PRACTICAL REPORT : Social Engineering Lab: Intel Gathering & Vishing Simulation

Aim / Objective

The objective of this practical is to study **social engineering attack techniques** by simulating a **vishing (voice phishing) and pretexting scenario** in a controlled virtual environment. The lab focuses on **open-source intelligence (OSINT) gathering**, **relationship mapping**, and **understanding social engineering payload workflows**, without performing any real attack.

Scope and Ethical Disclaimer

This experiment was conducted **strictly for educational purposes** using:

- Dummy target identities
- Fictional phone numbers
- Role-play based simulations
- No real victims, calls, payloads, or exploitation

The goal is to understand **attacker methodology** in order to design **better defensive controls**.

Tools Used

Tool	Purpose
Kali Linux	Security testing operating system
PhoneInfoga	OSINT tool for phone number analysis
Maltego	Relationship and link analysis
Social-Engineer Toolkit (SET)	Social engineering attack simulation
VirtualBox / VMware	Virtual lab environment

Theoretical :

❖ Social Engineering

Social engineering is a psychological manipulation technique where attackers exploit **human trust, fear, authority, or urgency** to obtain sensitive information. Unlike technical hacking, it targets **people instead of systems**.

Examples:

- Phishing (email)
- Vishing (voice)

- Smishing (SMS)
- Pretexting

❖ Vishing (Voice Phishing)

Vishing is a type of social engineering attack where the attacker uses **phone calls** to impersonate trusted entities (IT support, bank officials) to extract confidential information.

Key characteristics:

- Authority impersonation
- Urgency creation
- Emotional manipulation

❖ Pretexting

Pretexting involves creating a **false but believable story** to convince the victim to share information.

Example:

> “I am calling from the IT department regarding a security incident.”

Pretexting is often used **before phishing or vishing**.

❖ OSINT (Open-Source Intelligence)

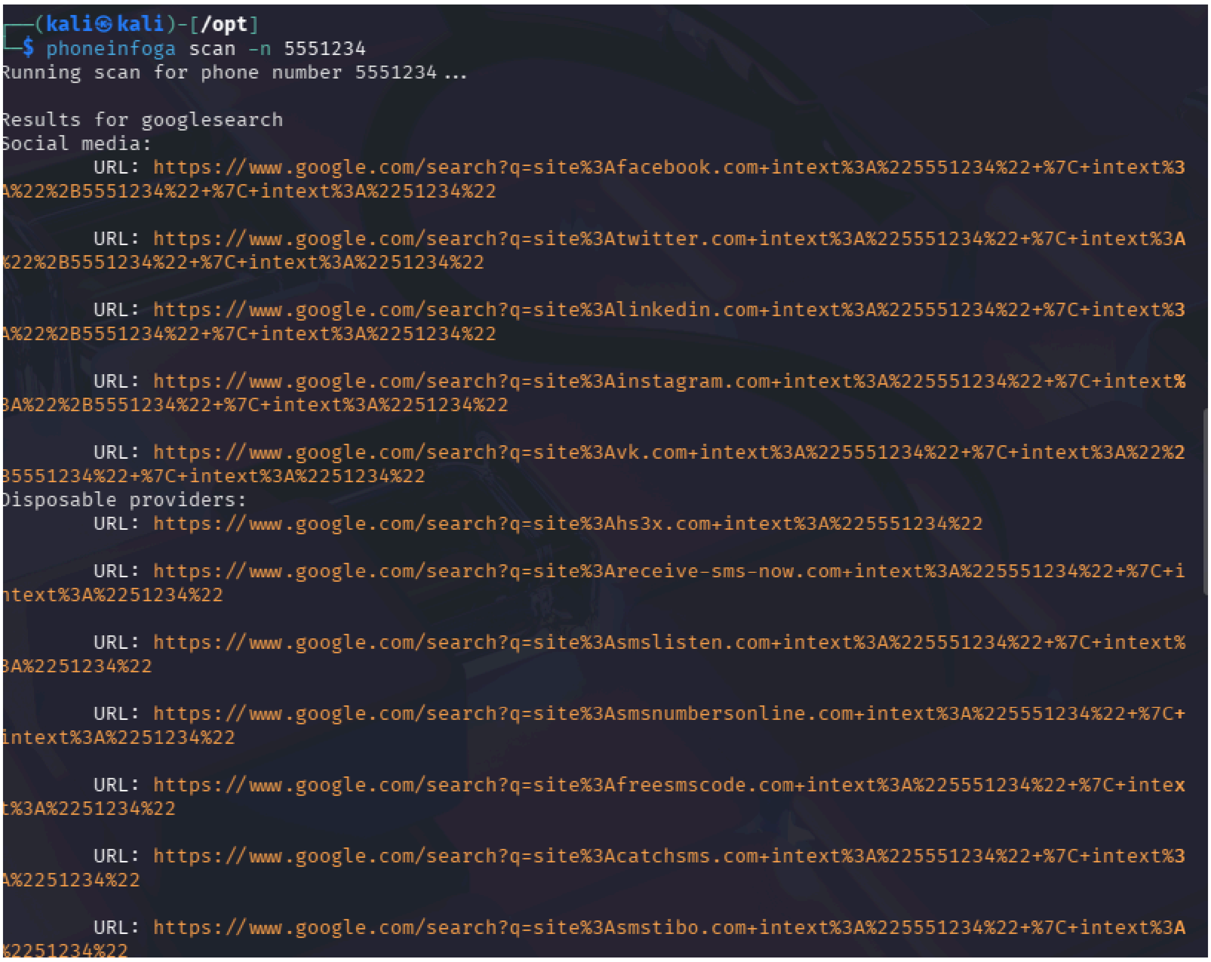
OSINT refers to collecting information from **publicly available sources** such as:

