Practice Questions for TYBSc(Information Technology) –Sem 6

Subject : Security in Computing

1. _______ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
   a) Network Security
   b) Database Security
   c) Information Security
   d) Physical Security
2. From the options below, which of them is not a vulnerability to information security?
   a) flood
   b) without deleting data, disposal of storage media
   c) unchanged default password
   d) latest patches and updates not done
3. Compromising confidential information comes under _________
   a) Bug
   b) Threat
   c) Vulnerability
   d) Attack
4. Lack of access control policy is a _____________
   a) Bug
   b) Threat
   c) Vulnerability
   d) Attack
5. Which of the following represents attributes/goals of information security?
   (a) Prevention, detection, and response
   (b) People controls, process controls, and technology controls
   (c) Network security, system security, and application security
   (d) Availability, Integrity, Authenticity
6. Which of the following terms best describes the chances that a threat to an information system will materialize?
   (a) Threat
   (b) Vulnerability
   (c) Weakest link
   (d) Risk
7. Which of the following terms best describes the weakness in a system that may possibly be exploited?
   (a) Threat
   (b) Vulnerability
   (c) Weakest link
   (d) Risk

8. The two models of security defense are :
   (a) lollipop, carrot
   (b) carrot, onion
   (c) lollipop, onion
   (d) tomato,onion
9. The lollipop model is made up of __________ layer(s) of security
   (a) one
   (b) two
   (c) three
   (d) four
10. Three D's of Security relate to ____________
    (a) disruption, detection and defense
    (b) defense, detection, and deterrence
    (c)defense, default and detection
    (d) defect, detection and destroy
11. Many applications use _________________ where two independent factors are used to identify a user.
    a) Two-factor authentication
    b) Cross-site request forgery
    c) Cross-site scripting
    d) Cross-site scoring scripting
12. Which of the following is an authentication service that uses UDP as a transport medium?
    (a) TACACS+
    (b) LDAP
    (c) RADIUS
    (d) Kerberos
13. RADIUS provides which of the following?
    (a)Authentication, Authorization, Availability
    (b) Authentication, Authorization, Auditing
    (c)Authentication, Accounting, Auditing
    (d) Authentication, Authorization, Accounting
14. A security administrator implements access controls based on the security classification of data and need-to-know information, which of the following BEST describes this level of access control?
    (a) implicit deny
    (b) role-based access control
    (c)mandatory-based access control
    (d) least privilege
15. Which of the following is best practice to put at the end of an ACL?
    (a) Implicit deny
    (b) time of day restrictions
    (c) Implicit allow
    (d) SNMP listing

16. Which of the following is an example of multifactor authentication?
(a) Credit card and PIN
(b) Username and password
(c) Password and PIN
(d)Fingerprint and Retina Scan

17. Which of the following is an authentication method that can be secured by using SSL?
(a) RADIUS
(b) LDAP
(c) TACACS+
(d) Kerberos

18. _______ uses the idea of certificate trust levels.
(a) X.509
(b) PGP
(c) KDC
(d)CA

19. _______________ creates a protected zone where only identified devices within that zone are allowed to communicate with each other.
(a) Isolation
(b) Segmentation
(c) Zoning
(d) Segregation

20. This type of encryption makes use of a public and a private key
(a) symmetric encryption
(b) asymmetric encryption
(c) phishing
(d) pharming

21. The distribution Layer in Cisco hierarchical model is similar to ____________ layer of OSI model
(a) Data link
(b) Network
(c) Transport
(d) Physical

22. The Cisco hierarchical model is consists of _________ layers.
(a) Three
(b) Four
(c) Five
(d) six

23. Intranet and Extranet differs at ___________________________.
(a) Intranet: Private , Extranet: Public
(b) Intranet: Public, Extranet: Public
(c) Intranet: Private, Extranet: Private and also allowed authorized partners
(d) Intranet: Public, Extranet: Private

24. Which direction access cannot happen using DMZ zone by default?
(a) Company computer to DMZ
(b) Internet to DMZ

(c) Internet to company computer
(d) Company computer to internet

25. _______________ security framework provides the most specific guidance for network design considerations.
(a) NIST
(b) COBIT
(c) ISO27002
(d) IEEE802

26. 26. TCP is __________________ and UDP is __________________________
(a) connection oriented, connectionless
(b) connectionless, connection-oriented
(c) connection-oriented, connection-oriented
(d) connectionless, connectionless

