SRM VALLIAMMAI ENGINEERING COLLEGE
(An Autonomous Institution)

SRM Nagar, Kattankulathur– 603203

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

VII SEMESTER

Regulation–2019

Academic Year 2025–2026(ODD)

Prepared by

Dr. M.MAYURANATHAN, Associate Professor/CSE

Dr.C.PABITHA, Associate Professor/CSE

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur– 603203.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

SUBJECT : 1904711 ETHICAL HACKING

SEM / YEAR: VII / IV

	UNIT I - ETHICAL HACKING OVERVIEW & VULNERABILITIES		
	Understanding the importance of security, Concept of ethical hacking and essential Terminologies Threat, Attack, Vulnerabilities, Target of Evaluation, Exploit. Phases involved in hacking.		
	PART A		
Q.No	**Questions**	**BT Level**	**Competence**
1.	Define Ethical hacking.	BTL1	Remember
2.	List the types of the Vulnerabilities.	BTL1	Remember
3.	Differentiate Threat and Attack.	BTL2	Understand
4.	List out the importance of security.	BTL1	Remember
5.	List out the purpose of hacking.	BTL1	Remember
6.	Give the types of Hacking Technologies.	BTL2	Understand
7.	What is Exploit in hacking?	BTL1	Remember
8.	List out the various groups in hackers.	BTL1	Remember
9.	Name the tasks performed by an ethical hacker.	BTL1	Remember
10.	Define a hacker.	BTL1	Remember
11.	State the use of penetration test process.	BTL2	Understand
12.	List the various aspects of hacking.	BTL1	Remember
13.	Differentiate hacking and ethical hacking.	BTL2	Understand
14.	Give the activities during the phase of the attacks.	BTL2	Understand
15.	Show the importance of white hats in hacking.	BTL2	Understand
16.	Classify the essential Terminologies involved in hacking.	BTL2	Understand
17.	State the role which is played by zombie system.	BTL2	Understand
18.	Show why ethical hacking is allowed? Justify your answer.	BTL2	Understand
19.	Brief about the target of Evaluation strategy.	BTL1	Remember
20.	Show the phases involved in hacking.	BTL1	Remember
21	Discuss types of testing on the system.	BTL2	Understand
22	Discuss the most common entry points for an attack.	BTL2	Understand
23	Classify the tools that a hacker may employ during the scanning phase.	BTL2	Understand
24	Define the Passive and Active Reconnaissance methods.	BTL1	Remember
	PART – B		
1.	(i)Analyze the various types of hacker classes. (7) (ii)Explain in detail about ethical Hacking. (6)	BTL4	Analyze

