Course Code: 23CS1018 **R23**

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR
(AUTONOMOUS)
Siddharth Nagar, Narayanavanam Road – 517583

QUESTION BANK (DESCRIPTIVE)

Subject with Code: Ethical Hacking (23CS1018) **Regulation:** R23

Course & Branch: B.Tech – CIC **Year & Sem:** IV Year & I

UNIT-I
ETHICAL HACKING OVERVIEW

1	**a)**	What is Ethical Hacking?	**[L1] [CO1]**	**[2M]**
	b)	List out the different types of hackers?	**[L1] [CO1]**	**[2M]**
	c)	Give examples of malicious software.	**[L2] [CO1]**	**[2M]**
	d)	How can malware attacks be prevented?	**[L1] [CO1]**	**[2M]**
	e)	What is phishing?	**[L1] [CO1]**	**[2M]**
2	**a)**	Explain in detail about ethical Hacking	**[L4] [CO1]**	**[5M]**
	b)	Analyze the various types of hacker classes.	**[L4] [CO1]**	**[5M]**
3		Explain the Ethical Hacking Terminology with suitable examples.	**[L1] [CO1]**	**[10M]**
4		Summarize the issues involved in ethical hacking.	**[L5] [CO1]**	**[10M]**
5	**a)**	Explain methods for protecting systems from malware attacks.	**[L2] [CO1]**	**[5M]**
	b)	Explain the importance of physical security and its measures.	**[L3] [CO1]**	**[5M]**
6		Differentiate between hats involved in hacking.	**[L2] [CO1]**	**[10M]**
7	**a)**	How do gray hats act under various situations? Justify your Statement.	**[L1] [CO1]**	**[5M]**
	b)	Identify the use of pen test in hacking.	**[L1] [CO1]**	**[5M]**
8		Explain Attack Types and Attack Vectors in detail.	**[L4] [CO1]**	**[10M]**
9	**a)**	Evaluate the effectiveness of various intruder attack methods against modern security systems	**[L4] [CO1]**	**[5M]**
	b)	Analyze the role of physical security in preventing threats to organizational assets.	**[L4] [CO1]**	**[5M]**
10		Explain Threat Categories and their impact on information systems.	**[L3] [CO1]**	**[10M]**

Course Code: 23CS1018 **R23**

UNIT II
RECONNAISSANCE AND SCANNING

1	**a)**	What is Footprinting?	**[L1][CO2]**	**[2M]**
	b)	Define Port Scanning.	**[L1][CO2]**	**[2M]**
	c)	List the types of Reconnaissance.	**[L1][CO2]**	**[2M]**
	d)	How does a ping sweep help network scanning?	**[L2][CO2]**	**[2M]**
	e)	Name any two port scanning tools.	**[L2][CO2]**	**[2M]**
2	**a)**	Explain Footprinting and its significance in ethical hacking.	**[L2][CO2]**	**[5M]**
	b)	Differentiate between Passive and Active Reconnaissance.	**[L2][CO2]**	**[5M]**
3		Analyze how social engineering and technical scanning complement each other during penetration testing.	**[L4][CO2]**	**[10M]**
4	**a)**	What is a Ping Sweep? Explain its working.	**[L2][CO2]**	**[5M]**
	b)	Compare TCP and UDP port scanning.	**[L2][CO2]**	**[5M]**
5		Compare different port scanning techniques such as SYN, FIN, NULL, XMAS, and UDP scans.	**[L4][CO2]**	**[10M]**
6	**a)**	Explain DNS Zone Transfer with an example.	**[L2][CO2]**	**[5M]**
	b)	Define Reconnaissance. Explain its objectives in cybersecurity.	**[L2][CO2]**	**[5M]**
7		Discuss DNS Enumeration and DNS Zone Transfers. Explain their advantages and security implications.	**[L4][CO2]**	**[10M]**
8		Explain Social Engineering attacks with suitable examples and preventive measures.	**[L3][CO2]**	**[10M]**
9	**a)**	Analyze the security risks associated with DNS Zone Transfers?	**[L4][CO2]**	**[5M]**
	b)	Write short notes on Nmap, Netcat, or Angry IP Scanner.	**[L2][CO2]**	**[5M]**
10		Explain web-based reconnaissance tools and their role in information gathering.	**[L3][CO2]**	**[10M]**

