CYBS 7357 Lab 09 Quiz

\* Answers are highlighted in Yellow

1. Which of the following statements is true regarding social engineering?

a. Social engineering is when an attacker attempts to take advantage of a weakness in a network, device, or application.

b. Security professionals consider social engineering a highly sophisticated “technical” form of attack.

c. Social engineering will never be as effective as a traditional technical attack.

d. Hackers, cybercriminals, or cyberterrorists often save time and achieve what they could not otherwise by simply asking.

2. Which of the following statements is true regarding a properly configured Virtual Private Network (VPN) that uses IPSec and adheres closely to best practices, such as strong authentication, network segmentation, device validation, posture assessment, etc.?

a. This VPN will not protect information while it is in transit from one location to the other.

b. Actually “breaking” into a VPN tunnel such as this one will take significant technical prowess.

c. This VPN security will be impenetrable by less technically savvy cybercriminals, hackers, and others.

d. This VPN will be immune to social engineering and reverse social engineering techniques.

3. Social engineering and reverse social engineering are used to gain access by:

a. pretending to be a legitimate user.

b. applying technical prowess.

c. unleashing a brute-force attack.

d. using outdated passwords and credentials.

4. The hidden part of the Internet where one can buy just about any product or service, pay in a currency called “bitcoins,” and transact business anonymously is referred to as the:

a. spudnet.

b. darknet.

c. blacknet.

d. webmarket.

5. Which of the following refers to a website that was a black market for drugs, weapons, and killers for hire?

a. Darknet

b. Black Road

c. Silk Road

d. The Club

6. Which of the following statements is true regarding Kitty Kat (KK) in the fictitious scenario used in the lab?

a. KK began her work with an Internet search to find information about the target company and its owners.

b. KK obtained the employees’ travel itinerary from the article in Cincinnati Journal.

c. KK and her accomplices did not commit any type of crime at the airport.

d. KK’s efforts were unsuccessful at obtaining valuable information about the target company.

7. In the scenario in the lab, Marina neglected to use a(n) \_\_\_\_\_\_\_\_\_\_ on her smartphone, which meant that anyone could gain immediate access to her contacts and other private information.

a. VPN

b. pass key

c. screen lock

d. IMAP protocol

8. In the scenario in the lab, Marina and Rita’s Cupcakes used the \_\_\_\_\_\_\_\_\_\_, which stores copies of all emails on the server.

a. Bitcoin account

b. VPN password

c. VPN protocol

d. IMAP protocol

9. In the scenario in the lab, Kitty Kat (KK) was able to access the Marina and Rita’s Cupcakes’ \_\_\_\_\_\_\_\_\_\_ via the VPN, which was set-up for Marina’s convenience to use a pre-stored password and automatic sign-in.

a. email

b. Facebook page

c. Website

d. Internet history

10. In the scenario in the lab, Kitty Kat (KK) was able to open the VPN and download the email of key employees after sending an email to the employees asking them to:

a. send copies of their email history.

b. reset their VPN passwords.

c. delete their VPN accounts.

d. establish new email accounts.

11. Which of the following statements is true regarding the emails that were collected from Marina and Rita’s Cupcakes’ key employees?

a. The emails were password protected and unable to be read.

b. The emails included very little useful information.

c. The emails included only personal information such as information about relationships and gossip.

d. The emails included both professional and personal information that could be exploited.

12. Which of the following steps can make VPN access more secure?

a. Assure Perfect Forward Secrecy during IKE key exchange.

b. Allow access only from specific MAC addresses and specific MAC/IP address pairs.

c. Use foreign words as passwords.

d. Change password letters to numbers, such as all Ls to 7s and all Os to 0s.

13. Instead of relying just on a user ID and password systems, VPN access can be protected by tokens like SecurID and other \_\_\_\_\_\_\_\_\_\_ methods.

a. multi-factor authentication

b. multi-use password

c. uniform authentication

d. universal password

14. Which of the following strengthens access procedures and makes a VPN more secure?

a. Make sure that all parameters for the VPN are identical, regardless of the type of information being protected.

b. Make sure that all parameters for the VPN are applied uniformly.

c. Make sure that configuration procedures are not reviewed or changed once they are in place.

d. Do not use devices that generate one-time use passwords or parts of passwords

15. A well-designed malicious email campaign can expect \_\_\_\_\_\_\_\_\_\_ responses, or click-throughs, as a legitimate commercial email campaign.

a. far more

b. somewhat more

c. about the same number of

d. fewer

16. Which of the following statements is true regarding spam emails?

a. Regardless of the purpose of the campaign, there is only a single type of spam email that can be sent.

b. A good spam email can be considered a valid part of a legitimate marketing campaign.

c. The effectiveness of a spam email has nothing to do with the relationship between the sender and receiver.

d. A spam email can be part of a larger campaign of deception, or it can be the entire campaign.

17. Which of the following statements is true regarding phishing?

a. Phishing emails are spam emails that rely on the recipient remaining passive and inactive.

b. Phishing emails that are general in nature, rather than targeted to a specific audience, are called spear phishing emails.

c. Spear phishing emails use social engineering techniques to appeal to the target.

d. Neither phishing nor spear phishing emails are very effective.

18. What type of emails are used to either get credentials that make breaking into or using a VPN easier, or are designed to ask users to do things like send money, disclose VPN credentials, or change passwords?

a. Spear phishing

b. VPN phishing

c. Password phishing

d. Password noodling

19. Which of the following statements is true regarding creating a successful spam email campaign?

a. The sender’s identity has to be a person or entity that is unknown or unfamiliar to the recipient.

b. Most spam campaigns use an actual sender email address, rather than a temporary one.

c. The decision to use a real or false sender address depends on whether or not the spammer wishes the recipient to ultimately delete the email.

d. When the sender is a known contact of the target, using the sender’s actual email address increases the appearance that the email is proper.

20. Which of the following statements is true regarding the body (or content) of a spam email?

a. The body of the email is generally not very important to the effectiveness of a spam email campaign.

b. The body of the email depends entirely on the objectives and goals of the recipient.

c. If the intent of the campaign is to verify that the email account is active, the recipient only has to open the email, not read the content.

d. If the intent of the campaign is to encourage the recipient to do something, then the body is not very important.

NAME:

Natnael kebede