

King Saud University
College of Computer and Information Science
IT Department
Course : Information Security CAP 430
Instructor : Prof. Mona Mursi

Sample Exam

Multiple Choice Answers :

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|----|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| | | | | | | | | | | | | |

| | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| | | | | | | | | | | | | |

| | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
| | | | | | | | | | | | | |

| | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|
| 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 |
| | | | | | | | | | | | |

QUESTION # 1

1. The primary goal of information security is to protect _____.

| | |
|-----------------|----------------|
| A - People | C - Procedures |
| B - Information | D - Computers |

2. Each of the following factors illustrates why information security is increasingly difficult, except _____.

| | |
|------------------------------------|---------------------------------------|
| A - Distributed attacks | C - Faster computer processors |
| B - Faster detection of weaknesses | D - Growing sophistication of attacks |

3. A federal act that broadens the surveillance of law enforcement agencies to enhance the detection of terrorism is the _____.

| | |
|-------------------------|----------------------------|
| A - USA Patriot Act | C - HIPAA |
| B - Sarbanes-Oaxley Act | D - Gramm-Leach-Bliley Act |

4. _____ ensures that information is correct and that no unauthorized person has altered the data.

| | |
|---------------------|---------------------|
| A - Authentication | C - Integrity |
| B - Non-repudiation | D - Confidentiality |

5. While most attacks today take advantage of vulnerabilities that someone has already uncovered, _____ occurs when a hacker discovers and exploits a previously unknown flaw.

| | |
|--------------------------|------------------------|
| A - Back-door attack | C - Ground zero attack |
| B - Vulnerability attack | D - Day zero attack |

6. _____ is the most significant cause of financial loss due to a security breach .

| | |
|------------------------|---------------------|
| A - Expert brain drain | C - Virus attacks |
| B - Data theft | D - Equipment theft |

7. There are _____ available port numbers , while _____ are called available port numbers.

| | |
|------------------|--------------------|
| A - 65,535 , 512 | C - 32, 765 , 1024 |
| B - 16K , 1K | D - 65,535 , 1024 |

8. The port number for the HTTP protocol is _____.

| | |
|--------|--------|
| A - 21 | C - 23 |
| B - 80 | D - 25 |

9. To determine the established connections and the ports on which your computer is listening for new connections , you can type _____ in DOS

| | |
|-------------------|-----------------|
| A - netstat - a | C - netstat - p |
| B - netstat - ano | D - view-ports |

10. Of the following types of security, which would be primarily concerned with someone stealing the server from the premises?

| | |
|--------------------------|---------------------------|
| A - Physical security | C - Management and policy |
| B - Operational security | D - Authentication |

11. Which of the following authentication methods uses more than one authentication process for log on?

| | |
|------------------|----------------|
| A - Multi-factor | C - Smart Card |
| B - Biometrics | D - Kerberos |

12. Which of the following protocols allows an organization to present a single IP address to the Internet while utilizing private IP addressing across the LAN?

| | |
|----------|---------|
| A - VLAN | C - DMZ |
| B - VPN | D - NAT |

13. Of the following services, which one would be most likely to utilize a retinal scan?

| | |
|--------------------|--------------------------|
| A - Auditing | C - Authentication |
| B - Access control | D - Data Confidentiality |

14. A computer virus is considered a _____ to a computer system..

| | |
|-------------------|------------------|
| A - Vulnerability | C - Threat agent |
| B - Threat | D - risk |

15. Of the top five jobs in the computer field are the following except _____

| | |
|--------------------------|----------------------------|
| A - Software maintenance | C - Security analyst |
| B - Web developers | D - Database administrator |

16. _____ is the prevention of unauthorized withholding of information or resources

| | |
|---------------------|--------------------|
| A - Integrity | C - Access control |
| B - Confidentiality | D - Availability |

17. DoS attacks are attacks on the _____ of a system

| | |
|---------------------|------------------|
| A - Integrity | C - Availability |
| B - Confidentiality | D - Services |

18. Main goals of security are the following except _____

| | |
|----------------|---------------|
| A - Assertion | C - Reaction |
| B - Prevention | D - Detection |

19. Firewalls are part of _____ security , for the sake of _____

| | |
|-----------------------|--------------------------|
| A - Host , prevention | C - Network , detection |
| B - Host , detection | D - Network , prevention |

20. _____ involves using someones' s SSN to establish a bank account

| | |
|----------------|--------------------|
| A - Data theft | C - Card theft |
| B - Bank theft | D - Identity theft |

