SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

III SEMESTER

1923301 – INTRODUCTION TO CYBER THREATS

Regulation – 2019

Academic Year 2022 – 2023 (ODD SEMESTER)

Prepared by

Ms.R.Sivasankari, Assistant Professor/CYS

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203.

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

SUBJECT: 1923301 –INTRODUCTION TO CYBER THREATS

SEM / YEAR: III Sem / II Year

UNIT I -INTRODUCTION			
Ethical hacking process, Hackers behavior & mindset, Maintaining Anonymity, Hacking Methodology, Information Gathering, Active and Passive Sniffing, Physical security vulnerabilities and countermeasures. Internal and External testing. Preparation of Ethical Hacking.			
PART – A			
Q.No	**Questions**	**BT Level**	**Competence**
1.	Who are Hackers?	BTL1	Remembering
2.	List out the types of hackers.	BTL1	Remembering
3.	Define Ethical hacking.	BTL1	Remembering
4.	Why do you need Ethical hacking?	BTL2	Understanding
5.	What is an Asset?	BTL1	Applying
6.	Define Gray hat hackers.	BTL1	Remembering
7.	Illustrate the principles of a hacking mind set.	BTL3	Applying
8.	What is Information gathering?	BTL1	Remembering
9.	What should do after hacked? Illustrate it.	BTL3	Applying
10.	What is meant by vulnerability?	BTL2	Understanding
11.	How to predict the sniffing?	BTL2	Understanding
12.	Distinguish between black hat hacker and White hat hacker.	BTL4	Analyzing
13.	Compare Active and passive sniffing	BTL4	Analyzing
14.	Classify the different types of sniffing tools	BTL3	Applying
15.	Explain the ethical hacking tools.	BTL4	Analyzing
16.	Give the required skills of an Ethical hacker.	BTL2	Understanding
17.	Describe the concepts of Penetration testing.	BTL2	Understanding
18.	Conclude how Threat causes harms.	BTL5	Evaluating
19.	What are the various types of attacks?	BTL3	Applying
20.	Analyze the methods of Identification of Vulnerabilities.	BTL4	Analyzing
21.	Quote: Ethical hackers are not criminal hackers, justify your answer	BTL6	Creating
22.	Summarize the advantages of Ethical hacking	BTL5	Evaluating
23.	Compare the concepts of enumeration and foot printing.	BTL5	Evaluating
24.	Create the hacker language translation from this example 1 d1d n0t h4ck th1s p4g3, 1tw4s l1k3 th1s Wh3n 1 h4Ck3d 1n	BTL6	Creating
25.	List three differences between Internal and External Test.	BTL1	Remembering
PART – B			

1.	Describe in detail about the Ethical hacking process and its types. (13)	BTL1	Remembering
2.	(i) Describe in detail about the types of hackers. (7) (ii) Describe in detail about the various types of attacks. (6)	BTL1	Remembering
3.	What is Vulnerability? Describe in detail about the top ten vulnerabilities. (13)	BTL1	Remembering
4.	Describe in detail about cracking of Hacker mind set. (13)	BTL1	Remembering
5.	Discuss about Ethical Hacking in detail. (13)	BTL2	Understanding
6.	Summarize the concept of Sniffing in detail. (13)	BTL2	Understanding
7.	Summarize in detail about the methodology of Hacking. (13)	BTL2	Understanding
8.	Explain the Physical vulnerabilities and counter measures to overcome from those vulnerabilities.	BTL2	Understanding
9.	(i).Describe in detail about the hacker's language translation. (8) (ii).Describe in detail about the cryptography and steganography (5)	BTL3	Applying
10.	Illustrate the concepts of Information gathering in detail. (13)	BTL3	Applying
11.	(i).Classify the sniffing tools in detail. (7) (ii).Illustrate the concepts of sniffing countermeasures. (6)	BTL3	Applying
12.	(i).Explain in detail about the types of sniffing. (8) (ii).Explain in detail about the indication of sniffing. (5)	BTL4	Analyzing
13.	Analyze the concepts on (i). Hackers (4) (ii). Malicious users (4) (iii). Ethical hackers Vs Auditing (5)	BTL4	Analyzing
14.	What is an Attack? Explain various types of attacks in detail. (13)	BTL4	Analyzing
15.	(i).Explain in detail about the types of Hacking. (8) (ii).Point out the advantages and disadvantages of hacking. (5)	BTL5	Evaluating
16.	(i).Summarize in detail about the Vulnerability Assessment. (6) (ii).Explain in detail about the Penetration testing. (7)	BTL5	Evaluating
17.	Generalize the techniques can be used to gather the information from your Organization in detail. (13)	BTL6	Creating
	PART – C		
1.	Generalize the Cyber threat tool box in detail with example. (15)	BTL6	Creating
2.	Design the cyber threat actors diagram and explain the cyber threat activities in detail. (15)	BTL6	Creating
3.	What is ethical hacking? Why ethical hacking? Evaluate the identification of vulnerabilities and exploit the vulnerabilities. (15)	BTL5	Evaluating
4.	Explain in detail about the potentially unwanted program or application in cyber security field. (15)	BTL5	Evaluating
5.	What are the measurements a hacker would do to hack any system? (15)	BTL5	Evaluating