2.	Discuss in detail the different phases involved in Ethical Hacking.	(13)	BTL3	Apply
3.	(i)Compare and contrast white hats and black hats. (ii)Analyze the skills required for an ethical Hacker.	(7) (6)	BTL4	Analyze
4.	(i)Demonstrate the Purpose of Ethical Hacking. (ii) Demonstrate the role of white hats.	(7) (6)	BTL3	Apply
5.	(i)How do gray hats act under various situations? Justify your Statement. (ii)Identify the use of pen test in hacking.	(7) (6)	BTL4	Analyze
6.	Explain the Ethical Hacking Terminology with suitable examples.	(13)	BTL5	Evaluate
7.	Compare the different hats involved in hacking.	(13)	BTL4	Analyze
8.	(i)Classify the groups involved in hacking. (ii)Examine how the goals attackers try to achieve security breach.	(7) (6)	BTL3	Apply
9.	Discuss the different Ethical Hacking Terminology	(13)	BTL4	Analyze
10.	(i) Examine the characteristics Ethical Hacker's Skill Set. (ii) Describe Sniffing the network.	(7) (6)	BTL5	Evaluate
11.	Explain the different types of hacking technologies in detail.	(13)	BTL4	Analyze
12.	Discuss: (i) Vulnerability research (ii) Hacktivism	(7) (6)	BTL3	Apply
13.	(i)Describe the role of Port scanners. (ii) Identify the role Internet Control Message Protocol (ICMP) scanners.	(7) (6)	BTL5	Evaluate
14.	Summarize the issues involved in ethical hacking.	(13)	BTL5	Evaluate
15.	List the five stages of ethical hacking.	(13)	BTL5	Evaluate
16.	Describe the ways of conducting ethical hacking.	(13)	BTL3	Apply
17.	Interpret the legal implications of hacking	(13)	BTL3	Apply
	PART –C			
1.	Do you agree with the following statement: "White-hat hackers are "good" guys who use their skills for defensive purposes". Support your answer.	(15)	BTL5	Evaluate
2.	Briefly explain how to Be Ethical. Compose a scenario to illustrate Ethical hacking is suitable in that environment.	(15)	BTL4	Analyze
3.	Assess the different categories of hackers. Identify the situations under which hackers from one category would be preferable over the other categories.	(15)	BTL5	Evaluate
4.	Estimate Testing Types used in penetration test in security systems.	(15)	BTL5	Evaluate
5	Analyze the types of Ethical Hacks in an organization's security system also identify most common entry points for an attack.	(15)	BTL4	Analyze
	UNIT II -FOOTPRINTING & PORT SCANNING			
	Foot printing - Introduction to foot printing, Understanding the information gathering methodology of the hackers, Tools used for the reconnaissance phase. Port Scanning - Introduction, using port scanning tools, ping sweeps, Scripting Enumeration-Introduction.			
	PART – A			
1.	Define footprinting	BTL1	Remember	
2.	What is meant by Reconnaissance?	BTL1	Remember	
3.	Express the idea of Competitive intelligence.	BTL2	Understand	
4.	What do you know about NSlookup?	BTL1	Remember	

5.	Predict the countermeasures that can be taken against footprinting?	BTL2		Understand
6.	Differentiate NSlookup and DNSstuff.	BTL2		Understand
7.	Show a plan to create pieces of information to be gathered about a target during footprinting.	BTL2		Understand
8.	Show the ways to gain information that can be used to perform DNS	BTL2		Understand
9.	Define Types of DNS Records	BTL1		Remember
10.	List the seven steps of Information-Gathering Methodology	BTL1		Remember
11.	Give the functions of the EDGAR database	BTL2		Understand
12.	Brief the use of "Whois" for footprinting?	BTL2		Understand
13.	Compare and Contrast Domain name lookup and Whois	BTL2		Understand
14.	Name a solution to Find the Address Range of the Network.	BTL1		Remember
15.	Show why the Who is tool is used?	BTL1		Remember
16.	Point out the features of ARIN database.	BTL2		Understand
17.	Brief the term Computer-based social-engineering attacks.	BTL1		Remember
18.	List the tools used for the reconnaissance phase.	BTL1		Remember
19.	Show the process of DNS enumeration.	BTL2		Understand
20.	Define Phishing Attacks.	BTL1		Remember
21.	Interpret countermeasures can be taken against footprinting.	BTL2		Understand
22.	Discuss are objectives of network scanning?	BTL2		Understand
23.	List the pre-requisites for system hacking. What are the steps for hacking a system?	BTL1		Remember
24.	Brief on the statement "As Security increases system's functions and ease of use decreases for users".	BTL2		Understand
PART-B				
1.	Examine why do attacker need footprinting? What are the objectives of footprinting?	(13)	BTL3	Apply
2.	Give the comparison of various common tools used for footprinting and information gathering.	(13)	BTL5	Evaluate
3.	Describe the following terms in detail: (i) Active information gathering. (ii) Pseudonymous footprinting (iii) Internet footprinting	 (5) (4) (4)	BTL4	Analyze
4.	Explain what are the countermeasures against identity theft?	(13)	BTL4	Analyze
5.	Demonstrate the principle of Information-Gathering Methodology.	(13)	BTL3	Apply
6.	Summarize the pieces of information to be gathered about a target during footprinting.	(13)	BTL5	Evaluate
7.	With a scenario, explain Human-Based Social Engineering.	(13)	BTL4	Analyze
8.	Examine the risks of social networking. What type of behaviours can be vulnerable to social engineering attacks?	(13)	BTL5	Evaluate
9.	Explain what is vulnerability scanning? What can it be detected?	(13)	BTL4	Analyze
10.	i) Summarize Port-Scan measures. ii) What are the counter measures against the port scanning?	(7) (6)	BTL3	Apply
11.	Summarize the Tools used for the reconnaissance phase.	(13)	BTL3	Apply
12.	Explain the scanning methodology in detail.	(13)	BTL5	Evaluate

