

C|PENT

Certified Penetration Testing Professional



Module 04

Social Engineering Penetration Testing

MODULE OBJECTIVE

Learn how to implement a comprehensive penetration testing methodology for assessing human behaviors that increase susceptibility to potential social engineering attacks.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objective

Social engineering is one of the most attempted malicious activities that attackers use to gain access to the sensitive data of an individual or an organization. Social engineering penetration testing refers to the process of evaluating the security of an organization against potential social engineering attacks. This module discusses the process of performing social engineering penetration tests to test the susceptibility of the employees of an organization to social engineering attacks. It also describes the skills and tools required for various stages of penetration testing (also called “pen testing”).



Social Engineering Penetration Testing Concepts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering Penetration Testing Concepts

This section introduces social engineering penetration testing, skills required to perform pen tests, black- and white-box pen testing, and different testing modes.

Social Engineering Penetration Testing: An Overview



- Social engineering is the art of **manipulating people to divulge sensitive information** with the objective of performing a malicious action.



- The objective of performing social engineering penetration testing is to **test the strengths and weaknesses of human factors** in a security chain within the organization.



- Social engineering pen test is often used to **raise the level of security awareness among employees** by allowing them to experience a real attack, without having an actual breach.



- The tester **should demonstrate extreme care and professionalism** when conducting the social engineering pen test, as it might involve legal issues such as violation of privacy and may create embarrassing situations for the organization.



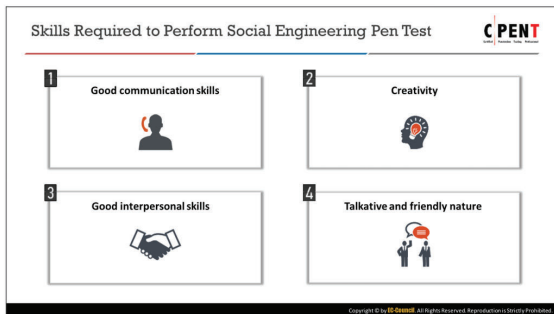
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering Penetration Testing: An Overview

Social engineering is the art of manipulating people to divulge sensitive information with the objective of performing a malicious action. Social engineering penetration testing involves using various techniques to trick the employees of the target organization into disclosing sensitive information or perform actions that create security vulnerabilities that can be further exploited by the attacker.

The objective of performing social engineering penetration testing is to test the strengths and weaknesses of human factors in a security chain within the organization. It also checks the commitment of the employees towards protecting the organization's sensitive data, their awareness regarding social vulnerabilities, their ability to comply with security policies, and the effectiveness of the security training. A pen tester should first obtain the appropriate authorization from the organization's administrators to perform social engineering. The pen tester must gather all the relevant information about the employees and then implement various social engineering techniques to lure employees into revealing the organization's sensitive information. To succeed, the pen tester needs to take a special interest in developing social engineering skills and must be proficient enough that the victims do not even notice the fraud.

The pen tester needs to design social engineering penetration tests that mimic real attacks by employing various techniques that include all methods such as phone, email or online, and physical intrusions. After the completion of the tests, the pen tester needs to generate a full report of the findings and their mitigation recommendations. This report must include measures that correct existing issues and prepare the organization against future attacks. The tester should demonstrate extreme care and professionalism when conducting the social engineering pen test, as it might involve legal issues such as violation of privacy and may create embarrassing situations for the organization.



Skills Required to Perform Social Engineering Pen Test

Social engineering penetration tests require tricking target employees into disclosing sensitive private or professional data, corrupting their computers with malware, or enticing them to click links to malicious sites. Therefore, pen testers should possess the following skills to persuade or elicit the targets into performing favorable actions.

- **Good communication skills:** To perform social engineering, penetration testers must have good verbal and nonverbal communication skills. These skills will help them confidently present themselves as vendors or customers and manipulate targets to reveal private information. Good verbal skills will help in direct or mobile conversations, while nonverbal skills will make it easy to create efficient phishing emails.
- **Creativity:** Being creative helps testers think of fake events, scenarios, and messages based on the interests of the targets to provoke them into revealing information. Pen testers use the social media activities of victims to determine their interests, after which they use their creativity to build scenarios based on these results. In addition, creativity helps in devising and implementing strategies that testers can use to take advantage of new technologies and situations within an organization.
- **Good interpersonal skills:** Interpersonal skills include skills such as listening, questioning, and understanding the body language of a person. These skills help testers build rapport with the victims, gain their trust, and request them to provide the required data.
- **Talkative and friendly nature:** Having an extroverted and outgoing personality may help the pen tester, as the victim may be more willing to converse and reveal sensitive information.

Black-Box or White-Box Testing?



Black-Box

- ✚ The **client/organization provides information** such as names, phone numbers, e-mail addresses, and location of the target to be tested.



White-Box

- ✚ The **tester needs to obtain information** about the target using open source intelligence (OSINT) techniques.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Black-Box or White-Box Testing?

We now discuss two techniques of social engineering penetration testing, namely, black-box or white-box testing. These techniques differ in terms of the information disclosed by the organization to the tester.

▪ White-box social engineering penetration testing

In white-box social engineering penetration testing or clear-box testing, the organization provides testers with the information of target employees. The provided information includes names, phone numbers, email addresses, and location of the target. In some cases, the organization may also define specific social engineering methods that the tester needs to implement.

Advantages:

- The clients can decide the target and the information they need to test.
- It helps in detecting insider threats quickly.
- Testing consumes less time, as the client provides most of the information about the target and the organization's security structure.

Disadvantages:

- The scope of testing is limited to the assigned targets only.
- This method may not cover physical means of accessing information.

▪ Black-box social engineering penetration testing:

In black-box social engineering penetration testing, also called a trial-and-error approach, the client does not provide any information about the target to the tester.

The tester must employ open-source intelligence techniques to gather information about the targets. This technique is the same as real-world social engineering attack situations. This type of testing is time-consuming, as the tester needs to collect information about the employees, systems, and security, and implement customized techniques based on the target.

Advantages:

- This method mimics real-life attack situations.
- Testers can decide the type and methods of the attack.

Disadvantages:

- This type of testing is difficult to design due to the wide range of targets.
- Gathering information is time-consuming.

Social Engineering Penetration Testing Modes

Off-Site Testing

- Off-site testing involves testing the employees' **security awareness** during their daily activities.
- Techniques used:
 - Phishing
 - Vishing
 - SMishing



On-Site Testing

- On-site testing involves testing the **physical security** of an organization and the security policies in place.
- Techniques used:
 - Piggybacking/Tailgating
 - Eavesdropping
 - Shoulder surfing
 - Baiting
 - Reverse Social Engineering
 - Dumpster Diving
 - Elicitation
 - Motivation Techniques

Note: Eavesdropping can be used for both on-site and off-site testing.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering Penetration Testing Modes

When considering security, users are believed to be the weakest link; however, many organizations allow users to have more than the necessary privileges to perform their jobs. Social engineering pen testing allows the pen tester to test such types of users and identify those who are susceptible to social engineering tactics.

Social engineering pen testing involves two different modes, namely off-site testing and on-site testing:

■ Off-site testing

Off-site testing involves testing employees' security awareness during their daily activities. To perform off-site social engineering pen testing, first, the tester needs to gather publicly available information about the organization through passive reconnaissance techniques. The tester can obtain important information from the company's website, search engines, social networking sites, the company's annual reports, etc.

Techniques used in off-site social engineering include the following:

○ Phishing

Phishing is a technique in which the pen tester sends an email or provides a link that falsely claims to be from a legitimate site in an attempt to acquire a user's personal or account information. When the user clicks on the email link, it redirects them to a fake webpage, where they are lured into sharing sensitive details such as address and credit card information without knowing that they are on a phishing site.

- **Vishing**

Vishing (voice phishing or Voice over IP (VoIP) phishing) is an impersonation technique in which the pen tester uses VoIP technology to trick individuals into revealing their critical financial and personal information. In this technique, pen testers call employees, pretending to be a customer or vendor who needs assistance and requests them for information. Pen testers generally choose nontechnical employees and request them to provide basic information regarding the organization. The testers can also use real names of vendors or customers associated with the organization to convince the employees. After gaining their trust, pen testers try to gather sensitive information.

- **SMiShing**

In SMiShing (SMS Phishing), the SMS text messaging system is used to lure users into instant action such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number. SMiShing messages are crafted to provoke an instant action from the victim, requiring them to divulge their personal information and account details.

- **On-site testing**

On-site testing involves testing the physical security of an organization and the security policies in place. To perform on-site social engineering pen testing, the pen tester disguises themselves as an authorized person to enter the target premises.

Techniques used in on-site social engineering include the following:

- **Piggybacking**

Piggybacking usually implies entry into the building or security area with the consent of an authorized person who is not aware of the pen tester's identity. For example, pen testers request an authorized person to unlock a security door, saying that they have forgotten their ID badge. In the interest of common courtesy, the authorized person might allow the pen tester to pass through the door.

- **Tailgating**

Tailgating implies access to a building or secured area without the consent of an authorized person. It refers to the act of following an authorized person through a secure entrance, exploiting the fact that a polite user opens and holds the door for those following them. In this technique, a pen tester wears a fake badge/ID and attempts to enter the secured area by closely following an authorized person through a door requiring key access.

- **Eavesdropping**

Eavesdropping refers to an unauthorized person listening to a conversation or reading others' messages. It includes interception of any form of communication, including audio, video, or written communication, using channels such as telephone lines, email, and instant messaging. The pen tester can obtain sensitive information such as passwords, business plans, phone numbers, and addresses.

- **Shoulder surfing**

Shoulder surfing is the technique of observing or looking over someone's shoulder as they key in information into a device. The pen tester can use shoulder surfing to find out passwords, personal identification numbers (PINs), account numbers, and other information.

- **Baiting**

Baiting is a technique in which pen testers tempt the target user with something alluring in exchange for important information such as login details and other sensitive data. In this technique, pen testers leave a physical device such as a USB flash drive containing malicious files in locations where people can easily find them including parking lots, elevators, and bathrooms. This physical device is labeled with a legitimate company logo relevant to the target user, which is used to trick them into finding and open such devices on their systems. Once the device is connected and opened by the victim, a malicious file gets downloaded and the system becomes infected, which allows pen testers to take control over the victim's system.

- **Reverse social engineering**

In reverse social engineering, the pen tester assumes the role of a person in authority so that employees ask them for information. The pen tester manipulates the questions that employees ask in a manner than the employees themselves give up the required information.

- **Dumpster diving**

Dumpster diving is the process of retrieving sensitive personal or organizational information by searching through trash bins. The pen tester can extract confidential data such as user IDs, passwords, policy numbers, network diagrams, account numbers, bank statements, salary data, source code, sales forecasts, access codes, phone lists, credit card numbers, calendars, and organizational charts on paper or disk.

