KUMARAGURU
college of technology
character is life

B.E/B.TECH DEGREE EXAMINATIONS: NOV/DEC 2024

(Regulation 2020)

Third Semester

MASTER OF COMPUTER APPLICATIONS

P20CAE0230: Ethical Hacking and Network Defence

COURSE OUTCOMES

CO1: Illustrate the legal and ethical requirements related to ethical hacking.

CO2: Interpret the vulnerabilities, mechanisms to identify vulnerabilities, threats, attacks.

CO3: Perform penetration & security testing to identify the vulnerabilities in the application .

CO4: Examine the different tools and techniques that ethical hackers employ.

Time: Three Hours   **Maximum Marks: 100**

Answer all the Questions:-
PART A (10 x 2 = 20 Marks)
(Answer not more than 40 words)

1. Define ethical hacking and its importance in cybersecurity.	CO1	[K$_2$]
2. Differentiate between threat and exploit in the context of a security breach.	CO1	[K$_2$]
3. List the phases of ethical hacking.	CO1	[K$_2$]
4. Illustrate the role of reconnaissance in ethical hacking.	CO2	[K$_2$]
5. Explain the significance of port scanning in identifying network vulnerabilities.	CO2	[K$_2$]
6. Illustrate how ping sweeps can be used to identify live hosts before conducting a port scan.	CO3	[K$_2$]
7. Describe the concept of ARP spoofing in network attacks.	CO3	[K$_2$]
8. Explain the process of session hijacking and its impact on network security.	CO4	[K$_2$]
9. List two eavesdropping tool with the technique used.	CO4	[K$_2$]
10. Discuss the difference between active and passive sniffing.	CO4	[K$_2$]

Answer any FIVE Questions:-
PART B (5 x 16 = 80 Marks)
(Answer not more than 400 words)

11.	a)	Analyze the legal and ethical considerations of ethical hacking in organizations, and how they impact penetration testing.	8	CO1	[K$_3$]
	b)	Conduct a vulnerability assessment using generic tools to identify potential weaknesses in a corporate network and suggest remediation steps.	8	CO1	[K$_3$]

12.	a)	Apply footprinting techniques to gather information on a target network and evaluate the potential security threats.	8	CO2	[K$_3$]
	b)	Demonstrate port scanning using generic tools to identify open ports and vulnerabilities in a network.	8	CO2	[K$_3$]
13.	a)	Apply various password guessing techniques to crack passwords in a compromised system.	8	CO3	[K$_3$]
	b)	Illustrate how sniffing tools can be used to capture network traffic, and suggest measures to secure networks against sniffing attacks.	8	CO3	[K$_3$]
14.	a)	Apply the process of detecting and mitigating a DNS spoofing attack in a local network. Discuss the tools and techniques used in ethical hacking to prevent such attacks.	8	CO3	[K$_3$]
	b)	Perform a side-channel attack on cryptographic hardware using generic techniques and recommend strategies to prevent these attacks.	8	CO3	[K$_3$]
15.	a)	Apply the steps involved in performing a SQL injection attack on a vulnerable web application and recommend countermeasures.	8	CO4	[K$_3$]
	b)	Demonstrate the process of session hijacking and discuss strategies to mitigate these attacks in a web environment.	8	CO4	[K$_3$]
16.	a)	Perform a penetration test on a wireless network using generic techniques and suggest measures to enhance security.	8	CO4	[K$_3$]
	b)	Use ethical hacking techniques to evaluate the weaknesses in a wireless network protected by WEP encryption and propose improvements.	8	CO4	[K$_3$]

****