TT TEXTBOOK TESTBANKS

Test Bank for CompTIA Security SY0 601 Cert Guide 5th Santos

TEST BANK SAMPLE PREVIEW

PUBLISHER

Pearson

COPYRIGHT

2022

RESOURCE TYPE

Test Bank

ISBN

9780136770008

Chapter 1: Comparing and Contrasting Different Types of Social Engineering Techniques

1. Which of these is an example of social engineering?

A. Phishing
B. Virus
C. Worm
D. Trojan horse

Answer: A

2. Impersonating someone's identity for the purpose of gaining information is called:

A. Phishing
B. Spear phishing
C. Pretexting
D. Tailgating

Answer: C

3. Smishing attacks are carried out using what medium?

A. Email
B. Text messages
C. Websites
D. Voice

Answer: B

4. Which of these describes a threat actor redirecting a victim from a valid website to a malicious fake?

A. Pharming
B. Tailgating
C. Dumpster diving
D. Phishing

Answer: A

5. Whaling is most similar to which other kind of attack?

A. Credential harvesting
B. Watering hole attack
C. Shoulder surfing
D. Phishing

Answer: D

6. Which of these is NOT a type of social engineering attack?

A. Prepending
B. Piggybacking
C. Spear phishing
D. Pretexting

Answer: A

7. Which kind of attack targets users based on the common websites they frequent?

A. Pretexting
B. Watering hole attack
C. Eavesdropping
D. Vishing

Answer: B

8. A social engineer calls an IT specialist sounding panicked and stating that they are an employee who needs to get into their email account right away to address a time-sensitive request from an important client. Which motivation technique are they using?

A. Urgency
B. Scarcity
C. Authority
D. Intimidation

Answer: A

9. Which of these is NOT a best practice for avoiding social media attacks?

A. Never share passwords or PINs.
B. Shield keypads and screens when entering authentication information.
C. Examine any unknown removable media to make sure it does not contain malware.
D. Shred any sensitive information destined for garbage or recycling.

Answer: C

10. What government funded research association provides a set of matrices that document the tactics attackers use to compromise systems?

A. The MITRE Corporation
B. W3C
C. The Social Engineering Toolkit
D. MAL*WAR

Answer: A

Chapter 2: Analyzing Potential Indicators to Determine the Type of Attack

1. Ransomware is a type of what?

A. Cryptoviral extortion
B. Distributed denial of service attack
C. Worm
D. Trojan horse

Answer: A

2. Which of these is a program that appears useful but allows an attacker administrator-level access to a system?

A. Worm
B. Keylogger
C. Rainbow table
D. Remote access Trojan (RAT)

Answer: D

3. What is the purpose of a rootkit?

A. Encrypt important files and ask for payment to decrypt them
B. Spread virus code by attaching to executable files
C. Install at a low level and then perform malicious operations without being detected
D. Secretly record all keystrokes, including passwords

Answer: C

4. Which of these is a key characteristic of a worm?

A. Replicates by attaching itself to executable files
B. Self-replicates
C. Is able to crack weak passwords
D. Appears to be a legitimate program but contains malware

Answer: B

5. A keylogger is a form of what type of malware?

A. Spyware
B. Logic bomb
C. Virus
D. Ransomware

Answer: A

6. Suppose a user clicks on an offer to install a web browser toolbar that is supposed to provide helpful shortcuts, but a side effect is that it changes his default search engine to one owned by that company. What kind of malware is this an example of?

A. Ransomware
B. Grayware
C. Brute-force attack
D. Remote access Trojan

Answer: B

7. Which of these is an attack that attempts to discover a user's password?

A. Worm
B. Ransomware
C. Logic bomb
D. Rainbow table

Answer: D

8. Which of these is a type of attack that uses a physical device to do its work?

A. Logic bomb
B. Fileless virus
C. Skimming
D. Backdoor

Answer: C

9. Which of these attacks is a potential attack vector for an attack on a cloud computing system?

A. Session hijacking
B. Card cloning
C. PUP
D. Collision

Answer: A

10. What does a birthday attack target?

A. Local hard disk file system
B. Hashing system
C. Certain types of files, such as graphics
D. Physical equipment such as USB flash drives

Answer: B

INSTRUCTOR'S GUIDE TO ACCOMPANY COMPTIA SECURITY+ SY0-601 CERT GUIDE (ISBN 9780136770312)

CHAPTER 1

COMPARING AND CONTRASTING DIFFERENT TYPES OF SOCIAL ENGINEERING TECHNIQUES

CHAPTER OBJECTIVES

When students have finished reading this chapter, they will understand the following:

- The major categories of social engineering attacks
- How social engineering attacks take place and what conditions create vulnerabilities
- The importance of in-depth and frequent user security awareness training

CHAPTER OVERVIEW

In this chapter, students will learn the methods and techniques that social engineers can employ to gain access to buildings and systems and obtain company data and personal information. They will also learn the various ways that these social engineers can be defeated.