UNIT II – SOCIAL ENGINEERING			
Social Engineering attacks and countermeasures. Password attacks, Privilege Escalation and Executing Applications, Network Infrastructure Vulnerabilities, IP spoofing, DNS spoofing			
PART – A			
Q.No	**Questions**	**BT Level**	**Competence**
1	List out the some examples of Social engineering.	BTL1	Remembering
2	Why attackers use social engineering?	BTL1	Remembering
3	List few social engineering attacks.	BTL4	Analyzing
4	What are all the information can obtain by the effectives social engineers?	BTL1	Remembering
5	Examine the hackers commonly overlooked attack points	BTL3	Applying
6	Define Phishing.	BTL1	Remembering
7	What are all the specific policies help ward off social engineering in the long term?	BTL3	Remembering
8	Give the four steps for social engineering attacks performed by the hackers.	BTL2	Understanding
9	How important do you think physical security is in relation to technical security issues? Summarize it.	BTL2	Understanding
10	Point out meaning of Privilege in Computer security?	BTL4	Analyzing
11	List the types of privileges available in computer?	BTL4	Analyzing
12	Compare the types of privilege escalation.	BTL2	Understanding
13	Give few points about network infrastructure vulnerabilities.	BTL2	Understanding
14	Classify the two general classifications of password vulnerabilities.	BTL1	Applying
15	Define Rainbow attacks.	BTL1	Remembering
16	Write few steps to protect your password from password attack.	BTL2	Understanding
17	Analyze the Nigerian 419 email fraud scheme	BTL3	Analyzing
18	Apply the concepts of key stroke logging.	BTL3	Applying
19	Point out the tips to help for the users to prevent social engineering attacks.	BTL4	Analyzing
20	Classify the various password cracking tools.	BTL4	Analyzing
21	Summarize the concepts of DNS spoofing.	BTL5	Evaluating
22	Evaluate the vulnerability assessment tools.	BTL5	Evaluating
23	Generalize the term on password cracking.	BTL6	Creating
24	Explain the term IP Spoofing.	BTL5	Evaluating
25	Develop the countermeasures against network analyzer attacks.	BTL6	Creating
PART – B			

1	Describe the concepts of Social engineering. Elaborate why attackers use Social Engineering? (13)	BTL1	Remembering
2	Summarize why social engineering is effective? Identify the impacts of socialengineering. (13)	BTL2	Understanding
3	Describe in detail about the social engineering counter measures. (13)	BTL1	Remembering
4	(i).Identify the basic physical security vulnerabilities in detail. (7) (ii).Examine and pinpointing the physical vulnerabilities in your office. (6)	BTL1	Remembering
5	Describe the concepts of password vulnerabilities in detail. (13)	BTL1	Remembering
6	Describe the various password cracking tools in detail. (13)	BTL2	Understanding
7	Discuss the topic on (i) Dictionary attacks (4) (ii) Brute force attacks (4) (iii) Rainbow attacks (5)	BTL2	Understanding