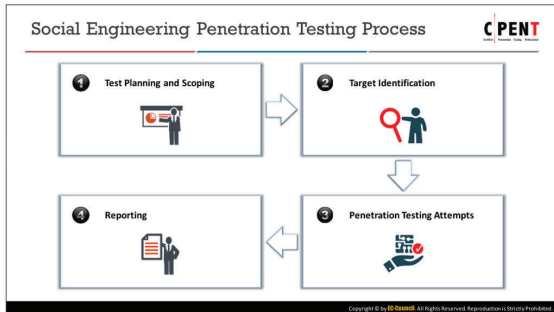
- **Elicitation**

Elicitation is the technique of extracting information from the victim by drawing them into normal and disarming conversations. To elicit information, the pen tester needs to initiate a casual conversation with the target user to extract information without making them realize that they are being socially engineered.

- **Motivation techniques**

The pen tester can use motivation techniques such as authority, intimidation, consensus/social proof, scarcity, and urgency, in order to make the victims reveal sensitive information about the organization.

Note: Eavesdropping can be used for both on-site and off-site testing.



Social Engineering Penetration Testing Process

To perform social engineering penetration testing, the pen tester needs to follow the below-mentioned four well-defined steps.

- **Step 1:** Test Planning and Scoping
- **Step 2:** Target Identification
- **Step 3:** Penetration Testing Attempts
- **Step 4:** Reporting

Step 1: Test Planning and Scoping



- The pen tester needs to **conduct a meeting** between the management of the client organization and the pen testing team to **define the scope** of pen testing and decide how to perform it.



- The scoping document must contain all the **techniques and methods** to be used in the pen test.



- Test planning and scoping **help you create a clear contract** that is agreed upon and signed by all parties involved before the pen testing is undertaken.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Step 1: Test Planning and Scoping

Test planning and scoping is the most important step in social engineering pen testing. In this step, the pen tester must define the scope of pen testing and decide how to perform it. To perform this, the pen tester needs to conduct a meeting between the management of the client organization and the pen testing team. The number of people involved in the team must be as minimum as possible to prevent more people from knowing about the test and to obtain accurate results from the test.

The scoping document must contain all the techniques and methods to be used in the pen test. For example, if the pen tester intends to use piggybacking/tailgating, these must be clearly specified in the scope of the test.

Test planning and scoping help create a clear contract that is agreed upon and signed by all the parties involved before the pen test is undertaken. This contract document is key to the success of the pen test.

Do Remember: Before Social Engineering Pen Test



"Penetration testers must be aware of local laws, as some of their actions may infringe on liberty, resulting in potential legal action."

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Do Remember: Before Social Engineering Pen Test (Cont'd)



"Be aware of social engineering pretext agreed to in the Rules of Engagement (ROE)."

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Do Remember: Before Social Engineering Pen Test

Penetration testers must be aware of local laws, as some of their actions may infringe on liberty, resulting in potential legal action. Therefore, it is necessary to read and understand the operating laws of the region where tests are being conducted prior to initiating them.

Pen testers must be aware of the social engineering pretext agreed to in the rules of engagement (ROE). They must assess the scope and limitations of the tests agreed upon in the contract and strictly adhere to them.

Step 2: Target Identification



- Based on the scoping document and pen testing contract, you need to identify the victim.
- Choose **victims** or **groups of victims** who can be easily tricked.

Common Targets of Social Engineering Pen Test

- Users/Clients
- Receptionists/Help-desk personnel
- Vendors of the organization
- Technical support executives
- System administrators
- Disgruntled/Mistreated Employees
- Employees who are less aware
- Recently fired employees

Gather Information About the Targets

- Search for names, phone numbers, designation, and other details of employees on the company's website.
- Search through online platforms, phone, and email.
- Search using social networking sites.
- Search on job sites such as LinkedIn and Glassdoor.

Note: For complete coverage of information gathering techniques, refer to Module 03 Open Source Intelligence (OSINT) Methodology.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Step 2: Target Identification

Based on the scoping document and pen testing contract, the pen tester needs to identify a victim carefully. A single victim or groups of victims who can easily be tricked should be chosen.

Common Targets of Social Engineering Pen Tests

Penetration tests can find suitable victims by searching for names, phone numbers, designation, and other employee details on the company's website; selecting those employees who are accessible through online platforms, phone, and email as the primary targets of the tests; and using professional and social networking sites to find employees who share their personal and professional information across those sites. The pen tester can search for job sites such as LinkedIn and Glassdoor to track the reviews and comments posted by current and former employees.

Note: For complete coverage of information gathering techniques, refer to *Module 03: Open Source Intelligence (OSINT) Methodology*.

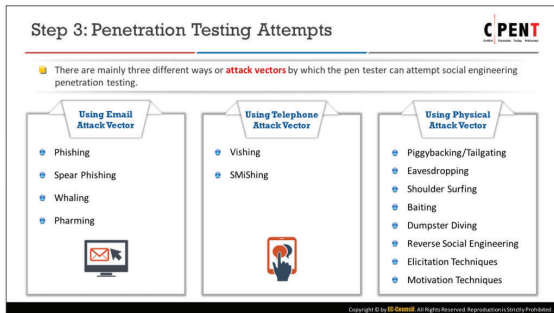
Apart from these employees, pen testers can try to befriend nontechnical staff, including janitors, security personnel, and support staff to gain access to trash dumps and other physical resources.

The most common targets of social engineering penetration testing are discussed below:

- Users/clients:** Pen testers can approach users and clients of the target organization, pretending to be a tech support personnel to extract sensitive information.
- Receptionists and help-desk personnel:** Pen testers can approach receptionists, service-desk, or help-desk personnel of the client organization in order to trick them into divulging confidential information about the organization. To extract information, such

as a phone number or a password, the tester must first win the trust of the individual who has the information. On winning their trust, the pen tester can manipulate them to get valuable information. Receptionists and help-desk staff may readily share information if they feel that they are doing so to help a customer.

- **Vendors:** Pen testers may also target the vendors of the organization to gain critical information that could be helpful in executing other attacks.
- **Technical support executives:** Another target of social engineering pen testing is technical support executives. The pen testers may contact technical support executives to obtain sensitive information by pretending to be senior management, customer, vendor, and so on.
- **System administrators:** A system administrator in an organization is responsible for maintaining the IT systems, and they may thus have critical information such as the type and version of operating system and admin passwords that could be helpful for a pen tester in planning an attack.
- **Disgruntled/mistreated employees:** Unhappy employees or contract workers who are not satisfied with the organization are a good target for social engineering tactics. Disgruntled employees, who intend to take revenge on their company, are easy prey to social engineering tactics and will always be ready to compromise the security of the organization.
- **Employees who are less aware:** Newly joined employees or employees who are less aware of the security policies of the organization could be easily tricked. Pen testers can approach such employees to gather sensitive information about the organization.
- **Recently fired employees:** Recently fired employees will most certainly be dissatisfied with the company and might even be ready to share secrets about the company with strangers. Pen testers can approach such employees to obtain more information about the company.



Step 3: Penetration Testing Attempts

There are mainly three different ways or attack vectors by which the pen tester can attempt social engineering penetration testing.

■ Using email attack vector

The pen tester can leverage the email addresses collected in the target identification phase to perform email-based social engineering attacks. They can send phishing or spear-phishing emails to the victims, trick them, and gather sensitive information. They can also actively gather information using email messages.

The tester can perform the following attacks using the email attack vector:

- Phishing
- Spear phishing
- Whaling
- Pharming

■ Using telephone attack vector

Using a telephone attack vector is the oldest and most effective social engineering technique. The pen tester can use the telephone numbers of the employees to send fake SMS or make fake calls masquerading as a legitimate bank professional and trick them into revealing sensitive information. Social engineering using telephone calls not only reveals sensitive information; in some cases, it can even compromise the security of the whole organization.

The pen tester can perform the following attacks using telephone attack vector:

- Vishing
- SMiShing

▪ **Using physical attack vector**

Using a physical attack vector, the pen tester can test the physical security of an organization or building. Based on the gathered information such as employee names, their designations, contact details, and company information, the pen tester must focus on entering the buildings of the target company. The pen tester must create various target scenarios based on the identified target in order to identify specific vulnerabilities and meet clear objectives.

Before using the physical attack vector, the pen tester must gather the following information:

- How many branches does the company have?
- Does the company have any other businesses?
- Does the company have secured parking lots?
- Does the company have a trained security guard or guards?
- Is the security guard's office located outside or inside?
- Is the main reception secured?
- How many people work in the reception at any one time?
- Does the company implement security controls such as radio-frequency identification (RFID) or magnetic strip tags?
- Who are the third parties working with the target company?

The above information will help the tester in creating various targeted social engineering scenarios to gain physical access to the target company and identify physical vulnerabilities in the company's security systems.

The pen tester can perform the following attacks using the physical attack vector:

- Piggybacking/Tailgating
- Eavesdropping
- Shoulder surfing
- Baiting
- Dumpster diving
- Reverse social engineering
- Elicitation techniques
- Motivation techniques

Please note that **Step 4: Reporting** is explained at the end of this manuscript under the main section "Reporting and Countermeasures/Recommendations."



Social Engineering Penetration Testing Using E-mail Attack Vector

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

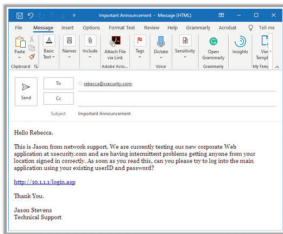
Social Engineering Penetration Testing Using E-mail Attack Vector

Pen testers can leverage various open source intelligence (OSINT) gathering techniques to harvest the business email addresses of the target organization employees and use them in various social engineering tests. The information gathered through emails helps the pen testers in designing other pen tests that mimic real-life attacks. In this section, you will learn how to use the email attack vector for performing social engineering attempts through phishing and gather sensitive information from the target.

Attempt Social Engineering Using Email



- The pen tester creates a web page that **spoofs the company's identity**.
- The pen tester sends an email to an employee of the company to visit <http://x.x.x.x/login.asp>? and asks them to **log in again** to activate the **server upgrade**.
- The email should look **legitimate** and **authentic** (company fonts, colors, logo, etc.)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Social Engineering Using Email

A common social engineering method is to send an email posing as a member from a technical support team. The tester can send a fake mail that informs the user about the migration or upgradation of the company's web server. A link to the fake website is included in the mail, and the user is asked to click on the link to log into the new application to activate their account. When the user clicks the link, they are redirected to the fake website. The pen tester can then collect the user's login credentials through the fake website.

For example, the pen tester creates a web page that spoofs the company's identity. The pen tester sends an email to an employee of the company to visit <http://x.x.x.x/login.asp>? and asks them to log in again to activate the server upgrade. The email should look legitimate and authentic (company fonts, colors, logo, etc.).

