Academic Year: 2021-22

Programme: B.Tech (IT)   Year: III   Semester: VI

Subject: Introduction to Cybersecurity

Date: 08 April 2022

Marks: 100
Time: 10.00 am to 1.00 pm
Durations: 3 (hrs)
No. of Pages: __02__

Final Examination

Instructions: Candidates should read carefully the instructions printed on the question paper and on the cover of the Answer Book, which is provided for their use.

1) Question No. 1 is compulsory.
2) Out of remaining questions, attempt any 4 questions.
3) **In all 5 questions to be attempted.**
4) All questions carry equal marks.
5) **Answer to each new question to be started on a fresh page.**
6) **Figures in brackets on the right hand side indicate full marks.**
7) **Assume Suitable data if necessary.**

Q1		Answer briefly:	[20]
	a.	Explain NSTISSC Security Model with an example.	
	b.	Which security goal (confidentiality, integrity or availability) is affected in the following cases? Justify your answer. 　i.　A student hacks into a professor's laptop to obtain a copy of the next day's test paper. 　ii.　A student sends hundreds of emails per day to another student using a spoofed return email address.	
	c.	Explain defense in depth principle with an example.	
	d.	Explain screened host firewall architecture.	
	e.	In online dictionary attack, attacker has an access to authentication function, L and try guesses until one succeeds. How will you counter such an attack?	
Q2	A	What is information security policy? Explain characteristics of effective information security policies.	[10]
	B	Alice wants to use RSA algorithm for encryption and decryption. What will be her private key if following values are used? P=13; q=17; e=23, d=? If the message is 5, what will be the encrypted and decrypted value?	[10]

Q3	A	The Diffie-Hellman key exchange is to be used to establish a shared secret key between Alice and Bob. Explain DH-Algorithm. Alice and Bob have agreed to use the prime n = 17 and base value g = 3. a. If Alice chooses the random value x = 4, what value does Alice send to Bob? b. If Alice receives the value 11 from Bob, what is the value of the shared secret key?	[10]
	B	Explain encryption and decryption process in CBC mode. List advantages and disadvantages of the same.	[10]
Q4	A	Explain the following malware terms: 1. Logic bomb 2. Trojan horse 3. Rabbit 4. Trapdoor 5. Rootkit	[10]
	B	A large advertising company handles campaigns for a number of different clients, including two competing banks ICICI and HDFC, and two rival soft drink manufacturers Coca Cola and Pepsi. Suresh is working as a relationship manager for the advertising company. Company implements Chinese wall model for access control. Explain the read and write rule. Apply the read and write rule to answer the following questions (with justification). 1. Will Suresh be able to read HDFC records if he has already accessed ICICI records? 2. Will Suresh be able to read Pepsi records if he has accessed ICICI records but not Coca Cola records? 3. Will Suresh be able to write to Pepsi records if he has already accesses ICICI records which contains unsanitized data?	[10]
Q5	A	Explain following IDPS terminologies: i. Alert or alarm ii. False Attack Stimulus iii. False negative iv. False positive v. Noise	[10]
	B	What are various ways to manage risk?	[10]
Q6	A	Explain the framework to implement cybersecurity culture at an organization.	[10]
	B	What is cybercrime? Why it is difficult to prosecute a cybercrime?	[10]