SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

V SEMESTER

1923502 – ETHICAL HACKING

Regulation – 2019

Academic Year 2022 – 2023(ODD SEMESTER)

Prepared by

Dr. M. Senthil Kumar, Associate Professor

SRM VALLIAMMAI ENGINEERING COLLEGE
(An Autonomous Institution)
SRM Nagar, Kattankulathur – 603 203
DEPARTMENT OF CYBER SECURITY
QUESTION BANK

SUBJECT : 1923502 - Ethical Hacking

SEM/YEAR: V/ III

UNIT I - INTRODUCTION			
Ethical hacking process, Hacker behavior & mindset, Vulnerability versus Penetration test, Penetration Test. Categories of Penetration test–Black box–White box–Grey box–Types of Penetration Test.			
PART – A			
Q.No	**Questions**	**BT Level**	**Competence**
1	Define Hacker.	BTL 1	Remembering
2	Explain about Penetration test?	BTL 2	Understanding
3	Summarize Risk with equation.	BTL 5	Evaluating
4	Describe the term "Vulnerability".	BTL 2	Understanding
5	List Out the Types of hackers.	BTL 1	Remembering
6	Define threads.	BTL 1	Remembering
7	Implement the rules of Engagement in hacking.	BTL 3	Applying
8	Execute the categories of Penetration test.	BTL 3	Applying
9	State the top 5 hacking techniques?	BTL 1	Remembering
10	Classify Ethical hacking process.	BTL 3	Applying
11	Investigate the similarities between penetration and vulnerability testing?	BTL 6	Creating
12	Identify the different types of ethical hacking?	BTL 2	Understanding
13	Compare what is meant by Vulnerability versus Penetration test?	BTL 4	Analyzing
14	Distinguish the 3 phases of penetration testing?	BTL 4	Analyzing
15	Compare Black box And White box.	BTL 2	Understanding
16	Evaluate the methodologies in Penetration test?	BTL 5	Evaluating
17	Relate the important terminologies in Hacking?	BTL 3	Applying

18	Define Gray box.	BTL 1	Remembering
19	Write the categories of audience in Penetration test?	BTL 6	Creating
20	Defend the limitations for vulnerability assessment?	BTL 5	Evaluating
21	Discuss about ethical hacking.	BTL 2	Understanding
22	Judge the importance in field of hacking?	BTL 4	Analyzing
23	Examine Vulnerabilities?	BTL 4	Analyzing
24	What are the similarities between penetration testing and ethical hacking?	BTL 1	Remembering

PART – B				
Q.No.	**Questions**	**Marks**	**BT Level**	**Competence**
1	Define Hacker with its types.	13	BTL 1	Remembering
2	Classify the different Categories of Penetration test?	13	BTL 2	Understanding
3	Write a detail about important terminologies in Hacking.	13	BTL 2	Understanding
4	Examine about OSSTMM with diagram.	13	BTL 4	Analyzing
5	(i) Explain the Related function about OSWP. (ii) Write the complete Concept about NIST?	5 8	BTL 3	Applying
6	Draw a flowchart and explain the steps for penetration testing methodology?	13	BTL 3	Applying
7	Describe about ethical hacking process with suitable example.	13	BTL 1	Remembering
8	Illustrate the different types of penetration tests?	13	BTL 4	Analyzing
9	(i) Describe difference between Vulnerability and Penetration test? (ii) Describe executive summary in penetration test?	6 7	BTL 1	Remembering
10	Sketch and explain about the structure of penetration testing report?	13	BTL 3	Applying
11	Design the phase of ethical hacking process in detail?	13	BTL 6	Creating
12	(i) Explain Risk Assessment with suitable example. (ii) Evaluate the importance of reporting in penetration testing?	6 7	BTL 2	Understanding

13	Write a detail about report writing with its importance in penetration testing?	13	BTL 1	Remembering
14	Discuss the summary about types of methodologies about penetration test.	13	BTL 2	Understanding
15	(i) Explain the classification of hackers based on the intent of hacking the system? (ii) Elaborate the roles of hackers played in hacking process.	6 7	BTL 4	Analyzing
16	Explain hacking process with diagram and steps.	13	BTL 5	Evaluating
17	Discuss about penetration test and explain the need for repeated penetration testing.	13	BTL 5	Evaluating