13.	Identify the countermeasures against SMTP, LDAP and SMB enumeration. Explain	(13)	BTL5	Evaluate
14.	Analyze the common social engineering targets and defence strategies.	(13)	BTL4	Analyze
15.	State how the footprinting is done through social engineering? Explain.	(13)	BTL3	Apply
16.	Demonstrate the footprinting tools used in hacking.	(13)	BTL3	Apply
17.	Analyze why is banner grabbing used? What are its types? Explain.	(13)	BTL4	Analyze
	PART-C			
1.	Evaluate the reasons for insider attacks? How can these attacks be prevented?	(15)	BTL5	Evaluate
2.	Analyze the solutions to stop your website getting hacked.	(15)	BTL4	Analyze
3.	Assess the counter measures against banner grabbing?	(15)	BTL5	Evaluate
4.	A hacker broke into the database of Zomato, India's largest online restaurant guide, and accessed five vital details – names, emails, numeric user IDs, user names and password hashes – of around 17 million users. Estimate its impact and bring out its vulnerabilities which can be overcomed by ethical hacking.	(15)	BTL5	Evaluate
5	Explain the CEH scanning methodology.	(15)	BTL5	Evaluate
	UNIT III - SYSTEM HACKING			
	Aspect of remote password guessing, Role of eavesdropping ,Various methods of password cracking, Keystroke Loggers, Understanding Sniffers ,Comprehending Active and Passive Sniffing, ARP Spoofing and Redirection.			
	PART – A			
1.	Define Offline Attacks.	BTL1	Remember	
2.	Tabulate the services of Shoulder surfing	BTL1	Remember	
3.	Show the importance of Keyloggers and Other Spyware Technologies.	BTL1	Remember	
4.	What ways to crack passwords?	BTL1	Remember	
5.	Define the threats due to packet sniffing.	BTL1	Remember	
6.	What is packet sniffing? How is it done? What are the threats due to packet sniffing?	BTL1	Remember	
7.	Summarize sniffers work.	BTL2	Understand	
8.	Identify different types of sniffing attacks.	BTL2	Understand	
9.	Show the two types of sniffing. What protocols are vulnerable to sniffing.	BTL1	Remember	
10.	Discuss about Norton Internet Security	BTL2	Understand	
11.	Give the limitations of the automatic password cracking algorithm.	BTL2	Understand	
12.	Show the purpose of Rainbow attack? How is it carried out?	BTL1	Remember	
13.	List the elements of password-cracking tools.	BTL1	Remember	
14.	Classify the different types of password attacks.	BTL2	Understand	
15.	Show the different ways to develop anonymity.	BTL2	Understand	
16.	Differentiate ImageHide and blindside Steganography Technologies	BTL2	Understand	
17.	Show the differences between phishing and spoofing.	BTL2	Understand	

