Bihar Engineering University, Patna
End Semester Examination - 2022

Course: B.Tech.
Code: 103713

Semester: VII
Subject: Cyber Security

Time: 03 Hours
Full Marks: 70

Instructions:-

(i) The marks are indicated in the right-hand margin.
*(ii) There are **NINE** questions in this paper.*
*(iii) Attempt **FIVE** questions in all.*
(iv) Question No. 1 is compulsory.

Q.1 *Choose the correct answer of the following: (Answer any Seven)* **[2 x 7 = 14]**

(a) Which of the following is not a type of cybercrime?
- I. Data Theft
- II. Forgery
- III. Damage to data and systems
- IV. Installing antivirus for protection

(b) Which of the following is considered as the unsolicited commercial email?
- I. Malware
- II. Spam
- III. Virus
- IV. All of the above

(c) _____ 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 programme.
- I. Non-repudiation
- II. Authorization
- III. Authentication
- IV. All of the above

(d) Among the following, identify the one which does not need any host program and is independent.
- I. Trap door
- II. Virus
- III. Trojan Horse
- IV. Worm

(e) Identify the element which is not considered in the triad, according to the CIA.
- I. Availability
- II. Authenticity
- III. Integrity
- IV. Confidentiality

(f) When information is modified in authorized ways, the result is known as_____
- I. Loss of confidentiality
- II. Loss of integrity
- III. Loss of availability
- IV. All of the above

(g) Under which section of IT Act, stealing any digital asset or information is written as cyber crime.
- I. 65
- II. 65-D
- III. 67
- IV. 70

(h) What is the full form for ITA-2000?
- I. Information Tech Act-2000
- II. Indian Technology Act-2000
- III. International Technology Act-2000
- IV. Information Technology Act-2000

P.T.O.

(i) _____ is a technique used by penetration testers to compromise any system within a network for targeting other systems.

I. Exploiting
II. Cracking
III. Hacking
IV. Pivoting

(j) Which of the following is not a vulnerability of the network layer:

I. Route spoofing
II. Identity & Resource ID vulnerability
III. IP address spoofing
IV. Weak or non-existent authentication.

Q.2 (a) Consider a scenario where you receive the following email from an email ID: [7]

Dear XYZ Email user,

Beginning next week, we will be deleting all inactive email accounts in order create space for more users. You are required to send the following information in order to continue using your email account. If we do not receive this information from you by the end of the wee, your email account will be closed.

- *Name (first and last)*
- *Email Id.*
- *Password*
- *Alternate Email*

Please contact the Webmail Team with any questions.

Thank you for your immediate attention

What should you do? What type of cybercrime is it? List and explain in detail with major risks associated with this scenario

(b) What is digital signature? How it is different from digital certificate? Explain in detail. [7]

Q.3 (a) Define an insider attack? Explain it with an example. [7]

(b) Explain the impact of cybercrime on cloud computing. [7]

Q.4 (a) What is credit card fraud? Mention the tips to prevent credit card frauds. [7]

(b) Give an overview of National Cyber security policy. [7]

Q.5 (a) Explain about Trojan Horses and Backdoors in details with examples. [7]

(b) Differentiate between Worms and Virus with examples. [7]

Q.6 (a) How should risk management in Information security systems be improved on social media portals. [7]

(b) What steps will you take to secure a server? [7]

Q.7 (a) What are DDoS attacks? Explain how to protect from DDoS attacks. [7]

(b) Discuss about the Intrusion Detection and Prevention Techniques in detail. [7]

Q.8 (a) Describe Access Control. Differentiate between Discretionary Access Control (DAC) and Mandatory Access Control (MAC) [7]

(b) Discuss about SQL Injection in detail. [7]

Q.9 (a) Write short notes on any two of the following:- [7 X 2]

I. Firewall
II. Steganography
III. Cyber security safeguards
IV. Cyber forensics.