Mock Questions for Online Examination

1.is not the computer system assets

    a. Hardware

    b. Data

    c. Software

    d. Money

2. Traffic Analysis is…………..

    a. Active Attack

    b. Passive Attack

    c. Cryptosystem

    d. Vulnerability

3. Confidentiality means keeping data……….

    a. Open

    b. Secret

    c. Scattered

    d. Easy

4. Which of the following is not a layer of security?

  a. Physical Security

  b. Intermediate Security

  c. Operations Security

  d. Network Security

5. VPN stands for _____

    a. Visual Private Network

    b. Visual Public Network

    c. Virtual Private Network

    d. Visual Public Network

6. Which of the following is not a benefit of Security Program?

    a. Business Agility

    b. Cost Reduction

c. Portability

d. Frees RAM

7. **Firewalls, network access control, spam and malware filtering are _____ types of controls**

    a. Defensive

    b. Detective

    c. Deterrent

    d. Managerial

8. **Which of the following is not a type of detective control?**

    a. Surveillance camera

    b. Web content filtering

    c. Motion sensors

    d. Car alarm systems

9. **A _____ analysis compares the desired state of the security program with the current state and identifies the differences**

    a. risk

    b. security

    c. remedy

    d. gap

10. **A _____ is a plan of action for how to implement the security remediation plans.**

    a. Incident plan

    b. Response plan

    c. Roadmap

    d. Risk plan

11. **The actions that should be taken when security event occurs are defined in the_____**

    a. Project Plan

    b. Remedy Plan

    c. Incident response plan

    d. Policy plan

12. **"The job of the attacker is difficult than the job of the defender"**

    a. False

    b. True

13. **What is transitive Security?**

a. All security controls need not complement each other and each should be equally as strong as the others

b. All security controls need not complement each other and should be unequal

c. All security controls should complement each other and each should be equally as strong as the others

d. All security controls should complement each other and should be unequal

14. **PBX stands for _____**

a. Public Branch Exchange

b. Private Branch Exchange

c. Public Branch Environment

d. Private Branch Environment

15. **What is difference between strategy and tactic?**

a. Strategy are done in small time frame whereas tactic is small time goal

b. Strategy are smaller steps whereas tactic are large concrete steps

c. Strategy are small-term goals whereas tactic are large concrete steps

d. Strategy are long-term goals whereas tactic are small concrete steps

16. **Content attacks, Buffer overflows and Password cracking are attacks of which layer?**

a. Transport

b. Physical

c. Application

d. Network

17 **_____ occurs when an unauthorized third party captures network packets destined for computers other than their own.**

a. Tracking

b. SQL Injection

c. Sniffing

d. Traffic replay

18. **NIC stands for _____**

a. Network Interface Card

b. Network Intermediate Card

c. Network Interface Configuration

d. Network Intermediate Configuration

19. **_____ refers to the restriction of access to data only to those who are authorized to use it**

a. Integrity

b. Confidentiality

c. Availability

d. Privacy

20. Perimeter model is like _____

a. Onion

b. layer

c. lollipop

d. sponge