VALLIAMMAI ENGINEERING COLLEGE SRM

18.	List the features of how we can defend against password cracking.	BTL1		Remember
19.	Show the suggestions of Defending Against Password Guessing	BTL1		Remember
20.	Define Escalating Privileges	BTL1		Remember
21	Classify the steganography techniques.	BTL2		Understand
22	Define the Active Online Attacks.	BTL1		Remember
23	Define Automated Password Guessing.	BTL1		Remember
24	How hash passwords stored in Microsoft security accounts manager?	BTL2		Understand
	PART – B			
1.	Explain the steps involved in cracking a Password?	(13)	BTL5	Evaluate
2.	Describe the in detail various password-cracking tools.	(13)	BTL4	Analyze
3.	Illustrate the different types of sniffing attacks.	(13)	BTL3	Apply
4.	(i) Demonstrate elements of password cracking tools. (ii) Demonstrate briefly about types of passwords	(7) (6)	BTL3	Apply
5.	Develop a solution to store hash passwords in Microsoft security accounts manager. Explain Microsoft authentication mechanism?	(13)	BTL4	Analyze
6.	Describe the classification of steganography.	(13)	BTL4	Analyze
7.	Classify briefly about the various categories of online attacks.	(13)	BTL4	Analyze
8.	(i) Discuss in detail Spector hacking tool. (ii)Interpret the functions of SpyAnywhere.	(7) (6)	BTL5	Evaluate
9.	Describe the NetBIOS DoS Attacks with suitable example.	(13)	BTL3	Apply
10.	Summarize the characteristics of SMB Relay MITM Attacks and Countermeasures.	(13)	BTL3	Apply
11.	(i)Explain the ImageHide Steganography Technologies. (ii)Explain the Blindside Steganography Technologies.	(7) (6)	BTL1	Remember
12.	Summarize the Shoulder surfing technique with a suitable real time scenario.	(13)	BTL5	Evaluate
13.	Know how evidence of hacking activity is eliminated by attackers? Justify your answer.	(13)	BTL4	Analyze
14.	Explain the similarities and dissimilarities between the types of non-electronic attacks.	(13)	BTL4	Analyze
15	What is sniffing? Summarize its types in Ethical Hacking.	(13)	BTL3	Apply
16	Interpret NTFS File Streaming. Also mention the countermeasures.	(13)	BTL3	Apply
17	Assess how to Cover Tracks and Erase Evidence.	(13)	BTL5	Evaluate
	PART-C			
1.	Give an overview of the working of password cracking pen testing. Briefly Evaluate the distinguishing features of the same.	(15)	BTL5	Evaluate
2.	Prepare a list of important functional differences and similarities between steganography techniques.	(15)	BTL4	Analyze
3.	What do you understand by rootkits? Mention a few characteristic feature of this. Assess its objectives? How does an attacker place rootkit? What are the different types of rootkits?	(15)	BTL5	Evaluate

4.	Estimate the reasons as to why a spyware is used? How can it be propagated? What are different types of spywares?	(15)	BTL5	Evaluate
5	What is privilege escalation? What are its types? Develop a solution so that system be protected against privilege escalation.	(15)	BTL4	Analyze
UNIT IV - HACKING WEB SERVICES & SESSION HIJACKING				
	Web application vulnerabilities, application coding errors, SQL injection into Backend Databases, cross-site scripting, cross-site request forging, authentication bypass, web services and related flaws, protective http headers Understanding Session Hijacking, Phases involved in Session Hijacking, Types of Session Hijacking.			
PART – A				
1.	Define SQL injection.	BTL1	Remember	
2.	Show the vulnerabilities of Web application.	BTL1	Remember	
3.	Summarize the characteristics of Session Hijacking.	BTL1	Remember	
4.	List the requirement for session fixation.	BTL1	Remember	
5.	What is cross-site scripting?	BTL1	Remember	
6.	List the Types of Session Hijacking.	BTL1	Remember	
7.	Brief a solution for the identification of cross-site request forging.	BTL1	Remember	
8.	Give a comparison between cross-site scripting, cross-site request forging.	BTL2	Understand	
9.	Discuss about the term ‘spoofing’.	BTL2	Understand	
10.	Express what is cookie poisoning? How does it work?	BTL2	Understand	
11.	Differentiate patches and hotfixes.	BTL2	Understand	
12.	List the characteristics of LDAP injection.	BTL1	Remember	
13.	Differentiate HTTP response splitting and web cache poisoning.	BTL2	Understand	
14.	List the steps in the operation of signature evasion techniques.	BTL1	Remember	
15.	Drae a schematic model of parameter tampering attack. .	BTL2	Understand	
16.	Interpret the impact of webserver attacks.	BTL2	Understand	
17.	Tabulate the different threats to web applications.	BTL1	Remember	
18.	Identify the issues that are addressed by web attack vectors.	BTL1	Remember	
19.	Interpret the concept of simple and union SQL injection attacks.	BTL2	Understand	
20.	Show the strategies of injection flaws that be deployed in a web applications.	BTL2	Understand	
21	Classify the Man-in-the-middle and man-in-the-browser attacks.	BTL2	Understand	
22	Demonstrate database, table and column be enumerated using SQL injection?	BTL2	Understand	
23	Examine how invalidated redirects and forwards make web applications vulnerable?	BTL2	Understand	
24	Show the effects of webserver misconfiguration.	BTL2	Understand	
PART – B				
1.	(i)Discuss the characteristics of cross site scripting attacks. (ii)Summarize the cross site request forgery attack.	(7) (6)	BTL4	Analyze
2.	(i)Illustrate in brute force be used for session hijacking detail. (ii)Show the working of referrer attack.	(7) (6)	BTL3	Apply
3.	Demonstrate how session hijacking is successfully carried out.	(13)	BTL3	Apply

