UNIT – III

Preparing for a Hack & Reconnaissance

PART – A (Short Answer Questions)

S.No	Questions	BT	CO	PO
1	Define Technical Preparation.	L1	CO3	PO2
2	What is Engagement Management?	L1	CO3	PO1
3	Define Reconnaissance.	L1	CO3	PO1
4	What is Social Engineering?	L1	CO3	PO1
5	List common Social Engineering techniques.	L2	CO3	PO1
6	What is Physical Security Assessment?	L2	CO3	PO1
7	Define Internet Reconnaissance.	L1	CO3	PO1
8	What is Footprinting?	L2	CO3	PO1
9	Explain Open Source Intelligence (OSINT).	L2	CO3	PO1
10	State the objectives of Reconnaissance.	L2	CO3	PO1

PART – B (Long Answer Questions)

S.No	Questions	BT	CO	PO
11	Explain the Technical Preparation required before a penetration test.	L2	CO3	PO2
12	Discuss Managing the Engagement in Ethical Hacking.	L2	CO3	PO3
13	Explain Reconnaissance and its importance in penetration testing.	L3	CO3	PO2
14	Describe Social Engineering attacks and countermeasures.	L3	CO3	PO1
15	Explain Physical Security Testing with examples.	L3	CO3	PO2
16	Discuss Internet Reconnaissance techniques in detail.	L3	CO3	PO3
17	Explain Footprinting and Information Gathering methods.	L4	CO3	PO2
18	Compare Active and Passive Reconnaissance.	L4	CO3	PO1
19	Explain OSINT tools and their applications in Ethical Hacking.	L3	CO3	PO2
20	Describe a complete Reconnaissance methodology for a target organization.	L5	CO3	PO3