

| | | | | | | | | | |
|----------|--|--|--|--|--|--|--|--|--|
| Reg. No. | | | | | | | | | |
|----------|--|--|--|--|--|--|--|--|--|



MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

VII SEMESTER B.TECH. (COMPUTER SCIENCE & ENGINEERING) DEGREE
END SEMESTER EXAMINATION-NOV 2018
SUBJECT: INFORMATION SECURITY (CSE 4014)
REVISED CREDIT SYSTEM
(29/11/2018)

Time: 3 Hours

MAX. MARKS: 50

Instructions to Candidates:

- ❖ Answer **ALL** the questions.
- ❖ Missing data may be suitably assumed.

- 1A. You are asked to design a SecSDLC model for managing the patient and doctor information in a hospital. Draw a neat diagram and explain the various issues that need to be addressed in each phase of the model. 3M
- 1B. What is 4-1-9 fraud? Is there a business need for information security? Explain. 3M
- 1C. Explain the following: 4M
- | | |
|---------------|--------------|
| i) Spyware | ii) Exploit |
| iii) Sniffers | iv) Pharming |
- 2A. What is profile based intrusion detection? Explain the various tests that are carried out in profile based intrusion detection. 3M
- 2B. Enumerate the requirements for an effective worm counter measure scheme. Give the classification and explain the various types of malicious software. 4M
- 2C. What is a stateful inspection firewall? It is required to design a stateful inspection firewall for a government organization. Write the firewall rule set for the following firewall policies: 3M
- i. All incoming DNS response messages from the DNS server to the insiders is allowed only if a query has been sent.
- ii. Outgoing messages from all ports of the machine with IP address 201.64.123.75 are allowed for only the well known ports of outside machines irrespective of their IP addresses.

iii. Write the default rule.

- 3A. What is the need for Two-phase update? Give a suitable example and explain how two phase update works. Clearly write all the steps in both the phases. 5M
- 3B. What is inference? Briefly explain the different types of inference attacks. 5M
- 4A. What is SSL change cipher spec protocol? Explain how TLS protocol differs from that of SSL protocol. 3M
- 4B. Explain the following: 4M
i. Radix-64 conversion.
ii. S/MIME functions.
- 4C. Draw the flowchart and explain IPSec processing model for outbound packets. 3M
- 5A. Explain the following: 4M
i. Transport and tunnel modes.
ii. IKE header format.
- 5B. Explain the sources of cyber crimes. 3M
- 5C. Explain IT Act 2000. 3M
