ASSIGNMENT - 3

Social engineering

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems.

Most social engineering attacks depend on real communication between attackers and victims. Instead of using **brute force methods to** breach the data, the attacker prompts the user to compromise.

Prepare by gathering background information on a large group.

Infiltrate by building trust, establishing a relationship or starting a conversation.

Establish the victim once more to confront the attack with confidence and weakness.

Once the user takes the desired action, release it.

Many employees and consumers are unaware that certain information can give hackers access to **multiple networks** and **accounts**.

By sending messages for IT support personnel as legitimate users, they grab your details - such as **name, date of birth** or **address**. It is a simple matter to reset the password and get almost unlimited access. They can steal money, spread social engineering malware, and many more.

Characteristics of Social Engineering Attack

Social engineering attack centers on the attacker's use of **persuasion** and **confidence.**

High emotions: Emotional manipulation gives attackers the upper hand in any conversation. The below feelings are used equally to explain to you.

Fear

excitement

Curiosity

Anger

Crime

Sadness

Types of Social Engineering Attacks

Every type of cybersecurity attack involves some social engineering. **For example**, **classic email** and **virus scams** are laden with social overtones. Some of the standard methods used by **social engineering attackers** are below:

Phishing Attacks

Phishing attackers pretend to a trusted institution or person in an attempt to convince you to uncover personal data and valuables. Attacks by using phishing are targeted in two ways:

Spam phishing is a widespread attack for some users. The attacks are non-personal and try to capture any irresponsible person.

Phishing and **whaling** use personal information to target particular users. The whaling attacks are aimed at high-profile individuals such as celebrities, upper management and higher government officials. Whether it is direct communication or by a fake website, anything you share goes directly into the **seamster's pocket.** You can also be fooled into the next stage of the phishing attack malware download. The methods used in phishing are unique methods of delivery.

Voice phishing (Wishing) phone calls can be an automated messaging system recording all your inputs. The person can speak with you to build trust.

SMS phishing (SMS) texts or mobile app messages may indicate a web link or follow-up via a web link or phone number. A web link, phone number, or malware attachment may be used.

Angler phishing takes place on social media, where the attacker mimics the customer service team of a trusted company. They interrupt your communication with a brand and turn the conversations into private messages, where they escalate the attack.

Search engine phishing attempts to place links to fake websites at the top of any search results. The advertisements will be paid or use valid optimization methods to manipulate search rankings. The links are given in **email, text, social media messages** and **online advertisements**.

- **In-session phishing** appears as an interruption to the **normal web browsing**. For example, you can see fake **pop-ups** on the webpages you are currently viewing.

Baiting Attack

Baiting abuses your natural curiosity of exposing yourself as an attacker. The potential for something exclusive is used to exploit us. An attack involves infecting us with malware. Popular methods of baiting are:

- USB drives are left in public places, such as libraries and parking lots.
- Email attachment with details with free offer.

Physical Breach Attack

Physical violations include attackers, who would otherwise present themselves as legitimate to access unauthorized areas or information.

This type of attack is common in enterprise environments, like the **government, businesses**, or other **organizations**. Attackers pretend to be a representative of a trusted vendor for the company. Some attackers may have recently been fired in retaliation against their former employers.

They obscure their identity but are reliable enough to avoid questions. It requires little research on the part of the attacker and involves high risk. Therefore, if someone is attempting this method, they have identified a clear potential for a highly valued reward if successful.

- **Preceding Attack: Trusting** uses a misleading identity as a "trust" to establish trusts, such as applying directly to a vendor or facility employee. The approach requires the attacker to interact with you more actively. Once exploited, they are convinced that you are legitimate.
- **Access tailgating attack:** Tailgating or piggybacking is the act of **trapping** any authorized staff member in a **restricted-access area**.

Unusual Social Engineering Methods

Fax-based Phishing: When a bank's customers receive a fake email that claims to be from the bank - asking the customer to confirm their access code - by regular email. The customer was asked to print out the form in an email, fill in their details and fax the form to the cyber **criminal's** telephone number.

Traditional Mail Malware Delivery: Cybercriminals use a **home-delivery** service to deliver **CDs** infected with **Trojan** spyware in Japan. The disc was delivered to customers of a Japanese bank. The addresses was firstly stolen from the **bank's database**.

How to Solve anySocial Engineering Attack

To avoid social engineering, you have to practice self-awareness. Always slow down and think before you do anything or react.

Have my feelings increased? When you are particularly curious, scared, or excited, you are less likely to evaluate your actions' results. If your emotional state is advanced, consider it a red flag.

Did the message come from a valid sender? Carefully inspect email addresses and social media profiles when receiving suspicious messages. There could be characters that mimic others, such as "torn@example.com" instead of "tom@example.com." Fake social media profiles that mimic your friend's photo, and many details are also standard.

