200

SVKM's NMIMS
MUKESH PATEL SCHOOL OF TECHNOLOGY MANAGEMENT & ENGINEERING

Programme: B. Tech (IT) Year: IV Semester: VII

Academic Year: 2019-20

Subject: Information Security

Date: 13 November 2019

Marks: 70
Time: 2.00 pm - 5.00 pm
Durations: 3 (hrs)
No. of Pages: 2

Final Examination (2019-20)

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. **ONE** is compulsory.
2) Out of remaining questions, attempt any **FOUR** questions.
3) **In all FIVE 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 the following questions

a) Classify the following attack as active or passive. Justify your answer. (05)
   i. Modification
   ii. Replaying
   iii. Denial of service
   iv. Snooping
   v. Spoofing

b) 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? (05)

c) Why cybercrime is hard to prosecute? (04)

Q2

a) What is separation of privilege and least privilege principle? Explain with an example. (07)

b) Explain various phases of a virus lifecycle. (07)

Q3

a) Generate private key for Alice using RSA algorithm. She uses prime numbers 11 and 13 and public key (7, 143). Hence encrypt and decrypt message, M = 9 using generated keys. (07)

b) Internet voting is defined as an election system that uses electronic ballots that would allow voters to transmit their voted ballot to election officials over the Internet. For such a system, analyze at least three threat and suggest countermeasures for the same. (07)

Q4

a) What is difference between intrusion detection system (IDS) and intrusion prevention system (IPS)? Explain statistical anomaly based IDPS. (07)

b) What is role based access control? Explain with an example. (07)

Q5

a) Explain working of a Kerberos in detail. (07)

b) What is business continuity plan? Explain business impact analysis. (07)

Q6

a) Explain following terms with an example with respect to Clark Wilson model. (07)

1. CDIs: constrained data items
2. UDIs: unconstrained data items
3. IVPs: integrity verification procedures
4. TPs: transaction procedures

b) Explain various types of attacks on cryptosystem. (07)

Q7

a) A company has a datacenter located near forest area. Value of the datacenter building is $100,000. Forest fires occur about once every five years and present a risk to a building. Forest fire is expected to reduce the value of the building by 20%. Calculate following based on given data: (07)

1. Annual rate of occurrence (ARO)
2. Single loss expectancy(SLE)
3. Annual loss expectancy (ALE)
4. If the cost of insurance is $1000, will it be beneficial to have an insurance.
5. If the cost of insurance is $10,000, will it be beneficial to have an insurance.

b) Explain professional code of ethics in digital forensics. (07)
