PANIMALAR ENGINEERING COLLEGE
(An Autonomous Institution, Affiliated to Anna University Chennai)

QUESTION BANK

Details of the Course

Name of the Department	**: COMPUTER SCIENCE AND ENGINEERING**
Name of the Course	**: ETHICAL HACKING**
Course Code	**: 23IT1909**
Semester	**: V**
Common To Programme(s)	**: DEPARTMENT OF INFORMATION TECHNOLOGY**

Instructions

Blooms Level: Blooms Level 1 & 2 is Lower Order (LO) Cognitive type, Blooms Level 3 & 4 is Intermediate Order Cognitive Type (IO) and Blooms Level 5 & 6 is Higher Order (HO) cognitive type.

2 Marks: For **each unit five questions should be of lower order (LO)** cognitive type and **five Questions should be of Intermediate order (IO)** cognitive type.

13 /15 /16 Marks: For each Unit **four questions should be of lower order (LO) cognitive type** i.e. remembrance type questions, **five should be of intermediate order** (IO) cognitive type i.e. understanding type questions and **One Question should be on Higher Order (HO)** Application / Design / Analysis / Evaluation / Creativity / Case study questions.

* HO Order is not applicable if the Question Pattern does not have Part C. In Such cases consider HO as IO.

** If the Mark for Part B &C is less than the maximum mark of the Question, Sub Divisions shall be added.

Course Outcome: (List the Course Outcomes of the Course)

CO1: To express knowledge on basics of computer based vulnerabilities

CO2: To gain understanding on different foot printing, reconnaissance and scanning methods

CO3: To demonstrate the enumeration and vulnerability analysis methods

CO4: To gain knowledge on hacking options available in Web and wireless applications

CO5: To acquire knowledge on the options for network protection.

CO6: To use tools to perform ethical hacking to expose the vulnerabilities

Bloom's Level: **BL1** - Remembering, **BL2** - Understanding, **BL3** - Applying, **BL4** - Analyzing, **BL5**– Evaluating,**BL6** - Creating.

Diagrams, Table Values, Equations must be legible and clear.

UNIT- I - INTRODUCTION

	PART A (2 Marks)	Bloom's Level	Course Outcome	Marks Allotted
1.	Define Hacker.	[BL1]	[CO1]	[2]
2.	Discuss Penetration testing.	[BL2]	[CO1]	[2]
3.	What is ethical hacking?	[BL1]	[CO1]	[2]
4.	Compare hacking and ethical hacking.	[BL4]	[CO1]	[2]
5.	What are the different penetration technology methodologies?	[BL1]	[CO1]	[2]
6.	Simulate a basic malware attack scenario and explain how it could affect a computer system.	[BL3]	[CO1]	[2]
7.	Illustrate intrusion attack.	[BL3]	[CO1]	[2]
8.	What do you mean by IP addressing?	[BL1]	[CO1]	[2]
9.	Compare TCP and IP protocols.	[BL4]	[CO1]	[2]

10.	Differentiate network and computer attack.	[BL4]	[CO1]	[2]
Descriptive Questions (13 /15/16 Marks)				
1.	Classify the different methodologies of penetration testing.	[BL4]	[CO1]	[13]
2.	Explain ethical hacking and what an ethical hacker can do legally.	[BL3]	[CO1]	[13]
3.	Give an overview about TCP / IP protocol.	[BL2]	[CO1]	[13]
4.	Explain the role of security and penetration testers.	[BL2]	[CO1]	[13]
5.	Define malware and intruder attacks and explain how to protect against it.	[BL1]	[CO1]	[13]
6.	State and explain application layer and its protocols.	[BL2]	[CO1]	[13]
7.	Determine the role of network layer routing and its various types in network security.	[BL3]	[CO1]	[13]
8.	(i) Explain the process of subnetting.	[BL3]	[CO1]	[6]
	(ii) If the IP Address is 172.16.0.0/25, then find the number of subnets and the number of hosts per subnet. Also, for the first subnet block, find the subnet address, first host ID, last host ID, and broadcast address.	[BL3]	[CO1]	[7]
9.	Perform the key strategies and technologies a company should employ to safeguard its systems against malware attacks and minimize Potential damage.	[BL3]	[CO1]	[13]
10.	A company is concerned about the physical security of its data centers, which house critical digital assets. Identify key physical security measures that should be implemented to safeguard these assets from unauthorized access and environmental threats. Additionally, discuss how these measures can be integrated into a comprehensive security strategy and recommend further steps to enhance overall protection.	[BL 6]	[CO1]	[15]