21. _____ threats involve the acceptance of false data, include all of the following except _____

| | |
|-----------------------|---------------------------|
| A - Denial of service | C - Spoofing |
| B - Modification | D - Repudiation of origin |

22. _____ is a skilled person who violates system security with malicious intent

| | |
|-------------|-------------------|
| A - Hacker | C - Script Kiddie |
| B - cracker | D - Employee |

23. The goals of cyberattacks are all of the following except _____

| | |
|-----------------------------------|--------------------------------------|
| A - Delay service to users | C - Deny service to legitimate users |
| B - Deface electronic information | D - Commit unauthorized intrusions |

24. _____ is a type of access attack

| | |
|----------------------|----------------------|
| A - Shoulder surfing | C - Snooping |
| B - Dumpster diving | D - All of the above |

25. Information gleaned from network management protocols that collect diagnostics about the network is

| | |
|----------------------------|---------------------------|
| A - Can be sensitive | C - Is public information |
| B - Is not a security risk | D - Is unusable |

26. _____ is one type of programming flaw exploited by hackers

| | |
|---------------------|----------------------|
| A - Back door | C - Buffer overflow |
| B - Buffer resizing | D - Any of the above |

27. To convince the switch to send traffic to the sniffer, the sniffer duplicates the ___ address of the target
- | | |
|----------|------------|
| A - Port | C - IP |
| B - MAC | D - Socket |
28. ___ is the easiest and cheapest way to attack a computer system
- | | |
|--------------|------------------------|
| A - Virus | C - Interception |
| B - Spoofing | D - Social engineering |
29. ___ involves sending people electronic requests for information that appears to come from a valid source
- | | |
|---------------------|--------------|
| A - Masquerading | C - Phishing |
| B - Dumpster diving | D - Spoofing |
30. To minimize password-guessing attacks , we should avoid ___
- | | |
|--|---|
| A - PWs should expire at least every 30 days | C - One secure PW should be used on all systems |
| B - PWs should have at least 8 characters | D - PWs cannot be reused for 12 months |
31. The birthday paradox states that the probability that you share the same birthday with one of the people in a room jumps to 99% if the room contains ___ people.
- | | |
|--------|---------|
| A - 25 | C - 99 |
| B - 60 | D - 999 |
32. When program files change size from the installed version , that signals a ___ attack
- | | |
|-----------|------------------|
| A - Worm | C - Trojan horse |
| B - Virus | D - Back door |
33. A ___ virus will try to hide from antivirus programs by changing form
- | | |
|-------------------|-----------------|
| A - Armored virus | C - Stealth |
| B - Retrovirus | D - Polymorphic |
34. A ___ virus exploits the default searchpath in DOS
- | | |
|---------------|-----------------|
| A - Stealth | C - Retrovirus |
| B - Companion | D - Polymorphic |
35. The most current list of viruses is at the ___ website
- | | |
|----------|----------------------|
| A - CERT | C - Semantec |
| B - NIST | D - All of the above |
36. Matilda was unhappy with her boss, so she planted a ___ in the system , to be active if she is fired
- | | |
|-----------|------------------|
| A - Worm | C - Trojan horse |
| B - Virus | D - Logic bomb |
37. Data should be protected with ___ layers of security
- | | |
|------------|--------------|
| A - Thick | C - Diverse |
| B - Strong | D - Multiple |
38. A security plan that is initiated by a(n)___ would be defined as a bottom-up approach.
- | | |
|--------------------------|----------------------------|
| A - CIO | C - Chief security officer |
| B - Help-desk technician | D - Security director |
39. Kerberos is an authentication system that is based on issuing___
- | | |
|------------------|------------------|
| A - Tickets | C - Receipts |
| B - Certificates | D - Session keys |
40. What is the process of determining who owns a particular database called?

| | |
|--------------------|---------------------|
| A - Auditing | C - Threat analysis |
| B - Access control | D - Accountability |

41. A server in your network has a program running on it that bypasses authorization. Which type of attack is that?

| | |
|----------|------------------------|
| A - DoS | C - Back-Door |
| B - DDoS | D - Social engineering |

42. You have discovered that an expired certificate is being used repeatedly to gain logon privileges. Which type of attack is this most likely to be?

| | |
|-----------------------|----------------------|
| A - Man-in-the middle | C - Replay |
| B - Back door | D - TCP/IP hijacking |

43. Your system has just stopped responding to keyboard commands. You noticed that this occurred when a spreadsheet was open and you dialed in to the Internet. Which kind of attack has probably occurred?

