M.Sc. Computer Science
MCSE-301: Cyber Security
UPC- 223412301
Semester-III
OBE Examination, Dec.-2021
Year of Admission: 2020

Time: 3 hours **Max. Marks: 70**

Note: Answer any four questions. All questions carry equal marks.

Q1. a) Security and risks are clearly related. The more at risk a system or data set is the more security is desirable to protect it. Discuss how prices for security products may be tied to the degree of risk? That is, will people of organization be willing to pay more if the risk is higher? Justify your answer.

b) What kinds of external access are needed for e-commerce? Does the webmaster or e-commerce administrator have control over the security of other servers? What are the possible threats? Discuss.

Q2. a) Compare various generations of firewalls. Comment on the security achieved and the ease of implementation of the various generations of firewalls. Also explain some methods which are available for Network Intrusion Prevention System.

b) How can anomaly-based detection schemes be used to detect unknown threats? What is the pitfall of such a mechanism? Compare it with other mechanisms of IDS/ IPS? Explain.

Q3. a) How can a system prevent guessing attacks on a password? How can a Bank prevent PIN guessing if someone has found or stolen a bank card and tries to use it? Discuss in detail. And also explain why identity theft is more serious than credit card number theft?

b) What is the security concern in WAP? How does GSM security work? Elaborate more about the difference between GSM and 3G technologies from a security standpoint.

Q4. a) Briefly discuss the following:-
-meaning and punishment for publishing or transmitting obscene material in electronic form
- Tampering with computer source documents

b) A person dishonestly uses the electronic signature, password or any other unique Identification features of any person. Is this a crime? If yes, what is the punishment? Justify your answer.

Q5. **a)** What do you mean by data acquisition in SCADA? Explain monitoring and event processing of SCADA. Is there any security challenge in SCADA? Explain.

b) What are the methods available to avoid Rootkits? Explain the need for centralized Authentication servers and discuss Kerberos in detail.

Q6. Write a note on –

- Types of Malware analysis
- Code analysis tools
- Memory forensics
- REM
- Legal and ethical issues in malware analysis