Course Code: 23CS1018 **R23**

UNIT 3
ENUMERATION

1	**a)**	Define Enumeration.	**[L1][CO3]**	**[2M]**
	b)	Define vulnerability assessment.	**[L1][CO3]**	**[2M]**
	c)	What is OS Hardening?	**[L1][CO3]**	**[2M]**
	d)	What is Unix/Linux Enumeration?	**[L1][CO3]**	**[2M]**
	e)	What is a NetBIOS Null Session?	**[L1][CO3]**	**[2M]**
2		Explain Enumeration in detail. Discuss its techniques, tools, and objectives.	**[L2][CO3]**	**[10M]**
3		Describe the complete Enumeration process used during penetration testing.	**[L3][CO3]**	**[10M]**
4		Discuss NetBIOS Null Sessions and explain how they can expose system information.	**[L4][CO3]**	**[5M]**
5		Compare Windows and Linux Operating System vulnerabilities.	**[L4][CO3]**	**[10M]**
6	**a)**	Discuss methods for hardening Windows Operating Systems.	**[L3][CO3]**	**[5M]**
	b)	Explain SMB and its role in Enumeration.	**[L6][CO1]**	**[5M]**
7		Evaluate various techniques used to secure network infrastructure from enumeration attacks.	**[L5][CO3]**	**[5M]**
8	**a)**	Define Linux OS vulnerabilities and explain any four common Linux security vulnerabilities with suitable examples.	**[L2][CO3]**	**[5M]**
	b)	Evaluate different mitigation techniques for Linux OS and network vulnerabilities and justify the most effective approach.	**[L5][CO3]**	**[5M]**
9		Analyze the role of Enumeration in identifying vulnerabilities within a network environment.	**[L4][CO3]**	**[10M]**
10		Design a security strategy to mitigate Windows, Linux, and Network vulnerabilities.	**[L6][CO3]**	**[10M]**

Course Code: 23CS1018 **R23**

UNIT –IV
WEB SERVER AND WIRELESS HACKING

1	**a)**	Define a web application.	**[L1][CO4]**	**[2M]**
	b)	Expand OWASP.	**[L1][CO4]**	**[2M]**
	c)	Define Cross-Site Scripting (XSS).	**[L2][CO4]**	**[2M]**
	d)	Define IEEE 802.11.	**[L1][CO4]**	**[2M]**
	e)	Mention any two wireless security threats.	**[L1][CO4]**	**[2M]**
2	**a)**	Explain SQL injection attacks and their prevention techniques.	**[L3][CO4]**	**[5M]**
	b)	Explain the OWASP Top 10 security risks.	**[L2][CO4]**	**[5M]**
3		Explain web application injection attacks. Compare code injection, SQL injection, and Cross-Site Scripting (XSS) with examples and prevention techniques.	**[L3][CO4]**	**[10M]**
4		Explain Cross-Site Scripting (XSS) attacks, their types, impacts, and prevention methods.	**[L3][CO4]**	**[10M]**
5		Discuss the tools used by web attackers and security testers. Explain how these tools are useful in vulnerability assessment.	**[L3][CO4]**	**[10M]**
6	**a)**	Explain wireless authentication methods.	**[L2][CO4]**	**[5M]**
	b)	Explain the tools used by web attackers and security testers.	**[L2][CO4]**	**[5M]**
7		Describe wireless authentication mechanisms and explain how they secure wireless networks.	**[L3][CO4]**	**[10M]**
8		Explain wireless technology and wireless network standards. Compare different IEEE 802.11 standards.	**[L4][CO4]**	**[10M]**
9		Analyze the security challenges in web applications and wireless networks. Suggest suitable countermeasures.	**[L4][CO4]**	**[10M]**
10	**a)**	Explain the concept of wardriving and its security implications.	**[L2][CO4]**	**[5M]**
	b)	Discuss common wireless hacking techniques and preventive measures.	**[L3][CO4]**	**[5M]**

Course Code: 23CS1018 **R23**

UNIT –V

CRYPTOGRAPHY ATTACKS AND NETWORK PROTECTION SYSTEMS

1	**a)**	Define a brute force attack.	**[L1][CO5]**	**[2M]**
	b)	Mention one example of replay attack.	**[L1][CO5]**	**[2M]**
	c)	Which cipher is vulnerable to frequency analysis?	**[L1][CO5]**	**[2M]**
	d)	State one limitation of ciphertext-only attacks.	**[L1][CO5]**	**[2M]**
	e)	State the purpose of a honeypot.	**[L1][CO5]**	**[2M]**
2		Explain brute force attacks in detail with diagram, working, advantages, disadvantages, and prevention techniques.	**[L3][CO5]**	**[10M]**
3		Compare replay attack with man-in-the-middle attack.	**[L2][CO5]**	**[10M]**
4		Explain frequency analysis attack with suitable examples, advantages, and limitations.	**[L5][CO5]**	**[10M]**
5		Analyze the role of routers in protecting enterprise networks.	**[L4][CO5]**	**[10M]**
6		Evaluate the effectiveness of firewalls in network security.	**[L5][CO5]**	**[10M]**
7		Evaluate IDS and IPS for enterprise network security.	**[L5][CO5]**	**[10M]**
8	**a)**	Explain signature-based and anomaly-based detection.	**[L2][CO5]**	**[05M]**
	b)	Differentiate IDS and IPS.	**[L4][CO5]**	**[05M]**
9	**a)**	Differentiate router and switch.	**[L4][CO5]**	**[05M]**
	b)	Compare ciphertext-only attack and known-plaintext attack.	**[L4][CO5]**	**[05M]**
10	**a)**	Explain the working of a honeypot.	**[L2][CO5]**	**[05M]**
	b)	Explain advantages and disadvantages of honeypots.	**[L2][CO5]**	**[05M]**

Prepared by: T M S Mekalarani, Assistant Professor, Dept of CSE (CCC-CIA-CIC)