اطلب من

بالأخلاق و العلم نرتقى

Lecture 7.

mcq

1-includes type of attack that is nontechnical in nature and that involves some type of human interaction with the goal of trying to trick or coerce a victim into revealing information or violate normal security practices Definition of the previous part is.

a. Social Engineering
b. Spyware
c. Viruses
d. Worms

2-Scams may include trying to make a victim believe the attacker is technical support or someone in authority.

a. True
b. false

3-in …….. An attacker may dress a certain way with the intent of fooling the victim into thinking the person has authority.

a. Social Engineering
b. Spyware
c. Viruses
d. Worms

4- in social engineering The end goal of each approach is for the victim to drop their guard or for the attacker to gain enough information to better coordinate and plan a later attack.

a. True
b. false

5-in …….. An attacker may prey on a victim's desire to provide assistance because they feel compelled to do so out of a sense of duty.

a. trust
b. Moral Obligation
c. Threats

d. Something for Nothing

6-in …….. Human beings have an inherent tendency to trust others. Social engineers exploit a human's tendency to trust by using buzzwords or other means. In the case of buzzwords, for example, use of familiar terms may lead a victim to believe that an attacker has insider knowledge of a project or place.

a. trust
b. Moral Obligation
c. Threats
d. Something for Nothing

7-in ……. A social engineer may threaten a victim if they do not comply with a request.

a. trust
b. Moral Obligation
c. Threats
d. Something for Nothing

8-in……. The attacker may promise a victim that for little or no work, they will reap tremendous rewards.

a. trust
b. Moral Obligation
c. Threats
d. Something for Nothing

9-in……. The reality is that many people do not realize the dangers associated with social engineering and don't recognize it as a threat.

a. trust
b. Moral Obligation
c. Threats
d. Ignorance

10-in…..One thing that technology has little or no impact on is blunting the effectiveness of social engineering.

a. Lack of a Technological Fix
b. Insufficient Security Policies

c. Difficult Detection
d. Lack of Training

11-in……The policies that state how information, resources, and other related items should be handled are often incomplete or insufficient at best.

a. Lack of a Technological Fix
b. Insufficient Security Policies
c. Difficult Detection
d. Lack of Training

12-in…… Social engineering by its very nature can be hard to detect. Think about it: An attack against technology may leave tracks in a log file or trip an intrusion detection system (IDS), but social engineering probably won't.

a. Lack of a Technological Fix
b. Insufficient Security Policies
c. Difficult Detection
d. Lack of Training

13-in…… Lack of training or insufficient training about social engineering and how to recognize it can be a big source of problems.

a. Lack of a Technological Fix
b. Insufficient Security Policies
c. Difficult Detection
d. Lack of Training

14-in……. When you see someone dressed a certain way (such as wearing a uniform) or hear them say the right words, you trust them more than you normally would.

a. Lack of a Technological Fix
b. Human Habit and Nature
c. Difficult Detection
d. **Trust**

15- A good social engineer can observe these habits and use them to track people or follow the actions of groups and gain entry to buildings or access to information.

a. True
b. False

16-which of the following is the phase of Social-Engineering.

17- Use footprinting and gather details about a target through research and observation. Sources of information can include dumpster diving, phishing, websites, employees, company tours, or other interactions.

a. True
b. False

18- Select a specific individual or group who may have the access or information you need to get closer to the desired target this is belongs to Social-Engineering Phases

a. True
b. False

19- Forge a relationship with the intended victim through conversations, discussions, emails, or other means this is belongs to Social-Engineering Phases.

a. True
b. False

20-Exploit the relationship with the victim, and extract the desired information this is belongs to Social-Engineering Phases

a. True
b. False

21- which of the following is the Process of Social-Engineering.

a. Research
b. Develop
c. Exploit
d. All of them

22- They see many people go in and out of an office, and they hear a lot of things. In addition, receptionists are meant to be helpful and therefore are not security focused this definition of…….

a. **Receptionists**
b. **Help desk personnel**
c. **System administrators**
d. **Executives**
e. **Users**

23- Also, some system admins possess far-reaching knowledge about the entire company's network and infrastructure.

a. True
b. False

25- Techniques I have used in the past include asking questions about their experience, career path, and such, and then using that to learn more about what they currently do.

a. True
b. False

26- Filing fake support requests or asking these personnel leading questions can yield valuable information this definition of……..

a. **Receptionists**
b. **Help desk personnel**
c. **System administrators**
d. **Executives**
e. **Users**

27- The typical administrator can be counted on to have very high level knowledge of infrastructure and applications as well as future development plans this definition of……...

a. **Receptionists**
b. **Help desk personnel**
c. **System administrators**
d. **Executives**
e. **Users**

28- because individuals in these types of positions are not focused on security. In fact, many of the people in these positions focus on business processes, sales, finance, and other areas this definition of……...

a. **Receptionists**
b. **Help desk personnel**
c. **System administrators**
d. **Executives**
e. **Users**

29- one of the biggest sources of leaks because they are the ones who handle, process, and manage information day to day this definition of……...

a. **Receptionists**
b. **Help desk personnel**
c. **System administrators**
d. **Executives**
e. **Users**

30- one of the biggest sources of leaks because they are the ones who handle, process, and manage information day to day all becaose of users

a. True
b. False

31- he rapid growth of these technologies lets millions of users each day post on Facebook, Twitter, and many other networks. What type of information are they posting?

a. Personal information and Friend information
b. Photos and Location information
c. Business information and Likes and dislikes
d. All of them

32- in …….. This type of post feeds on people's insatiable desire for information regarding celebrities or public figures.

a. **Secret Details about Some Celebrity's Death**

b. **I’m Stranded in a Foreign Country—Please Send Money**
c. **Did You See This Picture of J-Lo?**
d. **Test Your IQ**

33-in…… These types of scams target users by claiming that the message is from someone the user knows who is trapped without money in a foreign country or bad situation.

a. **Secret Details about Some Celebrity’s Death**
b. **I’m Stranded in a Foreign Country—Please Send Money**
c. **Did You See This Picture of J-Lo?**
d. **Test Your IQ**

34-in…… Both Facebook and Twitter have been plagued by phishing scams that involve a question that piques your interest and then directs you to a fake login screen, where you inadvertently reveal your Facebook or Twitter password.

a. **Secret Details about Some Celebrity’s Death**
b. **I’m Stranded in a Foreign Country—Please Send Money**
c. **Did You See This Picture of J-Lo?**
d. **Test Your IQ**

35-in…… This type of scam attracts you with a quiz. Everybody loves quizzes. After you take the quiz, you are encouraged to enter your information into a form to get the results.

a. **Secret Details about Some Celebrity’s Death**
b. **I’m Stranded in a Foreign Country—Please Send Money**
c. **Did You See This Picture of J-Lo?**
d. **Test Your IQ**

36- As an ethical hacker and security professional Discourage the practice of mixing personal and professional information in social networking situations.

a. True

b. False

37- As an ethical hacker and security professional Always verify contacts, and don’t connect to just anyone online.

a. True

b. False

38- As an ethical hacker and security professional Avoid reusing passwords across multiple social-networking sites.

a. True

b. False

39- As an ethical hacker and security professional post just anything online; remember that anything you post can`t be found, sometimes years later.

a. True

b. False

40- As an ethical hacker and security professional Avoid posting personal information that can be used to determine more about you, impersonate you, or coax someone to reveal additional information about you.

a. True

b. False