better cope with complicated work environments and communicate effectively with teams. Studies highlight that SI helps in better collaboration, conflict resolution, and leadership in multicultural industrial environments. Industrial engineers with high social intelligence are likely to be more effective in managing interpersonal relationships, adjusting to organizational culture, and promoting innovation, according to studies. Training in SI enables engineers to cultivate empathy, communication, and emotional intelligence skills, all of which are essential for maximizing teamwork and decision-making. As industries grow more collaborative and dynamic, incorporating SI training into engineering programs is key to developing balanced professionals[2].

” Engineering as a Social Profession”

Social aspects of engineering have garnered growing interest, especially in comprehending the profession's involvement with society and engineers' lived lives. Former research has examined the social role of engineering[2], highlighting its function in addressing needs in society and the significance of ethical behavior. But fewer efforts have been directed toward engineers' lived professional lives, a subject covered by autoethnographic observations in this research. Evidence indicates that social skills of engineers, especially negotiation and teamwork, are essential for practice in today's complex work setting. The public image of engineering and the real world that engineers experience has been a persistent issue, with numerous graduates facing problems as they enter the professional scene[3].

4. Methodology and Modules

Kali Linux social engineering pentesting

You may need to use a variety of methods to test your employees' susceptibility to social engineering attacks. To help you with this task, Kali includes a few tools. The following is a list of some of the best ones along with their applications [3]:

Maltego is a Kali Linux social engineering tool.

The OSINT (open-source intelligence) analysis tool called Maltego shows how different information units are related to one another. You can find relationships between people and various information assets, such as screen names, social media accounts, email addresses, and other informational units that link a person to a website or organization, by using Maltego [4].

With all of this information, you can assess your employees' security knowledge by simulating a social engineering attack. Maltego can be launched from the Kali Whisker Menu or by selecting Maltego number five under Applications > Kali Linux > Top 10 Security Tools.

The graphical user interface on which Maltego is built makes it simple to visualize relationships [5].

Social engineering tool for Kali Linux: Toolkit for Social Engineering (SET)

An open-source Python-based toolbox for social engineering penetration testing is called the Social Engineering toolbox (SET). With SET, you can develop a convincing exploit in just a few minutes thanks to its many configurable attack paths.

A web tool included with SET turns your Kali computer into a web server using a variety of exploits capable of taking over the majority of browsers. The idea is to send your victim an email with a link that will take them to your website, where the exploit will be downloaded and executed on their computer [6].

To make the attack seem more genuine, you may even use SET's built-in templates to replicate a legitimate website. Pre-formatted phishing sites of popular websites, like Facebook, Twitter, Google, and Yahoo, are included in SET [7].

To start SET with Kali Linux, either type setoolkit as a shell prompt or go to Applications > KaliLinux > Exploitation Tools > Social Engineering Toolkit | toolkit.

Wifiphisher is a Kali Linux phishing tool.

A specific social engineering tool called Wifiphisher will conduct scams against Wi-Fi networks in order to retrieve the target user base's WPA/WPA2 passwords. Any open Wi-Fi access point can be chosen by the tool, which can then the it (de-authenticate all users) and create a clone connection point that connects without a password (figure 2[8]).

Any user that connects to the malicious twin-like open networks is presented with a phishing website that purports to be legitimate and asks for their Wi-Fi password to attempt gain a firmware upgrade, which is cited as the reason why figure 3's Wi-Fi isn't working.

Wiifishiper lags behind and notifies the targets when they enter a password. To allow you time to verify the data collected password, it will display a modeled update screen and a mimicked reboot timer after you provide it. It's a handy tool for evaluating your security measures against social engineering over Wi-Fi figure 4[9].