27. Which networking device connects one LAN to another LAN using same protocol?
(a) Router
(b) Switch
(c) Bridge
(d) Repeater

28. IMAP works on port number ___________
(a) 21
(b) 443
(c) 161
(d) 143

29. Which of the following is a valid extended IP access list?
(a) access-list 102 permit ip host 164.42.20.0 any eq 80
(b) access-list 102 permit ip host 164.42.20.0 any eq www
(c) access-list 102 permit tcp host 164.42.20.0 any eq 80
(d) access-list 102 permit icmp host 164.42.20.0 any eq www

30. Smurf and fraggle are tools used to carry out _______________ attacks
(a) DOS attack
(b) Phishing
(c) Pharming
(d) Bandwidth amplification

31. What are the different ways to classify an IDS?
(a) anomaly detection
(b) signature based misuse
(c) stack based
(d) register based

32. What are the characteristics of anomaly based IDS?
(a) It models the normal usage of network as a noise characterization
(b) It doesn't detect novel attacks
(c) Anything distinct from the noise is not assumed to be intrusion activity
(d) It detects based on signature

33. A false positive can be defines as
(a) An alert that indicates nefarious activity on a system, that, upon further inspection turns out to represent legitimate network traffic or behavior
(b)An alert that indicates nefarious activity on a system that is not running on the network
(c)The lack of an alert for a nefarious activity

(d) Both (a) and (b)

34. _______________ IDSs focused on accurate attack detection

(a) Fourth generation
(b)Third generation
(c)Second generation
(d)First generation

35. At which two traffic layers do most commercial IDSes generate signatures?

(a) Application
(b) Network
(c) Session
(d) Transport

36. Where is an IPS commonly placed in a network?

(a)In front of the firewall
(b)In line with the firewall
(c)Behind the firewall
(d)On the end users' device

37. How does an intrusion prevention system differ from an intrusion detection system?

(a) It only alerts network security personnel
(b) It only blocks, but does not analyze
(c)It blocks in addition to discovering
(d)They are the same with different name

38. The _____________________ is the "brains" of operation of a VoIP system

(a) MCU
(b) call control element
(c)Voice gateway
(d) SBC

39. Mandatory Access Control is always prohibitive and not permissive.

(a) permissive, prohibitive
(b) permissive, blocking
(c) prohibitive, permissive
(d) prohibitive, blocking

40. What is the Bell-LaPadula model?

(a) A discretionary access control method
(b) A multiuser security system
(c) A multilevel security system
(d) A role base access control system

41. The hypervisor monitors and tracks the state of its guest OSs, which is commonly referred to as

(a) introspection
(b) Monitoring
(c) Tracking
(d) Inspection

42. In ___________________, the guest OS has direct access to the actual physical network interface cards (NIC) of the real server hardware.

(a) NAT
(b) VPN
(c) Host only networking
(d) Network bridging

43. ___________________ allows consumers to provision processing, storage, and networking resources, allowing them to deploy and run their own operating systems or applications in their own cloud environment.
(a) PaaS
(b) SaaS
(c) IaaS
(d) XaaS

44. Illegally (or deceptively) gaining access to information that a person is not authorized to access is termed as __________
(a) Misuse
(b) Espionage
(c) Hijacking
(d) Fraud

45. In _________________ attacks, the attacker manages to get an application to execute an SQL query created by the attacker.
a) SQL injection
b) SQL
c) Direct
d) Application

46. ___________________ is a popular method of verifying that the person on the other end is a human being, by showing a distorted image of letters and numbers and requiring the user to type them in correctly.
(a)OTP
(b) password
(c)Captcha
(d) PIN

47. A _________________ is classified as any device that uses distinctive personally identifiable characteristics or unique physical traits to positively identify an individual.
(a) biometric device
(b) authentication token
(c) CCTV
(d) smart card

48. SDL refers to ______________________
(a) Software development lifecycle
(b) System development lifecycle
(c)Secure Development Lifecycle
(d) Software design lifecycle

49. Cookies were originally designed for ____________
a) Client side programming
b) Server side programming
c) Both Client side programming and Server side programming
d) Socket programming

50. Hypervisor is also calles _____________
(a) Guest OS
(b) Host OS
(c)Virtual machine
(d) Kernel