QUESTIONS

1. An organization's building has a guard posted at the lone entrance. A door leads into a smaller room with a second door heading into the interior of the building. Which physical security measure is in place?
   - **A.** Guard shack
   - **B.** Turnstile
   - **C.** Man shack
   - **D.** Man trap
2. In your social engineering efforts, you call the company help desk and pose as a user who has forgotten a password. You ask the technician to help you reset your password, which they happily comply with. Which social engineering attack is in use here?
   - **A.** Piggybacking
   - **B.** Reverse social engineering
   - **C.** Technical support
   - **D.** Halo effect
3. Which of the following is a true statement regarding biometric systems?
   - **A.** The lower the CER, the better the biometric system.
   - **B.** The higher the CER, the better the biometric system.
   - **C.** The higher the FRR, the better the biometric system.
   - **D.** The higher the FAR, the better the biometric system.
4. A pen tester sends an unsolicited e-mail to several users on the target organization. The e-mail is well crafted and appears to be from the company's help desk, advising users of potential network problems. The e-mail provides a contact number to call in the event a user is adversely affected. The pen tester then performs a denial of service on several systems and receives phone calls from users asking for assistance. Which social engineering practice is in play here?
   - **A.** Technical support
   - **B.** Impersonation
   - **C.** Phishing
   - **D.** Reverse social engineering

5. A pen test member has gained access to a building and is observing activity as he wanders around. In one room of the building, he stands just outside a cubicle wall opening and watches the onscreen activity of a user. Which social engineering attack is in use here?
   - **A.** Eavesdropping
   - **B.** Tailgating
   - **C.** Shoulder surfing
   - **D.** Piggybacking
6. A recent incident investigated by the local IR team involved a user receiving an e-mail that appeared to be from the U.S. Postal Service, notifying her of a package headed her way and providing a link for tracking the package. The link provided took the user to what appeared to be the USPS site, where she input her user information to learn about the latest shipment headed her way. Which attack did the user fall victim to?
   - **A.** Phishing
   - **B.** Internet level
   - **C.** Reverse social engineering
   - **D.** Impersonation
7. Which type of social engineering attacks uses phishing, pop-ups, and IRC channels?
   - **A.** Technical
   - **B.** Computer based
   - **C.** Human based
   - **D.** Physical
8. An e-mail sent from an attacker to a known hacking group contains a reference stating, "Rebecca works for the finance department at *business-name* and is the administrative assistant to the chief. She can be reached at *phone-number*." What is most likely being communicated here?
   - **A.** The name of an administrative assistant is being published to simplify later social engineering attacks.
   - **B.** The administrative assistant for the chief of the finance department at this business is easily swayed by social engineering efforts.
   - **C.** The finance department has a lax security policy in place.
   - **D.** None of the above. There is not enough information to form a conclusion.

9. Which of the following constitutes the highest risk to the organization?
   - **A.** Black-hat hacker
   - **B.** White-hat hacker
   - **C.** Gray-hat hacker
   - **D.** Disgruntled employee
10. After observing a target organization for several days, you discover that finance and HR records are bagged up and placed in an outside storage bin for later shredding/recycling. One day you simply walk to the bin and place one of the bags in your vehicle, with plans to rifle through it later. Which social engineering attack was used here?
   - **A.** Offline
   - **B.** Physical
   - **C.** Piggybacking
   - **D.** Dumpster diving
11. An attacker waits outside the entry to a secured facility. After a few minutes an authorized user appears with an entry badge displayed. He swipes a key card and unlocks the door. The attacker, with no display badge, follows him inside. Which social engineering attack just occurred?
   - **A.** Tailgating
   - **B.** Piggybacking
   - **C.** Identity theft
   - **D.** Impersonation
12. Which threat presents the highest risk to an organization's resources?
   - **A.** Government-sponsored hackers
   - **B.** Social engineering
   - **C.** Disgruntled employees
   - **D.** Script kiddies
13. Which of the following may be effective countermeasures against social engineering? (Choose all that apply.)
   - **A.** Security policies
   - **B.** Operational guidelines
   - **C.** Appropriately configured IDS
   - **D.** User education and training
   - **E.** Strong firewall configuration

14. Which of the following are indicators of a phishing e-mail? (Choose all that apply.)
    - **A.** It does not reference you by name.
    - **B.** It contains misspelled words or grammatical errors.
    - **C.** It contains spoofed links.
    - **D.** It comes from an unverified source.
15. You are discussing physical security measures and are covering background checks on employees and policies regarding key management and storage. Which type of physical security measures are being discussed?
    - **A.** Physical
    - **B.** Technical
    - **C.** Operational
    - **D.** Practical
16. Which of the following resources can assist in combating phishing in your organization? (Choose all that apply.)
    - **A.** Phishkill
    - **B.** Netcraft
    - **C.** Phishtank
    - **D.** IDA Pro
17. In order, what are the three steps in a reverse social engineering attack?
    - **A.** Technical support, marketing, sabotage
    - **B.** Sabotage, marketing, technical support
    - **C.** Marketing, technical support, sabotage
    - **D.** Marketing, sabotage, technical support
18. Which type of social engineering makes use of impersonation, dumpster diving, shoulder surfing, and tailgating?
    - **A.** Physical
    - **B.** Technical
    - **C.** Human based
    - **D.** Computer based
19. In examining the About Us link in the menu of a target organization's website, an attacker discovers several different individual contacts within the company. She crafts an e-mail asking for information to one of the contacts that appears

to come from an individual within the company who would be expected to make such a request. The e-mail provides a link to click, which then prompts for the contact's user ID and password. Which of the following best describes this attack?

A. Trojan e-mailing

B. Spear phishing

C. Social networking

D. Operational engineering

20. A security admin has a control in place that embeds a unique image into e-mails on specific topics, which verifies the message as authentic and trusted. Which antiphishing method is being used?

A. Steganography

B. Sign-in seal

C. PKI

D. Captcha

21. Which of the following should be in place to assist as a social engineering countermeasure? (Choose all that apply.)

A. Classification of information

B. Strong security policy

C. User education

D. Strong change management process

22. Joe uses a user ID and password to log into the system every day. Jill uses a PIV card and a PIN. Which of the following statements is true?

A. Joe and Jill are using single-factor authentication.

B. Joe and Jill are using two-factor authentication.

C. Joe is using two-factor authentication.

D. Jill is using two-factor authentication.

23. A system owner has implemented a retinal scanner at the entryway to the data floor. Which type of physical security measure is this?

A. Technical

B. Single factor

C. Computer based

D. Operational

24. Which of the following is the best representation of a technical control?
    - **A.** Air conditioning
    - **B.** Security tokens
    - **C.** Automated humidity control
    - **D.** Fire alarms
    - **E.** Security policy
25. A security admin at an organization boasts that her security measures are top notch and cannot be breached. In discussing their biometric authentication mechanisms, which of the following presents a reason biometric systems may still fall under successful attack?
    - **A.** The digital representation of the biometric entry may not be unique, even if the physical characteristic is.
    - **B.** Biometric compares a copy to a copy instead of the original to a copy.
    - **C.** The stored hash in biometric systems is no longer "something you are" and instead becomes "something you have."
    - **D.** A stored biometric can be stolen and used by an attacker to impersonate the individual.