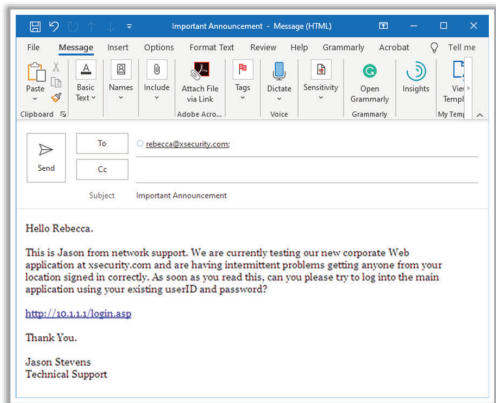


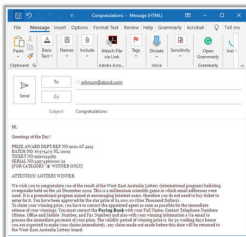
Figure 4.1: Social engineering attempt using an email

Example of Social Engineering Using Email



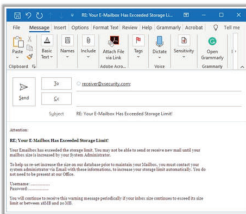
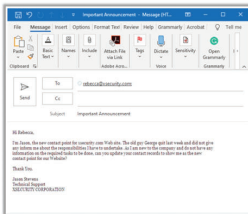
- The pen tester sends some information (**sweepstakes**) related to lottery or gifts to the user and requests them to provide their full **name**, email ID, **password**, and address through an **online submission form**.

- Another way to **obtain information online** is by posing as a network administrator and sending emails to users requesting them to provide a **password**.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Example of Social Engineering Using Email (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Example of Social Engineering Using Email

Pen testers can attempt social engineering by simply sending a fake email pretending to be a system administrator. In the email, the tester can ask the recipient to send the password urgently for system maintenance. Testers can send this email simultaneously to all the collected email addresses of the target users to increase the chances of response.

Some of the common techniques for performing social engineering pen testing through email are listed below:

- Identifying a list of users who use a common password for different online accounts
- Sending some information (sweepstakes) related to lottery or gifts to the user and requesting them to provide their full name, email ID, password, and address through an online submission form
- Introducing themselves as a network administrator, the pen tester sends emails to users through the network and asks them to provide a password.
- Installing pop-up windows on the network and asking users to re-enter their username and password
- Trying to trick victims by sending spoofed emails that seem to be coming from real sources. These emails can be warning messages asking users to manage their mailbox storage space by logging in to some fake website. The pen tester can also pretend to be an employee and send requesting emails that ask for company records.

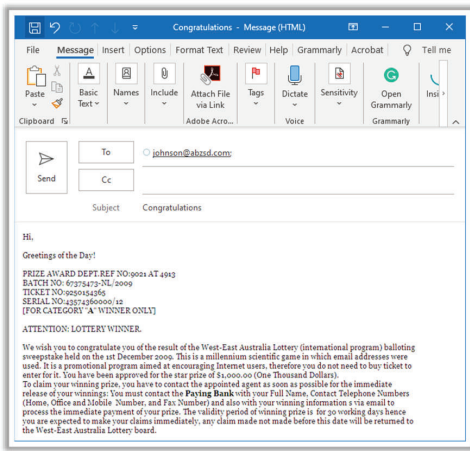


Figure 4.2: Example of a social engineering attempt using a sweepstakes email

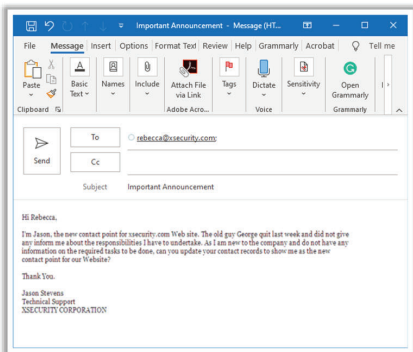


Figure 4.3: Social engineering attempt: posing as an employee

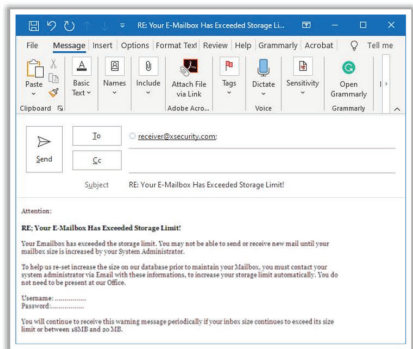
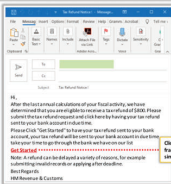
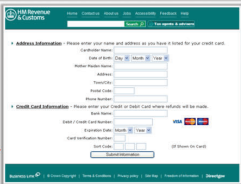


Figure 4.4: Social engineering attempt: posing as a system administrator



Attempt Social Engineering Using Phishing

- The pen tester uses **fake websites** to redirect employees to give out **passwords** and other sensitive information.
- Pop-ups can be used to trick users into **clicking hyperlinks** that redirect them to fake web pages asking for personal information or **downloading malicious programs** such as keyloggers, Trojans, or spyware.
- The pen tester sends an **email** to employees and provides a link to a fake site that **looks similar** to the original.

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Social Engineering Using Phishing

Phishing is a technique in which an attacker sends an email or provides a link that falsely claims to be from a legitimate site in an attempt to acquire a user's personal or account information.

To perform social engineering penetration testing for phishing, pen testers must register a fake domain name, build a lookalike website, and then email the fake website's link to several users. The tester must present themselves as a member of a trustworthy organization and send an attractive email that compels users to perform a certain action. When a user clicks on the email link, it redirects them to the fake webpage, where they are lured into sharing sensitive details such as address and credit card information without knowing that it is a phishing site. Some of the reasons behind the success of phishing scams include users' lack of knowledge, being visually deceived, and not paying attention to security indicators.

Different techniques to perform phishing include the following:

- Using fake websites to redirect employees to give out passwords and other sensitive information
- Using pop-ups to trick users into clicking a hyperlink that redirects them to fake web pages asking for personal information or downloading malicious programs such as keyloggers, Trojans, or spyware

The screenshot below shows an example of a pop-up used for tricking users.



Figure 4.5: Screenshot of a sample pop-up window

- Sending an email to employees and providing a link to a fake site that looks similar to the original

For example, the pen tester can send an illegitimate email that claims to be from a legitimate sender. The email link redirects users to a fake webpage and asks them to submit their personal or financial details.

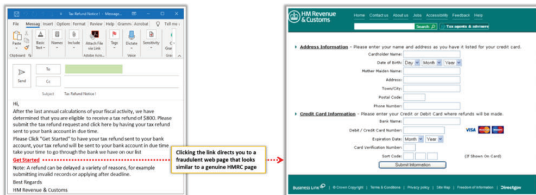


Figure 4.6: Screenshot demonstrating phishing attack

Examples of Phishing Emails



From: An Attacker
Sent: Sunday, June 9, 2019 1:58:52 PM
To: User
Subject: Important changes to your account

Activity Alert
PERSONAL CHECKING/SAVINGS ACCOUNTS
Online Banking Unauthorized Sign-in.

Dear Valued Customer: jousser@its.tntech.edu.

As part of our security measures, our system regularly scheduled account maintenance and verification procedures, we have detected a slight error in your online banking information. Our system requires account verification for more security and protection to your account. To confirm this verification

Log into [Online Banking](#) and update your information.

Want to get more alerts? Sign in to your online banking account at Bank of America and within the Accounts Overview page select the "Alerts" tab.

You can sign in to Online or Mobile Banking to review this activity, or contact us for help.

Security Checkpoint
To confirm the authenticity of messages from us, always look for this Security Checkpoint.

From: Compromised Account: jousser@its.tntech.edu
Sent: 4/13/19 6:51 AM (GMT-05:00)
To: jousser@its.tntech.edu
Subject: The Security of Your Account

Paypal

The Security of Your Account

Dear jousser@its.tntech.edu

We regret to inform you of this bad news.

We have put your account in the list of limited accounts because your account is safe and we need a little bit for a few information to protect your account.

Click the button below and follow the steps simply

Yours Sincerely

Confirm

Questions? Take a look at our FAQs or contact Customer Support.

Source: jousser@its.tntech.edu
Sent: Monday, May 13, 2019 9:57 AM
Subject: Tennessee Tech Job Placement

Tennessee Tech Job Placement & Student Services selected you as a **Secret Shopper**.

A job that will not affect your present employment or studies and no sign up fee. It's fast, rewarding and flexible. You can make up to \$1000 weekly also, to view details of the job and apply please visit website

<https://tntech.com/jobschool>

Job Placement & Student Services
Cookeville, TN 38505 USA

Source: <https://its.tntech.edu>

Copyright © by **IC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Examples of Phishing Emails

Source: <https://its.tntech.edu>

Today, most people use Internet banking. Many people use Internet banking for all their financial needs, such as online share trading and e-commerce. Pen testers can, therefore, use phishing to acquire sensitive information (e.g., passwords, credit card details) by masquerading as a trusted entity.

The pen tester can send a fake email to the target user that appears to be from the bank and request the user to click on the URL or the link provided. If the user is tricked into thinking that the email is authentic, they may provide their username, password, and other sensitive information.

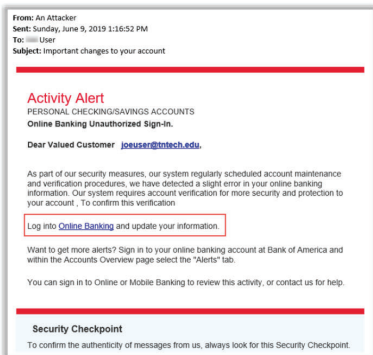


Figure 4.7: Screenshot of an example phishing email

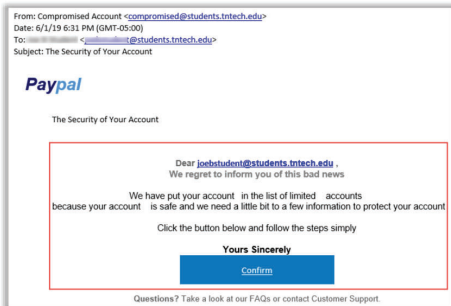


Figure 4.8: Screenshot of an example phishing email

From: Joe B Student

Sent: Monday, May 13, 2019 8:57 AM

Subject: Tennessee Tech : Part Time Job

Tennessee Tech Job Placement & Student Services selected you as a Secret Shopper.

A job that will not affect your present employment or studies and no sign up fee. It's fun, rewarding and flexible. You can make up to \$1000 weekly also, to view details of the job and apply please visit website

<https://tinyurl.com/y3o3xzst>

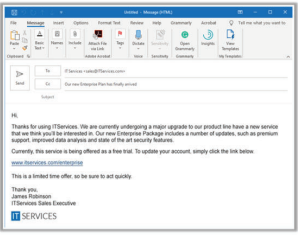
Job Placement & Student Services
Cookeville, TN 38505 USA

Figure 4.9: Screenshot of an example phishing email

Attempt Social Engineering Using Spear Phishing

Instead of sending several emails, the pen tester performs "spear phishing" by using **specialized social engineering content** directed at a specific employee or a small group of employees to obtain sensitive data.

