Sr.No.7121 8.5-17

Exam. Code: 217904
Subject Code: 6469

M.Sc. Information & Network Security - 4th Sem.

(2517)

Paper- I: Intrusion Detection System & Analysis

Time allowed: 3 hrs. **Max. Marks: 100**

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

Q1. a) Explain the need and scope of Intrusion Detection System (IDS). 10

b) What are different uses of IDS? Explain by taking examples. 10

Q2. a) What is firewall? How firewall works with IDS? Explain 10

b) Discuss common detection methodologies of IDS. 10

Q3. a) What is Anomaly based detection methodology? How signature based detection works in IDS? Explain. 10

b) Discuss the significance of stateful protocol analysis. 10

Q4. Compare and contrast any two IDS technologies in detail. 20

Q5. a) Draw and explain network architecture of IDS. 10

b) How information gathering capabilities are implemented in IDS? Explain. 10

Q6. a) What kind of prevention capabilities can be implemented in IDS? Explain. 10

b) What are the tasks performed in IDS Deploying? Explain. 10

Q7. a) What is meant by Integrated-IDS? Why integration of different technologies is required in IDS? Explain. 10

b) Discuss the working of Direct IDS. Compare similarities of Direct IDS with Indirect IDS. 10

Q8. Explain the following:

a) Anti-Malware Technologies 10

b) Working model of Honeypots 10

****

Sr. No. 7122

Exam. Code: 217904
Subject Code : 6470

M. Sc. Information & Network Security - 4th Sem.

(2517)

Paper -II: Reverse Engineering & Malware

Time allowed: 3 hrs. **Max. Marks: 100**

Note: Attempt any FIVE questions. All questions carry EQUAL marks.

1. a) Define Malware. Explain its important characteristics. (2+8)

   b) Explain Malware taxonomy and importance of each component in taxonomy in detail. (10)

2. Explain:-

   a) Examining ClamAV Signatures (10)

   b) Malware Indicators. (10)

3. a) Give Malware Classification with the importance of each classification. (10)

   b) Explain any two tools to perform Malware analysis. (10)

4. a) How Code Analysis is carried out? Why is it useful to do so? Explain. (10)

   b) Explain Reverse Engineering Malware Methodology in detail. (10)

5. a) Which are executable resources for REM? Explain Sandboxing executables in detail. (10)

   b) Explain Compression and Obfuscation in detail. (10)

6. a) Explain Portable Executable (PE 32) file format and its importance in detail. (10)

   b) What is the role of Software Debuggers to examine Malware? (10)

PTO

Sr. No. 7122

Exam. Code: 217904
Subject Code : 6470

7. a) How the Reverse Engineering Process is automated? Explain. (10)

b) How Malicious Microsoft Office Documents are analyzed? Explain in detail. (10)

8. Write short notes on any TWO:-

a) Custom Clam AV databases.

b) Behavioural Analysis

c) Executable Metadata & Executable Packers. (10+10)

****

Sr. No. 7123

Exam. Code: 217904
Subject Code : 6471

M.Sc. Information & Network Security - 4th Sem.

(2517)

Paper - III: Ethical Hacking

Time allowed: 3 hrs.

Max. Marks: 100

Note: Attempt any FIVE Questions. All Questions carry 20 marks.

1) What is computer security? Why information security is important? What are the elements of security?
2) What is ethical hacking and why do we need it? Describe various phases involved in hacking.
3) What is foot printing? Why is foot printing necessary? Describe the major steps involved in foot printing. List some of tools used in gathering information.
4) How are passwords attacked, and what are the countermeasures? What are the following tools used for: John the Ripper, Crack?
5) What is a sniffer? What is active/passive sniffer? Give examples? What are the capabilities of major sniffers such as ethereal, snort, dsniff?
6) What is denial of service attack? What is local, remote , and distributed DoS? How is spoofing used in DNS attacks?
7) What is wired equivalent privacy (WEP) Protocol? Explain the goal of WEP for wireless networks. Name and explain various wireless hacking tools.
8) Write short notes on:
   a) Defence against network eavesdropping
   b) Securing wireless networks

****