316315

25226

3 Hours / 70 Marks Seat No. | | | | | | | | |

Instructions – (1) All Questions are *Compulsory.*

(2) Answer each next main Question on a new page.

(3) Illustrate your answers with neat sketches wherever necessary.

(4) Figures to the right indicate full marks.

(5) Assume suitable data, if necessary.

(6) Mobile Phone, Pager and any other Electronic Communication devices are not permissible in Examination Hall.

Marks

1. Attempt any FIVE of the following : **10**

a) Enlist any two rules of digital forensics that must be followed during an investigation.

b) State any four application of computer forensics in public sector.

c) List any four unethical norms for investigations.

d) Define Digital forensic investigation model. Write names of any two investigation models used in digital forensics.

e) List any two types of attacks that computer systems commonly face.

f) Define penetration testing.

g) Define social engineering with one example.

Marks

2. Attempt any THREE of the following : **12**

a) Describe computer forensics and network forensics.

b) Define order of volatility. Explain its importance in digital evidence collection.

c) Explain Network - Infrastructure attack with suitable example.

d) Define scanning SNMP. Explain its working in detail.

3. Attempt any THREE of the following : **12**

a) Explain the impact of emerging technologies. (cloud, IoT, AI, mobile devices) on digital forensic investigation.

b) Explain the concept of digital crime scene. Describe the procedure for collecting evidence from removable media and cell phones.

c) Explain operating system attacks and their possible consequences.

d) Explain Network Analysis using Network Analyzers.

4. Attempt any THREE of the following : **12**

a) Describe cyber attacks. Explain any 2 common cyber attacks.

b) Explain the challenges in digital forensic investigation.

c) Digital evidence collected from a crime scene must be presented in court. Explain how proper documentation and chain of custody help in ensuring the admissibility of evidence.

d) Define Ethical hacking. Distinguish between hackers and malicious users.

e) During a security audit, an administrator wants to identify active hosts and open ports in the network. Explain how ping sweeping and port scanning would be applied and what information each technique provides.

Marks

5. Attempt any TWO of the following : **12**

a) Explain the stages of digital forensics investigation process in detail.

b) Describe the UML modeling of digital forensic process model. (UMDFPM) and mention its advantages.

c) Define live acquisition. Discuss its advantages and concerns in digital forensic investigations.

6. Attempt any TWO of the following : **12**

a) Explain the purpose of cloning in digital forensics and describe the basic cloning process.

b) Explain Ethical hacking principles in detail.

c) Describe phases of ethical hacking in detail.
