Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 1/30/2022 11:20:10 am • Time spent: 01:00

Score: 100% Passing Score: 80%

Question 1: ✓ Correct

Ron, a hacker, wants to get access to a prestigious law firm he has been watching for a while. June, an administrative assistant at the law firm, is having lunch at the food court around the corner from her office. Ron notices that June has a picture of a dog on her phone. He casually walks by and starts a conversation about dogs. Which phase of the social engineering process is Ron in?

○ Research phase

➡ ● Development phase

○ Elicitation phase

○ Exploitation phase

EXPLANATION

The development phase involves two parts. These are selecting individual targets within a company and forming a relationship with those individuals.

The exploitation phase is when the attacker takes advantage of the relationship with the victim and uses the victim to extract information, obtain access, or accomplish the attacker's purposes in some way.

The research phase is when the attacker starts gathering information about the target company or organization.

Elicitation is a technique used to extract information from a target without arousing suspicion.

▼ Question 2: ✓ Correct

Social engineers are master manipulators. Which of the following are tactics they might use?

○ Shoulder surfing, eavesdropping, and keylogging

○ Keylogging, shoulder surfing, and moral obligation

○ Eavesdropping, ignorance, and threatening

➡ ◉ Moral obligation, ignorance, and threatening

EXPLANATION

Social engineers are master manipulators. Some of the most popular tactics they use are moral obligation, innate human trust, threatening, an easy reward, and ignorance.

Social engineering attacks include shoulder surfing, eavesdropping, USB and keyloggers, spam and spim, and hoaxes.

▼ Question 3: ✓ Correct

Any attack involving human interaction of some kind is referred to as what?

➡ ◉ Social engineering

○ An opportunistic attack

○ A white hat hacker

○ Attacker manipulation

EXPLANATION

Social engineering refers to any attack involving human interaction of some kind. Attackers who use social engineering try to convince a victim to perform actions or give out information they wouldn't under normal circumstances.

An opportunistic attack is typically automated and involves scanning a wide range of systems for known vulnerabilities, such as old software, exposed ports, poorly secured networks, and default configurations.

A white hat hacker helps companies find vulnerabilities in their security infrastructure.

Social engineers are master manipulators and use multiple tactics on their victims.

▼ **Question 4:** ✓ Correct

An organization's receptionist received a phone call from an individual claiming to be a partner in a high-level project and requesting sensitive information. The individual is engaging in which type of social engineering?

○ Social validation

○ Persuasive

➡ ● Authority

○ Commitment

EXPLANATION

Authority social engineering entails an attacker either lying about having authority or using their high status in a company to force victims to perform actions that exceed their authorization level.

Persuasive social engineering entails an attacker convincing a person to give them information or access that he or she shouldn't.

Social validation entails an attacker using peer pressure to coerce someone else to bend rules or give information he or she shouldn't.

Commitment social engineering entails convincing someone to buy into an overall idea and then demanding or including further specifics that were not presented up front.

Question 5: ✓ Correct

Which of the following is a common social engineering attack?

- ○ Using a sniffer to capture network traffic
- ○ Logging on with stolen credentials
- ○ Distributing false information about an organization's financial status
- ➡ ● Distributing hoax virus-information emails

EXPLANATION

Distributing hoax virus-information emails are a social engineering attack. This type of attack preys on email recipients who are fearful and will believe most information if it is presented in a professional manner. The victims of these attacks fail to double-check the information or instructions with a reputable third-party antivirus software vendor before implementing the recommendations. Usually, these hoax messages instruct the reader to delete key system files or download Trojans.

Social engineering relies on the trusting nature of individuals to take an action or allow an unauthorized action.

Question 6: ✓ Correct

Which of the following BEST describes an inside attacker?

- ➡ ● An unintentional threat actor. This is the most common threat.
- ○ A good guy who tries to help a company see their vulnerabilities.
- ○ An attacker with lots of resources and money at their disposal.
- ○ An agent who uses their technical knowledge to bypass security.

EXPLANATION

An insider could be a customer, a janitor, or even a security guard. But most of the time, it's an employee. Employees pose one of the biggest threats to any organization. An unintentional threat actor is the most common insider threat.

A hacker is any threat agent who uses their technical knowledge to bypass security, exploit a vulnerability, and gain access to protected information.

A white hat hacker is a good guy who tries to help a company see the vulnerabilities that exist in their security infrastructure.

Attacks from nation states are generally extremely well-supported and funded.

Question 7: ✓ Correct

Which of the following are examples of social engineering attacks? (Select three.)

- ➡ ☑ Impersonation
- ➡ ☑ Shoulder surfing
- ➡ ☑ Keylogging
- □ War dialing
- □ Port scanning

EXPLANATION

Social engineering leverages human nature. Internal employees are often the targets of trickery, and false trust can quickly lead to a serious breach of information security. Shoulder surfing and dumpster diving are examples of social engineering. Shoulder surfing is the act of looking over an authorized user's shoulder in hopes of obtaining an access code or credentials. Social engineers often employ keystroke loggers to capture usernames and passwords. Impersonation is pretending to be trustworthy and having a legitimate reason for approaching the target. This is done with the purpose of asking for sensitive information or access to protected systems. These low-tech attack methods are often the first course of action that a hacker pursues.

Port scanning and war dialing are technical attacks that seek to take advantage of vulnerabilities in systems or networks.

Question 8: ✓ Correct

Compliments, misinformation, feigning ignorance, and being a good listener are tactics of which social engineering technique?

- ➡ ● Elicitation
- ○ Interrogation
- ○ Impersonation
- ○ Preloading

EXPLANATION

Elicitation is a technique that aims to extract information from a target without arousing suspicion. Some elicitation tactics are giving compliments, delivering misinformation, feigning ignorance, and being a good listener.

Preloading is used to set up a target by influencing the target's thoughts, opinions, and emotions.

In the interrogation phase, the attacker talks to the target about their statements.

Impersonation is pretending to be trustworthy and approaching the target to ask him or her for sensitive information or convincing him or her to grant access to protected systems.

Question 9: ✓ Correct

Having a legitimate reason for approaching someone to ask for sensitive information is called what?

- ○ Pretexting
- ○ Footprinting
- ○ Preloading
- ➡ ● Impersonation

EXPLANATION

Impersonation is pretending to be somebody else and approaching a target to extract information.

Pretexting is using a fictitious scenario to persuade someone to perform an action or give information they aren't authorized to share.

Footprinting is similar to stalking, but in a social engineering context.

Preloading is influencing a target's thoughts, opinions, and emotions before something happens.

Question 10: ✓ Correct

Jason is at home, attempting to access the website for his music store. When he goes to the website, it has a simple form asking for a name, email, and phone number. This is not the music store website. Jason is sure the website has been hacked. How did the attacker accomplish this hack?

○ Social networking

➡ ● DNS cache poisoning

○ Feigning ignorance

○ Host file modification

EXPLANATION

In DNS cache poisoning, the attacker launches the attack on the chosen DNS server. Then the attacker changes a target website's IP address to a fake IP address. When the user enters the target website's URL, the DNS server redirects them to the fake IP address that was modified by the attacker. This ends up taking the target to a fake website controlled by the attacker.

In host file modification, the attacker sends a malicious code as an email attachment. When the user opens the attachment, the malicious code executes and modifies local host files on the user's computer.

Many social engineers use applications such as Facebook, Twitter, and Instagram to gather information and steal identities, among other nefarious acts.

An attacker feigning ignorance might make a wrong statement and then admit to not knowing much about the subject, but that event does not occur in this attack scenario.