8	Describe in detail about countermeasures for password cracking. (13)	BTL2	Understanding
9	Explain the concept of Privilege in Computer Security. Classify and explain the types of privilege escalation in detail. (13)	BTL3	Applying
10	What is meant by Attack? List the various types of attacks. (6) Illustrate the concepts of various password attacks in detail. (7)	BTL3	Applying
11	What do you mean by Firewalls? Why are they used?Illustrate the concepts of testing firewall rules. (13)	BTL3	Applying
12	Explain DoS Attack. Apply the countermeasures that can be applied against DoS attacks. (13)	BTL5	Evaluating
13	Explain in detail about creating password policies. (13)	BTL4	Analyzing
14	i).Explain in detail about the securing operating systems. (7) (ii).Classify the commonly hacked ports in detail. (6)	BTL4	Analyzing
15	(i).Analyze the concepts of ARP spoofing. (7) (ii).Explain in detail about DNS spoofing. (6)	BTL4	Analyzing
16	(i).Summarize the port scanning tools in detail. (7) (ii).Explain in detail about countermeasures against banner grabbing attacks.	BTL5	Evaluating
17	Develop the countermeasures against ping sweeping and port scanning. (13)	BTL6	Creating
18	Explain the Password Attacks in detail. (13)	BTL4	Analyzing
	PART – C		
	Develop the countermeasures against ARP poisoning and MAC address		

1.	spoofing attacks in detail. (15)	BTL6	Creating
2.	Detecting common Router, Switch and firewall weaknesses in detail. (15)	BTL6	Creating
3.	What you need to know about advanced malware? Evaluate it. (15)	BTL5	Evaluating
4.	Evaluate the DNS spoofing in following way (i).How DNS spoofing occurs? (4) (ii). How to check DNS settings in windows? (6) (iii). What are the aims of attackers for DNS spoofing? (5)	BTL5	Evaluating
5.	What is meant by Privilege Escalation? Why do we need Privilege Escalation? Explain in detail. (13)	BTL5	Evaluating

UNIT III – WIRELESS HACKING			
Wireless Hacking: Wireless footprint, Wireless scanning and enumeration, Gaining access (hacking 802.11), WEP, WPA, WPA2			
PART – A			
Q.No	**Questions**	**BT Level**	**Competence**
1.	List out the components of wireless network.	BTL1	Remembering
2.	Define Access point.	BTL1	Remembering
3.	What is service Set Identifiers (SSIDs)?	BTL1	Remembering
4.	Identify the wireless configuration options.	BTL5	Evaluating
5.	What is Wireless Router?	BTL1	Remembering
6.	List out the main functions of Wireless NIC.	BTL1	Remembering
7.	Give some wireless network standards.	BTL1	Remembering
8.	Summarize the concepts Extensible Authentication Protocol(EAP)	BTL2	Understanding
9.	Discuss on the term WPA.	BTL2	Understanding
10.	Point out two characteristics of Infrared Rays.	BTL4	Analyzing
11.	Describe the concepts of Wireless hacking.	BTL2	Understanding
12.	Compare the types of wireless connection.	BTL2	Understanding
13.	Describe PPP.	BTL2	Understanding
14.	Point out the more secure EAP methods.	BTL4	Analyzing
15.	Illustrate the concepts of Challenge Handshake Authentication Protocol (CHAP) vulnerability.	BTL3	Applying
16.	Illustrate the concepts of WIFI modes.	BTL3	Applying