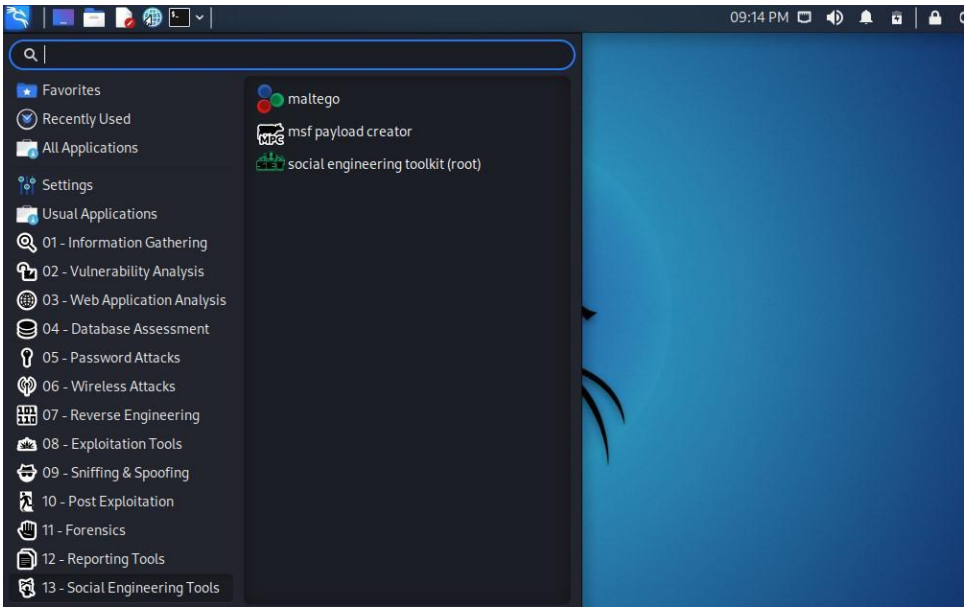
Has my friend sent me the message? It is always good to ask the sender if they were the actual sender of the message in question. They can be hacked, and they may not be detected, or someone may impersonate their accounts.

Are attachments or links suspicious? If a link or filename appears unclear or odd in a message, rethinking the entire communication's authenticity. Besides, consider when the message itself raises an odd reference, time, or other red flags.

Can this person prove his identity? It applies both **in-person** and **online**, as physical violations require that you ignore the attacker's identity.

Social Engineering Tools

Linux offers a bunch of social engineering tools that can be used to perform some of the most common and popular attacks like phishing. you can in the image below we can find these tools in the applications under the social engineering tools categories.



Some of the tools that are often used and popular for social engineering are:

Tool 1: Maltego

It is an OSINT(open source intelligence) investigation tool that shows the information that is linked with each other. This tool is used for finding the relations between people and various other information, like email addresses, social profiles, and many more. Maltego tool offers users to analyze real-time data and helps to gather information from a domain or website, This tool enables users to track data and find connections and relations between different types of data. It uses Graphical data analysis and supports multiple formats of data like Images(bmp, png, and jpg), Generating PDF reports, and Tabular formats like CSV, XLS and graphicML also. Maltego tools are also considered under Intelligence and cyber forensics.

Tool 2: Social engineering Toolkit

It is the most used and popular tool for social engineering among hackers, it is an open-source, python based toolkit that is used for penetration testing. It offers different methods and implementation strategies to perform attacks. This includes tools for website hacking, phishing, and many more to make fake websites just like original ones which let users believe that they are visiting the original websites.

This kit almost covers all the attacks that one can perform with social engineering skills below is the list of all attacks SET offers:

1. Spear phishing attack
2. Website attacks
3. Infectious media generator
4. Payload creation and setting listener

5. Arduino-based hardware attacks
6. Wireless access points attacks
7. QR code-based attacks
8. PowerShell Attacks

Tool 3: MSF payload creator

This is a tool that is used by hackers to generate various Basic interpreter Payloads with the help of MSF venom which comes under the Metasploit framework. it is a wrapper to generate multiple types of payloads, based on user preferences. This tool is very easy to use and comes in handy when you practice using the Metasploit framework for exploitation. MSF venom comes with Metasploit Framework and it is a standard command line interface that allows users to make or generate Basic payloads for platforms like Windows systems, Unix systems, and Android, and many more like backend servers which make this tool so important.

This tool comes in handy when you want to generate basic payloads quickly without altering so many options and parameters. it can also be used to generate a Reverse TCP shell from a running host.

Example 2: Hardware Hacking Through SET (Social Engineering Toolkit)

Well, SET can be used in many ways for outstanding purposes in ethical hacking. we are going to look at a simple example where, we will be sending a malicious website link to our victim's Gmail address, which can lead the victim to reveal credentials, giving access to an attacker without knowing it. To do so we are going to use SET which comes pre-installed in Kali Linux.

We are performing a Mass Mailer Attack with the help of SET.

Step 1: Open the Linux environment and open the terminal, then type setoolkit to open options.

root#-/ setoolkit

Step 2: Choose option 5 to select Mass Mailer Attacker and you will get the output same as below:

Step 3: We will Choose option 1, to perform an E-mail attack for a single email address.

Within this option you can see in the above image we need to provide the target email address, and then we have to specify from where we want to perform the attack.

Step 4: We are going to use option 1, to perform an attack from our own email address to the victim's address.

After **choosing option 1,** you need to provide some information as per the requirements. provide **your email address.** provide the **name of** your target will be shown, from where the email came. Now you need to choose whether you want to **prioritize our message** you can type **yes.** You will see a bunch of other options like attaching an inline file, or a separate file, you can attach if you want but we are only showing you how to perform this attack practically so we are going to avoid these options for now. provide the **subject for your attack email**, this can be anything that interests the victim to click on the link. select the message format, between plain and HTML you can simply go with plain.

Step 5: Now we can type the body of the email basically what your email will consist of, after completing it type END and hit enter.