Exam. Code : 217903
Subject Code : 7019

M.Sc. Information & Network Security 3rd Semester

CLOUD COMPUTING AND ITS SECURITY

Paper—II

Time Allowed—3 Hours] [Maximum Marks—100

Note :– Attempt **five** questions in total. All questions carry equal marks.

1. What do you understand by cloud computing ? Compare and contrast it with grid computing and traditional computing paradigms. 20
2. Discuss the following topics in cloud computing context : 20
   - Evolution of cloud computing
   - Essential characteristics of cloud environment
   - Models of cloud deployment.
3. Describe the economics of cloud service models. Also discuss the gravity of various threats and their mitigation in cloud environment. 20
4. Describe the virtualization concept in cloud computing environment. Also discuss the virtualization of processing elements and memory devices in cloud. 20
5. Discuss explain the following issues in cloud security context:
   (a) Characteristics of security in cloud computing 10
   (b) Issues in and recommendations for data centre security. 10

6. Write notes on the following :
   (a) Trust model in cloud services 7
   (b) Forensics in cloud security 6
   (c) Disaster recovery in cloud environment. 7

7. Describe the following in cloud architecture : 20
   - Computing as a service
   - Storage as a service
   - Software as a service
   - Data as a service
   - Development as a service
   - Platform as a service
   - Infrastructure as a service.

8. Describe the concepts of (1) secure computations and (2) security issues in virtual machines. Also discuss the various regulatory and compliance issues in cloud environment. 20

Exam. Code : 217903
Subject Code : 7020

M.Sc. (Information & Network Security) 3rd Semester

PROACTIVE SECURITY TOOLS & TECHNOLOGY

Paper—III

Time Allowed—3 Hours] [Maximum Marks—100

Note :— Attempt any ***five*** questions. All carry equal marks.

1. (a) Define security. Explain various reconnaissance tools in detail. 3+7

   (b) How do you do security planning ? Explain through example. 10

2. (a) Explain in detail various security strategies with their importance for different applications. 10

   (b) What are the various security threats ? Explain in detail. 10

3. (a) What is active scanning ? Explain how Network Mapper, NMAP, is used to perform it. 3+7

   (b) Why Netcat is called "sniff army knief" ? Explain its various features in detail. 2+8

4. (a) Draw comparison of high-low interaction and virtual honeypots. 10

   (b) Write about the Nessus a penetration testing. 10

5. (a) Write a detailed note on "TCP DVMP" along with its special features. 10

(b) Explain the Wireshark to capture to traffic of client in detail. 10

6. (a) What is firewalling ? Explain the use of iptables to carry out. Also explain Reverse firewalling. 2+4+4

(b) Explain :

(i) Securing Honeypots

(ii) Argos. 5×2=10

7. (a) How malware is analyzed to secure your information ? Explain in detail. 10

(b) Why Botnets are required ? Explain their tracking in detail. 10

8. Write notes on with their importance :

(a) Network Traffic Visualization

(b) Attack and Penetration Tools. 10×2=20

Exam. Code : 217903
Subject Code : 7021

M.Sc. Information & Network Security 3rd Semester
PENETRATION TESTING & AUDITING
Paper—IV

Time Allowed—3 Hours] [Maximum Marks—100

Note :— Attempt any ***five*** questions. All questions carry equal marks.

1. (a) What is risk identification ? How is it different from risk mitigation ? Give suitable examples.
   (b) What is a legal agreement ? What is a legal agreement that defines the ways in which you may use a computer program ? 10,10
2. Define "Penetration Testing". What are the scope and goals of "Penetration Testing" ? Discuss three types of penetration tests, namely, black-box, white-box and grey-box with suitable examples. 20
3. (a) Differentiate between application-layer and network-layer penetration testing.
   (b) What is meant by "password cracking" ? How is password cracking penetration testing realized ? Explain. 10,10
4. (a) List and explain various activities that are carried out for scheduling a penetration test.
   (b) What is a firewall ? How is firewall penetration testing done ? Explain. 10,10

5. List the benefits that can be provided by an Intrusion Detection System (IDS). Describe the procedure to perform penetration testing for IDS. 20

6. (a) What is the purpose of a risk management plan ? List some areas it should include.

   (b) Name and explain three general monitoring tools/ methodologies that are used to examine network traffic and activities. 10,10

7. What are the guidelines for developing and writing a formal document of a penetration test report ? Explain in detail. 20

8. Write short notes on :

   (a) 'Policies and Controls Testing' for wireless networks

   (b) Social engineering penetration testing. 10,10

Exam. Code : 217903
Subject Code : 7018

M.Sc. Information & Network Security 3rd Semester

CYBER INCIDENT HANDLING & REPORTING

Paper—I

Time Allowed—3 Hours] [Maximum Marks—100

Note :— There are ***eight*** questions, attempt any ***five,*** all questions carry equal marks.

1. Why is computer and information security required ? Which are different types of computer security incidents ?
2. Explain various plans and procedure related to incident reporting and response.
3. (a) Explain the role of diagnosis matrix in incident detection and analysis.
   (b) What is use of incident response SLA matrix ?
4. What is DoS attack ? Which are different types of DDoS ? How DDoS can be prevented ?
5. Write short notes on :
   (a) Incident Documentation
   (b) Incident Prioritization
   (c) Incident Notification.
6. Explain the following :
   (a) Malicious code incident
   (b) Centralized logging.
7. Explain the usefulness of various incident handling tools available.
8. What is use of Disk Digger Utility ? What is use of NTFS Walker ?