CEH v12 Lesson 9 : Social Engineering Exploits

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 — Social Engineering

After completing this module, you will have further knowledge of:

- Social Engineering Concepts
- Social Engineering Techniques
- Insider Threats
- Impersonation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures

Lab Duration

It will take approximately **30 minutes** to complete this lab.

Exercise 1 — Social Engineering

Social engineering is the art of manipulating and utilizing human behavior to conduct a security breach. During social engineering, the victim, who is being used as a subject for a security breach, does not realize that an attacker is using them to gain access to a system. Because of the unpredictability of users, they are considered the weakest link in the security chain and are easy to exploit to proficient social engineering attempts.

An attacker can use various methods in social engineering to gain sensitive and confidential information. The attacker can use methods such as sending an e-mail or redirecting the user to a malicious webpage. Several methods can be used, but each intends to get sensitive and confidential information for a security breach.

In this exercise, you will learn about social engineering.

Learning Outcomes

After completing this exercise, you will have further knowledge of:

- Social Engineering Concepts
- Social Engineering Techniques
- Insider Threats
- Impersonation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures

Social Engineering Concepts

With Social Engineering, an attacker psychologically manipulates a victim and uses misdirection to obtain desired information and can be considered the basis of passive information gathering techniques. With one user as a target in an organization, the attacker can perform a security breach of the entire network. It is just a matter of getting inside the network using the information provided by the user.

There can be various types of users targeted by social engineering. Some of the standard targets are:

- Receptionist
- IT Helpdesk
- HR department
- Top management

Social Engineering Techniques

An attacker may use different social engineering principles to gain information. An attacker uses various methods or techniques to obtain the desired information when using social engineering. The attacker in social engineering can use various techniques and methods, such as:

- **Authority**: An attacker displays confidence in pretending to be someone with authority and pressurizes the victim to provide information. For example, an

attacker may call the reception and tell the receptionist that he is calling from the police department and needs specific information.

- **Scarcity and urgency**: With this technique, a sense of urgency is created, which forces the victim to make a quick decision without thinking much. For example, an attacker may call a user to share the password to be reset immediately, or his account will be terminated.
- **Social proof**: Social proof is mainly used when the victim is in a situation that they do not know how to deal with. The victim decides by observing others. An attacker can apply this technique in more than one way by displaying an act that convinces them that this is the correct behavior.
- **Fear**: An attacker uses fear to make the victim do what they want. An attacker dramatizes the victim's situation to avoid a dangerous outcome quickly.
- **Consensus**: In this method, an attacker may create malware or rogueware and put fake testimonials to convince the people to use it. People are generally more convinced if they are convinced that many other people are using these products.
- **Familiarity**: In this method, an attacker becomes your friend. They share their likes and dislikes with you. When you are convinced that they are like you, an attacker may convince you to do something, such as provide information.
- **Trust**: An attacker creates a trusted channel with you in this method. You start trusting the person and believe that they are the fallback point if you have a problem. Once the trust is established, you are convinced to share the information they are looking for.
- **Baiting**: This is a technique in which an attacker offers something in exchange for important information such as login details and other sensitive data. Often attackers will leave a USB flash drive loaded with malware that has a corporate logo on it which can trick users into trusting the USB flash drive and opening it from their computer.
- **Quid Pro Quo**: This is a baiting technique where an attacker offers something in return for information. For example, an attacker might call various numbers retrieved from the corporate directory pretending to be from the IT department. The attacker will ultimately find someone with a technical issue, and they ask the user to

install some malicious files in an attempt to fix their issue. The malware will then collect sensitive information.

- **Elicitation**: A technique of extracting specific information from the victim by involving them in normal and disarming conversations.

Insider Threats

The term Insider Threat refers to people internal to an organization who carry out malicious activities, intentionally or unintentionally. Some of the activities they perform are handing out confidential or sensitive information to others, unintentionally releasing information to another threat actor who wants to misuse the information.

It is challenging to detect an insider threat as the person is part of the system. They would likely have access to data and knowledge of internal operations and processes. Since they are inside the network, traditional tools such as a firewall make their actions difficult to track.

