

Social Engineering Attacks Module-9

Social engineering consists in manipulating people to obtain sensitive information or to perform actions that could lead to a security incident. It is a formidable method of attack which makes it possible to bypass technical protections even if they are solid

The aim of a **social engineering audit** is twofold: to assess the reflexes of employees in order to find out the company's degree of vulnerability, and to make them aware of this type of attack through concrete situations that can make an impression.

Understanding Social Engineering

There are many different methods for performing penetration testing, which evaluates the security posture of a company, but in this article, we are going to focus on one: social engineering.

Social engineering penetration testing focuses on people and processes and the vulnerabilities associated with them. These pen tests typically consist of an ethical hacker conducting different social engineering attacks such as phishing, USB drops, or impersonation that a person could face during the course of their work. The goal of this test is to identify weaknesses in a person, group of people, or process and identify vulnerabilities with a clear path to remediation.

Your challenge

Social engineering is a proven attack vector for attackers to gain access to your organisation. Cyber criminals use social engineering techniques to influence employees into giving up privileged information or access to an organisation.

Social engineering is popular among criminal hackers because it can be easier to exploit people than to find a network or software vulnerability. By gaining access to the building or the network, an attacker can access data, steal assets or even harm people.

What Are Social Engineering Attacks?

Social engineering attacks come in a variety of forms, but the most common are phishing, vishing, smishing, impersonation, dumpster diving, USB drops, and tailgating.

Phishing

Phishing is a method that occurs via email and attempts to trick the user in to giving up sensitive information or opening a malicious file that can infect their machine.

Vishing

Vishing is similar to phishing but occurs via phone calls. These phone calls attempt to trick the user into giving up sensitive information.

Smishing

Smishing is similar to phishing but occurs via sms text messages. These text messages have the same intent as phishing.

Impersonation

Impersonation is a method where the attacker attempts to fool a person into believing they are someone else.

For example, an attacker could impersonate an executive with the goal of convincing employees to provide financial payments to fictitious vendors or to grant access to confidential information.

An impersonation attack could also target a user with the goal of gaining access to their account. This could be accomplished by requesting a password reset without the administrator verifying their identity.

Another example of this attack would be pretending to be a delivery person. In some cases, delivery personnel have little restrictions and can gain access to secure areas without question.

Dumpster Diving

Dumpster diving is a method where an attacker goes through not only trash but other items in plain sight, such as sticky notes and calendars, to gain useful information about a person or organization.

USB Drops

USB drops is a method that uses malicious USB's dropped in common areas throughout a workspace. The USBs typically contain software that, when plugged in, install malicious software that can provide a backdoor into a system or transfer files with common file extensions.

Tailgating

Tailgating is a method that is used to bypass physical security measures. You typically see this method used in locations that require a person to scan a key fob to gain entrance.

In this type of attack, the attacker will follow closely behind an employee and enter the room when they scan their key fob and open the door.

Benefits of Social Engineering

Social engineering pen testing can provide some significant benefits when it comes to testing the security of your organization. Some of the key benefits include:

- Establish the information that an attacker could obtain about your organisation that is freely available in the public domain;
- Establish how susceptible your employees are to social engineering attacks;
- Determine the effectiveness of your information security policy and your cyber security controls to identify and prevent social engineering attacks; and
- Develop a targeted awareness training programme.

The Social-Engineer Toolkit (SET)

The Social-Engineer Toolkit is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack quickly. SET is a product of TrustedSec, LLC – an information security consulting firm located in Cleveland, Ohio

User Manual of SET



PDF file



Other Phishing Tool

PyPhisher

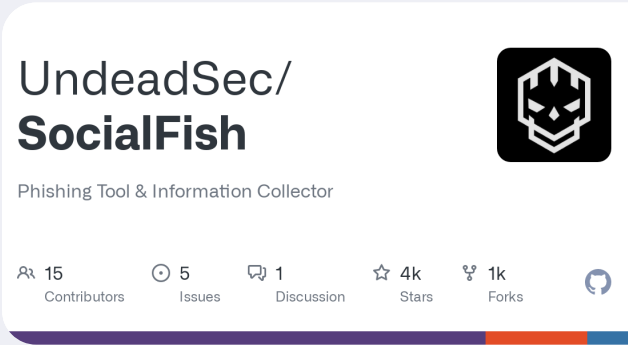
- `git clone https://github.com/KasRoudra/PyPhisher`
- `cd PyPhisher`
- `python3 pyphisher.py`

OR



GitHub - htr-tech/zphisher: An automated phishing tool...

An automated phishing tool with 30+ templates. This Tool is made for educational purpose only ! Author will not be responsible for any misus...



GitHub - UndeadSec/SocialFish: Phishing Tool &...

Phishing Tool & Information Collector . Contribute to UndeadSec/SocialFish development by creating an account on GitHub.



GitHub - htr-tech/nexphisher: Advanced Phishing tool

Advanced Phishing tool. Contribute to htr-tech/nexphisher development by creating an account on GitHub.


SPOOFING

Spoofing is a technique in which someone or something impersonates or mimics something else in order to deceive, manipulate, or gain unauthorized access to a system, network, or information. It is often used for malicious purposes.

Email Spoofing

Email spoofing involves sending an email that appears to come from a different sender than the actual one. This can be used for phishing attacks, where the attacker tries to trick the recipient into revealing sensitive information or clicking on malicious links.

Steps

 app.brevo.com

Brevo

[🔗](#)

Now we clone sendmail of github
`git clone https://github.com/mogaal/sendmail.git`

now let change to sendmail file so type
`cd sendmail`

now what we do it type `./sendmail --help`

so we wanna send the email to target first of all we type `sendmail -f test@test.com -t test@test.com -u "hello" -m "i how are you" -s mail.smtp2go.com:2525 -xu test@test.com -xp *****`

-f is the email u wanna use

-t is the targets email

-u is the subject of the email

-m is the message of the email we you can add links

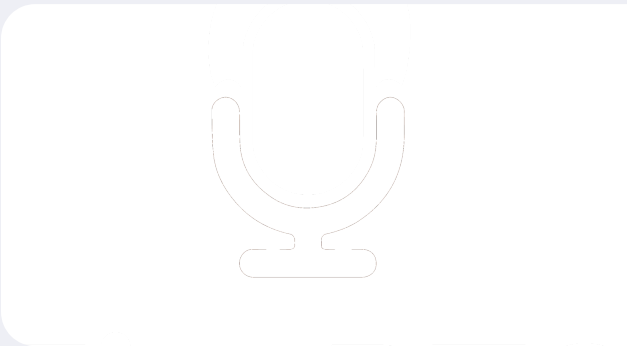
-s u add thte smtp server url and posts


-xu is the email you use to log in

-xp is the password of the server

Caller ID Spoofing

Caller ID spoofing is indeed a common practice used in telecommunications to deceive recipients about the true identity of a caller. It allows the caller to manipulate the phone number displayed on the recipient's caller ID to make it appear as if the call is coming from a different, often legitimate, or trusted source. While it can be used for legitimate purposes, such as maintaining privacy, it is often associated with fraudulent activities, including telemarketing scams, phishing, and other forms of social engineering.



 FireRTC - No Nonsense Free Phone Calls To the US and Canada

FireRTC - No Nonsense Free Phone Calls To the US and...

FireRTC enables you to make and record phone calls right from your Chrome or Firefox web browser for free.

[🔗](#)