17.	Discover the flaws of WEP.	BTL3	Applying
18.	Analyze the concepts of Wired Equivalent Privacy (WEP).	BTL4	Analyzing
19.	Point out the tools for WEP hacking.	BTL4	Analyzing
20.	Explain the commands on ipconfig and iwconfig.	BTL5	Evaluating
21.	Evaluate the term on Net Stumbler.	BTL5	Evaluating
22.	List the counter measures for wireless attacks.	BTL3	Applying
23.	Design the basic architecture of 802.11.	BTL6	Creating
24.	Generalize the concepts of War driving.	BTL6	Creating
25.	Write short notes on WPA2.	BTL2	Understanding
	PART – B		
1	Describe in detail about the implications of wireless network vulnerabilities. (13)	BTL1	Remembering
2	Describe in detail about the wireless network attacks and taking Counter measures. (13)	BTL1	Remembering
3	Identify the countermeasures against encrypted traffic attacks. (13)	BTL1	Remembering
4	Describe in detail about the cracking a WPA/WPA2 wireless network using Aircrack-ng. (13)	BTL1	Remembering
5	Describe in detail about using reaver to crack WPS-enabled wireless networks. (13)	BTL2	Understanding
6	Compare the concepts of WPA and WPA2 in detail. (13)	BTL2	Understanding
7	Describe in detail about the WEP attacks. (13)	BTL2	Understanding
8	List and explain the various attacking methods in detail. (13)	BTL2	Understanding
9	Apply the commands you can get the password of WEP network in detail. (13)	BTL3	Applying
10	Illustrate the techniques for hacking wireless networks. (13)	BTL3	Applying
11	Explain the wireless LAN standards of IEEE's 802.11 group. (13)	BTL3	Applying
12	Explain in detail about the wireless hacking and its requirements. (13)	BTL4	Analyzing
13	Explain the concepts of bypassing MAC filters on wireless networks. (13)	BTL4	Analyzing
14	Explain in detail about the tools for WEP hacking. (13)	BTL4	Analyzing
15	Explain in detail about the types of wireless connection. (13)	BTL5	Evaluating
16	Explain Wireless Footprint in detail. (13)	BTL5	Evaluating
17	Draw the WEP schema and generalize the authentication methods in detail. (13)	BTL6	Creating
18	Explain WPA and WPA2 in detail. (13)	BTL5	Evaluating

PART – C			
1.	Generalize the features of Netstumbler, Kismet and CCSF war driving in detail. (15)	BTL6	Creating
2.	Design a supplicant connecting to an Access point and a RADIUS server and 802.1 X components in detail. (15)	BTL6	Creating
3.	Explain in detail about Extensible Authentication Protocol (EAP) and also mention the authentication methods in detail. (15)	BTL5	Evaluating
4.	Evaluate the basic concepts of PPP and EAP in detail. (15)	BTL5	Evaluating
5.	Explain WEP and WPA in detail. (15)	BTL5	Evaluating

UNIT IV – ATTACKS			
DoS attacks. Web server and application vulnerabilities, SQL injection attacks, Vulnerability Analysis and Reverse Engineering, Buffer overflow attacks. Client–side browser exploits			
PART– A			
Q.No	**Questions**	**BT Level**	**Competence**
1.	List out the types of attacks.	BTL1	Remembering
2.	Define Computer Security.		
3.	Define DoS attack.	BTL4	Analyzing
4.	Why should we study Computer Security?		
5.	Identify the classification of DoS attacks.	BTL1	Remembering
6.	State any three firewall capabilities.	BTL1	Remembering
7.	How to know if an attack is happening?	BTL4	Analyzing
8.	Define Spoofed DoS attack.	BTL1	Remembering
9.	Difference between DoS and DDoS attack.	BTL2	Understanding
10.	Illustrate the concepts of SQL injection.	BTL3	Applying
11.	Describe the term on Default Deny.	BTL2	Understanding
12.	Distinguish between first order and second order attacks.	BTL2	Understanding
13.	Classify the other injection types.	BTL3	Applying
14.	Discover the stack based buffer overflow vulnerabilities.	BTL2	Applying
15.	How SQL injection works?	BTL1	Remembering
16.	Point out the SQL injection tools.	BTL4	Analyzing
17.	List the impact of SQL Injection.	BTL4	Analyzing
18.	Evaluate how First Order Attacks work.	BTL3	Understanding
19.	Analyze the pros & cons of exploit frameworks.	BTL4	Analyzing

