# SRM VALLIAMMAI ENGINEERING COLLEGE

*(An Autonomous Institution)*

SRM Nagar, Kattankulathur – 603 203

## DEPARTMENT OF CYBER SECURITY

## QUESTION BANK

**V SEMESTER**

**CY3562– ETHICAL HACKING PRACTICES**

**Regulation – 2023**

**Academic Year 2025-2026 (ODD SEMESTER)**

*Prepared by*

**Dr.V. Santhana Marichamy / Assoc. Prof**

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

**SUBJECT : CY3562 – ETHICAL HACKING PRACTICES**

**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 the term Ethical Hacker. | BTL 1 | Remembering |
| 2 | List out different phases of the ethical hacking process? | BTL 1 | Remembering |
| 3 | What is reconnaissance in ethical hacking? | BTL 1 | Remembering |
| 4 | What does vulnerability assessment mean? | BTL 2 | Understanding |
| 5 | What is meant by exploitation? | BTL 1 | Remembering |
| 6 | Mention any two tools commonly used for scanning during ethical hacking. | BTL 2 | Understanding |
| 7 | Define social engineering in ethical hacking. | BTL 1 | Remembering |
| 8 | What is the difference between active and passive reconnaissance? | BTL 2 | Understanding |
| 9 | Differentiate between black hat and white hat hackers. | BTL 2 | Understanding |
| 10 | List the common motivations behind hacking. | BTL 1 | Remembering |
| 11 | What type of test attempts to exploit vulnerabilities? | BTL 2 | Understanding |
| 12 | Define the term penetration testing.. | BTL 1 | Remembering |
| 13 | How does a vulnerability scan differ from a penetration test? | BTL 2 | Understanding |
| 14 | What is meant by vulnerability in cyber security? | BTL 1 | Remembering |
| 15 | Mention the primary goal of a penetration test?. | BTL 1 | Remembering |
| 16 | What is meant by Gray box testing? | BTL 2 | Understanding |
| 17 | Name three types of penetration tests based on the target system. | BTL 1 | Remembering |

| | | | |
|---|---|---|---|
| 18 | How does Grey Box testing differ from White Box testing? | BTL 2 | Understanding |
| 19 | What is the outcome of a penetration test report? | BTL 1 | Remembering |
| 20 | Mention the advantage of White Box penetration testing. | BTL 1 | Remembering |
| 21 | Which penetration testing category is typically faster due to available information? | BTL 2 | Understanding |
| 22 | Which category does the tester have no prior information about the system? | BTL 2 | Understanding |
| 23 | Differentiate between internal and external penetration testing. | BTL 2 | Understanding |
| 24 | List the common challenges in Black Box penetration testing. | BTL 1 | Remembering |

**PART – B**

| Q.No. | Questions | Marks | BT Level | Competence |
|---|---|---|---|---|
| 1 | Explain in detail the various types of Hackers. | 16 | BTL4 | Analyzing |
| 2 | Explain the concept of ethical hacking and how it differs from malicious hacking. | 16 | BTL5 | Evaluating |
| 3 | Describe the importance of different Hacking terminologies in detail | 16 | BTL4 | Analyzing |
| 4 | Describe in detail the different phases of the ethical hacking process and their significance. | 16 | BTL4 | Analyzing |
| 5 | Discuss the role of reconnaissance in ethical hacking and the techniques used to gather information. | 16 | BTL4 | Analyzing |
| 6 | Analyze the motivations behind hacking and how they influence hacker behavior. | 16 | BTL6 | Creating |
| 7 | Draw a flowchart and explain the steps for penetration testing methodologies? | 16 | BTL3 | Applying |
| 8 | i. Describe the various differences between Vulnerability and Penetration test?<br>ii. How does understanding hacker behavior help organizations improve their security? | 8<br>8 | BTL4 | Analyzing |
| 9 | Discuss the responsibilities and ethical duties of a penetration tester during and after a penetration test. | 16 | BTL4 | Analyzing |
| 10 | i. Compare and contrast vulnerability assessment and penetration testing.<br>ii. Explain how a hacker's mindset differs from that of a typical IT professional. | 8<br>8 | BTL4 | Analyzing |
| 11 | Describe the objectives and procedures of a penetration test in an organization. | 16 | BTL3 | Applying |
| 12 | Describe the difference in approach between black hat, white hat, and grey hat hackers. | 16 | BTL3 | Applying |
| 13 | Explain the importance of combining both vulnerability assessment and penetration testing in a security program. | 16 | BTL5 | Evaluating |
| 14 | Analyze the importance of combining both vulnerability assessment and penetration testing in a security program. | 16 | BTL5 | Evaluating |
| 15 | Explain the differences between network, web application, and wireless penetration tests. | 16 | BTL4 | Analyzing |
| 16 | Analyze the challenges and techniques used in internal versus external penetration testing. | 16 | BTL5 | Evaluating |

| | | | | |
|---|---|---|---|---|
| 17 | Compare and contrast Black Box and White Box penetration testing methodologies. | 16 | BTL4 | Analyzing |

