Q.P. Code: 24910

(3 Hours) **Total Marks: 80**

Instructions: - 1) Question No 1 is compulsory; solve any 3 questions from remaining 5 questions.
2) Assume suitable data wherever necessary.
3) Figures to the right indicate full marks.

Q1 a) What is enumeration? What information can be enumerated by intruders? Explain the different enumeration techniques. (**10**)
b) How are Trojans deployed? What are the different techniques used by Trojans to evade antivirus software? (**10**)

Q2) a) What is packet sniffing? How is it done? What are the threats due to packet sniffing? (**10**)
b) Why is session hijacking successful? What are the key session hijacking techniques? Explain. (**10**)

Q3) a) Explain the following techniques of firewall identification:
i) Port scanning ii) Banner grabbing iii) Firewalking (**10**)
b) Explain how law enforcement is done in computer forensics. (**10**)

Q4) a) Discuss the process of handling a digital crime scene with an example. (**10**)
b) How does rootkit work? Explain. How can the system be protected against rootkit? (**10**)

Q5) a) What types of denial of service attacks can be launched against intrusion detection systems? Explain. (**10**)
b)What knowledge require to create to program Buffer overflows? What are the steps to create Buffer overflow. (**10**)

Q6) Write short notes on (Any four). (**20**)

i) Biometric Security System.
ii) Legal implications of hacking.
iii) Netcat.
iv) Challenges in event handling
v) Password attacks on Windows OS.