CHAPTER OUTLINE

1. Social Engineering Fundamentals

2. User Security Awareness Education

SUGGESTED CLASS STRUCTURE

Direct students to take the "Do I Know This Already?" quiz and then to read the chapter before class.

During class, lead a discussion of the chapter's concepts using the PowerPoint presentation provided in the instructor materials. The PowerPoint slides provide some basic facts and topics, but you will want to supplement this information with information from the textbook and other resources and with stories from your own experience.

End with the Review Questions in the text and the Activities for Class at the end of this chapter's Instructor's Guide.

TEACHING NOTES AND TIPS PER TOPIC

1. **Social Engineering Fundamentals**

Teaching Note: This section introduces the vast scope of social engineering and its impact to organizations and individuals. Social engineering can be done in person by an insider or an outside entity or through many digital methods.

Teaching Tip: The main reason social engineering succeeds is that there are many techniques and relatively low user awareness. Review the common social engineering techniques with students and ask them to share which ones they have knowledge. Which ones have they actually experienced in their personal or professional lives?

Teaching Tip: Phishing and pretexting are two common methods of obtaining information by pretending to be someone else. Review these two concepts and explain that the main differences between phishing and pretexting is that pretexting is the act of impersonating someone's identity. In the last 90 days how many phishing attempts on average have students experienced? Has this number increased over the last 12 months?

Teaching Tip: Spam is the receipt of unwanted and unsolicited email messages. Most users have been on the receiving end of spam and have put measures in place to block them. Ask students what filters they have set up to address spam in their ongoing daily lives.

Teaching Tip: Review shoulder surfing, piggybacking, and tailgating. These are methods where the user is physically followed or tagged by an unauthorized person. What physical methods can be put in place in a professional environment to prevent this?

Teaching Tip: Attackers have become adept and very sophisticated at eliciting information without directly asking. Review examples of open-ended questions that attacker could potentially use to learn about an end user's habits, preferences, and vulnerabilities.

Teaching Tip Identity fraud is a social engineering technique that has the most financial impact on the unfortunate recipient. What are the key pieces of personally identifiable information (PII) that everybody should lock down and keep secure to prevent identity theft?

Teaching Tip: Hoaxes are attempts to lower the confidence of a potential attack recipient or confuse them. Both have the end goal of lowering a person's guard in order to perpetrate an attack. Ask students to share any hoax experiences that they have personally experienced or have heard of.

2. **User Security Awareness Education**

Teaching Note: User awareness is critical to preventing security breaches. However, attackers are coming up with methods faster than organizations can keep up. How can automation help with this endeavor?

Teaching Tip: Every organization has some level of technology and security training for employees. Typically, this training is mandatory and is refreshed and retaken at least once a year. Given the rapid rise in security incidents and attacker aggressiveness, ask students if they feel that training frequency should be increased. What are the advantages and disadvantages to increasing training frequency?

ACTIVITIES FOR CLASS

I. Discussion Topics

Question 1: Review the two hoax examples in the chapter: Google's supposed name change to "Topeka" and the supposed assassination of Bill Gates. What would have been the impacts of these hoaxes were people to believe them?

Answer 1: Both hoax examples would have had major financial market implications. The market value of an organization is impacted by its brand, name, and perception of leadership strength. In both hoax examples, these factors would have been compromised.

Question 2: In a post-pandemic, increased work-from-home environment, what social engineering attacks would likely be on the rise and why?

Answer 2: Digital social engineering attacks would most likely be increasing because employees are conducting most if not all work from home. Examples are phishing, pharming, and credential harvesting. Because employees use their personal Internet Service Provider to connect to company systems from home, there is a potential for attackers to tap into those connections.

Question 3: Compromised corporate information can have severe business impact if it gets into the wrong hands. Should employees be subjected to punitive action if they do not keep up with security training and awareness on a timely basis?

Answer 3: Many organizations are putting strict deadlines, multiple reminders, and system lockout processes in place if employees do not complete mandatory training as required.

II. Exercises and Activities

Web Search Exercise: Zoom is one of the most common platforms for meetings and its use has increased exponentially. Research the security hardening features Zoom has put in place since the pandemic. Report your findings to the class.

Web Search Exercise: Find examples of employee security awareness training workshops. What topics are covered? Report your findings to the class.

Web Search Exercise: Review the MITRE matrices at https://attack.mitre.org. Which tactics and techniques are the most common and why? Report your findings to the class.