You can launch the python script by entering this command:

```
$ sudo python wifiphisher.py
```

Kali Linux social engineering tool: Metasploit MSF

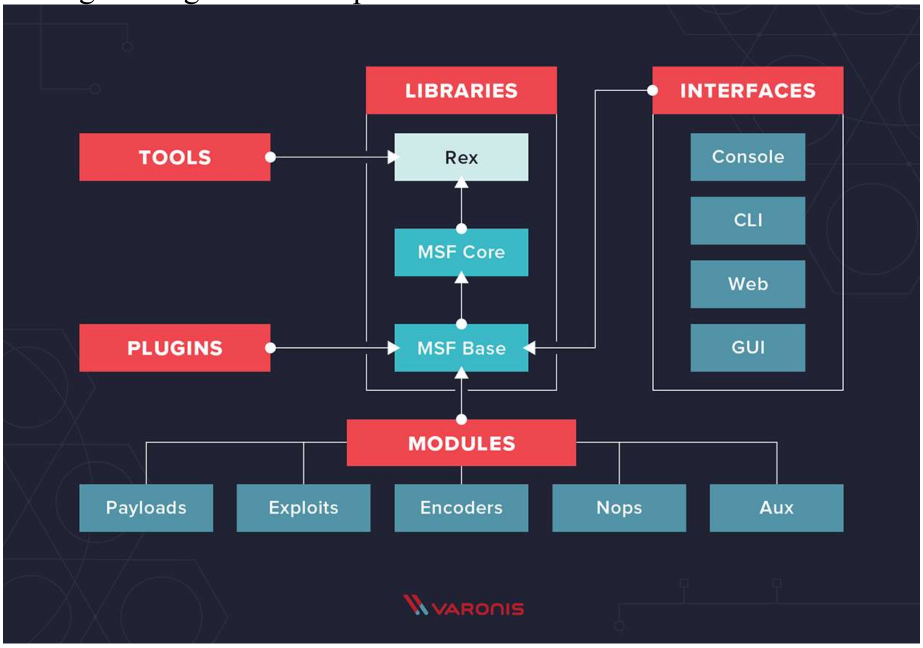


Figure 1. Metasploit Framework is a penetration testing tool

5. Implementation

Install via requirements.txt

pip3 install -r requirements.txt
python3 setup.py

Install SET

=======

Mac OS X

You will need to use a virtual environment for the Python install if you are using an M2 Macbook with the following instructions in your CLI within the social-engineer-toolkit directory[11].

```
# to install dependencies, run the following:
python3 -m venv path/to/venv
source path/to/venv/bin/activate
python3 -m pip install -r requirements.txt
# to install SET figure 2.
sudo python3 setup.py
```