The pen tester selects employees who post their **personal information on the Internet**, acts as a friend or well-known person, and sends a fake email to retrieve information such as financial information and trade secrets.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Social Engineering Using Spear Phishing

Instead of sending several emails, the pen tester can also attempt "spear phishing" by using specialized social engineering content directed at a specific employee or a small group of employees in the target organization to obtain sensitive data such as financial information and trade secrets.

Spear phishing messages appear to originate from a trusted source with an official-looking website. The email also appears to be from an individual from the recipient's company, generally someone in a position of authority. However, the message is sent by a pen tester in an attempt to obtain critical information about a specific recipient and their organization such as login credentials, credit card details, bank account numbers, passwords, confidential documents, financial information, and trade secrets. Spear phishing generates a higher response rate when compared to a normal phishing attack, as the source closely resembles a trusted company source.

To perform this attack, the pen tester can select employees of the target organization who post their personal information on the Internet. Such employees post their details such as email address, geographic location, friends list, recently purchased items, or their interests in the public domain. With this information, the pen tester can act as a friend or a well-known person and send a fake email to the target employee or employees. In some scenarios, the pen tester can also include urgent-sounding explanations on why they need sensitive information.

Examples of spear phishing:

1. The pen tester can send a spoofed mail embedded with a fake link to the system administrator of the target organization claiming that they are an authorized professional for IT services.

2. The pen tester can claim that their company is offering a free new service for a limited time to the target organization and invite the user to sign in using business email to avail the free service
3. When the user clicks on the link, they will be redirected to a fake website that looks legitimate, through which the pen tester can collect sensitive information about the target organization.

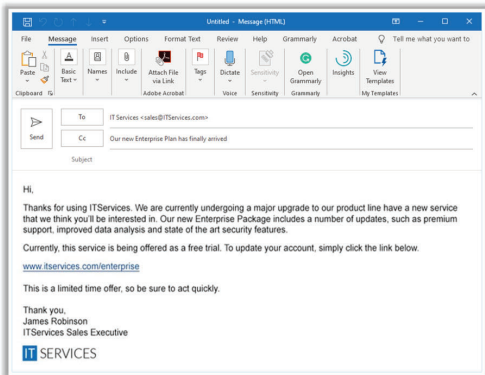
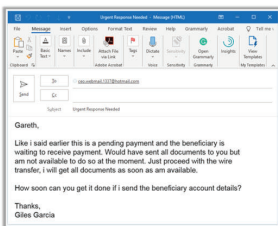


Figure 4.10: Screenshot of an example spear phishing email

Attempt Social Engineering Using Whaling



- The pen tester can target high-profile executives such as **CEO**, **CFO**, **politicians**, and **celebrities** who have complete access to confidential and highly valuable information.
- The pen tester can trick them into revealing critical corporate and personal information through email or **website spoofing**.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Social Engineering Using Whaling

The pen tester can use the whaling technique to target high-profile executives such as CEOs, CFOs, politicians, and celebrities who have complete access to confidential and highly valuable information. The pen tester can use whaling to trick executives to reveal critical corporate and personal information (such as bank account details, employee details, customer information and credit card details) generally through email or website spoofing. To perform whaling, the email or website that is used for the attack must be carefully designed as the target is someone in an executive position.

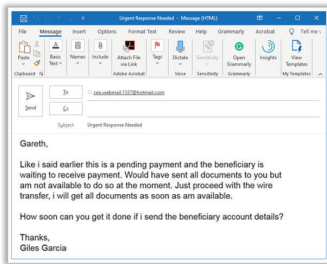


Figure 4.11: Screenshot of an example whaling email

Attempt Social Engineering Using Pharming



- The pen tester sends **malicious code** as a download link or an email attachment that redirects the user to a pharming website.



- The pen tester retrieves **sensitive information** such as credentials, banking details, and other information related to **web-based services** through the pharming website.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Social Engineering Using Pharming

Pharming is also known as “Phishing without a Lure.” Pen testers use the pharming method to send malicious code to the target users as an email attachment or download link. To perform this attack, the pen tester first needs to create a fake pharming website to retrieve sensitive information from the user. When the user clicks on the link or downloads the code, the code will automatically trigger execution, may corrupt the files on the victim’s system, and redirect the victim to the pharming website. Through this pharming website, the pen tester can obtain confidential information such as credentials, banking details, and other information related to web-based services.

Example of pharming:

- The pen tester sends a malicious code as an email attachment.
- When the user clicks on the attachment, the code is executed on their personal computer, modifying local host files.
- When the victim enters the target website’s URL in the browsers address bar, the compromised host file automatically redirects the user’s traffic to the pharming website created by the pen tester.

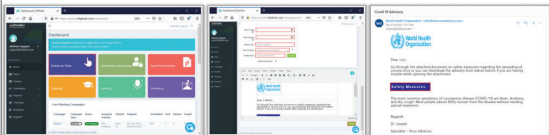
Launch a Phishing Campaign



- The pen tester can launch a phishing campaign on the organization using different **frameworks** such as OhPhish, BLACKEYE, ShellPhish, Phishing Frenzy, LUCY, Social-Engineer Toolkit (SET), SpeedPhish Framework (SPF), and Gophish.



OhPhish



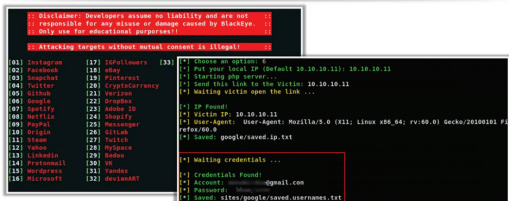
Source: <https://ohphish.eccouncil.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Launch a Phishing Campaign (Cont'd)



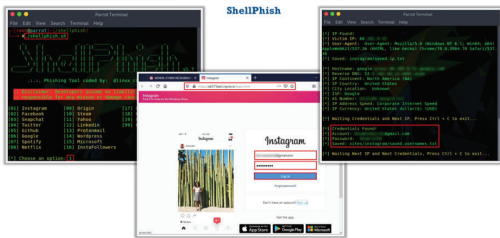
BLACKEYE



Source: <https://github.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

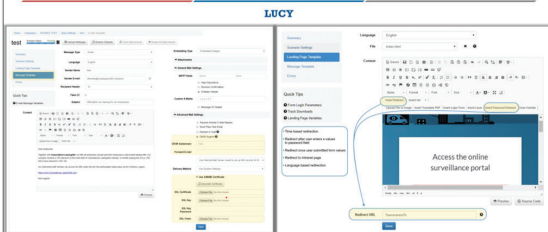
Launch a Phishing Campaign (Cont'd)



Source: <https://github.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Launch a Phishing Campaign (Cont'd)



Source: <https://www.lucysecurity.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Launch a Phishing Campaign (Cont'd)



Social-Engineer Toolkit (SET)

```

01 Spear-phishing Attack Vectors
02 Module Attack Vectors
03 Installation Module Generator
04 Create a Payload and Listener
05 Word Multitask Attack
06 Arbitrary-Based Attack Vector
07 Multitask Remote Point Attack Vector
08 OMSide Generator Attack Vector
09 RemoteShell Attack Vectors
10 Third Party Modules

991 Return back to the main menu.

set> 1

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

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

01 Perform a Basic Email Attack
02 Create a Filetransfer Payload
03 Create a Social-Engineering Template

991 Return to Main Menu

set> 1
  
```

Source: <https://www.trustedsec.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Launch a Phishing Campaign

Pen testers can use frameworks such as OhPhish, Phishing Frenzy, LUCY, Social-Engineer Toolkit (SET), SpeedPhish Framework (SPF), and Gophish to generate fake login pages to capture usernames and passwords, send spoofed emails, and obtain victims' IP addresses and session cookies. This information will help the pen tester impersonate a legitimate user and launch further attacks on the target organization.

- OhPhish

Source: <https://ohphish.eccouncil.org>

OhPhish is a web-based portal that tests employees' susceptibility to social engineering attacks. OhPhish is a phishing simulation tool that provides the organization with a platform to trigger phishing simulation campaigns targeting their employees. The platform captures the responses and provides MIS reports and trends (on a real-time basis) that can be tracked according to the user's department or designation.

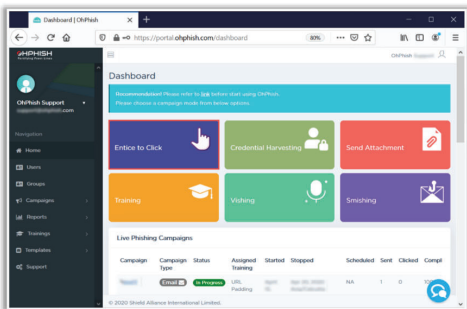


Figure 4.12: Screenshot of the OhPhish Dashboard

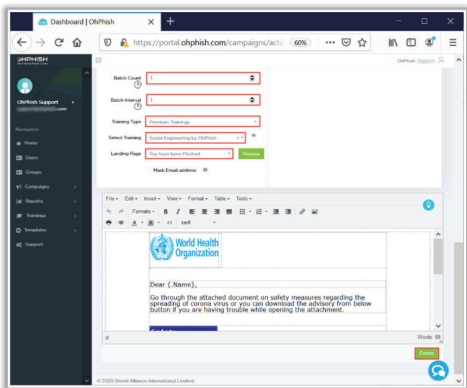


Figure 4.13: Screenshot of OhPhish: a new phishing campaign

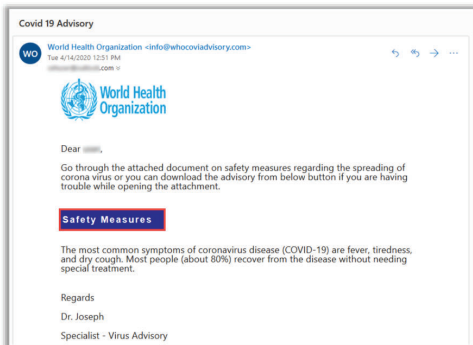


Figure 4.14: Screenshot of OhPhish: a phishing email

- **BLACKEYE**

Source: <https://github.com>

BLACKEYE is a phishing tool used by penetration testers to phish the target user's credentials from various social media platforms such as Gmail, Instagram, and Facebook.

Using this tool, pen testers can choose from various social media platforms and then create a fake link. This link is sent to the user through email, and once the user opens the link to login, an exact replica of the chosen social media platform is displayed. When the user inputs their credentials and clicks to login, BLACKEYE retrieves the user's credentials.



