KUMARAGURU
college of technology
character is life

Register Number:……..…

**MCA DEGREE EXAMINATIONS: NOV/DEC 2023**

(Regulation 2020)

Third Semester

**MASTER OF COMPUTER APPLICATIONS**

P20CAE0016**:** Ethical Hacking

**COURSE OUTCOMES**

**CO1:** Apply various open source security tools to assess the network and computing system.

**CO2:** Practice penetration testing to predict the vulnerabilities across any computing system.

**CO3:** Explain how to prevent the information and computing assets from any kind of attacks.

**CO4:** Understand how to protect the devices in a network from malicious software and worms.

**CO5:** Assess the wireless network flaws and be able to provide security solutions.

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

**Answer all the Questions:-**

**PART A (10 x 2 = 20 Marks)**

| | | | |
|---|---|---|---|
| 1. | Differentiate between vulnerability and exploit with a suitable example. | CO1 | [$K_3$] |
| 2. | Discuss how the Black box penetration testing different from the Grey box penetration testing. | CO1 | [$K_3$] |
| 3. | As a penetration tester, suggest a few methods to counter SNMP enumeration. | CO2 | [$K_3$] |
| 4. | What is the outcome SMTP enumeration? List any two commands which are used to perform the SMTP enumeration? | CO2 | [$K_2$] |
| 5. | Enumerate the pros and cons of a vulnerability scanner. | CO3 | [$K_2$] |
| 6. | Differentiate between active and passive sniffing. | CO3 | [$K_3$] |
| 7. | What is a client side exploit? Give an example. | CO4 | [$K_1$] |
| 8. | What is a password salt? | CO4 | [$K_1$] |
| 9. | Justify the need for security controls in a wireless network. | CO5 | [$K_3$] |
| 10. | Suggest two methods to protect the login operation from the brute force attacks. | CO5 | [$K_3$] |

## PART B (6 x 5 = 30 Marks)

| | | | |
|---|---|---|---|
| 11. | Enumerate the various types of penetration tests. Give example. | CO1 | [$K_2$] |
| 12. | What are the various sources of information gathering that help to perform an effective pen-test. | CO2 | [$K_2$] |
| 13. | Enumerate the common network services targeted at to launch remote attacks by the attackers. | CO3 | [$K_2$] |
| 14. | List any 5 operating system level commands used to perform post exploit reconnaissance. | CO4 | [$K_2$] |
| 15. | Explain how authentication in web application itself is vulnerable and prone to attacks. | CO5 | [$K_2$] |
| 16. | Assume you are a pentester, suggest and explain about a few methods to bypass authentication forms in a test environment. | CO5 | [$K_3$] |

**Answer any FIVE Questions**

## PART C (5 x 10 = 50 Marks)

| | | | |
|---|---|---|---|
| 17. | Consider you are assigned to conduct penetration testing for ACME software development company. Develop a "Rules of Engagement" document to be signed between you and ACME. | CO1 | [$K_3$] |
| 18. | Justify the need to protect sub-domains of an website with suitable example and block diagrams. | CO2 | [$K_3$] |
| 19. | Explain about DNS spoofing and DHCP spoofing. | CO3 | [$K_2$] |
| 20. | Explain how a client is very easily victimized by means of an email with malicious attachment and links. | CO4 | [$K_2$] |
| 21. | Explain about the various types authentication and suggest methodologies to overcome the inherent drawbacks in them. | CO5 | [$K_3$] |
| 22. | Explain about the firewall evading techniques. | CO2 | [$K_2$] |

**********