- Phone metadata
- Social media
- Public records
- Search engines

OSINT is legal and widely used in:

- Penetration testing
- Threat intelligence
- Digital forensics

❖ PhoneInfoga



```
┌──(kali㉿kali)-[/opt]
└─$ phoneinfoga scan -n 5551234
Running scan for phone number 5551234 ...

Results for googlesearch
Social media:
        URL: https://www.google.com/search?q=site%3Afacebook.com+intext%3A%225551234%22+%7C+intext%3
A%22%2B5551234%22+%7C+intext%3A%2251234%22

        URL: https://www.google.com/search?q=site%3Atwitter.com+intext%3A%225551234%22+%7C+intext%3A
%22%2B5551234%22+%7C+intext%3A%2251234%22

        URL: https://www.google.com/search?q=site%3Alinkedin.com+intext%3A%225551234%22+%7C+intext%3
A%22%2B5551234%22+%7C+intext%3A%2251234%22

        URL: https://www.google.com/search?q=site%3Ainstagram.com+intext%3A%225551234%22+%7C+intext%
3A%22%2B5551234%22+%7C+intext%3A%2251234%22

        URL: https://www.google.com/search?q=site%3Avk.com+intext%3A%225551234%22+%7C+intext%3A%22%2
B5551234%22+%7C+intext%3A%2251234%22
Disposable providers:
        URL: https://www.google.com/search?q=site%3Ahs3x.com+intext%3A%225551234%22

        URL: https://www.google.com/search?q=site%3Areceive-sms-now.com+intext%3A%225551234%22+%7C+i
ntext%3A%2251234%22

        URL: https://www.google.com/search?q=site%3Asmslisten.com+intext%3A%225551234%22+%7C+intext%
3A%2251234%22

        URL: https://www.google.com/search?q=site%3Asmsnumbersonline.com+intext%3A%225551234%22+%7C+
intext%3A%2251234%22

        URL: https://www.google.com/search?q=site%3Afreesmscode.com+intext%3A%225551234%22+%7C+intex
t%3A%2251234%22

        URL: https://www.google.com/search?q=site%3Acatchsms.com+intext%3A%225551234%22+%7C+intext%3
A%2251234%22

        URL: https://www.google.com/search?q=site%3Asmstibo.com+intext%3A%225551234%22+%7C+intext%3A
%2251234%22
```

PhoneInfoga is an OSINT tool used to gather intelligence about phone numbers, including:

- Carrier information
- Country/region
- Number validity
- Online references

Attackers use it to build **target profiles** before social engineering attacks.

