UNIVERSITY OF GHANA

BA/BSC.SECOND SEMESTER EXAMINATIONS SUPPLEMENTARY RE-SIT EXAMINATIONS 2017/2018

DEPARTMENT OF COMPUTER SCIENCE

CSIT204: INTRODUCTION TO INFORMATION SECURITY (3 CREDITS)

INSTRUCTIONS:

PLEASE READ THE INSTRUCTIONS AND QUESTIONS CAREFULLY

This exam comprises SECTIONS A and B. You will be graded for clarity and correctness. Write legibly and check answers before handing it in. Answer All Questions in SECTION A and THREE (3) Questions from SECTION B. Answer all questions in the answer booklet provided.

TIME ALLOWED:

TWO AND A HALF (2½) HOURS

SECTION A:

INDICATE THE RIGHT LETTERED ANSWER (A, B, C, D) in the answer book provided

1. If an attacker breaks into a corporate database and deletes critical files, this is an attack against the _____ security goal.
   A) integrity
   B) confidentiality
   C) Both A and B
   D) Neither A nor B

2. When a threat succeeds in causing harm to a business, this is called a _____.
   A) breach
   B) compromise
   C) incident
   D) All of the above

3. _____ are programs that attach themselves to legitimate programs.
   A) Virus
   B) Worms
   C) Both A and B
   D) Neither A nor B

4. A program that gives the attacker remote access control of your computer is specifically called a _____.
   A) Trojan horse
   B) spyware program
   C) Cookie
   D) RAT

5. You receive an e-mail that seems to come from your bank. Clicking on a link in the message takes you to a website that seems to be your bank's website. However, the website is fake. This is called a _____ attack. (Pick the most precise answer.).

A) social engineering
B) a hoax
C) Phishing
D) Spear fishing

6. The worst problem with classic risk analysis is that _____.
   A) protections often protect multiple resources
   B) resources often are protected by multiple resources
   C) we cannot estimate the annualized rate of occurrence
   D) costs and benefits are not the same each year

7. Which of the following is a way of responding to risk with active countermeasures?
   A) Risk reduction
   B) Risk acceptance
   C) Risk avoidance
   D) All of the above

8. Using both a firewall and host hardening to protect a host is _____.
   A) defense in depth
   B) Risk acceptance
   C) an anti-weakest link
   D) adding berms

9. A _____ is a mathematical process used in encryption and decryption.
   A) key
   B) cipher
   C) Plaintext
   D) Coding method

10. When two parties communicate with each other using symmetric key encryption, how many keys are used in total to encrypt and decrypt?.
   A) 1
   B) 2
   C) 4
   D) 8

11. If a key is 43 bits long, how much longer will it take to crack it by exhaustive search if it is extended to 50 bits?
   A) 7 times as long
   B) 14 times as long
   C) 128 times as long
   D) 256 times as long

12. Packaged sets of cryptographic countermeasures for protecting data transmission are _____.
   A) cryptographic standards
   B) metacryptographic systems
   C) cryptographic systems
   D) All of the above

13. Proving your identity to a communication partner is _____.
   A) validation
   B) identification
   C) Authentication
   D) Certification

14. What usually is the longest stage in a cryptographic system dialogue?
   A) Ongoing communication
   B) Negotiation of security methods and parameters
   C) Keying
   D) Mutual Authentication

15. In public key encryption for authentication, the supplicant uses _____ to encrypt.

A) the supplicant's private key
B) the supplicant's public key
C) the verifier's private key
D) the verifier's public key

16. The supplicant creates a message digest by _____.
A) adding the password to the challenge message and hashing the two
B) hashing the plaintext message
C) encrypting the message digest with its own private key
D) None of the above.

17. Two-factor authentication can be defeated if _____.
A) the user's computer is compromised
B) the attacker uses a man-in-the-middle attack
C) Both A and B
D) Neither A nor B

18. _____ is a social engineering trick where an intruder may follow an authorized user through a door that the authorized user opens with an access device.
A) Shoulder surfing
B) Shadowing
C) Trailing
D) Piggybacking

19. Long passwords that use several types of keyboard characters are called _____ passwords.
A) complex
B) reusable
C) Dictionary
D) one-time

20. A _____ card stores authentication data.
A) magnetic stripe
B) smart
C) Both A and B
D) Neither A nor B

21. The strongest form of authentication is _____.
A) biometrics
B) cryptographic authentication
C) reusable passwords
D) smart cards

22. A private key/public key pair is usually created by the _____..
A) client
B) PKI server
C) Both A and B
D) Neither A nor B

23. Ensuring appropriate network _____ means preventing attackers from altering the capabilities or operation of the network.
A) confidentiality
B) integrity
C) Availability
D) Functionality

24. In regards to network security, _____ is the policy-driven control of access to systems, data, and dialogues.

A) confidentiality
B) integrity
C) access control
D) Availability

25. Denial of Service (DoS) attacks can cause harm by _____.
A) stopping a critical service
B) slowly degrading services over a period of time
C) Both A and B
D) Neither A nor B

26. _____ is the process of obscuring an attacker's source IP address.
A) Backscatter
B) Spoofing
C) IP Flood
D) None of the above