Figure 4.15: Screenshot of BLACKKEY: phishing options

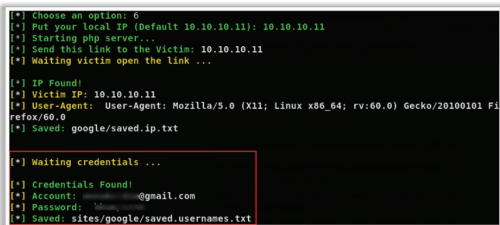


Figure 4.16: Screenshot of BLACKKEY: retrieving user credentials

▪ ShellPhish

Source: <https://github.com>

ShellPhish is a phishing tool used by penetration testers to phish user credentials from various social networking platforms such as Instagram, Facebook, Twitter, and LinkedIn. Using this tool, pen testers can send a fake login page via an email to the target user. When the user opens the page and enters their credentials, ShellPhish retrieves these credentials.

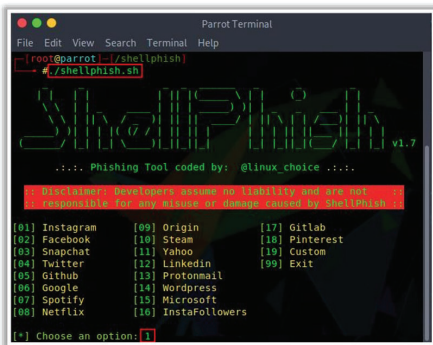


Figure 4.17: Screenshot of ShellPhish: phishing options

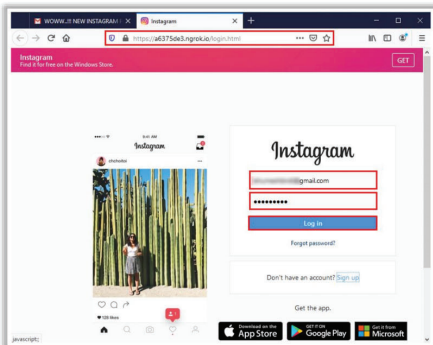
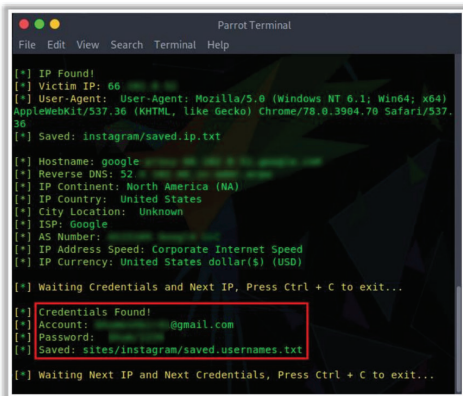


Figure 4.18: Screenshot of phishing page created by ShellPhish



```
Parrot Terminal
File Edit View Search Terminal Help

[*] IP Found!
[*] Victim IP: 66
[*] User-Agent: User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3994.70 Safari/537.
36
[*] Saved: instagram/saved.ip.txt

[*] Hostname: google
[*] Reverse DNS: 52
[*] IP Continent: North America (NA)
[*] IP Country: United States
[*] City Location: Unknown
[*] ISP: Google
[*] AS Number:
[*] IP Address Speed: Corporate Internet Speed
[*] IP Currency: United States dollar($) (USD)

[*] Waiting Credentials and Next IP, Press Ctrl + C to exit...

[*] Credentials Found!
[*] Account: @gmail.com
[*] Password:
[*] Saved: sites/instagram/saved.usernames.txt

[*] Waiting Next IP and Next Credentials, Press Ctrl + C to exit...
```

Figure 4.19: Screenshot of ShellPhish: retrieving user's credentials

▪ LUCY

Source: <https://www.lucysecurity.com>

LUCY enables the pen tester to perform phishing attacks as an attacker and identify gaps in both the technical infrastructure of the organization and security awareness of the employees. Using this tool, the tester can quickly carry out a variety of campaigns such as phishing simulations, awareness trainings, technology assessments, malware simulations, or simulated ransomware attacks.

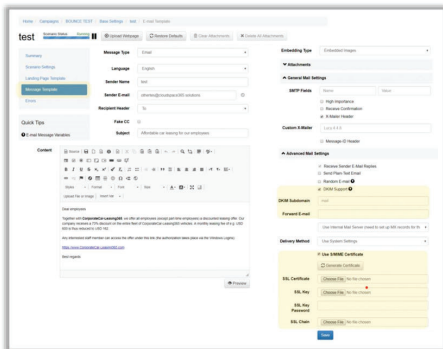


Figure 4.20: Screenshot of LUCY: creating a new scenario

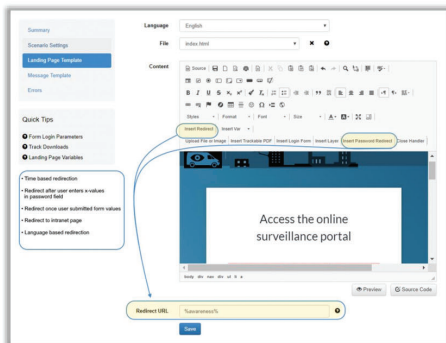


Figure 4.21: Screenshot of LUCY: landing page template

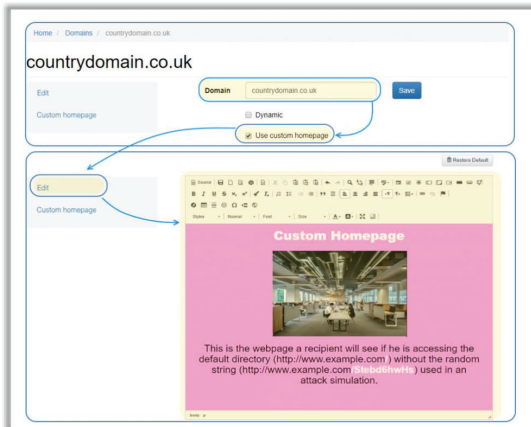


Figure 4.22: Screenshot of LUCY: creating a custom home page

- **Social-Engineer Toolkit (SET)**

Source: <https://www.trustedsec.com>

The SET is an open-source Python-driven tool that aims to perform social engineering penetration testing. It is a generic exploit designed to perform advanced attacks against human elements to compromise a target to offer sensitive information. SET categorizes attacks into email, web, and USB according to the attack vector used to deceive the target. The toolkit exploits human attributes that are weaknesses from an attacker's perspective such as trust, fear, avarice, and altruism.

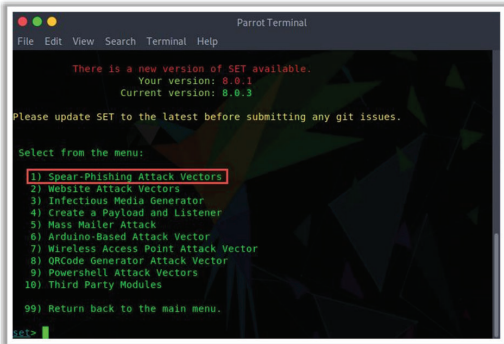


Figure 4.23: Screenshot of Social-Engineer Toolkit (SET)

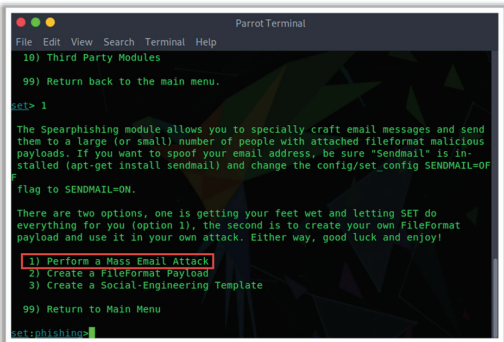


Figure 4.24: Screenshot of Social-Engineer Toolkit (SET) showing phishing options



Social Engineering Penetration Testing Using Telephone Attack Vector

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering Penetration Testing Using Telephone Attack Vector

The telephone attack vector can be used to gather information about the target organization, trick employees into revealing sensitive information, or trick them into performing actions that compromise the security of the organization. In this section, you will learn how to use the telephone attack vector for performing social engineering attempts through vishing and SMiShing to gather sensitive information from the target.

Attempt Social Engineering Using Phone (Vishing)

Three common techniques to perform social engineering using phone:

- Acting as a **customer** looking for sensitive information
- Posing as an **employee** who forgot their password
- Pretending to be a **technical support member** to deceive staff members



The pen tester tricks the users and looks for the following information:

- Contact or **schedule information** for other employees
- Username and passwords
- Trick employees into **running commands** on their computer and providing information



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Social Engineering Using Phone (Vishing)

Vishing (voice or Voice over IP (VoIP) phishing) is an impersonation technique in which pen testers use VoIP technology to trick individuals into revealing their critical financial and personal information. In this technique, the pen tester uses caller ID spoofing to forge identification. The pen tester can also include pre-recorded messages and instructions resembling those from a legitimate financial institution. Using this technique, the pen tester can attempt to trick users into providing bank account or credit card details for identity verification over the phone.

Vishing is a combination of phishing and VoIP technology. A pen tester can perform vishing by calling employees of the target organization pretending to be a colleague, vendor, or customer from a legitimate enterprise and request them to help in accomplishing a certain task or answer certain questions. The main targets of vishing include financial institutions, government organizations, online sales, payment services, and so on.

The tester can also send a fake SMS or email message to the target user asking them to call the financial institution for credit card or bank account verification. When the user calls on the number mentioned in the message, the tester can play the recorded instructions, which insist that the target must provide personal and financial information such as name, date of birth, social security numbers, bank account numbers, credit card numbers, and credentials like usernames and passwords.

Three common techniques to perform social engineering using the phone are as follows:

- Acting as a customer looking for sensitive information
- Posing as an employee who forgot their password
- Pretending to be a technical support member to deceive staff members

Pen testers trick users into giving up the following information/performing the following actions:

- Contact or schedule information of other employees
- Usernames and passwords
- Trick employees into running commands on their computer and providing information

Some of the techniques used to perform social engineering penetration testing using a telephone attack vector are discussed below:

- Calling the victim posing as a colleague and asking for sensitive information such as bank account number and passport number
- Calling the victim pretending to be an important user, gaining their trust, and then asking them various questions to collect information.
- Posing as an important person of the target organization and trying to collect information
- Offering various rewards to acquire sensitive information
- Using deceptive methodologies such as threatening with dire consequences like deactivation of the account unless the target provides sensitive information
- Making the victim believe that the call is from their organization's tech support team and requesting sensitive information
- Using reverse social engineering method and creating situations where victims approach the pen tester themselves and provide sensitive information. For example, sending an email or SMS, informing them that due to security-related issues, users must call a given number or send an email and provide certain details.

Example of Social Engineering Using the Phone

1 The pen tester should call the **company's help desk** and ask for sensitive information.

2 The pen tester should call the **receptionist**, engage in conversation, and extract various contact details of the company.