Review Key Terms: Review these terms from the chapter:

- phishing
- pretexting
- spear phishing
- whaling
- smishing
- vishing
- spam
- dumpster diving
- shoulder surfing
- pharming
- piggybacking
- tailgating
- eliciting information
- prepending
- credential harvesting
- hoax
- watering hole attack

- typo squatting,
- social media
- hybrid warfare

WEB RESOURCES

- Social Engineering Attacks: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
- Avoiding Social Engineering and Phishing Attacks: https://us-cert.cisa.gov/ncas/tips/ST04-014
- Email Spam: https://searchsecurity.techtarget.com/definition/spam
- What Is the MITRE Att&ck Framework?: https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html
- Personally Identifiable Information (PII): https://www.imperva.com/learn/data-security/personally-identifiable-information-pii/
- Dumpster Diving: An Easy Guide In 2021: https://www.jigsawacademy.com/blogs/cyber-security/dumpster-diving
- Zoom Security Issues: https://www.tomsguide.com/news/zoom-security-privacy-woes

uCertify

If you are using the uCertify course and labs product, be sure to review the associated online labs for this chapter. Students can do these labs as homework or during class time for hands-on practice to reinforce core learning objectives.

CHAPTER 2

ANALYZING POTENTIAL INDICATORS TO DETERMINE THE TYPE OF ATTACK

CHAPTER OBJECTIVES

When students have finished reading this chapter, they will understand the following:

- The different categories of malicious software
- How password attacks take place
- Physical attack exposures in buildings
- How attacks can target artificial intelligence and machine learning implementations
- The business implications of supply chain attacks
- How attacks are directed to on premises and cloud environments
- Attacks that are launched against encryption cryptography implementations

CHAPTER OVERVIEW

In this chapter, students will learn about the various security threats that can occur on a computer system—how they are classified, how they are delivered to the target computer, how to prevent security threats from happening, and how to troubleshoot them if they do occur.

CHAPTER OUTLINE

3. Malicious Software (Malware)

4. Password Attacks

5. Physical Attacks

6. Adversarial Artificial Intelligence (AI)

7. Supply-Chain Attacks

8. Cloud-based vs On-premises Attacks

9. Cryptographic Attacks

SUGGESTED CLASS STRUCTURE

Direct students to take the “Do I Know This Already?” quiz and then to read the chapter before class.

During class, lead a discussion of the chapter’s concepts using the PowerPoint presentation provided in the instructor materials. The PowerPoint slides provide some basic facts and topics, but you will want to supplement this information with information from the textbook and other resources and with stories from your own experience.

End with the Review Questions in the text and the Activities for Class at the end of this chapter’s Instructor’s Guide.

TEACHING NOTES AND TIPS PER TOPIC

3. **Malicious Software (Malware)**

Teaching Note: This section defines how malicious software (malware) infiltrates computer systems and damages them without the user's knowledge or consent. Malware includes viruses, worms, Trojan horses, spyware, adware, and other types of harmful software.

Teaching Tip: Review each category of malware and explain how each attack is initiated and is able to invade a computer system. What preventative measures can the IT department, as well as individuals, put in place to either reduce or eliminate the entry point for each type of attack?

Teaching Tip: Bots are particularly serious forms of malware because of their ability to multiply very quickly through the direction of a remote-controlled master computer. Review the example in the text around how bots are used to execute distributed denial-of-service (DDoS) attacks.

4. **Password Attacks**

Teaching Note: This section defines the techniques used by attackers to learn and steal credentials, known as passwords. Once a password is compromised, attackers usually have a broad array of resources within the system that they are now able to attack.

Teaching Tip: Review the types of password attacks. Point out to students that sophisticated attackers are able to reverse engineer and discover passwords that are encrypted. This is the reason why organizations now have put frequent mandatory password change cycles in place.

Teaching Tip: Most organizations use single sign-on. The benefit to the users is that they can leverage one password to access all the systems they need for their daily operations. However, once an attacker learns the password, they have a broader domain of resources to attack. What combination of password strategies can keep single sign-on safe?

5. **Physical Attacks**

Teaching Note: This section discusses how an organization's building and physical assets house resources that should be properly protected. This includes door access and physical media. Physical attacks are among the most common in an organization.

Teaching Tip: Review the physical media that can be easily compromised by an attacker to install malicious software. This includes commonly used devices such as USB drives, cables, and cards. What type of extra security measures can be put in place for these physical devices?

Teaching Tip: RFID tags are used extensively in organizations to manage inventory and other supply chain assets. Attackers can reverse engineer and RFID tag and learn the passcode. Review the technologies that can be used to harden and lock down RFID devices.