| | |
|----------------|----------------|
| A - Logic bomb | C - Virus |
| B - Worm | D - Ack attack |

44. The Smurf attacks uses the ___ protocol to conduct its attack.

| | |
|---------|----------|
| A - TCP | C - UDP |
| B - IP | D - ICMP |

45. You are working late one night, and you notice that the hard drive on your computer is very active even though you are not doing anything and you are not connected to the Internet. What is most likely happening?

| | |
|--------------------------------|---|
| A - A disk failure is imminent | C - Your system is under DoS attack |
| B - A virus is spreading | D - TCP/IP hijacking is being attempted |

46. MAC stands for ___

| | |
|---------------------------------|--------------------------|
| A - Message authentication code | C - media access control |
| B - Message acceptance code | D - None of the above |

47. The data added to a section of text when using MD algorithm is called ___

| | |
|-------------|---------------|
| A - Padding | C - Extender |
| B - Filler | D - Byte code |

48. Cryptography provides all the following except ___

| | |
|---------------------|--------------------|
| A - Confidentiality | C - Integrity |
| B - Speed | D - Authentication |

49. The ___ defines the overall process involved with developing a security policy.

| | |
|-------------------------------|----------------------|
| A - F security policy cycle | C - monitoring scope |
| B - risk identification cycle | D - evaluation cycle |

50. ___ are 64-bit block ciphers except ___

| | |
|---------|--------------|
| A - DES | C - IDEA |
| B - AES | D - Blowfish |

51. ___ is defined as the obligations that are imposed on owners and operators of assets to exercise reasonable care of the assets and take necessary precautions to protect them.

| | |
|-----------------|------------------|
| A - Proper care | C - Secure care |
| B - Due care | D - Maximum care |

QUESTION #2

- a) Explain how a Smurf attack is carried out.

QUESTION #3

- a) How can you prevent a guessing attack on a password ?

- b) What are the disadvantages of using a timestamp in Timestamp Challenge?

QUESTION #4

- a) Explain the key generation and encryption/decryption steps of the RSA encryption algorithm. Discuss the security of RSA.

b) The encryption key in a transposition cipher is (3, 2, 6, 1, 5, 4). Find the decryption key

c) Use the Rail Fence Cipher with key 2 to encode "**A man a plan a canal**"

QUESTION #5

Fill in the blanks :

1. Data that has been encrypted by an encryption algorithm (a cipher) is called ____
_____.
2. A(n) _____ cipher maps a single plaintext character to multiple ciphertext characters.
3. A(n) _____ cipher rearranges the letters without changing them.
4. A(n) ____ cipher manipulates an entire block of plaintext at one time.
5. The _____ was specifically designed to replace the weaker Data Encryption Standard (DES).
6. While most attacks today take advantage of vulnerabilities that someone has already uncovered, a(n) ____ ____ occurs when a hacker discovers and exploits a previously unknown flaw.
7. A(n) _____ is a security device that is used to authenticate the user by having the appropriate permission embedded into it.
8. _____ is a protocol that can be used to encrypt transmission over the Internet.
9. Restricting users to the lowest level of permissions they need to do their job is called _____
10. When an attacker sends out counterfeit e-mail messages to direct users to his own site this is called _____
11. With a(n) _____ attack the attacker attempts to create every possible password combination by systematically changing one character at a time and then using each newly generated password to access the system.
12. A(n) ____ ____ attack takes each word from a dictionary and encodes it in the same way in which the computer would encode a user's password.

13. A(n) _____ occurs when a computer program attempts to stuff more data into a temporary storage area than it can hold, overwriting valid computer data
14. Authentication based on a secret code you have memorized is an example of authentication by What you _ _____
15. Using your fingerprint to access a system is an example of authentication by what you _____
16. The ____ _ mode of IPsec is used to implement VPN.
17. To prevent replay attacks _____ is used in the IPsec protocol.
18. The _____ is a list of serial numbers of certificates that are no longer valid .
19. In a _____ trust model, one CA is not subordinate to another CA, and each root CA issues a certificate for the other root CA.
20. The _____ is the trusted authority for certifying individuals' identities and creating digital certificates.
21. The _____ is the standard for digital certificates .
22. The _____ is the organization that may be used to identify an individual for certificate issue .
23. The _____ is the process of storing keys for use by law enforcement when the need arises.
24. The _____ is the document that describes how a CA issues certificates and what they are used for.
25. (Spoofing / Snooping) _____ occurs when someone looks thru your files , either paper or electronic.