4.	(i)Integrate the problems caused by web services foot printing attack and web service XML poisoning. (ii)How are these problems addressed?	(7) (6)	BTL3	Apply
5.	Analyze the network level and application level session hijacking.	(13)	BTL4	Analyze
6.	Describe session hijacking? What are the steps to hijack a session? What are the dangers posed by hijacking a session?	(13)	BTL4	Analyze
7.	State the sophisticated matches, hex encoding and manipulating white spaces evasion techniques.	(13)	BTL3	Apply
8.	Describe the design issues of TCP/IP hijacking? How is it performed?	(13)	BTL5	Evaluate
9.	(i)Explain Session fixation. (ii)Point out the techniques used for session fixation.	(7) (6)	BTL5	Evaluate
10.	Write short notes on: (i) Threats to web applications (ii) Web attack vectors	 (7) (6)	BTL4	Analyze
11.	Explain the major types of security attacks that are possible in a computer system.	(13)	BTL5	Evaluate
12.	(i)Express the counter measures against session hijacking. (ii)How it is addressed in real world.	(7) (6)	BTL5	Evaluate
13.	Classify the different categories of hijacking.	(13)	BTL4	Analyze
14.	Point out the factors that make the SQL injection attacks with examples. a) Code analysis b) Attack Analysis c) Updating a table d) Adding new records e) Identifying table name f) Deleting the table	 (3) (2) (2) (2) (2) (2)	BTL4	Analyze
15.	Discuss cross site scripting attack. How is it done?	(13)	BTL3	Apply
16.	Demonstrate the web application vulnerability stack.	(13)	BTL3	Apply
17.	With respect to web applications, Assess the injection flaws? What are its different types? Explain.	(13)	BTL5	Evaluate
PART-C				
1.	How does insufficient transport layer security and improper error handling make web applications vulnerable? Explain.	(15)	BTL4	Analyze
2.	What do you mean by website defacement? Assess why are webservers compromised? What are the consequences of webserver compromisation?	(15)	BTL5	Evaluate
3.	Justify how can SQL injection be used for the following: a) Transfer database to attacker's machine. b) Interact with the operating system. c) Interact with the file system. d) Network reconnaissance.	(15)	BTL4	Analyze
4.	With respect to web applications, what are injection flaws? What are its different types? Evaluate.	(15)	BTL5	Evaluate
5.	Estimate the different types of attacks on authentication mechanisms of web applications?	(15)	BTL5	Evaluate
UNIT V HACKING WIRELESS NETWORKS				