Course Instructor
Name & Designation

Course Coordinator
Name & Designation

Head of the Department

UNIT- II - FOOT PRINTING, RECONNAISSANCE AND SCANNING NETWORKS				
	PART A (2 Marks)	**Bloom's Level**	**Course Outcome**	**Marks Allotted**
1.	What is footprinting? List out its types.	[BL1]	[CO2]	[2]
2.	Explain footprinting through search engines.	[BL2]	[CO2]	[2]
3.	How footprinting is done using social networking site?	[BL1]	[CO2]	[2]
4.	Describe Competitive Intelligence.	[BL2]	[CO2]	[2]
5.	Explain how social engineering aids in the process of footprinting.	[BL3]	[CO2]	[2]
6.	Explain website footprinting.	[BL2]	[CO2]	[2]
7.	Compare any three footprinting tools.	[BL4]	[CO2]	[2]
8.	Explain the concept of network scanning.	[BL2]	[CO2]	[2]
9.	Describe port scanning.	[BL2]	[CO2]	[2]
10.	Compare Scanning Beyond IDS and Firewall.	[BL4]	[CO2]	[2]
Descriptive Questions (13 /15/16 Marks)				
1.	Explain the concepts of footprinting.	[BL2]	[CO2]	[13]
2.	Discuss in detail about footprinting through web services.	[BL2]	[CO2]	[13]
3.	Explain footprinting through Social engineering.	[BL2]	[CO2]	[13]
4.	Give a brief description about the different tools used for port scanning.	[BL4]	[CO2]	[13]
5.	Analyze the methods used for footprinting through websites and emails. Discuss how these techniques can be leveraged to gather information about targets and evaluate the associated risks and mitigation strategies.	[BL4]	[CO2]	[13]
6.	Analyze the effectiveness of various network scanning tools. Discuss their strengths and limitations in the network security assessments.	[BL4]	[CO2]	[13]
7.	Discuss different techniques for detecting IP spoofing attacks	[BL4]	[CO2]	[13]
8.	Define an Intrusion Detection System (IDS) and provide a brief overview of its different types. Discuss how each type functions and its role in detecting and responding to security threats.	[BL1]	[CO2]	[13]
9.	Demonstrate various scanning techniques used in network security assessments, including port scanning, vulnerability scanning, and service enumeration. Discuss their roles in identifying potential security weaknesses, and analyze the advantages and limitations of each technique in ensuring a comprehensive security evaluation.	[BL3]	[CO2]	[13]

Course Instructor Name & Designation	Course Coordinator Name & Designation	Head of the Department

10.	Construct the recent security assessment, a company discovered unauthorized access attempts targeting its internal network. The security team suspects that attackers are leveraging publicly available information to identify vulnerabilities. Describe the footprinting techniques that the attackers might use to gather information about the company's network infrastructure and enumerate the potential risks associated with this process. How should the company enhance its security posture to mitigate these risks?	[BL5]	[CO2]	[15]