**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–What Web – Net craft–Interacting with DNS Servers

**PART – A**

| Q.No. | Questions | BT Level | Competence |
|---|---|---|---|
| 1 | What is meant by information gathering? | BTL 1 | Remembering |
| 2 | List out the types in information gathering? | BTL 2 | Understanding |
| 3 | Mention the name of tools used to gather information from websites. | BTL 2 | Understanding |
| 4 | Give one example of an active information gathering technique. | BTL 2 | Understanding |
| 5 | What is Passive Information Gathering? | BTL 2 | Understanding |
| 6 | Difference between active and passive information gathering? | BTL 2 | Understanding |
| 7 | List out the various techniques in Passive Information Gathering? | BTL 2 | Understanding |
| 8 | Mention some of the Purpose of the Traceroute Tool. | BTL 2 | Understanding |
| 9 | What are the five sources of data? | BTL 1 | Remembering |
| 10 | What is WHOIS information? | BTL 1 | Remembering |
| 11 | Define the term DNS server. | BTL 1 | Remembering |
| 12 | Differentiate between ICMP traceroute and TCP traceroute? | BTL 2 | Understanding |
| 13 | What is NeoTrace used for? | BTL 2 | Understanding |
| 14 | What protocol does ICMP traceroute use? | BTL 1 | Remembering |
| 15 | Define the term packet sniffing. | BTL 1 | Remembering |
| 16 | Define the purpose of Netcraft in information gathering. | BTL 1 | Remembering |
| 17 | How does Netcraft help in website reconnaissance? | BTL 2 | Understanding |
| 18 | Define the term UDP traceroute. | BTL 1 | Remembering |
| 19 | Mention the various supported methods in traceroute? | BTL 2 | Understanding |
| 20 | What is WhatWeb used for in ethical hacking? | BTL 1 | Remembering |
| 21 | Mention the benefits of Nslookup in information gathering. | BTL 2 | Understanding |
| 22 | Differentiate between TCP and UDP traceroute. | BTL 2 | Understanding |
| 23 | Differentiate between Whatweb and Netcraft. | BTL 2 | Understanding |
| 24 | How does Netcraft help in website reconnaissance? | BTL 2 | Remembering |

| PART – B | | | | |
|---|---|---|---|---|
| **Q.No.** | **Questions** | **Marks** | **BT Level** | **Competence** |
| 1 | Describe how an ethical hacker decides when to use active versus passive information gathering. | 16 | BTL 4 | Analyzing |
| 2 | Discuss about the various source of information gathering? | 16 | BTL 4 | Analyzing |
| 3 | Explain the architecture of ICMP traceroute in detail. | 16 | BTL 3 | Applying |
| 4 | Compare and contrast active and passive information gathering techniques. | 16 | BTL 6 | Create |
| 5 | Describe how traceroute tools assist in identifying network paths and potential vulnerabilities. | 16 | BTL 5 | Evaluating |
| 6 | Discuss limitations and challenges when using traceroute techniques for penetration testing. | 16 | BTL 5 | Evaluating |
| 7 | Explain how WHOIS databases are useful in information gathering | 16 | BTL 3 | Applying |
| 8 | Explain how web reconnaissance tools like Netcraft can aid an ethical hacker. | 16 | BTL 4 | Analyzing |
| 9 | Describe the concepts of TCP Taceout with its working functionalities in detail. | 16 | BTL 4 | Analyzing |
| 10 | Explain how NeoTrace helps in network mapping and information gathering | 16 | BTL 5 | Evaluating |
| 11 | Explain how WhatWeb aids in identifying technologies behind a website. | 16 | BTL 5 | Evaluating |
| 12 | Describe the following<br>i. NSlookup with its functions steps.<br>ii. Netcraft functions. | 8<br>8 | BTL 4 | Analyzing |
| 13 | Explain the importance of traceroute in the reconnaissance phase of ethical hacking. | 16 | BTL 3 | Applying |
| 14 | Describe the role of DNS servers in information gathering.? | 16 | BTL 4 | Analyzing |
| 15 | Explain countermeasures organizations can take to secure their DNS infrastructure. | 16 | BTL 5 | Evaluating |
| 16 | Describe the process and significance of intercepting responses during ethical hacking. | 16 | BTL 4 | Analyzing |
| 17 | Compare ICMP,TCP and UDP traceroute methods and their applications. | 16 | BTL 6 | Create |