Installation

Windows 10 WSL/WSL2 Kali Linux

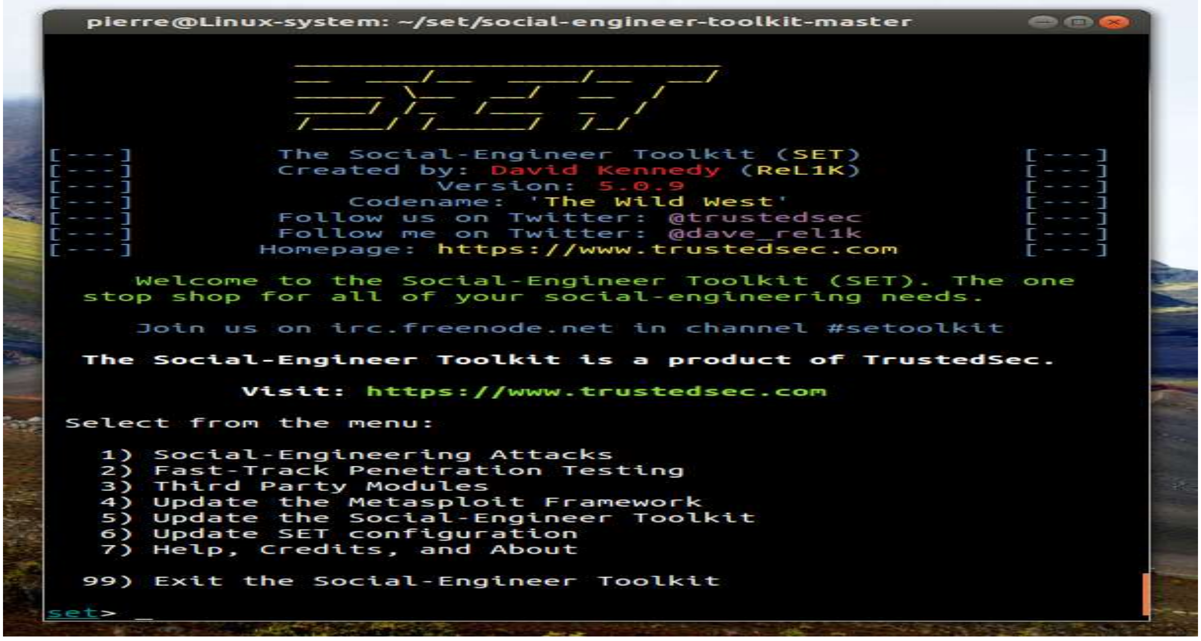
sudo apt install set -y

Kali Linux on Windows 10 is a minimal installation so it doesn't have any tools installed. You can easily install Social Engineer Toolkit on WSL/WSL2 without needing pip using the above command[10].

Linux

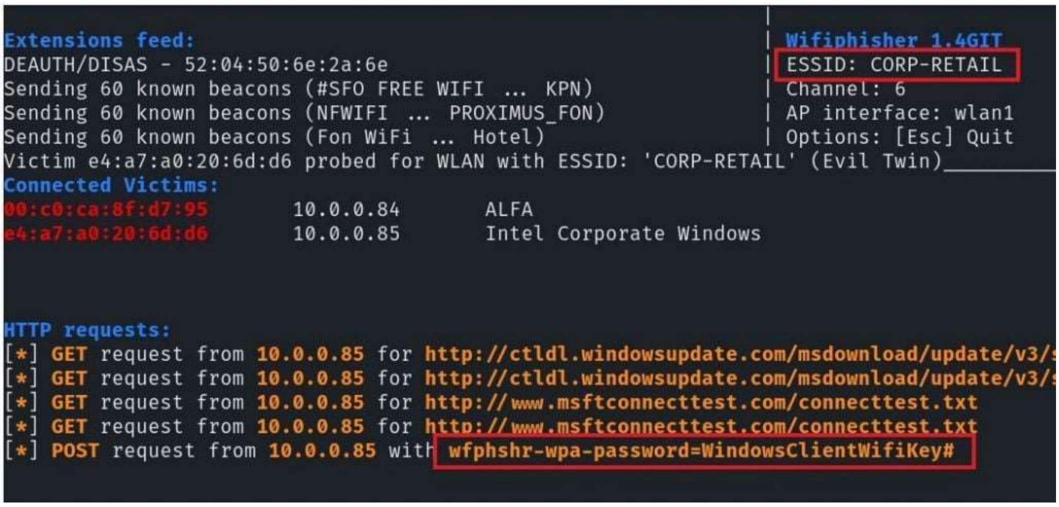
```
git clone https://github.com/trustedsec/social-engineer-toolkit/ setoolkit/
cd setoolkit
pip3 install -r requirements.txt
python setup.py
```