PART – C				
Q.No.	**Questions**	**Marks**	**BT Level**	**Competence**
1	State Hacking. Investigate about hackers and ethical hacking process in detail.	15	BTL 6	Creating
2	Explain penetration testing with vulnerability test. Define the types of penetration testing?	15	BTL 5	Evaluating
3	Compare detail about three categories of penetration testing? Evaluate a key factor for good report?	15	BTL 6	Creating
4	(i) Explain in detail the pre attack phase of penetration testing (ii) Explain in detail the post attack phase of penetration testing	7 8	BTL 5	Evaluating
5	Investigate case study about what was the motivation for hacking the system and government websites in detail.	15	BTL 6	Creating

UNIT II

INFORMATION GATHERING TECHNIQUES

Active Information Gathering–Passive Information Gathering–Sources of Information Gathering–NeoTrace–Traceroute–ICMP Traceroute–TCP Traceroute–UDP Traceroute – Intercepting a Response–WhatWeb – Netcraft–Interacting with DNS Servers

PART – A

Q.No.	Questions	BT Level	Competence
1	What is information gathering?	BTL 5	Evaluating
2	List the types in information gathering?	BTL 1	Remembering
3	Write the tools used in traceroute?	BTL 1	Remembering
4	List out the passive methods in Passive Information Gathering?	BTL 6	Creating
5	Define NeoTrace.	BTL 1	Remembering
6	What are the five sources of data?	BTL 2	Understanding
7	Define DNS server.	BTL 4	Applying
8	State the Purpose of the Traceroute Tool.	BTL 3	Applying
9	Expand the following Protocols: (i) ICMP (ii) TCP (iii)UDP (iv)DNS	BTL 1	Remembering
10	What is Passive Information Gathering?	BTL 2	Understanding
11	Write about the term “traceroute”?	BTL 4	Analyzing
12	Compare ICMP traceroute and TCP traceroute?	BTL 5	Remembering
13	Information gathering is not just a phase of security testing. Justify?	BTL 1	Remembering
14	State netcraft.	BTL 3	Applying
15	What is the purpose of information gathering?	BTL 4	Analyzing
16	Write the techniques in Passive Information Gathering?	BTL 3	Understanding
17	Illustrate whatweb.	BTL 2	Understanding
18	Define UDP traceroute.	BTL 4	Remembering
19	List out the supported methods in traceroute?	BTL 1	Remembering
20	What is netcraft used for?	BTL 5	Evaluating
21	Write the use of Nslookup in information gathering.	BTL 2	Remembering
22	Discuss the example for passive information gathering.	BTL 3	Applying
23	Compare Whatweb and Netcraft.	BTL 5	Evaluating
24	Illustrate the category in Nslookup.	BTL 2	Remembering

PART – B				
Q.No.	**Questions**	**Marks**	**BT Level**	**Competence**
1	Illustrate short note about Passive Information Gathering and its techniques.	13	BTL 4	Analyzing
2	(i) Write the Difference between passive information gathering and active information gathering? (ii) Explain the concept about source of information gathering?	7 6	BTL 2	Understanding
3	Explain the architecture of ICMP traceroute?	13	BTL 3	Applying
4	Describe about passive methods in Passive Information Gathering?	13	BTL 5	Evaluating
5	Explain the interacting with DNS servers in detail?	13	BTL 2	Understanding
6	Write a different type of way to gather information with examples.	13	BTL 1	Remembering
7	Illustrate the details about information gathering whois with suitable commands?	13	BTL 3	Applying
8	List out the steps followed in intercepting a response concept with detail?	13	BTL 4	Analyzing
9	Elaborate the detail about whatweb with example?	13	BTL 1	Remembering
10	Discuss about NSlookup with its steps?	13	BTL 1	Remembering
11	Write the fundamental for information gathering?	13	BTL 4	Analyzing
12	(i) What is Traceroute? Explain with purpose of Traceroute tools? (ii) Write the supported modes of Traceroute with explanation?	7 6	BTL 2	Understanding
13	Discuss about the function about netcraft?	13	BTL 6	Creating
14	Define Neo trace with explanation?	13	BTL 1	Remembering
15	Describe about active and passive information gathering with suitable example.	13	BTL 3	Applying
16	Explain the following terms: (i) ICMP Traceroute (ii) TCP Traceroute	4 4 5	BTL 5	Evaluating

	(iii)UDP Traceroute			
17	Enumerate about traceroute requirements and counter measures with example	13	BTL 2	Understanding

PART – C				
Q.No.	**Questions**	**Marks**	**BT Level**	**Competence**
1	Discuss detail about Traditional methods of Information Gathering with suitable examples?	15	BTL 6	Creating
2	Describe the types of traceroutes with its usage in detail?	15	BTL 5	Evaluating
3	Write a detail information about traceroute and its methodologies?	15	BTL 6	Creating
4	Execute the working steps and details for intercepting a response?	15	BTL 5	Evaluating
5	Explain the information gathering methodologies of the hackers.	15	BTL 6	Creating

