Reg. No. 3 7 0

B.Tech. DEGREE EXAMINATION, NOVEMBER 2018

3rd to 7th Semester

15IT412 – INFORMATION ASSURANCE AND SECURITY

(For the candidates admitted during the academic year 2015-2016 to 2107-2018)

Note:

(i) **Part - A** should be answered in OMR sheet within first 45 minutes and OMR sheet should be handed over to hall invigilator at the end of 45th minute.

(ii) **Part - B** and **Part - C** should be answered in answer booklet.

Time: Three Hours Max. Marks: 100

PART – A (20 × 1 = 20 Marks)

Answer **ALL** Questions

1. Why would a hacker use a proxy server?
   (A) To create a stronger connection with the target
   (B) To create a ghost server on the network
   (C) To obtain a remote access connection
   (D) To hide malicious activity on the network
2. To hide information inside a picture, what technology is used?
   (A) Rootkits
   (B) Bitmapping
   (C) Steganography
   (D) Image rendering
3. What are some of the most common vulnerabilities that exist in a network or system?
   (A) Changing manufacturer, settings of a newly installed application
   (B) Additional unused features on commercial software packages
   (C) Utilizing open source application code
   (D) Balancing security concerns with functionality
4. The first phase of hacking an IT system is compromise of which foundation of security?
   (A) Availability
   (B) Confidentiality
   (C) Integrity
   (D) Authentication
5. Identify the standard, which is NOT recognized as international standard of information security?
   (A) ISO027001
   (B) ITSEC
   (C) IEEE 802.11 b
   (D) ISO 27002
6. The main purpose of data protection act is to _____.
   (A) Protect personal privacy
   (B) Prevent viruses
   (C) Increase the security of computer systems
   (D) Reduce project failures
7. _____ are bundle of exclusive rights over creations of the mind, both artistic and commercial.
   (A) Intellectual property rights
   (B) Copyright
   (C) Patent
   (D) Trademark

8. Under the approaches to implement information assurance, which approach is good when organizations need immediate security attention.
   (A) Top-down approach
   (B) Benchmark approach
   (C) Base lining approach
   (D) Bottom-up approach

9. Which of the following is NOT typically included in a security policy?
   (A) Roles and responsibilities of different parties for making the policy effective
   (B) Information resources to be protected
   (C) Minimum measures to protect information resources
   (D) Description of specific technologies used

10. What is the best reason to implement a security policy?
   (A) It increase security
   (B) It makes security harder to enforce
   (C) It removes the employee's responsibility to make judgements
   (D) It decreases security

11. Risk identification process includes the following steps.
   (A) Identify vulnerabilities between assets and threats
   (B) Implement and monitor controls
   (C) Identify and classify assets and threats
   (D) Identify and quantify asset exposure

12. During which phase of the Software Development Lifecycle (SDLC) is thread modeling initiated?
   (A) Requirements analysis
   (B) Design
   (C) Implementation
   (D) Deployment

13. Phishing is a form of _____.
   (A) Spamming
   (B) Identify theft
   (C) Impersonation
   (D) Scanning

14. Why would HTTP tunneling be used?
   (A) To identify proxy servers
   (B) Web activity is not scanned
   (C) To bypass a firewall
   (D) HTTP is a easy protocol to work with

15. Services running on a system are determined by _____.
   (A) The systems IP address
   (B) The active directory
   (C) The systems network name
   (D) The port assigned

16. What are the types of scanning?
   (A) Port, network and services
   (B) Network, vulnerability and port
   (C) Passive, active and interactive
   (D) Server, client and network

17. Which of the following is not a major objective of security incident handling?
   (A) To disclose information related to incidents to all the staff as soon as possible
   (B) To ensure the required resources are in hand to deal with the incident
   (C) To ensure a systematic and efficient response and recovery to the affected system
   (D) To minimize possible impact of the incident on information leakage and system disruption

18. What is botnet?
(A) It is a program that spreads over network
(B) It is a computer software that detects and cleans spyware
(C) It is a network of zombie computers under the remote control of an attacker
(D) It is a type of virus that specifically looks for and removes another virus

19. The ability to recover and read deleted or damaged files from a criminals computer is an example of a law enforcement specialty called
(A) Attack simulation
(B) Computer forensics
(C) Robotic process
(D) Animated execution

20. Area of files and disks that are not apparent to the user, and sometimes not even to the operating system, is termed
(A) Latent data
(B) Missing data
(C) Hidden data
(D) Exceptional data

PART – B (5 × 4 = 20 Marks)
Answer **ANY FIVE** Questions

21. Define and explain polyalphabetic substitution ciphers.

22. Brief about the different states of information.

23. Write down the need for information assurance.

24. Illustrate the layers of defense-in-depth.

25. Differentiate computer forensics and incident response.

26. Why disaster recovery strategy is needed?

27. List out the vulnerability scanners and its functionalities.

PART – C (5 × 12 = 60 Marks)
Answer **ALL** Questions

28. a.i. Describe the security services, information states, and counter measures as defined by the MSR model in detail.

ii. Explain the information assurance in cyber security.

(OR)

b. Explain with neat diagrams, how cryptosystems offer the information security services-confidentiality, integrity, authentication and non-repudiation.

29. a.i. Describe the strategy approach and plans for information assurance. (8 Marks)

ii. Write short notes on current practices in handling information security. (4 Marks)

(OR)

b. Elaborate on information asset life cycle model with neat diagrams.

30. a. Explain in detail the "Information security policy and procedures" and brief the issues that should be addressed while drafting policies.

(OR)

b.i. Outline briefly the importance of information asset valuation. Explain with neat block diagram.

ii. Describe the secure design through threat modeling.

31. a. Elaborate in detail the "security system life-cycle" and its relationship to security with a neat diagram.

(OR)

b.i. What is meant by "Security mind set"? Discuss. (4 Marks)

ii. Detail on security education, training and awareness program with comparative framework of SETA from NIST. (8 Marks)

32. a. Explain about the different steps involved in digital forensics investigation.

(OR)

b. Elaborate in detail the intrusion prevention and intrusion detection systems with precise examples.