What is Social Engineering

Cyberattacks where attackers trick people into divulging sensitive information or performing actions they wouldn't normally do. The success of a social engineering attack depends on the attacker's ability to manipulate the victim's trust and emotions and can have serious consequences such as data breaches, identity theft, and financial loss.

4 million

IBM reports in their 2022 Cost of a Data Breach report that the average cost of a data breach with social engineering as the initial attack vector surpassed a cool $4 million.

Types of Social Engineering

Vishing

Attackers use telephony to trick people into falling for a scam

Phishing

Attackers send malicious emails designed to trick people into falling for a scam.

Whaling

a highly targeted phishing attack - aimed at senior executives - masquerading as a legitimate email.

Shoulder-surfing

a technique used to obtain information such as personal identification numbers, passwords, and other confidential data by looking over the victim's shoulder

Social engineering defenses

Controls & Policies

- Time-based account access control (TAAC)
- Role-based access control (RBAC),
- Multi-factor authentication (MFA)

Security Awareness Training

Educate users on types of social engineering methods, train users, and raise awareness on best practices to counter or defend against social engineering

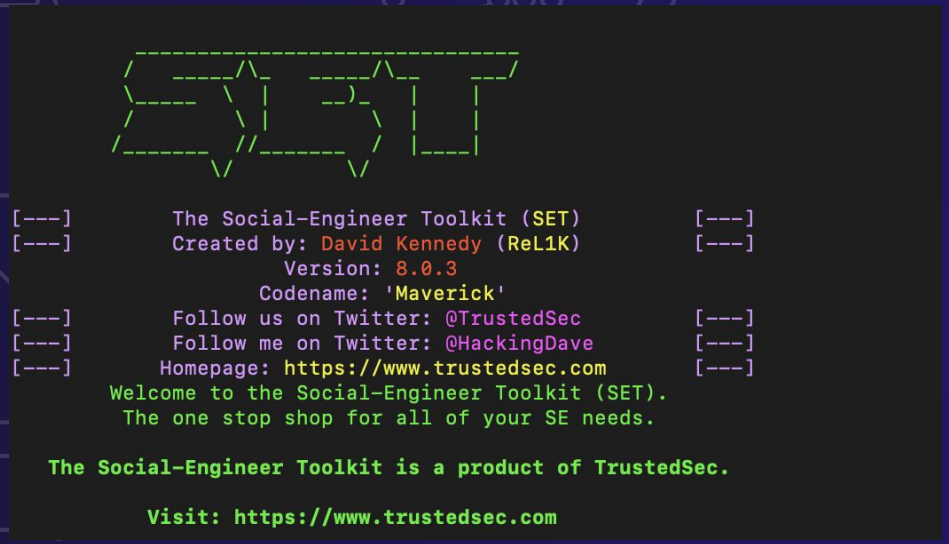
Technologies

- Spam filters and secure email gateways
- Firewalls

Free Dedicated phishing simulation tools

- Gophish
  Evilginx
- Social-Engineer Toolkit (SET)
- Phishing Frenzy
- BeEF

SET



For a cyber range, the Red Team can stimulate social engineering attacks with SET to provide real-life examples of how attackers operate. Clients and organizations can identify behaviors to look out for to mitigate risks.

SET using Kali Linux to stage attack:

1. https://github.com/trustedsec/social-engineer-toolkit

2. https://www.youtube.com/watch?v=F8tUPeMl_DU&ab_channel=SatishCJ

SET

1. SSH into Kali Linux

```
nancyuddin@Nancys-MacBook-Air downloads % ssh -i "kali.pem" kali@34.239.156.1
The authenticity of host '34.239.156.1 (34.239.156.1)' can't be established.
ED25519 key fingerprint is SHA256:3cTSNtCPzvFwqfQlfaq2xyzTUCDK0iCx8rAKCOHdTzo.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:19: 3.229.138.71
    ~/.ssh/known_hosts:29: 44.210.240.161
```

2. Enter the root user

```
┌──(kali㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/kali]
└─#
```

SET

3. Enter SET

```
┌──(root㉿kali)-[/home/kali]
└─# setoolkit
```

4. There are several options on which attack you want to administer

```
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
```