RV College of Engineering®

Go, change the world

22EM1C06-Introduction to Cyber Security

SAMPLE MCQ

1. We use _____ to ensure security and the confidentiality of our data

Password

2. Anytime an unknown device is used to sign into your Google account, the user has to provide a verification code in addition to the password. This is known as_____

2-step verification system

3. Wi-Fi is short for _____

Wireless fidelity

4.International Mobile Equipment Identity (IMEI) number contains _____ digits.

15

5. APK stands for_____

Android Application Packages

6. In this type of physical social engineering, the attacker acts like someone else to trap the victim.

A. Piggybacking
B. Eavesdropping
C. Dumpster Driving
D. Impersonation

Answer: Impersonation

- Piggybacking is **a process of attaching acknowledgment with the data packet to be sent**. It is an efficient solution for reducing the bandwidth utilization of the network. TCP is a full-duplex communication protocol, so piggybacking is used to transmit packets
- **Eavesdropping** is the act of secretly or stealthily listening to the private conversation or communications of others without their consent
- **Dumpster diving** is looking for treasure in someone else's trash.

7. State True or False:

It is not important to have your operating system up to date with the latest updates and security patches.

False

8. The decoding of the complex code to original text using key is known as _____.

A. decryption
B. encryption
C. steganography
D. digital signature

decryption

9. OTP stands for_____

One Time Password

10. The process of giving access to an individual to certain resources based on the credentials of an individual is known as _____

Authentication

11. State TRUE or FALSE:

Biometric data can be used in conjunction with username and password for two-way authentication.

TRUE

12. VPN stands for_____

Virtual Private Network

13. Special program which can detect and remove viruses from computer is called

A. Malware
B. Antivirus
C. Virus
D. Groupware

Antivirus

14 URL stands for_____

uniform resource locator

15. This is a techniques where every possible combination of letters, numbers and symbols in an attempt to guess the password.

A. DOS Attack
B. DDOS Attack
C. Brute-Force Attack
D. Dictionary Attack

Brute-Force Attack

- "Denial of service" or "DoS" **describes the ultimate goal of a class of cyber attacks designed to render a service inaccessible**.
- DDoS (Distributed Denial of Service) is a category of malicious cyber-attacks that hackers or cybercriminals employ in order to make an online service, network resource or host machine unavailable to its intended users on the Internet.
- A dictionary attack is **a method of breaking into a password-protected computer, network or other IT resource by systematically entering every word in a dictionary as a password**. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document.

16. YouTube is a service, owned by _____.

Google

17. Windows _____is software designed to detect and remove malware and it is built in Windows operating systems.

Defender

18. By default Windows enables _____, a feature where plugged in removable media (like USB drives or devices) are examined and, based on their content, such as pictures, music or video files, an appropriate application to play or display the content is launched.

AutoPlay

19. _____ is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

A. Vishing
B. Skimming
C. Social Engineering
D. Pharming

Social Engineering

- Vishing calls, smashing, and phishing are all types of social engineering attacks with the intent of **gaining personally identifiable information that will enable fraudsters to gain access to a user's account**.
- Skimming is **an illegal practice used by identity thieves to capture credit card information from a cardholder surreptitiously**. Fraudsters often use a device called a skimmer that can be installed at gas pumps or ATM machines to collect card data. Some machines act like point-of-sale technology.
- In a pharming attack, users aren't tricked into navigating to a malicious website. Instead, **the attacker steals data using malware background processes or automatically sends a user to a phishing website in their browser**.