3 The pen tester should make the call sound **realistic**; rehearsing many times before making the call is advised.

4 The pen tester should have **backup answers** for every question that the target person is asked.

5 The pen tester should record the **conversation** for reporting purposes.

"Hi, this is Jason, the VP of sales. I'm at the New York branch today, and I can't remember my password. The machine in my home office has that 'Remember password' set, so it's been months since I actually had to enter it. Can you tell me what it is, or reset it or something? I really need to access this month's sales reports ASAP."



"Hi, this is Joanna at the Boston branch. I'm the new LAN administrator, and my boss wants this done before he gets back from London. Do you know how I can:

- Configure our firewall to have the same policies as corporate?
- Download the latest DNS entries from the corporate DNS server to our local server?
- Run a transaction on a remote file and print server using a shell command?
- Back up the database to our offsite disaster recovery location?
- Locate the IP address of the main DNS server?
- Set up a backup dial-up connection to the corporate LAN?
- Connect this new network segment to the corporate intranet?"

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Example of Social Engineering Using Phone

The pen tester pretends to be an employee of a bank, calls a person, and asks them to check their personal information such as account number, debit card number, credit card number, password, or PIN. The pen tester records these details with the help of a video recorder and uses this information for identity theft.

The following are a few points to remember while making a call:

- The pen tester should call the company's help desk and ask for sensitive information.
- The pen tester should call the receptionist, engage them in a conversation, and extract various contact details of the company.
- The pen tester should make the call sound realistic; rehearsing many times before making the call is advised.
- The pen tester should have backup answers for every question that the target person is asked.
- The pen tester should record the conversation for reporting purposes.

Examples of conversation:

- Hi, this is Jason, VP of sales. I'm at the New York branch today, and I can't remember my password. The machine in my home office has that "Remember password" set, so it's been months since I actually had to enter it. Can you tell me what it is, or reset it or something? I really need to access this month's sales reports ASAP.
- Hi, this is Joanna from the Boston branch. I'm the new LAN administrator, and my boss wants this done before he gets back from London.

Do you know how I can:

- Configure our firewall to have the same policies as corporate?
- Download the latest DNS entries from the corporate DNS server to our local server?
- Run a transaction on a remote file and print server using a shell command?
- Back up the database to our offsite disaster recovery location?
- Locate the IP address of the main DNS server?
- Set up a backup dial-up connection to the corporate LAN?
- Connect this new network segment to the corporate Intranet?

Attempt Social Engineering Using SMiShing (SMS Phishing)



- ✦ The pen tester should send SMiShing message to **lure users into instant action** such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number.
- ✦ The pen tester should carefully **craft the SMiShing messages** to provoke an instant action from the victim, requiring them to divulge their personal information and account details.



Hi Dear,
Receive Rs.2000 Welcome Bonus
Play Rummy Now & Win Cash
Register For Free to9.me/
145n4qu



Rummy Online | Play Free
Play Online Rummy Card Game at
RummyCircle. ✓₹2500 BONUS ✓Daily
www.rummycircle.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Social Engineering Using SMiShing (SMS Phishing)

In SMiShing (SMS Phishing), the SMS text messaging system is used to lure users into instant action such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number. The pen test must craft SMiShing messages to provoke an instant action from the victim, requiring them to divulge their personal information and account details.

Example of SMiShing:

- Let us take the example of Tracy, a software engineer working in the target company
- The pen tester sends an SMS to her from the security department of XIM Bank. The SMS must claim to be urgent and say that Tracy should call up the phone number mentioned in the SMS immediately.
- Worried, Tracy calls up to check on her account, believing it to be an XIM Bank customer service number.
- The pen tester plays a recorded message that asks her to provide her credit card or debit card number as well as password.
- Tracy believes it to be a genuine message and shares the sensitive information.

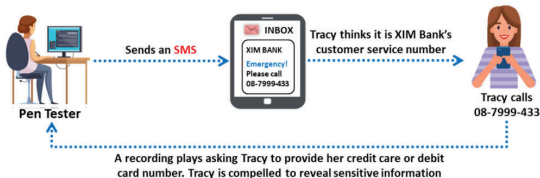


Figure 4.25: Example of SMishing

In some scenarios, the pen tester may also send a message that claims that the user has won money or has been randomly selected as a lucky winner and that they merely need to pay a nominal amount of money and share their email ID, contact number, or other information.

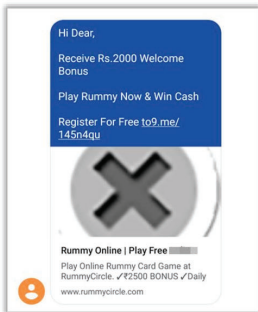


Figure 4.26: Screenshot of an example SMishing message



Social Engineering Penetration Testing Using Physical Attack Vector

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering Penetration Testing Using Physical Attack Vector

The physical attack vector is used to directly visit the company premises or meet employees and use social engineering techniques to acquire sensitive information. Visiting the target premises might also help the tester identify physical vulnerabilities such as security control vulnerabilities, entry and exit points of the building, and ways to make employees divulge sensitive information. In this section, you will learn how to use various physical attack techniques to perform social engineering penetration testing.

Visit the Company as an Inquirer and Extract Privileged Information



- The pen tester should visit the company's **physical premises** and ask the **receptionist** the following questions:

- I am a new customer, and I am interested in your products. Do you have a catalog?
- I would like to meet your vice president. Do you know how I can contact him?
- What time do you usually open and close?
- Do you have any office other than this?
- Do you have any other telephone numbers other than the one posted on the website?

- The pen tester should take a **picture** of the premises using a phone camera.

- The pen tester should ask if they can use the **restroom**; if the company has an internal restroom, observe various rooms (take photos if possible).

Example

"Hi, I'm Sharon, I'm a sales rep out of the New York office. **I know this is short notice, but I have a group of prospective clients** out in the car. I've been trying for months to get them to outsource their security training needs to us.

They're located just a few miles away and I think that, if I can give them a quick tour of our facilities, it should be enough to push them over the edge and get them to sign up.

Oh yeah, **they are particularly interested in what security precautions we've adopted.** Seems someone hacked into their website a while back, which is one of the reasons they're considering our company."

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Visit the Company as an Inquirer and Extract Privileged Information

Before performing social engineering pen testing, the pen tester should gather detailed information about the target organization and its employees. The pen tester must check the website of the company to retrieve the list of employees and their designations and gather all related information about the company, including information related to security checks, internal contacts, and products, before visiting the premises. The pen tester can also pose as a customer, vendor, or relative of an employee in order to obtain sensitive information from the employees.

- The pen tester should visit the company's physical premises and ask the receptionist the following questions:
 - I am a new customer, and I am interested in your products. Do you have a catalog?
 - I would like to meet your vice president. Do you know how I can contact him?
 - What time do you usually open and close?
 - Do you have any office other than this?
 - Do you have any other telephone numbers other than the one posted on the website?
- The pen tester should take a picture of the premises using a phone camera.
- The pen tester should ask if they can use the restroom; if the company has an internal restroom, observe various rooms (take photos if possible).

Example:

Hi, I'm Sharon. I'm a sales rep out of the New York office. I know this is short notice, but I have a group of prospective clients out in the car. I've been trying for months to get them to outsource their security training needs to us.

They're located just a few miles away, and I think that if I can give them a quick tour of our facilities, it should be enough to push them over the edge and get them to sign up.

Oh yeah, they are particularly interested in what security precautions we've adopted. Seems someone hacked into their website a while back, which is one of the reasons they're considering our company.

Visit the Company Locality



- The pen tester must visit the company location to gather general information, such as **number of people** working in the company, **names**, and **phone numbers** of the important persons from other sources including the following:

- Ancillary staff, including maintenance or cleaning personnel
- Agents providing service to the company staff
- Neighboring shopkeepers and vendors



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Visit the Company Locality

The pen tester can also acquire crucial information about the company by talking to other people associated with the company, such as cooks, cleaners, clerks, third-party agents, and people who stay near the company's premises. The pen tester should befriend staff members such as janitors, cleaners, security personnel, and third-party service providers to gather information.

In addition, the pen tester must also visit the company location to gather general information such as number of people working in the company and names and phone numbers of the important persons from other sources, including the following:

- Ancillary staff, including maintenance or cleaning personnel
- Agents providing service to the company staff
- Neighboring shopkeepers and vendors

Attempt to Use Fake ID to Gain Access



The pen tester should create an ID/badge that looks authentic and see if they can enter the office/restricted areas using the fake ID.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt to Use Fake ID to Gain Access

The pen tester should attempt to use fake ID cards with fake employee names to enter the company premises. Before using this technique, the pen tester should do appropriate research and gather sufficient information about the company, employee details, their designations, type of security checks, and so on. To act as a legitimate employee, the pen tester must also gather information about restricted areas in the company.

Attempt Piggybacking/Tailgating



The pen tester should try getting into an office or restricted areas by walking in with authentic staff without showing a valid ID using piggybacking or tailgating techniques



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Piggybacking/Tailgating

The pen tester can use techniques such as piggybacking or tailgating to enter an organization's premises. To use these techniques, the pen tester needs to follow the employees entering the company and take advantage of situations where an employee is busy on a call or carrying multiple items into the building.

The pen tester can use piggybacking to enter the company's building or security area with the consent of an authorized person. For example, the pen tester can request an authorized person to unlock a security door, saying that they have forgotten their ID badge. In the interest of common courtesy, the authorized person may allow the pen tester to pass through the door.

The pen tester can use tailgating to enter into a building or secured area without the consent of the authorized person. For tailgating, the pen tester needs to follow an authorized person through a secure entrance, act as a polite user, and remember to open and hold the door for those following them.

Listen to Employee Conversations in Communal Areas/Cafeteria



- The pen tester should try to listen to employee conversations in communal areas, such as cafeterias or hallways.
- The pen tester must listen and gather details such as the **latest on-going projects** within the company; persons involved with the projects; the **names of key personnel**, partners, or competitors of the company; or other useful information that could be exploited, including **disgruntled employees**.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Listen to Employee Conversations in Communal Areas/Cafeteria

The pen tester must follow the target company's employees and make a record of their activities. The pen tester should try to listen to employee conversations in communal areas, such as cafeterias or hallways. The pen tester must listen and gather details such as the latest on-going projects within the company; persons involved in the projects; the names of key personnel, partners, or competitors of the company; or other useful information that could be exploited, including disgruntled employees. This information will help the pen tester create phishing emails or serve as a communication point to befriend employees.

Identify “Disgruntled Employees” and Engage Them in Conversation to Extract Sensitive Information



- The pen tester should identify the disgruntled employees by trying to **overhear conversations** in the company cafeteria.