27. A _____ attack is when a webserver is flooded with application layer web requests.
A) SYN flood
B) Ping flood
C) HTTP flood
D) None of the above

28. An attacker controlling bots in a coordinated attack against a victim is known as a _____.
A) DoS attack
B) DDoS attack
C) ICMP
D) None of the above

29. If a firewall receives a provable attack packet, the firewall will _____.
A) log the packet
B) drop the packet
C) Both A and B
D) Neither A nor B

30. If a firewall receives a suspicious attack packet, the firewall will _____.
A) log the packet
B) drop the packet
C) Both A and B
D) Neither A nor B

31. If a firewall cannot keep up with traffic volume, it will _____.
A) continue passing all packets but slow operation
B) drop packets it cannot process
C) pass any packets it cannot filter
D) shut down, failing safely

32. Static packet filtering firewalls are limited to _____.
A) inspecting packets for which there are good application proxy filtering rules
B) inspecting packets in isolation from their context
C) Both A and B
D) Neither A nor B

33. If an attacker takes over a firewall, he or she will be able to _____.
A) allow connection-opening requests that violate policy
B) re-route internal data to alternate paths
C) provide the false sense that the firewall is still working correctly
D) All of the above

34. A(n) _____ is a security weakness that makes a program vulnerable to attack.
A) attack vector
B) exploit
C) Vulnerability
D) All of the above

35. What is the name for a small program that fixes a particular vulnerability?
A) Work-around
B) Patch
C) Service pack
D) Version upgrade

36. To prevent eavesdropping, applications should _____.
A) be updating regularly
B) use electronic signatures
C) use encryption for confidentiality
D) use encryption for authentication

37. In a(n) _____ attack, information that a user enters is sent back to the user in a webpage.
A) login screen bypass
B) buffer overflow
C) Cross-Site Scripting (XSS)
D) SQL injection attack

38. In a(n) _____ attack, the user enters part of a database query instead of giving the expected input.
A) login screen bypass
B) buffer overflow
C) Cross-Site Scripting (XSS)
D) SQL injection attack

39. In a(n) _____ attack, the user enters part of a database query instead of giving the expected input.
A) login screen bypass
B) buffer overflow
C) Cross-Site Scripting (XSS)
D) SQL injection attack

40. The process of keeping a backup copy of each file being worked on by backing it up every few minutes is called _____.
A) file backup
B) file/folder backup
C) Image backup
D) Shadowing

SECTION B

INSTRUCTIONS: *ANSWER* ***QUESTION ONE (1)*** *AND ANY OTHER* ***TWO (2)*** *FROM THIS SECTION* ***(TOTAL MARKS: 60)***

Q1:

a. A company has a resource XYZ. If there is a breach of security, the company may face a fine of GHS100, 000 and pay another GHS 20,000 to clean up the breach. The company believes that an attack is likely to be successful about once in five years. A proposed countermeasure should cut the frequency of occurrence in half. How much should the company be willing to pay for the countermeasure?

[10 marks]

b. Distinguish between keystroke loggers, password-stealing spyware, and data mining spyware.

[3 marks]

c. Explain the following access control functions, each in a sentence. **[6 marks]**
   i. Authentication,
   ii. Authorization and
   iii. Auditing.

d. What is a Distributed Denial of Service (DDoS) attack? **[1mark]**

Q2:

a. Addamark Technologies found that an employee of competitor Arcsight had accessed its webservers without authorization. Arcsight's vice president for marketing dismissed the hacking, saying, "It's simply a screen that asked for a username and password. The employee didn't feel like he did anything illicit." The VP went on to say the employee would not be disciplined. Comment on the Arcsight VP's defence.

[8 marks]

b. Distinguish between credit card theft and identity theft. **[2 marks]**

c. Determine the outcomes of the following problems:
   i. If a key is 43 bits long, how much longer will it take to crack it by exhaustive search if it is extended to 45 bits?

[4 marks]

   ii. If a key is 40 bits long, how many keys must be tried, on average, to crack it? **[4 marks]**

d. Julia encrypts a message to David using public key encryption for confidentiality. After encrypting the message, can Julia decrypt it? Explain your answer.

[2 marks]

Q3:

a. How does the city model relate to secure networking? **[3 marks]**
b. How can information be gathered from encrypted network traffic? **[3 marks]**
c. What is the difference between a direct and indirect DoS attack? **[4 marks]**
d. In what two (2) ways can password-cracking programs be used? Explain. **[4 marks]**
e. How do firewalls and antivirus servers work together? **[3 marks]**
f. How does the supplicant create a digital signature? **[1 marks]**
g. Can antivirus software detect keystroke capture software? Explain. **[2marks]**

Q4:

a. How can computing parity be used to restore lost data? **[4 marks]**
b. What is the difference between basic file deletion and wiping? **[4 marks]**
c. A company is warned by its credit card companies that it will be classified as a high-risk firm unless it immediately reduces the number of fraudulent purchases made by its e-commerce clients. Come up with a plan to avoid this outcome.

[8 marks]

d. What are one-time-password tokens? **[2 marks]**
e. Distinguish between verification and identification. **[2 marks]**