6. Results



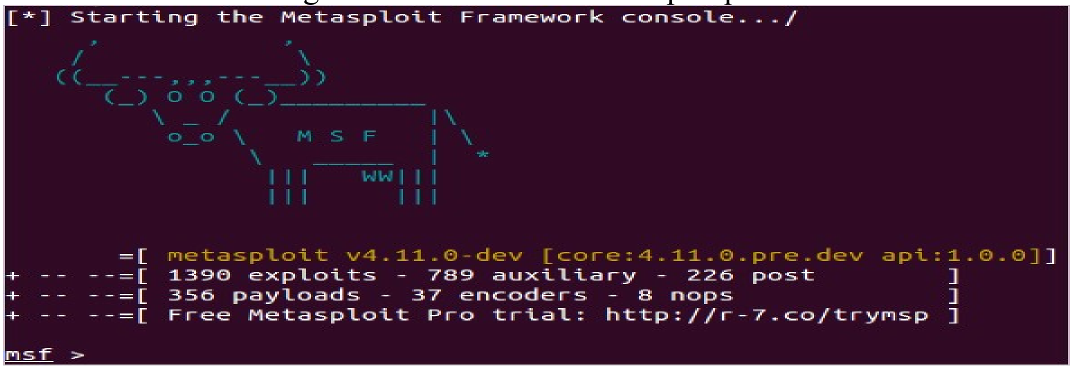
```
pierre@Linux-system: ~/set/social-engineer-toolkit-master

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
[---]                 Version: 5.0.9                   [---]
[---]           Codename: 'The Wild West'              [---]
[---]        Follow us on Twitter: @trustedsec         [---]
[---]        Follow me on Twitter: @dave_rel1k         [---]
[---]      Homepage: https://www.trustedsec.com        [---]

   Welcome to the Social-Engineer Toolkit (SET). The one
 stop shop for all of your social-engineering needs.

   Join us on irc.freenode.net in channel #setoolkit

 The Social-Engineer Toolkit is a product of TrustedSec.

          Visit: https://www.trustedsec.com

Select from the menu:

  1) Social-Engineering Attacks
  2) Fast-Track Penetration Testing
  3) Third Party Modules
  4) Update the Metasploit Framework
  5) Update the Social-Engineer Toolkit
  6) Update SET configuration
  7) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit

set> _
```

Figure 2: Installation of Social Engineering tool kit



```
                                                                |
Extensions feed:                                                | Wifiphisher 1.4GIT
DEAUTH/DISAS - 52:04:50:6e:2a:6e                                | ESSID: CORP-RETAIL
Sending 60 known beacons (#SFO FREE WIFI ... KPN)               | Channel: 6
Sending 60 known beacons (NFWIFI ... PROXIMUS_FON)              | AP interface: wlan1
Sending 60 known beacons (Fon WiFi ... Hotel)                   | Options: [Esc] Quit
Victim e4:a7:a0:20:6d:d6 probed for WLAN with ESSID: 'CORP-RETAIL' (Evil Twin)________
Connected Victims:
00:c0:ca:8f:d7:95       10.0.0.84       ALFA
e4:a7:a0:20:6d:d6       10.0.0.85       Intel Corporate Windows


HTTP requests:
[*] GET request from 10.0.0.85 for http://ctldl.windowsupdate.com/msdownload/update/v3/s
[*] GET request from 10.0.0.85 for http://ctldl.windowsupdate.com/msdownload/update/v3/s
[*] GET request from 10.0.0.85 for http://www.msftconnecttest.com/connecttest.txt
[*] GET request from 10.0.0.85 for http://www.msftconnecttest.com/connecttest.txt
[*] POST request from 10.0.0.85 with wfphshr-wpa-password=WindowsClientWifiKey#
```

