EXIT EXAMINATION FOR SOFTWARE AND INFORMATION SYSTEM

1. Which one of the following includes in the C.I.A. triangle
   A. Confidentiality, Integrity, Availability
   B. Accountability, Confidentiality, Integrity
   C. Confidentiality, Intrusion and Authorization
   D. Confidentiality, Integrity, Authentication
2. Among the things that can facilitate unauthorized access to a computer by attackers are:
   A. Software
   B. Hardware
   C. Procedural weakness of a safeguard
   D. All
3. The absence or weakness of a safeguard that could be exploited is called:
   A. Threat
   B. Vulnerability
   C. Attack
   D. Possibility
4. A threat is:
   A. The potential danger to information or systems
   B. Flaws in a computer system that weaken the overall security of the device/system.
   C. Try to gain illegal access to electronic data stored on a computer or a network.
   D. All
5. A cybersecurity safeguard could be:
   A. Software/ Application
   B. Physical security
   C. Both
   D. None
6. The statement, "Information systems should be configured to require strong passwords," is an example of a/an:
   A. Security requirement
   B. Security policy
   C. Security objective
   D. Security control
7. An information system that processes sensitive information is configured to require a valid user id and strong password from any user. This process of accepting and validating this information is known as:
   A. Authentication
   B. Strong authentication
   C. Two-factor authentication
   D. Single sign-on
8. Palm scan, fingerprint scan, and iris scan are forms of:
   A. Strong authentication
   B. Two-factor authentication
   C. Biometric authentication
   D. Single sign-on
9. When the means of authentication cannot later be refuted—the user cannot later deny that he or she performed the activity is known _____.
   A. Authentication
   B. Authorization
   C. non-repudiation
   D. None

10. _____ is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program.
    A. Authentication
    B. Authorization
    C. non-repudiation
    D. All of the above
11. When users cannot access the network or specific services provided on the network, they experience a _____.
    A. Availability
    B. Denial of service
    C. diagnostic problem
    D. All
12. Keyloggers are a form of _____.
    A. Spyware
    B. Shoulder Surfing
    C. Trojan
    D. Social Engineering
13. Phishing is a form of _____.
    A. Impersonation
    B. Spamming
    C. Identify Theft
    D. Scanning
14. To hide information inside a picture, what technology is used?
    A. Rootkits
    B. Bitmapping
    C. Steganography
    D. Image Rendering
15. An information security project team would include:
    A. System administrator but not a data custodian
    B. Risk assessment specialists but not security policy developers
    C. Data custodian but not a system administrator or an end user
    D. Data custodian, system administrators, security policy developers
16. In cryptography, what is cipher?
    A. algorithm for performing encryption and decryption
    B. encrypted message
    C. decrypted message
    D. All
17. In asymmetric key cryptography, the private key is kept by
    A. Sender
    B. Receiver
    C. Sender and Receiver
    D. all
18. In cryptography, the order of the letters in a message is rearranged by
    A. Transpositional ciphers
    B. Substitution ciphers
    C. Both
    D. None
19. _____ algorithm transforms ciphertext to plaintext.
    A. Encryption
    B. Decryption
    C. Both
    D. None
20. One commonly used public-key cryptography method is the _____ algorithm.
    A. RSS
    B. RSA
    C. RAS
    D. RAA
21. Which of the following is not a cybercrime?

A. Denial of Service
B. Man in the Middle
C. Malware
D. AES

22. Which of the following is defined as an attempt to steal, spy, damage or destroy computer systems, networks, or their associated information?
A. Cyber Attack
B. Computer security
C. Cryptography
D. Digital hacking

23. What are the features of cyber security?
A. Compliance
B. Defense against internal threats
C. Threat Prevention
D. All

24. A cyber-criminal or penetration tester uses the additional data that stores certain special instructions in the memory for activities to break the system in which of the following attack?
A. Clickjacking
B. Buffer-overflow
C. Phishing
D. SQL-injection

25. They are nefarious hackers, and their main motive is to gain financial profit by doing cyber-crimes. Who are "they" referred to here?
A. White Hat Hackers
B. Black Hat Hackers
C. Hactivists
D. Gray Hat Hackers

26. Which of the following DDoS in mobile systems wait for the owner to trigger the cyber attack?
A. Botnets
B. Programs
C. Virus
D. worms

27. What does SSL stand for?
A. Saving Sharing and Limits
B. Safe, Secured and Locked
C. Secure Socket Limbs
D. Secure Socket Layers

28. Firewalls are used to protect against
A. unauthorized attacks
B. virus attacks
C. data driven attacks
D. fire attacks

