

## Exam Report: 3.1.11 Practice Questions

Date: 4/4/29 5:08:57 pm  
Time Spent: 4:32

Candidate: Garsteck, Matthew  
Login: mGarsteck

## Overall Performance

Your Score: 50%



View results by: ☐ Objective Analysis ☒ Individual Responses

## Individual Responses

## ▼ Question 1:

Incorrect

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

- ➡ ☐ Moral obligation, ignorance, and threatening
- ☐ Keylogging, shoulder surfing, and moral obligation
- ☒ ~~Eavesdropping, ignorance, and threatening~~
- ☐ Shoulder surfing, eavesdropping, and keylogging

## 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.

## References

TestOut Ethical Hacker Pro - 3.1 Social Engineering  
[e\_social\_eng\_eh1.exam.xml Q\_SOCIAL\_ENG\_ATTACKER\_MANIP\_01\_EH1]

## ▼ Question 2:

Correct

Which of the following best describes a script kiddie?

- ☐ A hacker whose main purpose is to draw attention to their political views.
- ☐ A hacker willing to take more risks because the payoff is a lot higher.
- ☐ A hacker who helps companies see the vulnerabilities in their security.
- ➡ ☒ A hacker who uses scripts written by much more talented individuals.

## Explanation

A script kiddie is a hacker who uses scripts written by much more talented individuals.

A hacktivist is a hacker whose main purpose is to draw attention to their political views.

A white hat hacker is a hacker who helps companies see the vulnerabilities in their security.

A cybercriminal is a hacker willing to take large risks, such as spending time in jail or prison, for high payoffs.

## References

TestOut Ethical Hacker Pro - 3.1 Social Engineering  
[e\_social\_eng\_eh1.exam.xml Q\_SOCIAL\_ENG\_OVERVIEW\_FACTS\_01\_EH1]

## ▼ Question 3:

Correct

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

- ☐ An opportunistic attack
- ☐ Attacker manipulation
- ☒ Social engineering
- ☐ A white hat hacker

## 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.

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

## References

TestOut Ethical Hacker Pro - 3.1 Social Engineering

[e\_social\_eng\_eh1.exam.xml Q\_SOCIAL\_ENG\_OVERVIEW\_FACTS\_02\_EH1]

### ▼ Question 4:

Incorrect

Using a fictitious scenario to persuade someone to perform an action or give information they aren't authorized to share is called:

- ☐ Preloading
- ☒ Impersonation
- ☐ Pretexting
- ☐ Footprinting

## Explanation

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.

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

## References

TestOut Ethical Hacker Pro - 3.1 Social Engineering

[e\_social\_eng\_eh1.exam.xml Q\_SOCIAL\_ENG\_PRETEXTING\_01\_EH1]

### ▼ Question 5:

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?

- ☐ Elicitation phase
- ☐ Exploitation phase
- ☐ Research phase
- ☒ Development phase

## Explanation

The development phase involves two parts: 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.

## References

TestOut Ethical Hacker Pro - 3.1 Social Engineering

[e\_social\_eng\_eh1.exam.xml Q\_SOCIAL\_ENG\_SOCIAL\_PROCESS\_01\_EH1]

### ▼ Question 6:

Incorrect

You are instant messaging a coworker, and you get a malicious link. Which type of social engineering attack is this?

☐ Spam

➡ ☐ Spim

☒ Surf

☐ Hoax

## Explanation

Spim is a malicious link sent to the target over instant messaging.

Email hoaxes trick a target into sharing sensitive information with an attacker.

Spam emails include a malicious embedded URL or banner ads that entice users to click them.

Shoulder surfing involves looking over someone's shoulder while they work on a computer to see usernames, passwords, or account numbers.

## References

TestOut Ethical Hacker Pro - 3.1 Social Engineering

[e\_social\_eng\_eh1.exam.xml Q\_SOCIAL\_ENG\_SOCIAL\_ATTACKS\_01\_EH1]

### ▼ Question 7:

Correct

Brandon is helping Fred with his computer. He needs Fred to enter his username and password into the system. Fred enters the username and password while Brandon is watching him. Brandon explains to Fred that it is not a good idea to allow anyone to watch you type in usernames or passwords. Which type of social engineering attack is Fred referring to?