The pen tester should befriend the employee and express similar views about the company to extract the following information:

1	Company's policies and IT infrastructure
2	Workplace address and contact information
3	Personal information
4	Organization's computer network details
5	Organization's policies
6	Organization's structure
7	Organization's functions
8	Organization's future projects
9	Organization's employee details

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify “Disgruntled Employees” and Engage Them in Conversation to Extract Sensitive Information

Disgruntled employees are those who are not satisfied with the company's policies, work process, salary, and so on; such employees always complain about the company. The pen tester can identify them by listening to their conversations in the company cafeteria, where such employees vent their anger and frustration. The pen tester can also identify disgruntled employees by observing the surroundings where employees gather and talk to each other.

Disgruntled employees may also appear dejected or unenthusiastic. The pen tester should pay attention to facial expressions and body language to identify such employees and try to approach them and gather sensitive information about the company, such as company policies, functions, and future projects. Acquiring sensitive information about the company from a disgruntled employee might work well if the pen tester can find one.

The pen tester must befriend disgruntled employees and express similar views about the company to extract the following information:

- Company's policies and IT infrastructure
- Workplace address and contact information
- Personal information
- Organization's computer network details
- Organization's structure
- Organization's functions
- Organization's future projects
- Organization's employee details

Attempt Eavesdropping



- The pen tester should try to obtain information by eavesdropping on conversations that others are having in person, over the **phone** or by **video conference**.
- The pen tester should look for confidential information in **documents** that are left in plain sight.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Eavesdropping

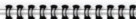
Eavesdropping is the act of secretly listening to the conversations of people over a phone or video conference without their consent. It also includes reading confidential messages from communication media (such as instant messaging or fax transmissions).

The pen tester must gain information by tapping the phone conversation or intercepting audio, video, or written communication. The pen tester should acquire confidential information in documents that are left in plain sight. They can also physically visit all the places where meetings or conversations take place and listen to the conversations of employees to gather sensitive information. The pen tester can also place audio recording devices in places such as meeting rooms and listen to them later. Using this technique, the pen tester can obtain information such as passwords, business plans, phone numbers, and addresses.

Try to Shoulder Surf Users Who Are Logging On



- The pen tester should walk or **stand behind the target employee** as they are typing and look at what is on their screen. The pen tester should note any confidential information that is viewable.



- The pen tester should attempt to obtain the target employee's **PIN or password** as they enter it on their keyboard. If the pen tester is not able to get close to them as they are typing, they should use **binoculars** or a **low-power telescope** to observe them from afar.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Shoulder Surf Users Who Are Logging On

Shoulder surfing is the technique of observing or looking over someone's shoulder as they key in information into a device. The pen tester can use shoulder surfing to discover passwords, PINs, account numbers, and other information. The pen tester can even use binoculars, a low-power telescope, or other optical devices or install small cameras to record actions performed on the victim's system to obtain login details and other sensitive information. The pen tester should make a note of any confidential information that can be viewed.

The pen tester can use the following techniques to shoulder surf and gather sensitive information:

- Looking at someone's password or PIN code with the help of binoculars or a low-power telescope
- Covering the keypad with a thin coat of ultraviolet paint to view the key or PIN entered by the user
- Listening and observing the keystrokes while the user types a password in order to identify the number of characters in the user's password.
- Listening to the telephone keypad when a user dials a PIN to determine the PIN code from the sounds of multi-frequency tones

Attempt Media Dropping/Baiting



- The pen tester should drop a media device somewhere conspicuous such as a **parking lot** or **building entrance area**.
- The pen tester can use media such as a **USB flash drive** containing malicious software, which when inserted into the computer, will automatically run and launch a client-side attack when opened.
- The pen tester could also **pose as a potential employee** and see if employees from the target organization will print their résumé from the planted USB flash drive.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Media Dropping/Baiting

The pen tester can use baiting to offer the target user something alluring in exchange for important information such as login details and other sensitive data. This technique exploits the human attributes of the target user such as curiosity and greed. The pen tester can perform this technique by leaving a physical device such as a USB flash drive containing malicious files in locations where people can easily find them such as building entrances, parking lots, elevators, or bathrooms. The pen tester must label the physical device with a legitimate company logo, thereby tempting the target user to find it and open it on their systems. When the USB containing malicious software is inserted into the victim's computer, the malicious software will automatically run and launch a client-side attack when opened.

The pen tester can also pose as a potential employee and see if employees from the target organization print their résumé from the planted USB flash drive. This type of attack is more effective if the employee connects the media to their office laptop or desktop.

For example, the pen tester should leave a bait in the form of a USB drive in the elevator with a label such as "Employee Salary Information 2020" and the legitimate company logo. Motivated by curiosity and greed, the victim may pick up the device, open it up on their system, and download the bait. Once the bait is downloaded, the malicious software is installed into the victim's system, launching a client-side attack on the victim's system.

Attempt Dumpster Diving



- ✎ The pen tester should look through trash cans and **paper bins** placed inside and outside office buildings. The pen tester should look for the following:

- Phone bills
- Contact information
- Financial information
- Operations-related information



- ✎ The pen tester should also look in **employee desks** and under their keyboards for sticky notes or other documents containing confidential information, including usernames and passwords.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Dumpster Diving

Dumpster diving can be metaphorically understood as looking for treasure in someone else's trash. It is the process of retrieving sensitive personal or organizational information by searching through trash bins. The pen tester can search disposal areas, trash bins, and employees' desks and under their keyboards for sticky notes or other documents containing confidential information, including usernames and passwords.

The pen tester can also collect improperly disposed papers, packaging covers, media, electronic devices, and other relevant objects as part of this attack. The pen tester must use appropriate techniques and devices to scan the collected material for useful information. While performing dumpster diving, the pen tester must ensure that they wear proper protective equipment such as latex surgical gloves.

Many organizations utilize hotel conference rooms or other unsecured facilities to conduct brainstorming sessions. Once the session is complete, generally, the whiteboards used to record the output of the meeting are not wiped. The pen tester can collect information from these boards as well. In some cases, the pen tester can also use pretexts to support dumpster diving attempts, such as posing as a repair person, technician, or cleaner.

The pen tester can use dumpster diving to obtain the following information:

- Phone bills
- Contact information
- Financial information
- Operations-related information
- Organizational charts
- Email printouts, notes, faxes, and memos
- Policy manuals
- Event notes, calendars, or computer use logs

Attempt Reverse Social Engineering



- The pen tester must assume the role of a **person in authority** so that employees ask them for information.



- The pen tester needs to create an incident/problem and then present themselves as the **problem solver** through general conversation, encouraging employees to ask questions as well.



- The pen tester should present themselves as a person in authority, and the target may **seek their advice** after or before offering the information that the pen tester needs.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Reverse Social Engineering

Generally, reverse social engineering is difficult to implement. This is primarily because it needs extensive preparation and skills for execution. In reverse social engineering, the pen tester must assume the role of a person in authority so that employees ask them for information. The pen tester needs to manipulate questions to draw out the required information from the employees themselves.

In this technique, first, the pen tester needs to create an incident/problem and then present themselves as the problem solver through general conversation, encouraging employees to ask questions as well. For example, an employee may ask how a particular problem has affected particular files, servers, or equipment. This provides pertinent information to the pen tester. Several different skills and experiences are required to carry out this tactic successfully.

Some of the techniques involved in reverse social engineering are provided below.

- **Sabotage:** Once the pen tester has gained access to a system/workstation, they corrupt it or make it appear as corrupted. Under such circumstances, users seek help as they face problems.
- **Marketing:** To ensure that the user calls, the pen tester must advertise themselves. The pen tester can do this by either leaving their business card in the target's office or by placing their contact number on the error message itself.
- **Support:** Even after obtaining the required information, the pen tester should continue assisting the users so that they remain ignorant about the pen tester's identity.

Attempt Elicitation



- The pen tester must extract information from the victim by drawing them into normal and **disarming conversations**.
- The pen tester must initiate a **casual conversation** with the target user to extract information without making them feel that they are being socially engineered.

Use of Flattery	The pen tester can use statements such as "You are the top-notch guy handling the project" and "I'll bet you are the clever brains behind the success of the company."
Bracketing	The pen tester might say to the target user "I'd guess the security of your company is pretty tight. I would assume you have ten surveillance cameras in the premises."
Use of False Statements	The pen tester can use statements such as the following: "I heard that your company has fifty systems, two servers, and a printer placed in a single room. People say that room is like Fort Knox! Nobody can get in!"
Artificial Ignorance	The pen tester can use statements such as the following: "I don't know anything about project development, but I'll bet you know everything about the project development process."
The Sounding Board	The pen tester should listen to the target's feelings and provide positive or negative judgment about their feelings. This creates trust between the pen tester and the victim, and the victim starts sharing additional information.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Elicitation

Elicitation is a technique of extracting information from the victim by drawing them into normal and disarming conversations. To use this technique, the pen tester must possess good social skills to take advantage of professional or social opportunities and communicate with persons having access to sensitive information. To perform elicitation, the pen tester needs to initiate a casual conversation with the target user to extract information without making them feel that they are being socially engineered. Further, to use this technique, the pen tester needs to create complex cover stories, plan, and may even need to involve co-conspirators.

■ Use of flattery

The pen tester can use flattery to sweet-talk the target user into offering sensitive information. For example, the pen tester can use statements such as "You are the top-notch guy handling the project," or "I'll bet you are the clever brains behind the success of the company." Such statements will facilitate the elicitation process and have been proven to be very effective in many scenarios.

■ Bracketing

The pen tester can use bracketing for elicitation to retrieve more precise information about the target organization. The pen tester can mention highly or slightly inaccurate information to tempt the user into responding with more specific information. For example, if the pen tester wants to know the number of surveillance cameras connected in the company, they might say to the target user, "I'd guess the security of your company is pretty tight. I would assume you have ten surveillance cameras in the premises."

- **Use of false statements**

The pen tester can use false statements while communicating with the target user so that the target user will correct the statement and volunteer correct information. For example, the pen tester can use statements such as the following: "I heard that your company has fifty systems, two servers, and a printer placed in a single room. People say that room is like Fort Knox! Nobody can get in."

- **Artificial ignorance**

The pen tester can use artificial ignorance as an elicitation technique so that the victim will teach and educate the pen tester about the relevant information. For example, the pen tester can use statements such as the following: "I don't know anything about project development, but I'll bet you know everything about the project development process."

- **The sounding board**

The pen tester can use the sounding board technique to take advantage of the behavior of the target user. When a person reveals their feelings to another person, an immediate kinship is formed. As a result, they will be ready to share more information, even with a stranger. To use this technique, the pen tester needs to be patient while communicating with the target user, listen to their feelings, and provide positive or negative judgment about their feelings. This creates trust between the pen tester and the victim, and the victim starts sharing additional information with the pen tester.