29. What port does Telnet use?
A. 22
B. 80
C. 20
D. 23

30. Enumeration is part of what phase of Ethical Hacking?
A. Reconnaissance
B. Maintaining Access
C. Gaining Access
D. Scanning

31. How do you prevent SQL injection?
A. Interrupt requests
B. Escape queries
C. Merge tables
D. All

32. Which of these software engineering techniques can catch buffer overflow errors?
A. Testing
B. Code inspection
C. Multi-platform testing
D. All

33. Which stage of risk management framework, we create a coherent strategy for offensive the risks in a cost-effective manner.
    A. Synthesize and Rank the Risks
    B. Identify the Business and Technical Risks
    C. Define the Risk Mitigation Strategy
    D. Carry Out Fixes and Validate
34. If the JS code is on the page *https://website.com/apple*, is a request to *https://subdomain.website.com* a same-origin request?
    A. Yes
    B. No
    C. It depends on port number
    D. None
35. Which one of the following refers to the technique used for verifying the integrity of the message?
    A. Digital signature
    B. Decryption algorithm
    C. Protocol
    D. Message Digest
36. Which one of the following principles of cyber security refers that the security mechanism must be as small and simple as possible?
    A. Open-Design
    B. Economy of the Mechanism
    C. Least privilege
    D. Fail-safe Defaults
37. Suppose system admin in BDU-SIMS have the root access to a BDU-SIMS system, and will create account to other staffs. Instructors have the right to prepare and submit student grade. Students have the right to view their grade and not to prepare and submit the grade. It can be considered as a perfect example of which principle of cyber security?
    A. Least privileges
    B. Open Design
    C. Separation of Privileges
    D. Both A & C
38. Security engineers build systems that have ___ their assets from attack.
    A. The ability to product
    B. The ability to project
    C. The ability to protect
    D. All
39. Software security provides ___ that enable a software system to protect its assets from attack.
    A. The mechanisms
    B. The ability to product
    C. The software process
    D. None
40. Amongst which of the following is / are; a security model needs to capture
    A. Security policy objectives, external interface requirements
    B. Software security requirements, rules of operation
    C. Specifications describing model-system correspondence.
    D. All
41. Hackers often gain entry to a network be pretending to be at a legitimate computer
    A. Spoofing
    B. Forging
    C. IP Spoofing
    D. All
42. Which of the following is the type of SQL Injection attack?
    A. It inserts the data
    B. It updates the data

C. It deletes the data
D. All

43. Point out the correct statement.
    A. Parameterized data cannot be manipulated by a skilled and determined attacker
    B. Procedure that constructs SQL statements should be reviewed for injection vulnerabilities
    C. The primary form of SQL injection consists of indirect insertion of code
    D. None
44. Select the correct statement which will return all the rows from the Table and then also deletes the Table_Add table?
    A. SELECT * FROM Table; DROP TABLE Table_Add
    B. SELECT * WHERE Table; DROP TABLE Table_Add
    C. SELECT * FROM Table; DELETE TABLE Table_Add
    D. SELECT * WHERE Table; DELETE TABLE Table_Add
45. Which of the following types of hacker attacks runs a program that simply throws billions of character combinations at a password?
    A. Dictionary attack
    C. Brute force attack
    B. Social engineering Attack
    D. Phishing attack
46. A type of malicious software designed to block access to a computer system until a sum of money is paid.
    A. Adware
    C. Malware
    B. Ransomwear
    D. Winterwear
47. A collection of cryptographic hashes, random-looking strings of characters into which the passwords have been mathematically transformed to prevent them from being misused.
    A. Trick or treat
    C. Encryption
    B. Hash
    D. Password
48. Which of the following is an example of passive online attack?
    A. Phishing
    B. Social Engineering
    C. Spamming
    D. Wire sniffing
49. Input validation should be based on _____
    A. Whitelisting
    B. Blacklisting
    C. Both
    D. None
50. Your application sets a cookie with secure attribute. What does this mean?
    A. The cookie cannot be accessed by JavaScript
    B. The cookie will not be sent cross-domain
    C. Client will send cookie only over an HTTPS connection
    D. none
51. _____ are programs that are created on your local computer when you visit websites.

A. Firewall
B. Cookies
C. History
D. All

52. Web browsers have _____ designed to store passwords used in forms on websites.
A. Cookies
B. Built – in password management
C. History
D. None of the above

53. One operation that frequently has cross-site scripting (XSS) vulnerabilities is_____
A. A user visits a site's homepage.
B. A site prompts the user for their user name and password.
C. A site produces an error message for an invalid user name.
D. A user clicks on a hyperlink to visit another page in the same site.