❖ Maltego

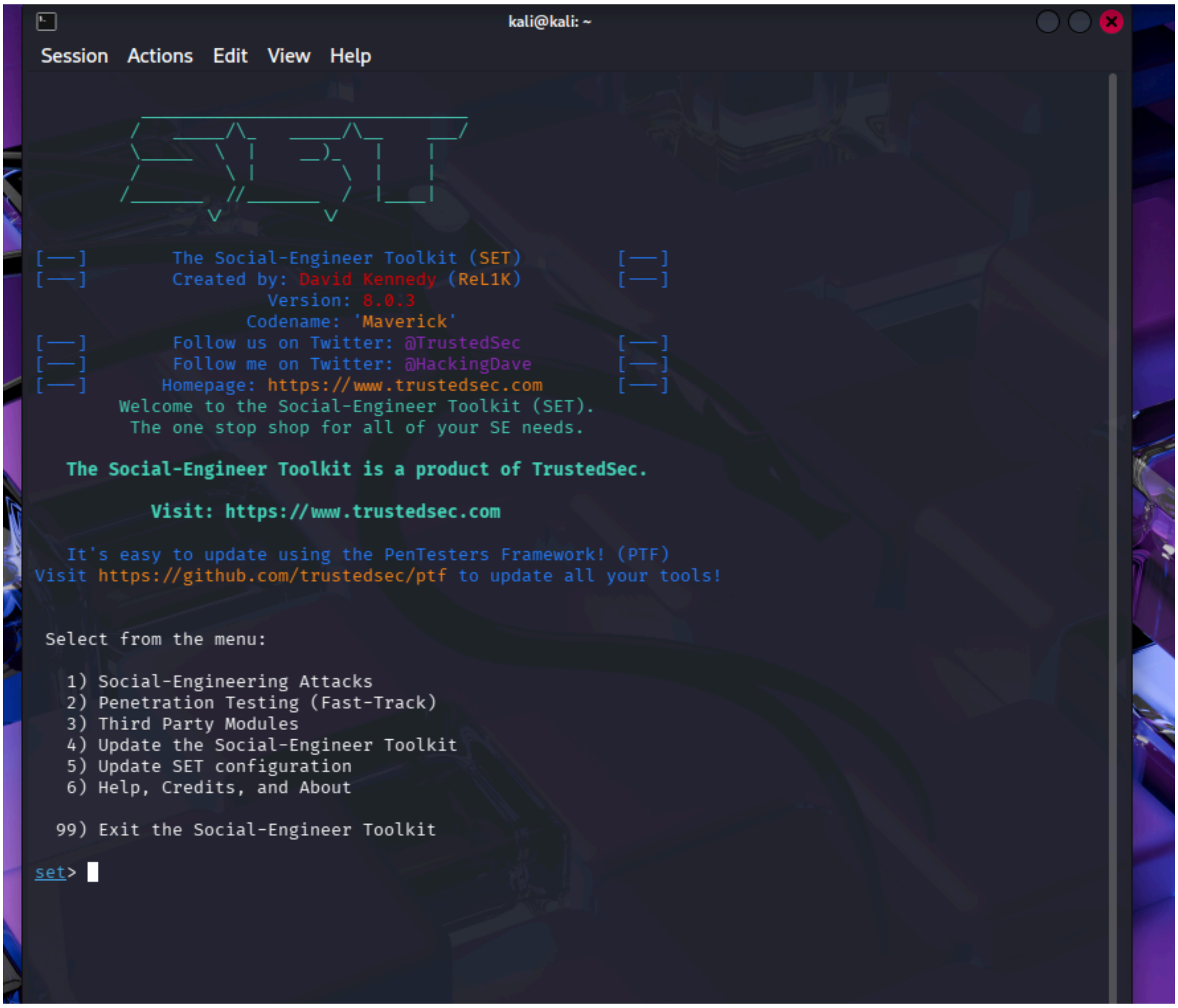
```
1-openjdk-amd64
21-openjdk-amd6
t-java (/usr/li
k-amd64
 /tmp/temp43842
path /tmp/temp4
 /tmp/temp71766
```

Maltego is a link-analysis tool used to visualize relationships between:

- People
- Phone numbers
- Emails
- Domains
- Organizations

It helps attackers correlate scattered data into **actionable intelligence**.