	Introduction to 802.11, Role of WEP, Cracking WEP Keys, Sniffing Traffic, Wireless DOS attacks, WLAN Scanners, WLAN Sniffers, Hacking Tools, Securing Wireless Networks.		
1.	What is service set identifier?	BTL1	Remember
2.	Give the features of Evil Twin attack.	BTL2	Understand
3.	Differentiate MAC spoofing attack and De-authentication and disassociation.	BTL2	Understand
4.	Show the HoneySpot Access point.	BTL1	Remember
5.	Explain Wi-Fi chalking.	BTL1	Remember
6.	List the different ways of footprinting wireless networks.	BTL1	Remember
7.	What is WEP encryption?	BTL1	Remember
8.	Show the process of bluejack a victim.	BTL2	Understand
9.	Express WPA.	BTL2	Understand
10.	Define WPA2.	BTL1	Remember
11.	Show what is GPS mapping? How does and attacker use it?	BTL1	Remember
12.	List the different attacks of Aircrack-ng suite.	BTL1	Remember
13.	Point out the drawbacks of Jamming signal attack	BTL2	Understand
14.	Show the features of temporal keys.	BTL2	Understand
15.	Describe the different authentication modes of Wi-Fi.	BTL2	Understand
16.	Develop rogue access point attack.	BTL2	Understand
17.	Describe the features of countermeasures against Bluetooth hacking.	BTL2	Understand
18.	Differentiate WEP, WPA and WPA2.	BTL2	Understand
19.	List the issues with WEP.	BTL1	Remember
20.	Enumerate the reasons that make initialization vectors weak.	BTL1	Remember
21	Discuss how WEP encryption be broken.	BTL2	Understand
22	Interpret how we can defend against WPS cracking.	BTL1	Remember
23	Distinguish wireless access control threats.	BTL2	Understand
24	Assess how integrity attacks be launched on wireless networks.	BTL2	Understand

PART – B

1.	Explain the 802.1X authentication process.	(13)	BTL5	Evaluate
2.	i) Discuss the ideas of Rogue Access Points. ii) Give the mechanisms of detection Rogue Access Points.	(7) (6)	BTL4	Analyze
3.	Compare and contrast the various Wi-Fi security.	(13)	BTL4	Analyze
4.	Evaluate the various features of Evil Twin or AP Masquerading.	(13)	BTL5	Evaluate
5.	Explain the Wireless Hacking Techniques with suitable illustration.	(13)	BTL3	Apply
6.	Illustrate following attacks on wireless networks: a) Client Mis-association. b) Mis-configured access point	 (7) (6)	BTL3	Apply
7.	i)Illustrate the impact of Wireless DOS attacks . ii)Examine the possible reasons to rapidly counter the Wireless DOS attacks	(7) (6)	BTL3	Apply
8.	Write detailed notes on Securing Home Wireless Networks.	(13)	BTL3	Apply

9.	(i)What do you understand by availability attacks that can be launched on wireless networks? (ii)Identify the situation of availability attacks and how it can be prevented?	(7) (6)	BTL4	Analyze
10.	Generalize the ideas of different confidentiality attacks that can be launched on wireless networks? What are the. What are the different authentication attacks that can be launched on wireless networks? Explain	(13)	BTL4	Analyze
11.	(i)Identify the properties of Honey-Spot Access point. (ii) Describe about Access point MAC spoofing.	(7) (6)	BTL3	Apply
12.	Describe the Wireless DOS attacks and security issues.	(13)	BTL3	Apply
13.	(i) Analyze how the WLAN Sniffers work. (ii) What do you understand by the Sniffing Traffic?	(7) (6)	BTL4	Analyze
14.	Explain the different wireless security layers.	(13)	BTL4	Analyze
15.	Identify the different confidentiality attacks that can be launched on wireless networks? Explain.	(13)	BTL5	Evaluate
16.	Interpret the wireless intrusion prevention systems. How are they deployed?	(13)	BTL3	Apply
17.	Summarize WEP encryption. What are its goals? What are flaws in WEP encryption?	(13)	BTL5	Evaluate
	PART-C			
1.	Assess the special features that ethical hacking tools should possess. Take any tool as example and explain the features of the ethical hacking.	(15)	BTL5	Evaluate
2.	Estimate the principle functions of sniffing tools and explain with an example implemented on wireless networks and the specific service that it make use of it.	(15)	BTL5	Evaluate
3.	What do you understand by wireless hacking? Summarize the different wireless hacking methodology that are available.	(15)	BTL5	Evaluate
4.	Analyze all possible attacks on wireless networks. Explain integrity attacks be launched on wireless networks in which is useful?	(15)	BTL4	Analyze
5.	Analyze how the following attacks be launched using Aircrack-ng suite. a) Revealing hidden SSID b) Fragmentation attack c) MAC spoofing attack d) De-authentication and disassociation e) Man in the middle attack	 (3) (3) (3) (3) (3)	BTL4	Analyze