Attempt Social Engineering Using Motivation Techniques



Authority	- Authority implies the right to exercise power in an organization. - The pen tester can impersonate a person of authority such as a technician or an executive in the target organization to gather important data.
Intimidation	- The pen tester intimidates a victim into taking several actions by using bullying tactics. - The pen tester impersonates another person and manipulates users to disclose sensitive information.
Consensus/Social Proof	- Consensus or social proof refers to the fact that people usually like or do things that other people like or do. - The pen tester can send a fake website link via phishing or SMiShing to lure users into believing fake testimonials on the benefits of a product.
Scarcity	- The technique that uses scarcity makes the target believe that the object/aim they desire is available only in limited quantities and, therefore, requires immediate action before supply runs out. - The pen tester sends a phishing email to the target users and encourages them to click on a link provided in the email to buy a popular/out-of-stock product.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Social Engineering Using Motivation Techniques (Cont'd)



Urgency	- Urgency implies encouraging people to take an immediate action. - The pen tester sends a phishing email indicating that a certain product is available at a low price and that to buy it, the user should click on the "Buy Now" link.
Familiarity /Likeness	- Familiarity or likeness implies the fact that people are more likely to get persuaded to do something when asked by someone they like - The pen tester should use a decent smile and talk warmly to deceive the target user so that they like the pen tester.
Trust	- Using the trust principle, the pen tester can often attempt to build a trust relationship with victims. - The pen tester should call a victim and introduce themselves as a security expert. The pen tester should then claim that they are working with a random company and that they noticed some unusual errors sent from the victim's system.
Greed	- Greed implies some people are possessive in nature and wish to acquire huge amounts of wealth from doing illegal activities. - The pen tester may pretend to be a competitor of the target organization and lure the employees of the target into revealing critical information by offering a huge ransom.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Social Engineering Using Motivation Techniques

■ Authority

Authority implies the right to exercise power in an organization. The pen tester can utilize this concept by impersonating a person of authority such as a technician or an executive in the target organization to gather important data.

For example, the pen tester can call a user on the phone and can claim that they are working as a network administrator in the same organization. The pen tester then informs the victim about a security incident in the network and asks them to provide their account credentials in order to protect their data from theft. After obtaining the victim's credentials, the pen tester can even gather sensitive information from the victim's account.

- **Intimidation**

Intimidation refers to an attempt that is made to frighten a victim into taking several actions by using bullying tactics. The pen tester can use this technique by intimidating the target into thinking that them not taking an action is going to have dire consequences and making them feel that they are somehow hindering the best interests of the organization.

For example, the pen tester can impersonate an executive's secretary and call the executive's receptionist with the following request:

"Mr. Tibiyani is about to give a big presentation to the customers, but he is unable to open his files; it seems they are corrupt. He told me to call you and ask you to send the files to me immediately, so that he can start his talk."

- **Consensus/Social proof**

Consensus or social proof refers to the fact that people usually like or do things that other people like or do.

For example, the pen tester can create a fake website and post fake testimonials on the benefits of some products such as anti-malware (rogueware). The pen tester then sends the fake website link via phishing or SMiShing to lure users into believing the fake testimonials. If this malicious product is downloaded by the users, the pen tester can then exploit the malicious software and perform further attacks.

- **Scarcity**

Scarcity implies the state of being scare. In the context of social engineering, the technique that uses scarcity makes the target believe that the object/aim they desire is available only in limited quantities and, therefore, requires immediate action before supply runs out. The pen tester can then control the information provided to victims in order to manipulate the decision-making process.

For example, assume that Apple iPhones released a new product, which became sold out and went out of stock. The pen tester can take advantage of this situation by sending a phishing email to the target users and encouraging them to click on a link provided in the email to buy the product. If the users click on this link, they get redirected to a fake website created and controlled by the pen tester. As a result, the users might end up giving their account details.

- **Urgency**

Urgency implies encouraging people to take an immediate action. The pen tester can take advantage of this by tricking victims into performing some pending tasks.

For example, ransomware often uses the urgency principle, which makes the victims take an urgent action in a limited time period. The victims see the countdown timer running on their infected systems, and failure to take a required decision under a specific time can result in loss of important data.

The pen tester can also send phishing emails indicating that a certain product is available at a low price and that to buy it, the user should click on the “Buy Now” link. The user is tricked, and they click on the link to take immediate action. As a result, the user is redirected to a malicious website and ends up entering their account details or downloading a virus file.

- **Familiarity/Likeness**

Familiarity or likeness implies the fact that people are more likely to get persuaded to do something when asked by someone they like. This indicates that people are more likely to buy products if they are advertised by celebrities they like.

For example, people are more likely to allow someone to look over their shoulder if they like that person or are familiar with them. Otherwise, if people do not recognize or like the person doing the act, they immediately recognize the shoulder surfing act and stop it. People might be more comfortable when they become aware that the person tailgating them is someone familiar who is headed to the same destination. A pen tester should ensure that they talk warmly to deceive the target user so that they like the pen tester.

- **Trust**

Using the trust principle, the pen tester can often attempt to build a trust relationship with victims.

For example, the pen tester can call a victim and introduce themselves as a security expert. The pen tester can then claim that they are working with a random company and that they noticed some unusual errors sent from the victim’s system. The pen tester builds trust by using the company name and their own experience in the security field. The victim starts trusting the pen tester who then guides them to follow a series of steps in order to view and disable the system errors. Later, the pen tester sends an email containing a malicious file and persuades the victim to click and download it. Through this process, the pen tester can even successfully install malware on the victim’s system and infect the system to steal important information.

- **Greed**

Greed implies that some people are possessive in nature and wish to acquire huge amounts of wealth from doing illegal activities. Pen testers can lure targets into divulging information by promising something in exchange for no effort or cost to the target, thereby exploiting greed.

For example, the pen tester may pretend to be a competitor of the target organization and lure the employees of the target into revealing critical information by offering a huge ransom.



Reporting and Countermeasures/Recommendations

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Reporting and Countermeasures/Recommendations

This section explains Step 4 in the social engineering testing process, namely, Reporting, and also presents common social engineering targets, various social engineering techniques, and defense strategies in a tabular format.

Document the Result



- Note **down the targets** (people) that you find vulnerable to social engineering attacks along with their name, contact details, department, etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Document the Result

Note down vulnerable targets (people) to social engineering attacks along with their details:

- Name and employee ID
- Official and personal email IDs and passwords
- Social security number and designation
- Workplace address and contact number
- Personal information
- Bank accounts and credit card numbers

Step 4: Reporting



- The social engineering pen test report should address all the relevant aspects pertaining to the **initial planning** and **scoping**, **target identification**, **tests conducted**, and identified **vulnerabilities**.
- The report must also include the **recommendations** and **countermeasures** required to mitigate the identified vulnerabilities and thwart future attacks.

Elements of social engineering pen test report

- Cover Page
- Title Page
- Disclaimer Page
- Table of Contents
- Social Engineering Overview
- Social Engineering Methodology

- Reporting
 - Introduction (What, Why, When, Where, and How)
 - An executive summary
 - Individual attack vectors
 - Identified technical risks
 - Potential impact of identified vulnerabilities
 - Remediation steps for each identified vulnerability
 - Recommendations for vulnerability elimination
 - Conclusions of the pen test

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Step 4: Reporting

Reporting is the final step. The pen tester must list all the results of the social engineering pen test in the report. While generating the report, the pen tester should consider the target audience of the report. Generally, in most cases, the audience comprises the senior management of the organization. The report should address all the relevant aspects pertaining to the initial planning and scoping, target identification, tests conducted, and identified vulnerabilities. Along with the identified vulnerabilities, the report must also include the recommendations and countermeasures required to mitigate the identified vulnerabilities and thwart future attacks.

The social engineering pen test report must contain the following elements.

- **Cover page:** Contains customer name, logo, and date of the report
- **Title page:** Contains the name of the author of the report along with version details
- **Disclaimer page:** Contains a disclaimer statement that describes the agreed upon terms and conditions between the tester/testing organization and the target organization/individual and extent of disclosure of sensitive information.
- **Table of contents:** Contains an index of the report
- **Social engineering overview:** Includes basic information about social engineering attacks and how to defend against such attacks
- **Social engineering methodology:** Includes the methodology used to perform the social engineering pen testing

- **Reporting:** After completing all the tests, the gathered information is used to construct the final report, which includes the following details:
 - Introduction (What, Why, When, Where, and How of the report)
 - An executive summary
 - Individual attack vectors
 - Identified technical risks
 - Potential impact of identified vulnerabilities
 - Remediation steps for each identified vulnerability
 - Recommendations for vulnerability elimination
 - Conclusions of the pen test

Social Engineering Countermeasures and Recommendations



Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk to never reveal passwords or other information by phone. Enforce policies for the front office and help desk personnel.
Technical support and system administrators	Impersonation, persuasion, intimidation, fake SMS, phone calls, and emails	Train technical support executives and system administrators to never reveal passwords or other information by phone or email.
Perimeter security	Impersonation, reverse social engineering, piggybacking, tailgating, etc.	Implement strict badge, token, or biometric authentication; employee training; and strict monitoring by security guards.
Office	Shoulder surfing, eavesdropping, ingratiation, etc.	Employee training, best practices, and checklists for using passwords. Ensure that all guests are escorted by an employee or relevant personnel.
Vendors of the target organization	Impersonation, persuasion, intimidation	Educate vendors about social engineering.
Mail room	Theft, damage, or forging of mails	Lock and monitor mail room, including employee training.
Machine room/Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to obtain the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep equipment inventory updated.
Company's executives	Fake SMS, phone calls, and emails to obtain confidential data	Train executives to never reveal identity, passwords, or other confidential information by phone or email.
Dumpsters	Dumpster diving	Keep all trash in secured and monitored areas, shred important data, and erase magnetic media.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering Countermeasures and Recommendations

The following table shows common social engineering targets, various social engineering techniques used, and the defense strategies to counter these attacks.

Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk to never reveal passwords or other information by phone. Enforce policies for the front office and help desk personnel.
Technical support and system administrators	Impersonation, persuasion, intimidation, fake SMS, phone calls, and emails	Train technical support executives and system administrators to never reveal passwords or other information by phone or email.
Perimeter security	Impersonation, reverse social engineering, piggybacking, tailgating, etc.	Implement strict badge, token, or biometric authentication; employee training; and strict monitoring by security guards.
Office	Shoulder surfing, eavesdropping, ingratiation, etc.	Employee training, best practices, and checklists for using passwords. Ensure that all guests are escorted by an employee or relevant personnel.
Vendors of the target organization	Impersonation, persuasion, intimidation	Educate vendors about social engineering.

Mail room	Theft, damage, or forging of mails	Lock and monitor mail room, including employee training.
Machine room/Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to obtain the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep equipment inventory updated.
Company's executives	Fake SMS, phone calls, and emails to obtain confidential data	Train executives to never reveal identity, passwords, or other confidential information by phone or email.
Dumpsters	Dumpster diving	Keep all trash in secured and monitored areas, shred important data, and erase magnetic media.

Table 4.1: Common social engineering targets and defense strategies