Course Instructor
Name & Designation

Course Coordinator
Name & Designation

Head of the Department

UNIT- III - ENUMERATION AND VULNERABILITY ANALYSIS				
	PART A (2 Marks)	Bloom's Level	Course Outcome	Marks Allotted
1.	Define enumeration.	[BL1]	[CO3]	[2]
2.	Describe SNMP protocol.	[BL2]	[CO3]	[2]
3.	Write short notes on vulnerability assessment.	[BL1]	[CO3]	[2]
4.	Name some tools for identifying vulnerabilities in Windows.	[BL1]	[CO3]	[2]
5.	Describe Linux OS vulnerability.	[BL2]	[CO3]	[2]
6.	Illustrate the vulnerabilities of embedded OS.	[BL4]	[CO3]	[2]
7.	How would you use Burp Suite to inject a reflected XSS payload and confirm its execution on a target web page?	[BL3]	[CO3]	[2]
8.	Demonstrate how you would configure an NTP client in client–server mode to synchronize its clock with an NTP server.	[BL4]	[CO3]	[2]
9.	Analyze the role of the MAIL FROM and RCPT TO commands in the SMTP protocol.	[BL4]	[CO3]	[2]
10.	Demonstrate how you would perform DNS enumeration on a target domain using a tool like *nslookup* or *dnsenum*.	[BL3]	[CO3]	[2]
	Descriptive Questions (13 /15/16 Marks)			
1.	Explain NetBIOS Enumeration.	[BL2]	[CO3]	[13]
2.	Write short notes on Windows OS Vulnerabilities.	[BL1]	[CO3]	[13]
3.	Explain Vulnerability Assessment Concepts.	[BL2]	[CO3]	[13]
4.	Compare Tools for Identifying Vulnerabilities in Windows- Linux OS Vulnerabilities.	[BL4]	[CO3]	[13]
5.	Demonstrate Vulnerabilities of Embedded OS.	[BL3]	[CO3]	[13]
6.	Explain in detail on Linux OS vulnerabilities and the tools to identity the same.	[BL1]	[CO3]	[13]
7.	Illustrate the processes of SNMP and SMTP enumeration. Discuss the methods used for gathering information through these protocols, the types of data that can be obtained, and their implications for network security assessments. Include examples of tools or techniques employed in each type of enumeration.	[BL3]	[CO3]	[13]
8.	Distinguish the process and significance of DNS enumeration in network security assessments. Explain the techniques used for DNS enumeration, their effectiveness in identifying potential vulnerabilities, and the implications for both attackers and defenders. Provide examples of common tools used for DNS enumeration and their role in a comprehensive security evaluation.	[BL4]	[CO3]	[13]

Course Instructor Name & Designation	Course Coordinator Name & Designation	Head of the Department

9.	Illustrate the significance of LDAP (Lightweight Directory Access Protocol) and NTP (Network Time Protocol) enumeration in network security assessments. Discuss the methods and tools used for enumerating LDAP and NTP services, and explain how such enumerations can reveal critical information about an organization's network infrastructure.	[BL3]	[CO3]	[13]
10.	Create a vulnerability assessment plan for a small office network. Your plan should include how you will gather system information using NetBIOS, SNMP, and DNS, what tools you will use to find security issues in Windows and Linux systems, and how you will check for problems in embedded devices. Explain why you chose these methods and tools.	[BL6]	[CO6]	[15]

Course Instructor Name & Designation	Course Coordinator Name & Designation	Head of the Department

UNIT- IV - SYSTEM HACKING				
	PART A (2 Marks)	**Bloom's Level**	**Course Outcome**	**Marks Allotted**
1.	Define web servers?	[BL1]	[CO4]	[2]
2.	What are the hacking methodologies?	[BL1]	[CO4]	[2]
3.	List the types of web server hacking.	[BL1]	[CO4]	[2]
4.	Describe web application components.	[BL2]	[CO4]	[2]
5.	What is vulnerability?	[BL1]	[CO4]	[2]
6.	Demonstrate wireless networks hacking.	[BL3]	[CO4]	[2]
7.	How would you identify a wireless access point using a network scanning tool?	[BL3]	[CO4]	[2]
8.	Analyze how wardriving reveals vulnerabilities in wireless networks compared to other reconnaissance methods.	[BL4]	[CO4]	[2]
9.	How would you use a tool like Aircrack-ng to capture and crack a WPA2 handshake on a wireless network?	[BL4]	[CO4]	[2]
10.	Explain “Tools of the Trade”	[BL2]	[CO4]	[2]
	Descriptive Questions (13 /15/16 Marks)			
1.	Outline on web servers hacking.	[BL1]	[CO4]	[13]
2.	Classify the tools used for web attackers and security testers.	[BL2]	[CO4]	[13]
3.	Describe on wireless networks.	[BL2]	[CO4]	[13]
4.	Explain the components of wireless networks.	[BL2]	[CO4]	[13]
5.	Analyzing in detail about wardriving.	[BL4]	[CO4]	[13]
6.	Illutrate the various techniques used in wireless hacking and analyze their potential impacts on network security.	[BL3]	[CO4]	[13]
7.	Perform the significance of hacking tools in ethical hacking.	[BL3]	[CO4]	[13]
8.	Simplify the core security problem faced by web applications when processing untrusted data.	[BL4]	[CO4]	[13]
9.	Predict the impact of the vulnerabilities on web security.	[BL3]	[CO4]	[13]
10.	UrbanTech Inc., a technology firm with multiple new office locations, conducted a war driving assessment to evaluate the security of their wireless network infrastructure. The assessment aimed to identify unauthorized or insecure wireless networks, analyze network configurations, and improve overall security. Using equipment such as a GPS-enabled laptop, high-gain antenna, and wardriving software, the IT team mapped and assessed networks in the vicinity. Discuss the	[BL6]	[CO4]	[15]