UNIT III

SNOOPING ATTACKS &PORT SCANNING TECHNIQUES

Enumerating SNMP–Problem with SNMP–Sniffing SNMP Passwords–SNMP Brute Force Tool-SMTP Enumeration–Types of Port Scanning–Understanding the TCP Three–Way Handshake–Anonymous Scan Types–OS Fingerprinting–Advanced Firewall/IDS Evading Techniques

PART – A

Q.No.	**Questions**	**BT Level**	**Competence**
1	Define enumerating SNMP with its versions?	BTL 2	Understanding
2	What is port scanning?	BTL 2	Understanding
3	Expand SNMP.	BTL 2	Understanding
4	Define firewall.	BTL 1	Remembering
5	Draw a diagram for TCP three-way handshake.	BTL 1	Remembering
6	State the TCP Flags.	BTL 4	Analyzing
7	What is password? Write its importance.	BTL 5	Evaluating
8	Justify a prerequisite for IDLE scan?	BTL 5	Evaluating
9	Illustrate the importance of firewall.	BTL 1	Remembering

10	List out the types in port scanning?	BTL 4	Analyzing
11	Write the problem with SNMP?	BTL 3	Applying
12	what is ICMP scanning? How is it carried out?	BTL 3	Applying
13	Illustrate OS fingerprinting?	BTL 1	Remembering
14	Demonstrate the IDS Evading Techniques?	BTL 3	Applying
15	Define scanning. why we used?	BTL 6	Creating
16	Describe the term "TCP three-way handshake "?	BTL 2	Understanding
17	Define brute force tool	BTL 1	Remembering
18	List out the anonymous scan types?	BTL 6	Creating
19	Summarize IDS.	BTL 3	Applying
20	How the enumeration is different from scanning?	BTL 6	Creating
21	Is brute force still effective?	BTL 2	Understanding
22	What are the three types of scanning?	BTL 1	Remembering
23	List out the techniques in enumeration.	BTL 6	Creating
24	Define sniffing.	BTL 4	Analyzing

PART – B

Q.No.	Questions	Marks	BT Level	Competence
1	Write about SNMP enumeration and implement with Brute force tool in detail.	13	BTL 3	Applying
2	What is enumeration? What information can be enumerated by intruders? Explain the different enumeration techniques.	13	BTL 2	Understanding
3	What is port scanning? Investigate about port scanning techniques.	13	BTL 6	Creating
4	(i) Define in detail about brute force tool. (ii) List out the different types of sniffing attacks? Explain each in brief.	6 7	BTL 4	Remembering
5	Explain the tools used in enumeration in detail.	13	BTL 5	Evaluating
6	Define scanning. Illustrate the phase of scanning	13	BTL 4	Analyzing
7	(i) What are the counter measures against the port scanning? (ii) Explain the scanning methodology in detail.	3 10	BTL 3	Applying

8	Explain the types of port status in TCP three-way handshake?	13	BTL 1	Remembering
9	Where we used TCP connect scan and draw a diagram with explanation?	13	BTL 5	Evaluating
10	What is scanning? list and explain the types of scanning performed.	13	BTL 1	Remembering
11	Write short explain about TCP three-way handshake.	13	BTL 1	Remembering
12	Explain in detail about OS finger printing?	13	BTL 2	Understanding
13	Sketch the types of port scanning and Write the counter measures against the port scanning?	13	BTL 3	Applying
14	Explain the techniques in firewall.	13	BTL 4	Analyzing
15	Discuss in detail about IDS with its importance.	13	BTL 1	Remembering
16	(i) How can firewalls be evaded using IP address spoofing? (ii) How source routing can be used to evade firewall restrictions?	7 6	BTL 2	Understanding
17	What are the countermeasures that provide protection against intrusion detection systems and firewalls?	13	BTL 2	Understanding

PART – C

Q.No.	Questions	Marks	BT Level	Competence
1	List out the tools used in SNMP enumeration and execute the process about brute force tool.	15	BTL 6	Creating
2	Explain in detail about scanning methods and attack with purpose.	13	BTL 5	Evaluating
3	(i) Elaborate the TCP Three-way handshake with neat diagram and steps in detail. (ii) Develop a case study to product your system into Brute force attack in detail.	7 8	BTL 6	Creating
4	(i) What is firewall? (ii) Discuss about technologies used in firewall? (iii)List the scan techniques in firewall?	2 10 3	BTL 6	Creating

