QP Code:

Reg. No

SAVEETHA ENGINEERING COLLEGE

(Autonomous, Affiliated to Anna University, Chennai)

B.E./B.Tech. End Semester Examinations – Apr/May 2025 (R2019/R2024)

Common to **AI&DS/AIML/CSE/IT/CSE(IoT)/CSE(CS)**

19CS417 – Ethical Hacking Techniques

Time: Three hours

Maximum marks: 100

Faculty Name	**Dr.J.PARAMESH**	**Department**	**CSE**

Answer All Questions

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

		CO	**Knowledge Level (Blooms)**	**Difficulty Level (1-5)**
QA101	What is ethical hacking?	CO1	K1	L2
QA102	Mention the name of the class of the network, networkID, host range, broadcast address for the IP Address 111.211.11.1	CO1	K2	L3
QA103	Do you think Linux is a kernel? What do you mean by kernel in an operating system?	CO1	K2	L1
QA104*	What are the key differences between TCP and UDP protocols in the context of the TCP/IP model?	CO1	K1	L2
QA105	Which type of penetration testing simulates a real-world attack by attempting to penetrate the target system without any prior knowledge of its security measures?	CO1	K4	L3
QA106	Compare the primary difference between a vulnerability assessment and a penetration test?	CO1	K2	L3
QA107*	What is the purpose of the subnet mask in the TCP/IP addressing scheme?	CO1	K1	L4
QA108	Sketch the two key components typically included in the Rules of Engagement (RoE) document for penetration testing?	CO1	K3	L2
QA201	What is Information Gathering in Ethical Hacking?	CO2	K1	L2
QA202*	Briefly explain the function of the trace route command and how it identifies network hops along the path to a destination.	CO2	K1	L2
QA203	How would you outline webserver fingerprinting and list out its techniques?	CO2	K4	L2
QA204*	What is passive information gathering in the context of cyber security, and how does it differ from active information gathering	CO2	K1	L2
QA205	What is DNS Cache Snooping?	CO2	K1	L2
QA206	Sketch the primary purpose of SNMP enumeration in a security assessment?	CO2	K3	L3
QA207	How can SMTP enumeration be used to gather information about a target email server?	CO2	K4	L2

QA208*	What are two common techniques used to evade Intrusion Detection Systems (IDS), and how do they work?	CO2	K1	L2
QA301	Extract vulnerability database and exploit database?	CO3	K2	L3
QA302	Define Network Sniffing. Mention the goal of a Network Sniffer.	CO3	K1	L2
QA303*	What is an ARP spoofing attack and how does it affect network security?	CO3	K1	L2
QA304	Infer the purpose of the searchsploit command?	CO3	K2	L3
QA305	How does SSL Strip work?	CO3	K4	L4
QA306*	What is SQL Injection and how can it be mitigated to secure SQL Servers?	CO3	K1	L3
QA307	Discover one common technique used in attacking SMTP servers, and what is its purpose?	CO3	K3	L2
QA308	What is a key indicator of weak authentication that penetration testers look for during a security assessment?	CO3	K1	L2
QA401	Define Metasploit?	CO4	K1	L1
QA402*	What are two common client-side exploitation methods and how do they compromise user security?	CO4	K1	L1
QA403	How would you describe pdf hacking?	CO4	K4	L3
QA404	Interpret about the post exploitation phase.	CO4	K2	L1
QA405	What is payload in Metasploit Framework?	CO4	K1	L2
QA406	Discover the two main types of password hashes used in Windows operating systems?	CO4	K3	L1
QA407*	What is a hashing algorithm?	CO4	K1	L2
QA408*	What are the primary hashing methods used for storing passwords in Windows operating systems, and how do they enhance security	CO4	K1	L2
QA501	Discover monitor mode in wireless network analysis?	CO5	K3	L1
QA502*	What is an Evil Twin Attack in the context of wireless networks and how can users protect themselves from it?	CO5	K1	L2
QA503	Infer Captcha Validation Flaw.	CO5	K2	L2
QA504*	What is an SSRF Attack?	CO5	K1	L2
QA505	How to Identify XSS Vulnerability?	CO5	K4	L1
QA506	How can Burp Suite be used to automate security testing for web applications?	CO5	K4	L2
QA507	Criticize SQL Injection and what can it potentially allow an attacker to do?	CO5	K5	L2
QA508*	Discover the three main types of Cross-Site Scripting (XSS) attacks, and how do they differ from each other?	CO5	K3	L2