20.	Describe the SQL injection Mechanism.	BTL3	Understanding
21.	Explain the concepts of injection mechanism.	BTL5	Evaluating
22.	Evaluate the harmful functions in C library.	BTL5	Evaluating
23.	Compose the three types of HTTP based authentication schemes.	BTL6	Creating
24.	Generalize the concepts of lateral injection.	BTL6	Creating
25.	List the pros and cons of Exploit Frameworks.	BTL4	Analyzing

PART – B

1	Describe in detail about the types of DoS attacks.	(13)	BTL1	Remembering
2	Identify the way how to defend from the DoS attack?	(13)	BTL1	Remembering
3	(i). Describe in detail about SQL injection. (ii).Describe in detail about three types of SQL injection attacks.	(7) (6)	BTL1	Remembering
4	Describe in detail about the HTTP based authentication scheme.	(13)	BTL1	Remembering
5	Discuss in detail about Stack based buffer overflow attack.	(13)	BTL2	Understanding
6	Summarize in detail about Heap based buffer overflow attack.	(13)	BTL2	Understanding
7	(i). Describe in detail about defence mechanism against SQL injection. (ii). Discuss on SQL injection to remote command execution.	(6) (7)	BTL2	Understanding
8	(i). Discuss the topic on preventing authentication and session attacks. (ii). Describe in detail about the Blind SQL injection.	(7) (6)	BTL2	Understanding
9	Explain in detail about the other injection types and SQL injection tools.	(13)	BTL5	Evaluating
10	Explain in detail the Vulnerability Analysis and Reverse Engineering.	(13)	BTL3	Applying
11	Discover the stack based buffer over flow vulnerabilities and explain in detail.	(13)	BTL3	Applying
12	Explain in detail about the first order attacks, second order attacks and Lateral injection.	(13)	BTL4	Analyzing
13	What is a buffer overflow attack? Explain its methods in detail.	(13)	BTL4	Analyzing
14	(i).Explain in detail about the web application exploitation. (ii). Explain in detail about the cross site scripting.	(7) (6)	BTL4	Analyzing
15	Explain the concept of Reverse Engineering with an Example.	(13)	BTL4	Analyzing
16	Illustrate the concepts of SQL injection in PHP.	(13)	BTL3	Applying
17	Summarize the Client-side Browser Exploits in detail.	(13)	BTL5	Evaluating
18	Illustrate the concepts on Flooding.	(13)	BTL3	Applying

PART – C

1	(i). Explain in detail about the Hacking web 2.0. (7) (ii). Evaluate the concepts of minimizing web security risks. (8)	BTL5	Evaluating
2	Explain in detail about harmful C library functions. (13)	BTL6	Evaluating
3.	(i).Create the sample program for finding stack based buffer overflow vulnerabilities. (8) (ii).Create sample vulnerable C code for view of the stack. (7)	BTL5	Creating
4.	(i).Design the vulnerable program with two different inputs by runningmode. (8) (ii)Create the program with a heap based buffer overflow vulnerability. (7)	BTL6	Creating
5.	Evaluate the concepts of penetration and Eaves dropping in DoS attack. (13)	BTL5	Creating

UNIT V – METASPLOIT

Introduction to Metasploit: Metasploit framework, Metasploit Console, Payloads, Introduction to Armitage, Installing and using Kali Linux Distribution, Introduction to penetration testing tools in Kali Linux.