5	Briefly explain about SNMP enumeration with techniques and its countermeasures.	15	BTL 5	Evaluating

UNIT IV

VULNERABILITY ASSESSMENT & NETWORK SNIFFING

Vulnerability Scanners–Vulnerability Assessment with Nmap–Nessus Vulnerability Scanner–Types of Sniffing–MITM Attacks–ARP Attacks–Using ARP Spoof to Perform MITM Attacks–Hijacking Session with MITM Attack–Sniffing Session Cookies with Wireshark–DNS Spoofing–DHCP Spoofing

PART – A

Q.No	Questions	BT Level	Competence
1	Define vulnerability assessment.	BTL 2	Understanding
2	What Are Vulnerability Scanners and How Do They Work?	BTL 4	Analyzing
3	Compare the difference between DNS spoofing and DHCP spoofing?	BTL 4	Analyzing
4	List out the things in vulnerability scanners?	BTL 1	Remembering
5	Elaborate the list of applications in ARP spoofing.	BTL 3	Applying
6	State-Scanning.	BTL 5	Evaluating
7	Defend sniffing?	BTL 4	Analyzing
8	Define vulnerability scanners.	BTL 1	Remembering
9	Write the relate explanation for SCADA and its arguments?	BTL 4	Analyzing
10	State the term “script”.	BTL 2	Understanding
11	Write the disadvantage for vulnerability scanner?	BTL 6	Creating
12	List out the flavors of nessus vulnerability?	BTL 2	Understanding
13	Draw a diagram for MITM attacks?	BTL 2	Understanding
14	Write the types in automated scanners?	BTL 5	Evaluating
15	Define the features of Nmap.	BTL 3	Applying
16	Investigate about the term “cookies”?	BTL 6	Creating
17	Write the main performance of middle attack?	BTL 1	Remembering
18	Define the steps involved in session hijacking.	BTL 1	Remembering
19	List out the vectors in ARP attacks?	BTL 1	Remembering
20	Write the main categories in sniffing?	BTL 3	Applying
21	What is MITM?	BTL 1	Remembering
22	Illustrate the concept for wireshark.	BTL 3	Applying

23	What can be sniffed?	BTL 5	Evaluating
24	Describe the term hijacking.	BTL 2	Understanding

PART – B

Q.No	Questions	Marks	BT Level	Competence
1	Discuss about the installation and usage of testing SCADA Environments with Nmap?	13	BTL 2	Understanding
2	What is vulnerability scanner? State the pros and cons.	13	BTL 1	Remembering
3	What is sniffing? Explain its types?	13	BTL 2	Understanding
4	Explain the concept about vulnerability assessment with Nmap and its features?	13	BTL 3	Applying
5	Describe attack? (i) Explain MITM attack. (ii) Explain ARP attack.	3 5 5	BTL 1	Remembering
6	Discuss about sniffing attack.	13	BTL 2	Understanding
7	Explain about preventing session hijacking?	13	BTL 1	Remembering
8	Defend about the nessus vulnerability and its flavors?	13	BTL 5	Evaluating
9	Write about ARP spoofing with workflow diagram.	13	BTL 4	Analyzing
10	(i) Demonstrate about session hijacking tools? (ii) List out the TCP occurs in three phases with explanation?	6 7	BTL 3	Applying
11	(i) Illustrate the concept about DNS spoofing? (ii) Write the steps in ARP spoof perform MITM attack.	7 6	BTL 4	Analyzing
12	What is sniffing? Write and explain the types in detail?	13	BTL 5	Evaluating
13	Describe the manipulate gateway for DHCP spoofing with suitable commands?	13	BTL 1	Remembering
14	What is session hijacking? Write its importance with explanation.	13	BTL 6	Creating
15	Explain the attacks performed in attacks with detail.	13	BTL 4	Analyzing
16	Discuss about the network sniffing.	13	BTL 2	Understanding

17	Define session hijacking. Describe the steps involved in session hijacking.	13	BTL 3	Applying

PART – C

Q.No	Questions	Marks	BT Level	Competence
1.	Elaborate in detail about installation of the nessus on backtrack with suitable commands?	15	BTL 5	Evaluating
2.	Examine the term vulnerability scanners. explain in detail	15	BTL 6	Creating
3.	Write a short note about. (i) DNS spoofing (ii) DHCP spoofing (iii)ARP spoofing	 5 5 5	BTL 5	Evaluating
4.	Discuss about network sniffing in detail.	15	BTL 6	Creating
5.	Illustrate the following with its importance. (i) Hijacking (ii) Spoofing (iii)Attacks &scanners	 5 5 5	BTL 5	Evaluating

