Exam. Code : 217904
Subject Code : 7059

M.Sc. Information & Network Security 4th Semester

INTRUSION DETECTION SYSTEM AND ANALYSIS

Paper–I

Time Allowed—3 Hours] [Maximum Marks—100

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

1. (a) Explain the purpose and scope of Intrusion Detection System (IDS). 10

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

2. (a) Differentiate between Firewall and IDS. 10

   (b) Discuss key functions of IDS. 10

3. (a) Differentiate between Anomaly based and Signature based detection. 10

   (b) How is stateful protocol analysis effective in IDS ? Explain. 10

4. Discuss any five types of IDS-Technologies in detail. 20

5. (a) Draw and explain various components of IDS. 10

   (b) How security capabilities are implemented in IDS ? Explain. 10

6. (a) Can IDS be used as a Prevention system ? Comment and justify the statement. 10

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

7. (a) What is the need of having integrated IDS technologies ? Explain by taking examples. 10

   (b) Differentiate between Direct and Indirect IDS. 10

8. Explain the following :

   (a) Forensic analysis 10

   (b) Honeypots. 10

Exam. Code : 217904
Subject Code : 7060

M.Sc. Information & Network Security 4th Semester

REVERSE ENGINEERING & MALWARE

Paper—II

Time Allowed—Three Hours] [Maximum Marks—100

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

1. Define malware. Give examples. What is a malware threat ? Explain in detail the various groups of malware threats facing an organization.

2. What is the need of malware analysis ? Differentiate between static analysis of malwares and dynamic analysis of malwares by taking examples. What are the various things to look for to identify artifacts associated with a malware infection ?

3. Discuss various key Malware Analysis tools and techniques for reverse engineering of Malware with appropriate utility of each.

4. (a) Differentiate between Behavioural analysis and Code analysis with examples.

   (b) What are the reasons for using the free Linux Antivirus package ClamAV ? Explain the procedure to create your own Anti-Virus Signatures with ClamAV.

5. (a) Explain the process of De-obfuscating malicious Java Script using debuggers and interpreters.

   (b) Explain the procedure for analyzing suspicious PDF files.

6. (a) What is Sandboxed Analysis ? How do you build your own Sandbox for Malware Analysis ?

   (b) How are "Initial Infection Vectors" used for Malware discovery ? Explain with examples.

7. What is meant by reverse engineering process to mitigate malwares ? How can you automate the reverse engineering of malware ? Discuss.

8. Write short notes on :—

   (a) Portable Executable (PE) File Format Exploit Analysis

   (b) Unpacking Packed/Protected Executables for malware analysis.

Exam. Code : 217904
Subject Code : 7061

M.Sc. Information & Network Security 4th Semester

ETHICAL HACKING

Paper—III

Time Allowed—Three Hours] [Maximum Marks—100

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

1. (a) Define security. Why it is impartial ? Explain in detail. 2+8

   (b) Explain Threat, Attack and Vulnerabilities in Context of ethical hacking. 10

2. (a) Define Hacking. Explain various principles to be followed by ethical hackers in detail. 3+7

   (b) How the hacker gathers information ? Explain the methodology in detail. 3+7

3. (a) What is foot printing ? Explain the tools used for reconnaissance phase. 3+7

   (b) What is System Hacking ? Explain various methods of password hacking in detail. 2+8

4. (a) Who are sniffers ? Explain the difference between Active and Passive Sniffing. 2+8

   (b) What is Spoofing ? Explain the role of ARP spoofing in context of System Hacking. 2+8

5. (a) What is Session Hijacking ? Explain various steps involved in it. 2+8

(b) Explain various Session Hijacking Tools in detail. 10

6. (a) Explain 802.11 in context of Wireless Networks in detail. 10

(b) What is the role of Wired Equivalent Privacy Protocol ? Explain how WEP keys are cracked ? 5+5

7. (a) How do you ensure security in Wireless Network ? 10

(b) Write about WLAN scanners and WLAN sniffers for Wireless Networks. 10

8. Write short notes on any **TWO** :—

(a) Hacking Tools

(b) DNS and IP sniffing

(c) Keystroke Loggers. 10×2=20