Reg. No.

B.E / B.TECH. DEGREE EXAMINATION, MAY 2023
Sixth and Eighth Semester
OE18804 – ETHICAL HACKING AND IT SECURITY
(Common to all branches)
(Regulation 2018)

TIME: 3 HOURS   **MAX. MARKS: 100**

Course Outcomes	Statements	RBT Level
CO 1	Interpret the core concepts related to malware, hardware and software vulnerabilities and their causes	3
CO 2	Relate ethics behind hacking and vulnerability disclosure	3
CO 3	Judge the vulnerabilities related to computer system and networks using state of the art tools and technologies	3
CO 4	Assess the strengths and weaknesses of general cyber security models	5
CO 5	Assess the possible consequences of misaligning enterprise strategy, security policy, and security plans	5

PART- A (10 x 2 = 20 Marks)

(Answer all Questions)

		CO	RBT LEVEL
1.	Demonstrate the role of ethical hacker.	1	3
2.	Highlight the importance of the term footprinting.	1	3
3.	Compare active and passive information gathering.	2	2
4.	Apply DIG command on www.edureka.com and write down the result.	2	3
5.	List the pros and cons of vulnerability scanner.	3	3
6.	Demonstrate the role of sniffing. Explain the categories of sniffing.	3	3
7.	Interpret the term threat vector.	4	3
8.	Define DDoS attack.	4	1
9.	Summarize the Benefit of risk analysis.	5	3
10.	Discuss how the quantitative risk assessment differ from qualitative risk assessment?	5	2

PART- B (5 x 14 = 70 Marks)

				Marks	CO	RBT LEVEL
11. (a)	(i)	Explain the various Linux OS network commands with example		(7)	1	2
	(ii)	Summarize the different types of penetration testing		(7)	1	2

(OR)

(b)	**(i)**	Explain NIST penetration testing model and justify how it is more comprehensive than other models	**(8)**	**1**	**2**
	(ii)	Describe in detail about various type of hackers and its role.	**(6)**	**1**	**2**

12. (a)		Illustrate detailed steps to install Kali Linux OS. Examine the usage of Fierce tool and execute the various commands.	**(14)**	**2**	**3**

(OR)

(b)		Outline in detail various types of Port Scanning techniques and how to prevent your system from the port scan attacks.	**(14)**	**2**	**3**

13. (a)		Determine the usage of COMMIX and Skipfish tools to perform web analysis using any of the URL's. Write down the installation procedures and execute the various commands.	**(14)**	**3**	**3**

(OR)

(b)	**(i)**	Explain the different categories of ARP attacks with neat scenario representation and explain how it works.	**(7)**	**3**	**3**
	(ii)	Illustrate the steps required to perform a DNS spoofing attack and how it differ from DHCP spoofing?	**(7)**	**3**	**3**

14. (a)		Sketch the structure of cyber security models in the network? Mention its merits and demerits.	**(14)**	**4**	**4**

(OR)

(b)	**(i)**	Categorize the different types of attacks with suitable illustrations	**(10)**	**4**	**4**
	(ii)	Describe in detail Roles and Responsibilities of Information Security	**(4)**	**4**	**4**

15. (a)		Illustrate about information security life cycle and the security planning stages in an enterprise with a neat sketch.	**(14)**	**5**	**3**

(OR)

(b)		Examine how Risk analysis works in mitigating risks in an Organization and also demonstrate about Risk management Framework.	**(14)**	**5**	**3**

PART- C (1 x 10 = 10 Marks)

		Marks	CO	RBT LEVEL
16.	Elaborate in detail, steps to install Network Mapper (NMap) software in Kali Linux OS and execute the following commands, i) Scanning a single IP ii) Scanning a range of IPs iii) Scanning a Single Port iv) Scanning Range of Ports v) NMAP timing command vi) Check for Vulnerabilities on Hosts vii) Scanning a host viii) Verbose Mode command ix) Ping Scanning x) Disable DNS Name Resolution.	**(10)**	**2**	**5**

****