## 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 1 | Remembering |
| 2 | How can SNMP passwords be intercepted? | BTL 2 | Understanding |
| 3 | What is the purpose of an SNMP brute force tool? | BTL 2 | Understanding |
| 4 | Mention the name of the tools used for SNMP brute force attack. | BTL 1 | Remembering |
| 5 | How can SNMP passwords be intercepted? | BTL 2 | Understanding |
| 6 | What is meant by SMTP enumeration? | BTL 1 | Remembering |
| 7 | What kind of information can be gathered via SMTP enumeration? | BTL 1 | Remembering |
| 8 | Mention some common uses of SMTP enumeration in ethical hacking. | BTL 2 | Understanding |
| 9 | List out any three types of port scanning techniques. | BTL 2 | Understanding |
| 10 | Define the term SYN scan. | BTL 1 | Remembering |
| 11 | Draw a diagram for TCP three-way handshake. | BTL 2 | Understanding |
| 12 | What is the purpose of a TCP three-way handshake? | BTL 2 | Understanding |
| 13 | Why might an attacker prefer an anonymous scan? | BTL 2 | Understanding |
| 14 | What is an meant by anonymous scan? | BTL 1 | Remembering |
| 15 | Define the term brute force attack. | BTL 1 | Remembering |
| 16 | List out the anonymous scan types? | BTL 1 | Remembering |
| 17 | How the enumeration is different from scanning? | BTL 2 | Understanding |
| 18 | What is meant by OS fingerprinting? | BTL 1 | Remembering |
| 19 | What kind of information does OS fingerprinting reveal? | BTL 1 | Remembering |
| 20 | Define the term stealth scan. | BTL 1 | Remembering |
| 21 | Mention the uses of evade IDS detection. | BTL 2 | Understanding |
| 22 | What is meant by the IDS Evading Techniques? | BTL 1 | Remembering |
| 23 | What is a firewall evasion technique? | BTL 1 | Remembering |
| 24 | What is packet fragmentation in evading firewalls? | BTL 1 | Remembering |

| PART – B | | | | |
|---|---|---|---|---|
| **Q.No.** | **Questions** | **Marks** | **BT Level** | **Competence** |
| 1 | Explain how SNMP enumeration can be used in penetration testing. . | 16 | BTL 3 | Applying |

| | | | | |
|---|---|---|---|---|
| 2 | i. Discuss the limitations of brute force tools in cracking SNMP passwords.<br>ii. Explain why SNMP versions prior to v3 are considered less secure. . | 8<br>8 | BTL 4 | Analyzing |
| 3 | i. Describe the process of sniffing SNMP passwords on a network.<br>ii. Analyze the risks SMTP enumeration poses to organizational security. | | BTL 6 | Create |
| 4 | i. Discuss how SMTP enumeration can lead to identifying valid email addresses.<br>ii. Explain how SMTP enumeration fits into the larger information gathering phase. | 16 | BTL 6 | Create |
| 5 | Explain how brute force attacks work against SNMP community strings. | 16 | BTL 6 | Creating |
| 6 | Discuss how SMTP enumeration can lead to identifying valid email addresses | 8<br>8 | BTL 4 | Analyzing |
| 7 | Explain the steps involved in the TCP three-way handshake. | 16 | BTL 5 | Evaluating |
| 8 | Compare and contrast SYN, TCP connect, and UDP scans | 16 | BTL 6 | Create |
| 9 | i. Describe methods to secure SNMP from unauthorized enumeration.<br>ii. Explain how brute force attacks work against SNMP community strings. | 8<br>8 | BTL 3 | Applying |
| 10 | Discuss the ethical concerns surrounding anonymous scanning techniques | 16 | BTL 4 | Analyzing |
| 11 | Explain the types of port status in TCP three-way handshake? | 16 | BTL 3 | Applying |
| 12 | Explain how OS fingerprinting aids penetration testers in customizing attacks. | 16 | BTL 5 | Evaluating |
| 13 | Explain how packet fragmentation can be used to bypass firewalls. | 16 | BTL 5 | Evaluating |
| 14 | i. Analyze the advantages and disadvantages of different port scanning types.<br>ii. Describe the limitations of anonymous scans. | 8<br>8 | BTL 4 | Analyzing |
| 15 | Analyze how anonymous scans evade detection by IDS/IPS systems. | 16 | BTL 6 | Create |
| 16 | i. How can firewalls be evaded using IP address spoofing?<br>ii. How source routing can be used to evade firewall restrictions? | 8<br>8 | BTL 5 | Evaluating |
| 17 | What are the countermeasures that provide protection against intrusion detection systems and firewalls? | 16 | BTL 4 | Analyzing |

