Application Security and Testing

Date:28/12/2017 Duration :01 Hour Max. Marks: 50

1. \_\_\_\_\_\_\_\_\_\_\_ is a principles of security

a. Integrity

b. Authentication

c. Availbility

d. All of above

2. \_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_ are basic types of Attacks .

a. Active and Passive

b. Alive and dead

c. Connected and Disconnected

d. None of Above

3. \_\_\_\_\_\_\_ function is used in Message Digest

a. Checksum

b. Digital

c. Hashing

d. Analog

4. \_\_\_\_\_\_\_\_\_\_ is Full form of DOS Attack

a. Denial of Service

b. Disk operating System

c. Denial Operationg system

d. Disk of service

5. \_\_\_\_\_\_\_\_\_\_\_ is a mechanisum of Encryption and decrypion

a. Cryptography

b. encoding

c. decoding

d. stegnography

6. Converting plain text to cipher text is called as \_\_\_\_\_\_\_\_\_

a. Encryption

b. Decryption

c. decoding

d. None of Above

7. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is used for Authencity.

a. Digital Signature

b. Analog Signature

c. signature

d. Digital code

8. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ full form of DDOS

a. Distributed Denial of Servive

b. Distributed Disk operating System

c. Distributed Denial Operationg system

d. Distributed Disk of service

9. Converting cipher text to plain text is called as \_\_\_\_\_\_\_\_\_

a. Encryption

b. Decryption

c. decoding

d. None of Above

10. ciphet text is \_\_\_\_\_\_\_\_\_\_ text

a. plain

b. decoded

c. Encrypted

d. converted

11. Modification Attack is due to \_\_\_\_\_\_\_\_\_\_

a. Availability

b. Intigrity

c. Authentication

d. Confidentility

12. packet sinnifing is \_\_\_\_\_\_\_\_\_\_ type of Attack

a. Active

b. Passive

c. Alive

d. dead

13. Key pair is used in \_\_\_\_\_\_\_\_\_\_ type of encryption

a. Symmetric

b. Asymetric

c. same

d. different

14. \_\_\_\_\_\_\_\_\_\_ software is used for packet sniffing

a. wired

b. wireshark

c. shark

d.None of Above

15. Ceaser Cipher uses \_\_\_\_\_ key number for cryptography

a. 1

b. 2

c. 3

d. None of Above

16. packet spoofing is \_\_\_\_\_\_\_\_\_\_ type of Attack

a. Dead

b. Passive

c. Alive

d. Active

17. \_\_\_\_\_\_\_\_\_\_ software is used for port scanning

a. map

b. pmap

c. nmap

d. None of Above

18. OWASP stands for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

a. open web application security project

b. open wise application security project

c. open web applicable security project

d. open web application security packet

19. \_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_ injection Attacks are there in OWASP

a. SQL and LDAP

b. SQL and Linux

c. QOS and LDAP

d. SQL and QOS

20. XSS specfies \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

a. Cascade Style Scripting

b. Cascase site scrpting

c. Cascade Style site

d. Cross site scripting

21. Threats have \_\_\_\_\_\_\_\_ sources

a. social

b. Technological

c. operational

d. All of above

22. Diffie Helman Algorithm is \_\_\_\_\_\_\_\_\_\_\_\_\_ type of cryptographic Algorithm

a. Asymmetric

b. Symmeteric

c. Non Symetric

d. None of above

23. \_\_\_\_\_\_\_\_\_\_\_\_\_ are a message Digest Algorithms

a. MD5, RSA

b. SPA, SPS

c. MDP, SPM

d. RDA, SPS

24. LDAP stands for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

a. Light ise application Development

b. Light weight application Deployment

c. Light weight application Development

d. Less weight application Development

25. IGMP stands for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

a. Internet Group Message Protocol

b. Internet guide Message protocol

c. Internet guide mac protocol

d. None of Above

26. Ceaser Cipher is \_\_\_\_\_\_\_\_\_\_\_\_\_\_ type of cateography of crypto Algorithm

a. Substitution

b. Transposition

c. Both A and B

d. None of above

27. packet sniffing is \_\_\_\_\_\_\_\_\_\_\_\_ type of Attack

a. Active

b. Passive

c. Both A and B

d. None of above

28. packet spoofing is \_\_\_\_\_\_\_\_\_\_ type of Attack

a. Passive

b. Active

c. Both A and B

d. None of above

29. War driving is used in \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Attack

a. Active

b. Passive

c. Both A and B

d. None of above

30. To avoid SQL injection Attack insert statement with parameter is \_\_\_\_\_\_

a. "insert into emp values('" & "cdac" &"'," & 11 & ")"

b. "insert into emp values('" & "cdac" &"'," & 11 & ")"

c. "insert into emp' values('" &cdac&"'," & 11 & ")"

d. "insert into emp values('" &cdac&"'," & 11 & ")"

31. \_\_\_\_\_\_\_\_\_\_\_\_\_ type of Attack can occur on maximum fill of stack frame

a. Buffer Flow

b. Buufer Frame

c. Sack frame

d. Stack Attack

32. DDOS Attacks can be targted on \_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_

a. Bandwith and resources

b. Bandwith and only Cpu

c. All of Above

d. None of Above

33. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is cateogry of DOS Attack

a. Sync Flooding

b. TCP Flooding

c. ICMP Flooding

d. All of above

34. Reflector DDOS Attack is \_\_\_\_\_\_\_\_\_ Attack

a. Direct

b. Indirect

c. None of Above

d. Both A and B

35. IDS stands for \_\_\_\_\_\_\_\_\_\_\_\_

a. Intrusion development system

b. intrusion detection system

c. intrusion detect section

d. Intrusion development section

36. Antivirus and spam protection is done in \_\_\_\_\_\_\_\_\_\_\_

a. Web server Security

b. Web server sytem

c. application server security

d. database server security

37. Cross site scripting is reffered as \_\_\_\_\_\_\_\_\_\_\_

a. XSSL

b. XSS

c. XBSL

d. SSX

38. SDL stands for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

a. Security Development Life

b. Security Development Lifecycle

c. Security Deployment Life

d. Security Deployment Lifecycle

39. OWASP Top 10.2017 has new feature Broken Access control is added

a. FALSE

b. TRUE

c. None of Above

d. Both A and B

40. XXE stands for \_\_\_\_\_\_\_\_\_\_\_

a. XML External Entities

b. XML EXTra Entities

c. XML Extra Era

d. XML Extra ERP

Check more questions @ **https://www.owasp.org/index.php/OWASP\_Top\_10\_Threats\_and\_Mitigations\_Exam\_-\_Single\_Select**