(2 ½ Hours) [Total Marks: 75]

N.B. 1) All questions are compulsory.
2) Figures to the right indicate marks.
3) Illustrations, in-depth answers and diagrams will be appreciated.
4) Mixing of sub-questions is not allowed.

Q. 1	**Attempt the following (Any FOUR)**	**(20M)**
(a)	Define the term Hacktivism and Explain Hacker Classes.	
(b)	Describe in detail any **one** method of Information gathering 1. Scanning 2.Footprinting	
(c)	Write a short note on keystroke logging.	
(d)	Explain any two common types of Attack?.	
(e)	State and explain the HTTP Tunneling Technique	
(f)	What are the various IP Spoofing techniques ?.	
Q. 2	**Attempt the following (Any FOUR)**	**(20M)**
(a)	Explain the various type of password effective in securing user account.	
(b)	Define Active and Passive sniffing and state its characteristics.	
(c)	Describe the ARP poisoning process.	
(d)	Write a short note on BOT and BOTNET's	
(e)	Differentiate between spoofing and Hijacking.	
(f)	Explain the types of attack on a Webserver	
Q. 3	**Attempt the following (Any FOUR)**	**(20M)**
(a)	State and explain the different Web Application Vulnerablities	
(b)	Describe the User authentication types used to verify User Identity	
(c)	Explain the sequence of steps involved in the SQL Inejction attack.	
(d)	State and explain the Mutation Techniques	
(e)	Explain the Term Wireless Hacking	
(f)	Describe the function of Penetration testing Automated tools	
Q. 4	**Attempt the following (Any FIVE)**	**(15M)**
(a)	Define the CIA triad	
(b)	Mention the different phases of Ethical Hacking	
(c)	What is meant by the term Smurf attack?.	
(d)	Mention the purpose of Web Hardening	
(e)	Define XSS.	
(f)	Describe the term passive Spraying.	

****