## 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 | Can Nmap be used for port scanning? Justify. | BTL 2 | Understanding |
| 2 | Define vulnerability assessment | BTL 1 | Remembering |
| 3 | What types of vulnerabilities can Nessus detect? | BTL 1 | Remembering |
| 4 | List some important vulnerability scanners. | BTL 2 | Understanding |
| 5 | What kind of reports does Nessus generate? | BTL 1 | Remembering |
| 6 | What is ARP spoofing? | BTL 1 | Remembering |
| 7 | How does an ARP spoofing attack work? | BTL 2 | Understanding |
| 8 | What is packet sniffing? | BTL 1 | Remembering |
| 9 | Mention any two types of sniffing techniques. | BTL 1 | Remembering |
| 10 | Mention some of applications of ARP spoofing. | BTL 1 | Remembering |
| 11 | What is the main goal of a MITM attack? | BTL 1 | Remembering |
| 12 | How can ARP spoofing enable a MITM attack? | BTL 2 | Understanding |
| 13 | What is session hijacking? | BTL 1 | Remembering |
| 14 | Can Wireshark be used to capture session information? Justify. | BTL 2 | Understanding |
| 15 | What kind of information is stored in session cookies? | BTL 6 | Creating |
| 16 | What protocol is commonly used to transmit cookies? | BTL 1 | Remembering |
| 17 | Define the term DHCP spoofing. | BTL 1 | Remembering |
| 18 | What is meant by DNS spoofing? | BTL 1 | Remembering |
| 19 | Differentiate between DNS spoofing and DHCP spoofing | BTL 2 | Understanding |
| 20 | How does DNS spoofing redirect users? | BTL 2 | Understanding |
| 21 | Mention the consequence of a successful DHCP spoofing attack | BTL 1 | Remembering |
| 22 | Does Nessus require credentialed access for scanning? | BTL 2 | Understanding |
| 23 | Can sniffing be legal in some circumstances? Justify. | BTL 2 | Understanding |
| 24 | What is the risk of sniffing session cookies? | BTL 1 | Remembering |

### PART – B

| Q.No | Questions | Marks | BT Level | Competence |
|---|---|---|---|---|
| 1 | Explain how vulnerability scanners help in securing networks. | 16 | BTL 5 | Evaluating |
| 2 | Describe the process of conducting a vulnerability assessment using Nmap. | 16 | BTL 4 | Analyzing |
| 3 | Discuss the advantages and limitations of automated vulnerability scanning. | 16 | BTL 3 | Applying |
| 4 | Describe how Nessus performs vulnerability scanning on a network. | 16 | BTL 3 | Applying |
| 5 | Analyze the role of Nessus in continuous security monitoring. | 16 | BTL 6 | Create |
| 6 | Explain how false positives and false negatives affect Nessus scan results. | 16 | BTL 5 | Evaluating |
| 7 | Explain how sniffing can be used for network troubleshooting and security testing. | 16 | BTL 5 | Evaluating |
| 8 | Describe tools commonly used for sniffing network traffic. | 16 | BTL 4 | Analyzing |
| 9 | Discuss in about ARP spoofing with workflow diagram in detail. | 16 | BTL 4 | Analyzing |
| 10 | Discuss the following<br>(i) Any Two Session hijacking tools.<br>(ii) Concept about DNS spoofing | 8<br>8 | BTL **3** | Applying |
| 11 | Explain the process of conducting a MITM attack using ARP spoofing. | 16 | BTL 4 | Analyzing |
| 12 | Explain how encryption protocols like HTTPS help mitigate MITM risks | 16 | BTL 5 | Evaluating |
| 13 | Analyze how attackers maintain access after hijacking a session. | 16 | BTL 6 | Create |
| 14 | Explain how Wireshark can be used to sniff session cookies on a network. | 16 | BTL 5 | Evaluating |
| 15 | Describe the mechanics of a DNS spoofing attack. | 16 | BTL 4 | Analyzing |
| 16 | Analyze the potential impact of DHCP spoofing on network security | 16 | BTL 6 | Create |
| 17 | Explain the role of DNSSEC and DHCP snooping in mitigating these attacks. | 16 | BTL 3 | Applying |