54. One common strategy to prevent XSS vulnerabilities is to _____
A. Educate your users to recognize safe vs. unsafe web pages.
B. Escape user's input is valid as soon as possible.
C. Avoid using JavaScript in your site.
D. Use an interpreted programming language such as Java or C#.

55. Cross-site request forgery (CSRF) vulnerabilities_____
A. Are partially corrected by adding and validating on submission a hidden field with a secure random number as its value.
B. Only affect pages with forms that do not include the user name in the data sent back to the server.
C. Are common in sites that avoid JavaScript on pages that contain one or more forms.
D. Are common in sites that rely heavily on JavaScript, especially on pages that contain one or more forms.

56. If a site has an unusually short session timeout (e.g.: 2 minutes) and has an unusually large logout button on the top of every page, one might assume that the site is trying to prevent what type of attack?
A. SQL Injection
B. Cross-Site Request Forgery (CSRF)
C. Cross-Site Scripting (XSS)
D. Session Management

57. Which of the following strategies prevents a SQL injection vulnerability
A. Carefully validating user input and rejecting invalid input before executing any SQL requests.
B. Ensuring that you use only database software that has been widely tested and is generally considered secure.
C. Using prepared statements at runtime instead of dynamically evaluating SQL.
D. All

58. _____ is the science to make them secure and art of transforming messages and immune to attacks
A. Cryptography
B. Cryptoanalysis

C. Both
D. None

59. The _____ cipher is the simplest monoalphabetic cipher. It uses modular arithmetic with a modulus of 26.
    A. Transposition
    B. Additive
    C. Shift
    D. None
60. A modern cipher is usually a complex _____ cipher made of a combination of different simple ciphers.
    A. Round
    B. Circle
    C. Square
    D. None
61. ECB and CBC are _____ ciphers
    A. Block
    B. Stream
    C. Field
    D. none
62. The _____ method provides a one-time session key for two parties
    A. Diffie-Hellman
    B. RSA
    C. DES
    D. AES
63. Is penetration testing used to help or for damaging a system?
    A. Helping
    B. Securing
    C. Damaging
    D. Both A & C
64. Which of the following are possible vulnerabilities in a database?
    A. Using DELETE to delete table data
    B. Using the DROP command
    C. SQL injection
    D. All
65. Penetration testing should focus on what scenarios?
    A. Most likely
    B. Most dangerous
    C. Both
    D. None
66. What is social engineering?
    A. Using force to gain access to the information you need
    B. Hacking either telecommunication or wireless networks to gain access to the information you need
    C. Using manipulation to deceive people that you are someone you are not to gain access to the information you need
    D. Using force to gain all the information available.
67. What is the risk involved in doing penetration testing?
    A. You have to pay for the testing.
    B. Some operations of the company might slow down.
    C. It is good to use WAF.
    D. None
68. Which of the following groups must a penetration testing review?
    A. Documentation, Log, System configuration, Ruleset, Network sniffing, File integrity

B. Documentation, Log, System Configuration, Network Sniffing, File Integrity
C. Documentation, Log, System Configuration, Network Sniffing, Ruleset, File Integrity, Personnel
D. None

69. What are the main penetration testing phases?
A. Discovery => Planning =>Report => Attack
B. Planning => Discovery => Report => Attack
C. Planning => Discovery => Attack => Report
D. Planning => Attack => Discovery=>Report

70. The command to remove a table customer from a database is:
A. REMOVE TABLE CUSTOMER;
B. DROP TABLE CUSTOMER;
C. DELETE TABLE CUSTOMER;
D. UPDATE TABLE CUSTOMER;

71. Which of the following protocols is used for translating IP addresses to MAC addresses?
A. DHCP
B. DNS
C. ARP
D. UDP

72. A DHCP server is responsible for providing which of the following to its client?
A. MAC Address
B. IP Address
C. Protocol
D. All

73. Which of the following helps detect malicious attacks over a network using the signature matching technique?
A. Router
B. Switch
C. Intrusion Detection System
D. All

74. Fingerprint scan is an authentication technique based on which of the following principles?
A. Something you have
B. Something you are
C. Something you know
D. None of the above

75. Denial of Service attacks affects which of the following factors?
A. Confidentiality
B. Integrity
C. Availability
D. All of the above

76. Which of the following is a test wherein the pen-tester has partial knowledge about the target system/network?
A. Black box testing
B. White box testing
C. Gray box testing
D. Blue box testing