PART B **(5 x 13 = 65 marks)**

			CO	**Knowledge Level (Blooms)**	**Difficulty Level (1-5)**
QB101	(a)	Compare the basic functionalities of Windows and Linux operating systems and discuss their file systems, user management, and package management systems, highlighting key commands in both OSs	CO1	K2	L3
		(OR)			
QB101*	(b)	Write briefly about TCP/IP Protocols	CO1	K4	L2
QB102*	(a)	Discuss in detail about topology and give explanation about all network types	CO1	K2	L3
		(OR)			

QB102	(b)	Write in detail about the Vulnerability Assessment and Elaborate on the process involved in conducting vulnerability assessment process to ensure the security of an organization.	CO1	K4	L2
QB103	(a)	What is Penetration Testing? Enumerate and describe each stage of penetration testing.	CO1	K2	L2
		(OR)			
QB103	(b)	Compare and contrast OSSTMM, NIST, and OWASP in terms of their approaches to security testing and assessment and discuss their methodologies, frameworks, and specific areas of focus, providing examples of how each can be applied in a real-world scenario.	CO1	K2	L2
QB104*	(a)	Explain in detail about OSI model.	CO1	K5	L2
		(OR)			
QB104	(b)	Explain the significance of effective reporting in vulnerability assessments, & actionable and understood by different stakeholders?	CO1	K5	L2
QB201*	(a)	Explain about Active Information Gathering and Passive Information Gathering in detail	CO2	K5	L2
		(OR)			
QB201	(b)	Discuss in detail about Nmap with an Example of One Output Introduction to Nmap.	CO2	K2	L2
QB202	(a)	Write a brief note on SMTP enumeration.	CO2	K4	L1
		(OR)			
QB202	(b)	What is network tracing? Explain the TCP/IP protocol header and the function of TTL in network tracing.	CO2	K5	L2
QB203	(a)	Compare and contrast ICMP Traceroute, TCP Traceroute, and UDP Traceroute and discuss their mechanisms, typical use cases, and advantages and disadvantages and provide an example of a situation where each type of traceroute might be preferred.	CO2	K5	L3
		(OR)			
QB203*	(b)	Discuss in detail about Google hacking	CO2	K2	L2
QB204	(a)	Explain the techniques that can be used to evade firewall detection.	CO2	K5	L4
		(OR)			
QB204	(b)	Correlate the various target enumeration and port scanning techniques used in network security. Include a detailed explanation of each technique, the tools commonly used, and the advantages and disadvantages of each with examples.	CO2	K4	L2

QB301	(a)	Define Network Sniffing and describe its types. Given an ftp server ftp.example.org, explain the procedure of how to use the dsniff tool to capture the username and password.	CO3	K5	L2
		(OR)			
QB301*	(b)	Explain about ARP attacks and denial of service attacks	CO3	K5	L3
QB302	(a)	Consider the website example.com. describe how the Wireshark can be used to sniff for the username and password.	CO3	K2	L2
		(OR)			
QB302	(b)	Write a brief note on DNS spoofing and DHCP spoofing.	CO3	K4	L2
QB303	(a)	What are session cookies? How session cookies can be sniffed for hijacking a session?	CO3	K3	L2
		(OR)			
QB303*	(b)	Give an overview of brute force attacks	CO3	K2	L4
QB304*	(a)	Discuss a detailed explanation of hijacking session with MITM attacks	CO3	K2	L4
		(OR)			
QB304	(b)	Discuss the methods used in attacking SQL servers by testing for weak authentication with Common Attack Techniques.	CO3	K2	L2
QB401	(a)	Explain the process of reconnaissance using Metasploit, with a focus on port scanning.	CO4	K5	L4
		(OR)			
QB401*	(b)	Explain in detail about Client-side exploitation methods	CO4	K5	L3
QB402	(a)	Discuss in detail about how rainbow crack tool can be used to crack the hashes.	CO4	K2	L2
		(OR)			
QB402	(b)	Describe the process of compromising a Windows host using Metasploit with exploiting a vulnerability and gaining control over the target system and discuss the importance of such an exercise in penetration testing.	CO4	K3	L2