	methodology, findings, and recommendations of this wardriving assessment, and evaluate how it contributed to strengthening UrbanTech Inc.'s wireless network security.			

Course Instructor
Name & Designation

Course Coordinator
Name & Designation

Head of the Department

UNIT- V - NETWORK PROTECTION SYSTEMS

PART A (2 Marks)		Bloom’s Level	Course Outcome	Marks Allotted
1.	What are Access control lists?	[BL1]	[CO5]	[2]
2.	Write short notes on CISCO Adaptive security appliance firewall.	[BL1]	[CO5]	[2]
3.	Describe intrusion detection.	[BL2]	[CO5]	[2]
4.	Discuss Intrusion Prevention System.	[BL2]	[CO5]	[2]
5.	What is web filtering?	[BL1]	[CO5]	[2]
6.	Contrast on security incident response team.	[BL4]	[CO5]	[2]
7.	Demonstrate on honey pot.	[BL3]	[CO5]	[2]
8.	Differentiate between firewall and IDS.	[BL4]	[CO5]	[2]
9.	Compare between HIDS and NIDS.	[BL4]	[CO5]	[2]
10.	Illustrate any three advantages and disadvantages of web filtering	[BL3]	[CO5]	[2]
Descriptive Questions (13 /15/16 Marks)				
1.	Write a brief note on Cisco adaptive security appliance firewall.	[BL1]	[CO5]	[13]
2.	List the configuration and risk analysis tools for firewalls and routers.	[BL1]	[CO6]	[13]
3.	Explain intrusion detection and prevention systems.	[BL2]	[CO5]	[13]
4.	Explain web filtering in detail.	[BL2]	[CO5]	[13]
5.	Explain the concept of honeypots briefly.	[BL3]	[CO5]	[13]
6.	Discuss the role and functionality of a Host-Based Intrusion Detection System (HIDS) in network security.	[BL4]	[CO5]	[13]
7.	Illustrate the key guidelines for configuring a firewall and establishing an effective firewall policy in a network.	[BL4]	[CO5]	[13]
8.	Classify the role and responsibilities of a Security Incident Response Team (SIRT) within an organization. Discuss the key steps involved in the incident response process and how a SIRT can effectively mitigate the impact of a security breach.	[BL4]	[CO5]	[13]
9.	Illustrate the various configuration and risk analysis tools available for firewalls and routers. Explain how these tools contribute to the overall security of a network, and highlight the potential risks associated with improper configuration.	[BL4]	[CO6]	[13]

Course Instructor
Name & Designation

Course Coordinator
Name & Designation

Head of the Department

10.	Design a comprehensive strategy for MegaTech Corporation as they discover that their network has been targeted by multiple unauthorized access attempts. Although these attempts have been unsuccessful, the security team is concerned that a more determined attacker might eventually breach the network. What steps can MegaTech take to attract and monitor hackers without compromising their internal systems? Discuss the advantages and disadvantages of this approach, and highlight any legal considerations involved.	[BL6]	[CO6]	[15]

Course Instructor Name & Designation	Course Coordinator Name & Designation	Head of the Department