29/11/2018 E-D

Exam. Code : 217903
Subject Code : 4713

M.Sc. Information & Network Security 3rd Sem.

CYBER INCIDENT HANDLING & REPORTING

Paper–I

Time Allowed—3 Hours] [Maximum Marks—100

Note :— There are **8** questions, attempt any **five**, **all** questions carry equal marks.

1. Which are different types of computer security incidents ?
2. Explain various features that an incident report must have.
3. (a) Write a note on Incident Analysis Methodology.
   (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 following :
   (a) Amplifier Attacks and Floods
   (b) Event Correlation
7. Explain the usefulness of various Incident handling tools or utilities. Are there any limitations of these tools ?
8. What is Log auditing ? What is use of NTFS Walker ?

Exam. Code : 217903
Subject Code : 4714

M.Sc. Information & Network Security 3rd Semester

CLOUD COMPUTING & ITS SECURITY

Paper—II

Time Allowed—3 Hours] [Maximum Marks—100

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

1. Discuss the basic idea of cloud computing and its benefits. Also discuss the business opportunities and challenges in cloud applications. 20

2. Discuss evolution and essential characteristics of cloud computing environment and various cloud deployment strategies and models. 20

3. What do you understand by the following :

   (a) Cloud service model

   (b) Cloud service vendor

   (c) Cloud computing threat

   (d) Cloud reference model ? 4×5=20

4. Describe the characteristics of virtualization in cloud computing environment. Also discuss input-output virtualization and various forms of processor virtualization. 20

(Contd.)

5. Discuss the challenges and principal requirements of security in cloud computing. Also discuss key management and access management issues in cloud security. 20

6. Write notes on the following :

   (a) Disaster recovery and business continuity 10

   (b) Cloud regulation and its compliance. 10

7. Describe trust model in cloud services and various forms of services purportedly provided by cloud service model. 20

8. (a) Describe the concepts of machine virtualization in cloud. 10

   (b) Discuss customized cloud security and application security. 10

Exam. Code : 217903
Subject Code : 4715

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 questions carry equal marks.

1. (a) Why N/W security is required ? Describe various security threats in detail. 3+7

   (b) Explain various Attack and Penetration Tools. 10

2. (a) Why network is analyzed using various tools ? Elaborate the use of defensive tools in detail. 3+7

   (b) How do you plan for security ? Explain various security strategies. 3+7

3. (a) What is active scanning ? Explain how network mapper NMAP is used for it. 3+7

   (b) Explain "Netcat utility" along with its special features to be used by penetration testers. 10

4. (a) What is Honeypot ? Why are they required ? Explain in detail. 3+5

   (b) Explain High Interaction, Low Interaction and Virtual Honeypots. 4×3=12

5. (a) What do you mean by passive traffic sniffing ? Explain along with its requirement for security. 2+8

   (b) Explain feature of NSLOOKUP for providing network security. 10

6. (a) What is firewalling ? How it is performed through "iptables" ? Illustrate. 3+7

   (b) What do you mean by traffic visualization ? Why is it important ? Explain. 3+7

7. (a) What are hybrid systems ? Explain in context of Networks Security in detail. 3+9

   (b) Write a brief note on "Hacking". 8

8. Write notes on :—

   (a) Botnets

   (b) Honeypots using Sedek tool. 10×2=20

Exam. Code : 217903
Subject Code : 4716

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) Discuss and illustrate the term 'risk' with reference to a software project. Is risk management becoming more and more relevant nowadays ?

   (b) Describe general features of agreements which make them legal. 10,10

2. What is "Penetration Testing" ? Why "Penetration Testing" is important ? What are the different components that make up a penetration test ? Explain. 20

3. (a) What is meant by the scope of a penetration test ? Differentiate between the scope of an external penetration test and the scope of an internal penetration test.

   (b) What is meant by "Social Engineering" ? How is social engineering penetration testing realized ? Explain. 10,10

4. (a) List and explain various activities that are carried out for planning a penetration test.

   (b) What is a router ? How is router penetration testing done ? Explain. 10,10

5. What do you understand by unauthorized intrusion ? List and explain the various steps to do penetration testing for intrusion detection system. 20

6. (a) What is risk mitigation in a software project ? What is risk mitigation by early exposure ?

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

7. What are the guidelines for developing, interpreting and evaluation a comprehensive penetration test report ? Explain in detail. 20

8. Write short notes on :—

   (a) Wireless networks and their penetration test

   (b) Password cracking penetration testing. 10,10