Different Types of Insider Threats

- Privileged users with permissions
- Disgruntled employees
- Terminated employees
- Third parties with access to information
- Untrained employees
- Employees who lost devices

Impersonation on Social Networking Sites

Impersonation is an act performed by an individual pretending to be someone else. In a cybersecurity context, impersonation is using a fake identity. If an attacker is wrongly identified as a trustworthy entity, the victim will likely disclose confidential information, such as passwords, information related to financial transactions, etc.

Identity Theft

Identity theft is not a new type of crime and has been practiced for many decades. Before the Internet existed, this method was practiced mainly by forging signatures. However, with the invention of computers and the Internet many years later, digital identity theft

came into existence. In this method, a hacker steals someone's identity for personal benefit or financial advantage.

Billions of users are connected to the Internet, and the vast majority have entered their personal information on one website or another. When you save your information on the Internet, it may get exposed to a hacker if the site is hacked and its data is stolen.

A hacker may use the stolen information somewhere else. For example, a hacker may create another user account using your credentials. The situation worsens if this account is misused for harassing or threatening someone or even conducting an unlawful activity, such as stealing information.

Methods to Conduct Identity Theft

An attacker may use various methods to steal the identity of an individual. Some of the essential methods are:

- **Internet Searches**: A surprising amount of information exists for many people online as part of their digital footprint. Some information can even be found via a simple method, such as performing searches using search engines.
- **Social Engineering Techniques**: an attacker may use a social engineering technique to get information about an individual.
- **Dumpster Diving**: using the dumpster diving method, an attacker may be looking for vulnerable information about an individual or anyone who can be victimized for identity theft.
- **Shoulder Surfing**: an attacker directly observes information entered by the victim by standing very close or behind the victim or using vision-enhancing aids or binoculars to observe from far. Shoulder surfing attackers also use the technique of fixing up closed-circuit cameras hidden behind a wall or ceiling to obtain sensitive information.
- **Phishing**: phishing is a type of attack that uses social engineering as its base. It uses technical deception to convince a user to provide personal information, such as passwords, social security numbers, credit card numbers, bank account details, and so on.
- **Pharming**: a user is redirected to a malicious copy of a genuine website. When a user types the correct URL in the Web browser, the user is instead redirected to a

look-alike Website. The intent is to capture the user's information, such as username and password.

There can be several other methods that an attacker may use, but it depends on the expertise and situation with an attacker.

Indications of Identity Theft

You may not be immediately aware that you have become a victim of the identity theft attack, although there are some indications that you should look out for, such as:

- Profile updated on your bank account or credit card
- Unknown expenses in the credit card or bank statement
- Unexpected cash withdrawals from your accounts
- More than one social networking accounts in your name

Social Engineering Countermeasures

It is challenging to counter social engineering attacks. Various methods can be employed to reduce the chances of a social engineering attack. Let's look at some of these methods.

- **Training**: individuals must be trained with security training. The intent is not to make everyone a security professional but to understand the fundamental concepts. Within an organization, the individuals should be trained on security policies.
- **Access Privileges**: administrators must ensure that the proper access methods have been implemented. Access should be granted on the need to know basis. In addition, the users must be granted only the access and permissions required to perform their normal tasks as part of their job.
- **Background checks**: when hiring individuals, ensure that background checks are done.
- **Off-boarding**: When a user leaves an organization, their user account(s) must be closed immediately, or if they are required, passwords should be changed instead.
- **Two-factor authentication**: to safeguard employees' accounts, you must enable two-factor authentication. If an attacker gains access to the password, the second authentication factor will provide an extra layer to protect against unauthorized access to the account.

- **Software Updates**: there should be a process to update the software and operating systems as and when their updates are available.

Other than these methods, security policies play an essential role in countermeasures against social engineering attacks. These policies should be written and used for training users, which will eventually drive them to make correct security decisions.

For example, you need to have password policies in place. You, as a user, should understand that the core intent of the password policies, such as:

- Change passwords regularly
- Don’t share passwords with anyone
- Avoid using easy passwords — this can be handled with the password policy implementation
- Block user accounts after a certain number of failed login attempts

In addition, the organization should also implement social engineering campaigns. This is an effective method to check the reality of social engineering attacks. Once you have run various campaigns with several users, you should conduct a gap analysis to identify gaps. After gaps are identified, you need to create a remediation plan to mitigate them. The core intent is to know where the employees have failed in the social engineering attacks and educate them so that they don’t fail again.