➡ ☒ Shoulder surfing

☐ Spam and spim

☐ Eavesdropping

☐ Keyloggers

## Explanation

Shoulder surfing involves looking over someone's shoulder while they work on a computer to see usernames, passwords, or account numbers.

Eavesdropping is when an unauthorized person listens to conversations when employees or other authorized personnel are discussing sensitive topics.

Social engineers often employ keyloggers to capture usernames and passwords. As the target logs in, the username and password are saved.

Spam is an email that includes a malicious embedded URL or a banner ad that entices the user to click on it. Spim is a malicious link sent to the target over instant messaging instead of email.

## References

TestOut Ethical Hacker Pro - 3.1 Social Engineering

[e\_social\_eng\_eh1.exam.xml Q\_SOCIAL\_ENG\_SOCIAL\_ATTACKS\_02\_EH1]

### ▼ Question 8: Correct

Which of the following best describes an inside attacker?

- ☐ A good guy who tries to help a company see their vulnerabilities.
- ☐ An attacker with lots of resources and money at their disposal.
- ➡ ☒ An unintentional threat actor; the most common threat.
- ☐ 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.

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

## References

TestOut Ethical Hacker Pro - 3.1 Social Engineering

[e\_social\_eng\_eh1.exam.xml Q\_SOCIAL\_ENG\_TYPE\_ATTACKERS\_01\_EH1]

### ▼ Question 9: Incorrect

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

- ☐ Impersonation
- ➡ ☐ Elicitation
- ☐ Interrogation
- ☒ Preloading

## Explanation

Elicitation is a technique that aims to extract information from a target without arousing suspicion. Some of the 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 them for sensitive information or convincing a target to grant a hacker access to protected systems.

## References

TestOut Ethical Hacker Pro - 3.1 Social Engineering

[e\_social\_eng\_eh1.exam.xml Q\_SOCIAL\_ENG\_TECHNIQUES\_ELICITATION\_01\_EH1]

### ▼ Question 10: Correct

You get a call from one of your best customers. The customer is asking about your company's employees,

teams, and managers. What should you do?

- ➡ ☒ You should not provide any information and forward the call to the help desk.
- ☐ You should put the caller on hold and then hang up.
- ☐ You should provide the information as part of quality customer service.
- ☐ You should not provide any information except your manager's name and number.

## Explanation

Every employee in the company should be taught that if somebody calls them and claims to be someone who needs employee information, especially usernames and passwords, they should forward that call to the help desk.

## References

TestOut Ethical Hacker Pro - 3.1 Social Engineering

[e\_social\_eng\_eh1.exam.xml Q\_SOCIAL\_ENG\_TECHNIQUES\_INTERVIEW\_01\_EH1]

### ▼ Question 11: Incorrect

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 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?

- ➡ ☐ DNS cache poisoning
- ☒ Feigning ignorance
- ☐ Social networking
- ☐ 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 website. When the user enters the target website's URL, the DNS server redirects them to the fake IP address modified by the attacker and then 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, but no social media is involved in this attack.

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.

## References

TestOut Ethical Hacker Pro - 3.1 Social Engineering

[e\_social\_eng\_eh1.exam.xml Q\_PHISHING\_TECHNIQUES\_OTHER\_ATTACKS\_01\_EH1]

### ▼ Question 12: Incorrect

An attack that targets senior executives and high-profile victims is referred to as:

- ☐ Vishing
- ☐ Pharming
- ☒ Scrubbing
- ➡ ☐ Whaling

## Explanation

Whaling is another form of phishing that targets senior executives and high-profile victims.

Pharming involves the attacker executing malicious programs on the target's computer so that when the user enters any URL, it redirects traffic to the attacker's malicious website.

Vishing is like phishing, but instead of an email, the attacker uses Voice over IP (VoIP) to gain sensitive information. The term is a combination of voice and phishing.

Scrubbing is one of the most common ways to pick a lock.

## References

TestOut Ethical Hacker Pro - 3.1 Social Engineering

[e\_social\_eng\_eh1.exam.xml Q\_PHISHING\_TECHNIQUES\_PHISHING\_01\_EH1]