QB403	(a)	Explain the process of browser exploitation, post-exploitation activities, and acquiring situation awareness in the context of cybersecurity.	CO4	K5	L3
		(OR)			
QB403	(b)	Explain how meterpreter can be used for escalating privileges and gain access to the OS.	CO4	K5	L4
QB404*	(a)	Explain in detail about hashing algorithms.	CO4	K5	L2
		(OR)			
QB404	(b)	What is the Social Engineering Toolkit (SET)? Describe the process of creating a backdoor with SET.	CO4	K3	L4
QB501	(a)	In the wireless networks, how hidden SSIDs are uncovered and bypass MAC Filters?	CO5	K3	L1
		(OR)			
QB501*	(b)	Explain the concept of wireless hacking inn detail	CO5	K5	L2
QB502	(a)	Discuss the significance of login protection mechanisms, focusing on Captcha validation and Captcha reset flaws.	CO5	K2	L3
		(OR)			
QB502	(b)	Describe the process of testing for vulnerabilities using Burp Suite and discuss how automation can enhance vulnerability testing efficiency.	CO5	K3	L4
QB503*	(a)	What is SQL injection and Explain about the attacks with a neat sketch.	CO5	K5	L3
		(OR)			
QB503*	(b)	Explain about Captcha Validation Flaw – Captcha RESET Flaw in detail.	CO5	K5	L2
QB504	(a)	Discuss the fundamental concepts of routers, firewalls, and risk analysis tools for firewalls in network security.	CO5	K2	L3
		(OR)			
QB504	(b)	Explain the concepts of Intrusion Detection and Prevention Systems (IDPS) and Honeypots in Ethical Hacking.	CO5	K5	L3

PART C **(1 x 15 = 15 marks)**

(Case study/Comprehensive type Questions)

			CO	Knowledge Level (Blooms)	Difficulty Level (1-5)
QC101	(a)	Classify the penetration testing approaches and detail each of the penetration testing types.	CO1	K4	L3
		(OR)			
QC101*	(b)	Explain about the concept of hacking and include all terminologies	CO1	K5	L3
QC201	(a)	Describe about the TCP port scanning using Nmap. Clearly explain with an example.	CO2	K3	L2
		(OR)			
QC201*	(b)	Explain the concept of enumerating and fingerprinting the web servers	CO2	K5	L3
QC301*	(a)	Explain in detail about SSL Strip.	CO3	K5	L3
		(OR)			
QC301	(b)	Compare vulnerability databases and exploit databases? Give examples. How organizations can benefit from these vulnerability data resources.	CO3	K2	L2
QC401*	(a)	Explain the steps involved in e-mails with malicious attachments in detail	CO5	K5	L2
		(OR)			
QC401	(b)	Discuss in detail about the John the Ripper tool with few examples.	CO4	K2	L4
QC501*	(a)	Define aircrack? Give explanation about cracking the WEP, WPA/WPA2 wireless network	CO5	K4	L3

		(OR)			
QC501	(b)	What is the authentication bypass attack using SQL injection? Explain in detail with example that how it is performed?	CO5	K5	L3

Knowledge Level (Blooms Taxonomy)					
K1	Remembering (Knowledge)	K2	Understanding (Comprehension)	K3	Applying (Application of Knowledge)
K4	Analysing (Analysis)	K5	Evaluating (Evaluation)	K6	Creating (Synthesis)

General Instructions

(i) For each Question, mention K1 or K2 etc. for Knowledge Level

(ii) For each Question, mention CO1, CO2 etc. for Course Outcomes.

Verify the COs with the Syllabus before framing the Questions.

An Either or type Question should have the same CO in both (a) and (b) parts.

(iii) For each Question, mention any number from 1 to 5 for Difficulty Level

(With 1 as Most Easy & 5 as Most Difficult)

(iv) Mark with * near the Q.No for those Questions which are framed newly and were not included in the QRs of LAST TWO SEMESTERs. Ensure minimum 2 new updations per unit in all Parts.

(v) Allot split up of marks for subdivisions.

(vi) DO NOT Copy and Paste Equations as Images.

All Mathematical Equations should be typed using the appropriate tools.

(vii) Type the Answer Key in the same QR template across the respective Q.Nos and delete the last 3 columns (CO,KL, Diff level) in the Answer Key file....