C.U.SHAH UNIVERSITY
Summer Examination - 2018

Subject Name: Cyber Security & Forensic Investigator

Subject Code: 5CS02WCY2   **Branch: M.Sc.IT (WebTech)**

Semester: 2   **Date: 23/04/2018**   **Time: 10:30 To 01:30**   **Marks: 70**

Instructions:
   (1) Use of Programmable calculator & any other electronic instrument is prohibited.
   (2) Instructions written on main answer book are strictly to be obeyed.
   (3) Draw neat diagrams and figures (if necessary) at right places.
   (4) Assume suitable data if needed.

SECTION-I

Que-1 Attempt all the following short questions.   **[7]**
   1. What is cyber security?
   2. Who is cybercriminal?
   3. Define firewall.
   4. Enlist the 5P "Natizens Mantras" for online security.
   5. Give the full form of DoS.
   6. Define network forensic.
   7. What is volatile information?

Que-2 Attempt all questions.   **[14]**
   1. What is IDS? Explain types of IDS in details.   [7]
   2. Write notes on CommView and OmniPeek network traffic capturing tools.   [7]

OR

Que-2 Attempt all questions.   **[14]**
   1. Explain non-volatile information.   [5]
   2. What is registry? Explain top level registry keys.   [5]
   3. What is event? Explain various event rules (ER) in details.   [4]

Que-3 Attempt all questions.   **[14]**
   1. What is metadata? Explain the types of metadata?   [7]
   2. Explain working of firewall with diagram and also explain its types in details.   [7]

OR

Que-3 Attempt all questions.   **[14]**
   1. Write a note on new line injection attack.   [5]

2. Explain prefatch file in details. [5]
3. Explain static analysis process. [4]

SECTION-II

Que-4 Attempt all the following short questions. **[7]**
1. Give the full form of MITM.
2. Define cookie.
3. What is email spoofing?
4. What is cyber law?
5. What do you mean by event?
6. What is passkey?
7. Enlist the names of offline password attack.

Que-5 Attempt all questions. **[14]**
1. Explain categories and roles of cyber criminals. [6]
2. Explain following cyber-attacks. [8]
   A. Salami technique
   B. Phishing
   C. Internet time theft
   D. Spamming

OR

Que-5 Attempt all questions. **[14]**
1. Why do we need cyber law? [5]
2. Explain types of password in details. [5]
3. Explain various online password attacks. [4]

Que-6 Attempt all questions. **[14]**
1. Write a detailed note on dictionary attack. [5]
2. Explain brute force attack. [5]
3. Explain message digest function: MD5. [4]

OR

Que-6 Attempt all questions. **[14]**
1. Explain strong and random password in brief. [5]
2. Explain DNS poisoning attack in detail. [5]
3. Explain following password cracking tools. [4]
   A. Cain & Abel
   B. John the Ripper