PART – A

Q.No	Questions	BT Level	Competence
1.	Define Metasploit.	BTL1	Remembering
2.	When to use metasploit?	BTL4	Analyzing
3.	List out the phases of penetration testing life cycle.	BTL1	Remembering
4.	What is Vulnerability?	BTL1	Remembering
5.	What is penetration testing?	BTL1	Remembering
6.	Define Kali Linux.	BTL1	Remembering
7.	Distinguish between passive information gathering and active information gathering.	BTL2	Understanding
8.	Give the causes of Vulnerabilities.	BTL2	Understanding
9.	Evaluate the meterpreter commands.	BTL2	Understanding
10.	Describe the term on Exploit.	BTL2	Understanding
11.	Illustrate the concepts on Enumeration.	BTL3	Applying
12.	Classify the terms of metasploit.	BTL3	Applying
13.	Illustrate the concepts on exploit modules.	BTL3	Applying
14.	Why conduct penetration testing? Analyze it.	BTL4	Analyzing
15.	Analyze the term on msfconsole.	BTL4	Analyzing
16.	Differentiate the categories of Kali Linux tools.	BTL4	Analyzing

17.	Describe the features of kali Linux.	BTL5	Evaluating
18.	What can be tested in penetration testing?	BTL6	Evaluating
19.	What is hydra tool? Integrate the information about target by before using the kali Linux tool hydra.	BTL5	Creating
20.	Generalize the concepts of Penetration testing Execution Standard (PTES).	BTL6	Creating
21.	What is Payload?	BTL1	Remembering
22.	List the Modules in Payload.	BTL1	Remembering
23.	What is the purpose of Armitage?	BTL4	Analyzing
24.	What are the differences between Metasploit and Armitage?	BTL2	Understanding
25.	What is the command to start Armitage?	BTL5	Evaluating
	PART – B		
1	(i).Describe in detail about metasploit framework. (07) (ii).Describe in detail about the metasploit terms. (06)	BTL1	Remembering
2	Explain the Penetration Testing stages in detail. (13)	BTL1	Remembering
3	Describe in detail about Open source Security Testing methodology Manual(OSSTM) (13)	BTL1	Remembering
4	Discuss the topic on (i). Msfconsole (06) (ii). Meterpreter commands (07)	BTL2	Understanding
5	(i).Describe in detail about the features of kali Linux and Kali tool kits (08) (ii). How to install Kali Linux? (05)	BTL1	Remembering
6	(i). Describe in detail about categories of pen testing. (07) (ii).Describe in detail about the phases of penetration testing. (06)	BTL2	Understanding
7	Describe in detail about the modular architecture of metasploit framework. (13)	BTL1	Remembering
8	Describe in detail about Exploit modules. (13)	BTL2	Understanding
9	Generalize the steps to install metasploit in detail. (13)	BTL4	Creating
10	Illustrate the phases of Penetration Testing Execution Standard (PTES). (13)	BTL3	Applying
11	Explain in detail about penetration testing using kali Linux. (13)	BTL4	Analyzing
12	(i).Explain in detail about the Kali Linux and its methodology. (07) (ii).Explain the categories of Kali Linux tools. (06)	BTL6	Analyzing
13	Analyze the various Metasploit components and modules that can be used across all stages of penetration testing in detail. (13)	BTL4	Analyzing
14	Evaluate the steps must be performed to gather the information about all host machines by before starting the penetration tests. (13)	BTL5	Evaluating
15	Illustrate the concepts on Nmap, metasploit and Hydra tool. (13)	BTL3	Applying
16	Explain in detail about Open Web Application Security Project Testing Guide(OWASP) (13)	BTL2	Understanding

17	Discuss the topic on 1. Enumeration (08) 2. Privilege Escalation. (05)	BTL5	Evaluating
18	What is Payload? Explain detail about the payload modules. (13)	BTL3	Applying
	PART – C		
1.	Generalize the concepts on how to scan your local VirtualBox subnet from Metasploit using the Nmap utility. (15)	BTL5	Creating
2.	(i). Kali Linux does excellent job separating these useful utilities into the categories. Generalize it. (07) (ii). Design the installation procedure for kali Linux and generalize the usesof it. (08)	BTL6	Creating
3.	(i).Explain in detail about Nmap and Nmap target selection. (07) (ii). How to perform a basic Nmap scan on Kali Linux. (08)	BTL5	Evaluating
4.	Evaluate the installation of kali Linux methods. (13)	BTL6	Evaluating
5.	Explain the procedure in detail about how to install Kali Linux using virtual box. (13)	BTL6	Creating