❖ Social-Engineer Toolkit (SET)



```
             _______________________________
            /   _____/\_   _____/\__    ___/
            \_____  \  |    __)_   |    |
            /        \ |        \  |    |
           /_______  //_______  /  |____|
                   \/         \/

[—]        The Social-Engineer Toolkit (SET)         [—]
[—]        Created by: David Kennedy (ReL1K)         [—]
                    Version: 8.0.3
                  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 from the menu:

   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> 
```

SET is a framework designed to simulate social engineering attacks. It includes modules for:

- Phishing
- Payload generation
- Vishing planning
- Attack workflow study

SET is commonly used in **red-team training labs**.

❖ Payload (Theory Only)

A **payload** is a piece of code delivered to a victim system to perform malicious actions such as:

- Reverse shell access
- Remote control
- Data exfiltration

⚠️In this lab, payloads were **not generated or executed**.

Lab Environment

- **OS**: Kali Linux
- **Target**: Dummy target (TID001)
- **Network**: Isolated virtual environment
- **Attack Type**: Simulated vishing & pretexting

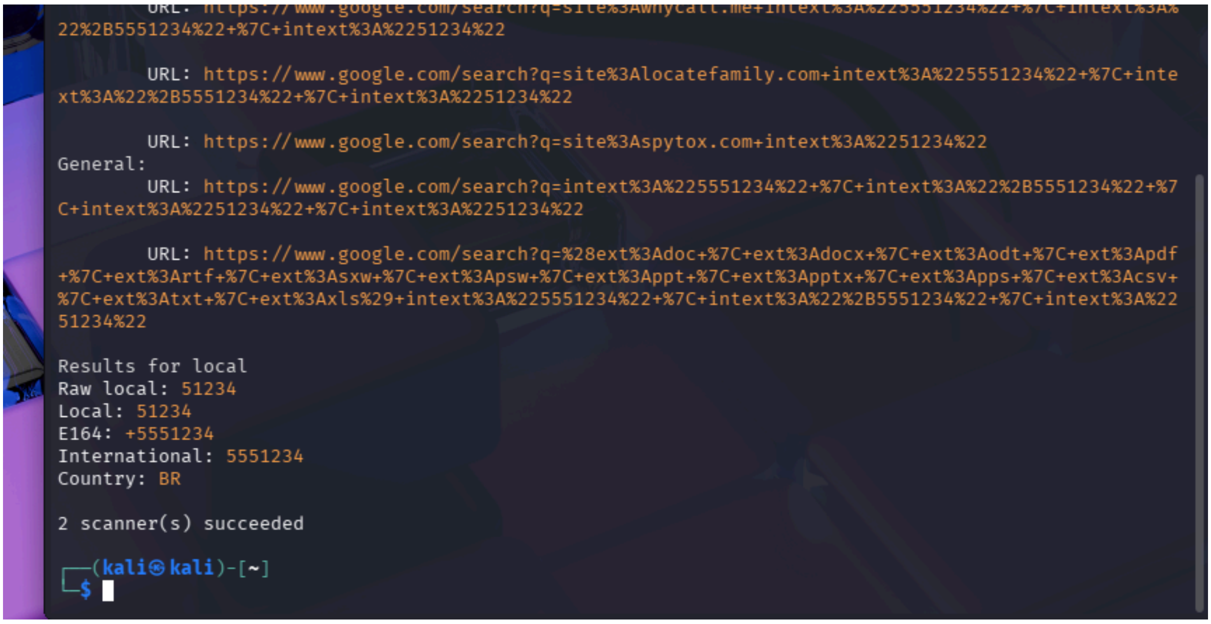
Step-by-Step Methodology

Dummy Target Creation

A fictional target profile was defined.