6. **Adversarial Artificial Intelligence**

Teaching Note: Artificial intelligence and machine learning may be new to students who have not already taken a class on this topic. Review the concepts of AI and ML, explain how large amounts of data are acquired, how models are trained to analyze the data.

Teaching Tip: Many organizations use machine learning extensively to improve operational processes as well as customer service. What is an ML example used in banking? In retail? How would data tainting affect the outcomes in these two use cases?

7. **Supply Chain Attacks**

Teaching Note: This section explains the business-critical implications of attacks on organizations' supply chains. Review the concept of supply chain to students who may not have already taken a class on this topic.

8. **Cloud-based vs On-premises Attacks**

Teaching Note: This section reviews security considerations when organizations move from on-premises to a cloud model. Threats that existed on-premises can still happen in the cloud. The cloud providers are responsible for access control, adhering to regulatory requirements, and regular audits.

Teaching Tip: Cloud providers operate on the concept of multi-tenancy. This means that organizations that subscribe to the cloud are placing their data in a pool of resources shared by other customers. Review the responsibilities and compliance requirements that every cloud provider typically has in their contract.

9. **Cryptographic Attacks**

Teaching Note: This section defines the common attacks that are launched against weak cryptography implementations. Review the concepts of encryption and hashing algorithms to students who may not have already taken a class on this topic.

Teaching Tip: Review collision, birthday, and downgrade attacks. Why are government and national security cryptography standards recommended and increasingly being used in the private sector?

ACTIVITIES FOR CLASS

I. Discussion Topics

Question 1: Why is spyware one of the most common types of malicious software?

Answer 1: Spyware is very easy to install on a computer because it is connected to advertising pop-ups and third-party applications. When an end-user visits any number of e-commerce sites or downloads free application, they are exposing their device to spyware.

Question 2: For troubleshooting purposes, system administrators often configure a network port as a backdoor to access a server in the event that it becomes unoperational. However, backdoors are potential points of entry for attackers. What technology can be used to potentially further lot down a backdoor?

Answer 2: Encryption or some type of multifactor authentication is typically used to ensure that only authorized users of the back door are getting access.

Question 3: Before signing a contract with the cloud provider, what security issues must be addressed and documented in the contract?

Answer 3: Encryption, compliance, audit, and incident response.

II. Exercises and Activities

Web Search Exercise: Ransomware is malware that holds an organization's critical data until a payment is received. Research a recent healthcare ransomware incident. Report your findings to the class.

Web Search Exercise: Keyloggers are legal in some countries and are designed to allow employers to oversee the use of computers issued to employees. Research the GDPR regulation to learn its position on keylogging and other security guidelines. Report your findings to the class.

Web Search Exercise: Public cloud providers have and continue to make significant investment in security. Use the Internet to research if there are any recent reported public cloud security incidents. Report your findings to the class.

Review Key Terms: Review these terms from the chapter:

- malware
- ransomware
- cryptomalware
- Trojans
- remote access Trojans (RATs)
- rootkit
- worm
- fileless malware
- bots
- botnet
- command and control
- logic bomb
- spyware
- potentially unwanted programs (PUPs)
- keylogger
- backdoors
- dictionary-based attack
- brute-force attack
- password spraying
- online password cracker
- offline password cracker
- rainbow table
- plaintext
- malicious flash drives
- malicious USB cables
- card cloning attacks
- skimming
- supply-chain attack
- cryptographic attacks
- collision
- birthday attack
- downgrade attack

WEB RESOURCES

- What Is Malware?: https://www.cisco.com/c/en_in/products/security/advanced-malware-protection/what-is-malware.html
- All About Ransomware: https://www.malwarebytes.com/ransomware
- Crypto-malware—A Look at the Latest Malware Threat: https://www.lastline.com/blog/crypto-malware-a-look-at-the-latest-malware-threat/
- What are Bots? – Definition and Explanation: https://www.kaspersky.com/resource-center/definitions/what-are-bots
- 9 of History's Notable Botnet Attacks: https://www.humansecurity.com/blog/9-of-the-most-notable-botnets
- How to Avoid Potentially Unwanted Programs: https://blog.malwarebytes.com/101/2016/02/how-to-avoid-potentially-unwanted-programs/
- Keyloggers: How They Work and How to Detect Them: https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/
- Password Spraying: https://www.coalfire.com/the-coalfire-blog/march-2019/password-spraying-what-to-do-and-how-to-avoid-it

uCertify

If you are using the uCertify course and labs product, be sure to review the associated online labs for this chapter. Students can do these labs as homework or during class time for hands-on practice to reinforce core learning objectives.