UNIT V

EXPLOITATION

Remote Exploitation–Attacking Network Remote Services–Overview of Brute Force Attacks–Common Target Protocols–Client Side Exploitation–Methods–Postexploitation–Escalating Privileges–Installing a Backdoor–MSFVenom–Cracking the Hashes–Rainbow Crack–Identifying and Exploiting Further Targets

PART – A

Q.No.	Questions	BT Level	Competence
1	What is remote exploitation?	BTL 1	Remembering
2	Define Brute force attacks.	BTL 2	Understanding
3	Write the categories in brute force attacks?	BTL 5	Evaluating
4	State Rainbow table.	BTL 1	Remembering
5	List out the methods in client side exploitation?	BTL 2	Understanding

6	Write the tools for crack user names and passwords.	BTL 4	Analyzing
7	Define hash.	BTL 4	Analyzing
8	Write various types of network services.	BTL 5	Evaluating
9	State the term “backdoor”	BTL 1	Remembering
10	Write the types of Exploit network services.	BTL 1	Remembering
11	Describe the categories for brute force attack.	BTL 2	Understanding
12	What are the vulnerabilities of remote access?	BTL 3	Applying
13	Summarize purpose of DOS	BTL 2	Understanding
14	What are the different types of brute force attacks?	BTL 3	Applying
15	List out the approaches for backdoor.	BTL 2	Understanding
16	Illustrate the term rainbow crack work	BTL 4	Analyzing
17	What is MSFVenom and write a command for MSFVenom.	BTL 3	Applying
18	Illustrate the importance of Rainbow crack.	BTL 6	Creating
19	Define client side exploitation.	BTL 6	Creating
20	What is a hash password cracking?	BTL 1	Remembering
21	Define rainbow crack.	BTL 4	Analyzing
22	Write the security features.	BTL 5	Evaluating
23	How to identify the further targets?	BTL 1	Remembering
24	List the examples for remote exploitation.	BTL 3	Analyzing

PART – B

Q.No.	Questions	Marks	BT Level	Competence
1	Explain the process of attacking network remote services in detail.	13	BTL 2	Understanding
2	State remote exploitation. discuss the history and examples for remote exploitation	13	BTL 1	Remembering
3	Describe the overview of brute force attacks in detail.	13	BTL 3	Applying
4	Define backdoor with its approaches and importance.	13	BTL 2	Understanding
5	Discuss about the methods in client side exploitation with example.	13	BTL 1	Remembering
6	List out the common target protocols with short description for each protocol.	13	BTL 4	Analyzing
7	Illustrate the working principles of rainbow crack.	13	BTL 5	Evaluating

8	Discuss the categories of brute force attacks in detail	`13	BTL 6	Creating
9	Briefly explain about (i) Remote exploitation (ii) Clientside exploitation	7 6	BTL 2	Understanding
10	Write and explain the importance of identifying and exploiting further targets.	13	BTL 1	Remembering
11	Explain the detail about post exploitation.	13	BTL 3	Applying
12	Illustrate the rules of engagement in post exploitation with detail.	13	BTL 2	Understanding
13	Elaborate detail about escalating privileges.	13	BTL 4	Analyzing
14	(i) Discuss and select the tools used in post exploitation in detail. (ii) Discuss the purpose of post exploitation and importance in detail.	7 6	BTL 5	Evaluating
15	Contrast and Explain the process of Rainbow crack in detail.	13	BTL 4	Analyzing
16	Write a short note about post exploitation in detail.	13	BTL 1	Remembering
17	Discuss the types of categories in client side exploitation	13	BTL 3	Applying

PART –C

Q.No.	Questions	Marks	BT Level	Competence
1	Write a short note about remote exploitation.	15	BTL 5	Evaluating
2	Briefly explain about brute force attacks and techniques.	15	BTL 6	Creating
3	What is backdoor? And explain why it is used? Investigate About the step to installing backdoor with explanation.	15	BTL 6	Creating
4	(i) Define client side exploitation. (ii) List out methods in client side exploitation. (iii)Define brute force attack with example.	5 5 5	BTL 5	Evaluating
5	Discuss and Develop following terms in detail. (i) Remote exploitation (ii) Post exploitation (iii)Client side exploitation	 5 5 5	BTL 6	Creating

VALLIAMMAI ENGINEERING COLLEGE
SRM

VALLIAMMAI ENGINEERING COLLEGE
SRM

VALLIAMMAI ENGINEERING COLLEGE
SRM

VALLIAMMAI ENGINEERING COLLEGE
SRM

VALLIAMMAI ENGINEERING COLLEGE
SRM