Figure 3. Demonstration of http requests



```
[*] Starting the Metasploit Framework console.../

       ,           ,
      /             \
    ((__---,,,---__))
       (_) O O (_)_____________
          \ _ /            |\
           o_o \    M S F  | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||


       =[ metasploit v4.11.0-dev [core:4.11.0.pre.dev api:1.0.0]]
+ -- --=[ 1390 exploits - 789 auxiliary - 226 post          ]
+ -- --=[ 356 payloads - 37 encoders - 8 nops               ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Figure 4. Starting the Metasploit framework console.

7. Conclusion:

For determining an organization's vulnerability to social engineering attacks, Kali Linux's social engineering penetration testing tools—Maltego, Social Engineering Toolkit (SET), Wifiphisher, or Metasploit—are invaluable resources. Every tool is designed to be used for a certain purpose. MalteGo makes it easier to gather open-source information (OSINT) for charting relationships and identifying potential social engineering targets. To assess how susceptible employees are to fraudulent online attacks, SET provides a number of customizable attack routes, most notably phishing.

8. References

[1]"Adolescents' and social engineering: The role of psychometrics factors in determining vulnerability and designing interventions". Published in: 2022 9th International Conference on Behavioural and Social Computing (BESC)Date of Conference: 29-31 October 2022, Date Added to IEEE Xplore: 28 December 2022.DOI: 10.1109/BESC57393.2022.9995705.Publisher: IEEE.

[2]The Need for Social Intelligence Training for Industrial Engineers Published in: 2020 Industrial & Systems Engineering Conference (ISEC)Date of Conference: 11-12 July 2020. Information:DOI: 10.1109/ISEC49495.2020.9230043Publisher: IEEE.Conference.

[3]Published in: 2024 World Engineering Education Forum - Global Engineering Deans Council (WEEF-GEDC)Date of Conference: 02-05 December 2024.Date Added to IEEE Xplore:2025DOI: 10.1109/WEEFGEDC63419.2024.10854937Publisher: IEEConference Location: Sydney, Australia.

[4]The engineering social role conception promoted in the engineering courses' advertising: looking from the point of view of women.Published in: 2021 IEEE Global Engineering Education Conference (EDUCON)Date of Conference: 21-23 April 2021Date Added to

IEEE Xplore: 18June2021DOI: 10.1109/EDUCON46332.2021.9454120Publisher: IEEEConference Location: Vienna, Austria.

[5]Francois Mouton, Mercia M. Malany, Louise Leenen and H.S. Venterz, ―Social Engineering Attack Framework‖, IEEE/2014.

[6]Aisha SuliamanAlazri, ―The Awareness of Social engineering in Information Revolution: Techniques and Challenges‖, IEEE/2015.

[7]Alazri, Aisha, ," The awareness of social engineering in information revolution: Techniques and challenges", 2015/12/01,DO - 10.1109/ICITST.2015.7412088.

[8]K. Mitnick and W. L. Simon, The Art of Deception: Controlling the Human Element of Security. New York, NY, USA: Wiley, 2002.

[9]Hadnagy, Social Engineering: The Science of Human Hacking, 2nd ed. Hoboken, NJ, USA: Wiley, 2018.

[10] R. M. Gonzalez and J. W. Cappel, "An exploratory study of social engineering practices," J. Inf. Syst. Educ., vol. 21, no. 2, pp. 99–108, 2010.

[11] M. Workman, "A test of interventions for security threats from social engineering," Inf. Manage. Comput. Secur., vol. 16, no. 5, pp. 463–483, 2008.

[12] D. P. Twitchell, "Social engineering in information assurance curricula," in Proc. 2006 InfoSec CD Conf., Kennesaw, GA, USA, 2006, pp. 1–7.

[13] C. Hadnagy and M. Fincher, Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. Indianapolis, IN, USA: Wiley, 2015.

[14] T. van der Wagen and B. Pieters, "Social engineering attacks: An analysis of techniques, tactics, and trends," in Proc. IEEE Int. Conf. Cyber Secur. Protect. Digit. Serv. (Cyber Security), Oxford, UK, 2020, pp. 1–6.

[15] N. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," J. Inf. Secur. Appl., vol. 22, pp. 113–122, 2015.

[16] R. G. Min and S. R. Grimshaw, "Modeling cyber attacker behavior: Characterization of attack surfaces in a network system," IEEE Transactions on Information Forensics and Security, vol. 14, no. 11, pp. 2981-2994, 2019.