Attribute	Value
Target ID	TID001
Role	Support Staff (Dummy)
Phone Number	555-1234
Organization	DemoCorp (Fictional)

Intelligence Gathering Using PhoneInfoga



```
        URL: https://www.google.com/search?q=site%3Awhycall.me+intext%3A%225551234%22+%7C+intext%3A%
22%2B5551234%22+%7C+intext%3A%2251234%22

        URL: https://www.google.com/search?q=site%3Alocatefamily.com+intext%3A%225551234%22+%7C+inte
xt%3A%22%2B5551234%22+%7C+intext%3A%2251234%22

        URL: https://www.google.com/search?q=site%3Aspytox.com+intext%3A%2251234%22
General:
        URL: https://www.google.com/search?q=intext%3A%225551234%22+%7C+intext%3A%22%2B5551234%22+%7
C+intext%3A%2251234%22+%7C+intext%3A%2251234%22

        URL: https://www.google.com/search?q=%28ext%3Adoc+%7C+ext%3Adocx+%7C+ext%3Aodt+%7C+ext%3Apdf
+%7C+ext%3Artf+%7C+ext%3Asxw+%7C+ext%3Apsw+%7C+ext%3Appt+%7C+ext%3Apptx+%7C+ext%3Apps+%7C+ext%3Acsv+
%7C+ext%3Atxt+%7C+ext%3Axls%29+intext%3A%225551234%22+%7C+intext%3A%22%2B5551234%22+%7C+intext%3A%22
51234%22

Results for local
Raw local: 51234
Local: 51234
E164: +5551234
International: 5551234
Country: BR

2 scanner(s) succeeded

┌──(kali㉿kali)-[~]
└─$ 
```

Command executed:

phoneinfoga scan -n 5551234

Observed Data:

- Phone number format
- Regional metadata
- Limited OSINT references

Problem Faced:

- Limited results returned

Reason:

- Dummy phone number used

Resolution:

- Data treated as simulated OSINT output

Relationship Mapping Using Maltego

Steps:

1. Launch Maltego
2. Create a new graph
3. Add Phone Number entity
4. Run OSINT transforms

Observation:

- Minimal results due to fictional data

Solution:

- Relationships manually documented for simulation

Intelligence Log

Target ID	Data Source	Information	Notes
TID001	PhoneInfoga	Phone: 555-1234	Dummy
TID001	Maltego	Org association	Simulated

Social Engineering Simulation Using SET

SET was launched:

sudo setoolkit

Menu path followed:

Social-Engineering Attacks

→ Create a Payload and Listener

At the payload selection screen, various payload options were displayed such as:

- Reverse TCP shell
- Meterpreter payloads
- HTTPS-based payloads

⚠️ **No payload was selected or generated.**

Mock Vishing Script

A pretext-based vishing script was designed.

Sample Script:

> “Hello, this is Alex from the IT security team. We detected suspicious login activity on your account. To prevent suspension, I need to verify your employee ID.”

The script was tested via **role-play only**.

Impact Analysis (Theoretical)

If such an attack were executed in real life, it could result in:

- Credential theft
- Unauthorized system access
- Data breaches
- Further network compromise

This demonstrates that **human vulnerability is a major security risk**.

Mitigation and Defensive Measures

1. Security awareness training
2. Caller verification procedures
3. Multi-factor authentication (MFA)
4. Incident reporting policies
5. Zero-trust communication
6. Regular social engineering drills

Result

- ❖ OSINT gathering simulated successfully
- ❖ Relationship mapping demonstrated
- ❖ Vishing and pretexting workflow understood
- ❖ SET payload workflow observed ethically

Conclusion

This demonstrated how attackers leverage **OSINT tools and psychological manipulation** to conduct social engineering attacks. Even without exploiting technical vulnerabilities, attackers can gain sensitive information by exploiting human trust. Proper training, verification mechanisms, and awareness are critical defenses against such attacks.