**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 a remote service in network security. | BTL 2 | Understanding |
| 3 | Give one example of a vulnerability exploited remotely. | BTL 2 | Understanding |
| 4 | What is the goal of attacking network remote services? | BTL 1 | Remembering |
| 5 | Name one protocol commonly targeted by brute force attacks. | BTL 2 | Understanding |
| 6 | What is a meant dictionary attack? | BTL 1 | Remembering |
| 7 | What makes a service vulnerable to brute force attacks? | BTL 2 | Understanding |
| 8 | What is a client-side exploitation? | BTL 1 | Remembering |
| 9 | List out the methods in client side exploitation? | BTL 1 | Remembering |
| 10 | What is phishing in the context of client-side attacks? | BTL 1 | Remembering |
| 11 | Mention the categories for brute force attack. | BTL 2 | Understanding |
| 12 | Define drive-by download attack. | BTL 1 | Remembering |
| 13 | Define privilege escalation. | BTL 1 | Remembering |
| 14 | Name one common technique for privilege escalation | BTL 1 | Remembering |
| 15 | Why is privilege escalation important for attackers? | BTL 2 | Understanding |
| 16 | Define MSFVenom. and write a command for MSFVenom. | BTL 2 | Understanding |
| 17 | State some the role of MSFVenom in penetration testing? | BTL 2 | Understanding |
| 18 | What are importance of Rainbow crack? | BTL 1 | Remembering |
| 19 | What is meant by Rainbow Crack? | BTL 1 | Remembering |
| 20 | What is meant by a Rainbow table? | BTL 1 | Remembering |
| 21 | Define pivoting in ethical hacking. | BTL 1 | Remembering |
| 22 | Name one technique used to discover additional targets on a network | BTL 1 | Remembering |
| 23 | How to identify the further targets? | BTL 2 | Understanding |
| 24 | Why is identifying further targets important after initial compromise? | BTL 2 | Understanding |

**PART – B**

| Q.No | Questions | Marks | BT Level | Competence |
|---|---|---|---|---|
| 1 | Explain the process of remote exploitation in penetration testing. | 16 | BTL 3 | Applying |
| 2 | Discuss common methods used to exploit network remote services. | 16 | BTL 3 | Applying |
| 3 | Analyze the risks posed by poorly secured remote services. | 16 | BTL 6 | Create |
| 4 | Describe how attackers identify vulnerable remote services on a network. | 16 | BTL 5 | Evaluating |
| 5 | Describe how brute force attacks are carried out on network protocols. | 16 | BTL 5 | Evaluating |

| | | | | |
|---|---|---|---|---|
| 6 | Explain methods to detect and prevent brute force attacks on network services | 16 | BTL 3 | Applying |
| 7 | Explain the following<br>(i). How defenders can detect and remove backdoors.<br>(ii). Strengths and weaknesses of different hash algorithms against cracking. | 8<br>8 | BTL 5 | Evaluating |
| 8 | Explain how backdoors are installed and used during a penetration test | 15 | BTL 6 | Creating |
| 9 | Describe the following<br>(i). The features of MSFVenom for generating payloads.<br>(ii). countermeasures to detect and prevent privilege escalation. | 8<br>8 | BTL 3 | Applying |
| 10 | Discuss techniques used to escalate privileges on compromised systems. | 16 | BTL 3 | Applying |
| 11 | Explain the difference between vertical and horizontal privilege escalation. | 16 | BTL 3 | Applying |
| 12 | Discuss ethical considerations when using backdoors in security testing. | 16 | BTL 4 | Analyzing |
| 13 | Explain how hash cracking is performed using rainbow tables. | 16 | BTL 6 | Create |
| 14 | Describe the following<br>(i). The role of pivoting in exploiting multiple targets.<br>(ii). Challenges faced during the exploitation of further targets. | 8<br>8 | BTL 4 | Analyzing |
| 15 | Explain how attackers use cracked hashes to further compromise systems. | 16 | BTL 5 | Evaluating |
| 16 | Describe how attackers identify and prioritize further targets within a network | 16 | BTL 5 | Evaluating |
| 17 | Describe defensive strategies to limit attacker movement after breach. | 16 | BTL 4 | Analyzing |