77. 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

78. Which of the following best describe the term ‘asset’ in the context of information security?
    A. Anything that an organization buys
    B. Anything that an organization sells
    C. Anything that has a value to the organization
    D. Anything that is situated within an organization’s premises
79. _____ Techniques rely on the manual examination and automated analysis of the code or other project documentation without the execution of the code.
    A. Static testing
    B. Dynamic testing
    C. Reviews
    D. All
80. What is true regarding static analysis tools?
    A. It compares actual and expected result
    B. It can detect memory leaks
    C. gives quality information about code without executing it
    D. It tell about percentage of a code coverage
81. Applications developed by programming languages like ____ and ___ have this common buffer-overflow error.
    A. C, Ruby
    B. Python, Ruby
    C. C, C++
    D. Tcl, C#
82. Who deploy Malwares to a system or network?
    A. Criminal organizations, Black hat hackers, malware developers, cyber-terrorists
    B. Criminal organizations, White hat hackers, malware developers, cyber-terrorists
    C. Criminal organizations, Black hat hackers, software developers, cyber-terrorists
    D. Criminal organizations, gray hat hackers, Malware developers, Penetration testers
83. This attack can be deployed by infusing a malicious code in a website’s comment section. What is “this” attack referred to here?
A. SQL injection
B. HTML Injection
C. Cross Site Scripting (XSS)
D. Cross Site Request Forgery (XSRF)
84. After performing _____ the ethical hacker should never disclose client information to other parties.
    A. hacking
    B. cracking
    C. penetration testing
    D. exploiting
85. Ideally, what characters should you use in a password to make it strong?
    A. Letters and Numbers only.
    B. Mixed Case Characters
    C. Special Characters
    D. All
86. Brute force attack is _____.
    A. Fast
    B. Inefficient
    C. Slow
    D. Complex to understand
87. Which one of the following comes under the advantage of dictionary attack?
    A. Moderate efficient
    B. Time-consuming

C. Complex to carry-out
D. Very fast

88. What are examples of network sniffing tools?
A. Bash, Nano, VI
C. Wireshark, Tshark, TCPdump
B. Nmap, Metasploit, Nessus
D. None

89. Which is the largest disadvantage of the symmetric Encryption?
A. More complex and therefore more time-consuming calculations.
B. Problem of the secure transmission of the Secret Key.
C. Less secure encryption function.
D. Isn't used any more.

90. If a DNS server accepts and uses the wrong details from a host that has no authority giving that information, then this technique is called …?
A. DNS hijacking
C. DNS spoofing
B. DNS lookup
D. All

91. Cryptography intercepts ____ type of data accessibility?
A. Authorized
C. Legitimate
B. Unauthorized
D. All

92. How many keys do Triple DES operates with?
A. 2
C. 3
B. 4
D. 5

93. Which folder contains Junk emails?
A. Inbox
C. Spam
B. Unwanted
D. None

94. Which of the following algorithm has overcome triple DES?
A. AES
C. DSA
B. Blow fish
D. All

95. SMTP stands for?
A. Simple Mail Text Processing
C. Simple Mail Transfer Protocol
B. Secure Mail Transfer Protocol
D. Secure Message Transfer Process

96. Which of the following data security principle does checksum verifies?
A. Integrity
C. Confidentiality
B. Authenticity
D. Repudentiality

97. _____ ciphers process message a bit or byte at a time when en/decrypting
A. Block
C. Substitution
B. Stream
D. Transposition

98. Use Caesar's Cipher to decipher the following
FRQILGHQWLDO
A. ENCRYPTED
C. CONFIDENTIAL
B. CONTINENTAL
D. ABANDONED

99. Vigenere cipher is an example of _____
A. Mono-Alphabetic Cipher
B. Poly-Alphabetic Cipher

C. Transposition Cipher
D. Additive Cipher

100. Which one of the following is the result of vigenere cypher using crypto key
Plaintext = “cryptography”

A. EIWEMCIIYEAM
C. IEWEMCIIYEAM
B. EIWEMCIIYENB
D. EIWEMCIIZAEM

101. One of the following attack categories and security requirement doesn’t match?

A. Interruption => Attack on availability
B. Fabrication => Attack on authenticity
C. Modification => Attack on integrity
D. Interception => Attack on integrity

102. Which one of the following is different from the others?

A. Adware
C. Trojan
B. Hacktivist
D. Spyware

103. Which one of the following cryptographic algorithms uses mathematical functions rather than substitution and permutation?

A. RSA
C. S-DES
B. DES
D. A and B

104. Which one of the following cryptographic algorithms is used to exchange a session key securely?

A. RSA
C. DES
B. Diffie-Hellman
D. Vigenere

105. What kind of cryptography makes key management less of a concern?

A. Asymmetric
C. Digital signature
B. Hashing
D. Symmetric