P.E.S. COLLEGE OF ENGINEERING

(AN AUTONOMOUS INSTITUTE)

CHH. SAMBHAJINAGAR-431002

Regular Summer Examination – 2026

Course: F.Y.M.Tech. **Branch : CSE(Cyber Security)** **Semester : II**

Subject Code & Name: Ethical Hacking, MTPESCS204TB

Max Marks: 60 **Date:06/07/2026** **Duration: 3 Hr.**

Q.1 A) i) Explain the concept of Ethical Hacking and discuss the responsibilities of an ethical hacker. (K2 / CO1) – 06 Marks

Detailed Solution:

Ethical Hacking:

Ethical Hacking is the authorized and legal process of identifying vulnerabilities, weaknesses, and security loopholes in computer systems, networks, applications, and databases. Ethical hackers use the same tools and techniques as malicious hackers, but their objective is to improve system security instead of causing damage.

Ethical hacking helps organizations:

- Prevent cyber attacks
- Protect sensitive data
- Improve network security
- Detect vulnerabilities before attackers exploit them

Ethical hackers are also known as:

- White Hat Hackers
- Security Analysts
- Penetration Testers

Responsibilities of Ethical Hacker:

1. Obtaining Permission

Ethical hackers must obtain written authorization before testing systems.

2. Maintaining Confidentiality

Sensitive information discovered during testing must remain confidential.

3. Identifying Vulnerabilities

The hacker must detect security weaknesses in systems and applications.

4. Reporting Findings

A detailed vulnerability assessment report must be submitted.

5. Avoiding System Damage

Testing should not harm the organization’s systems or data.

6. Following Legal and Ethical Standards

Ethical hackers must comply with cyber laws and professional ethics.

Advantages of Ethical Hacking

- Prevents cyber attacks
- Improves organizational security
- Protects customer information

- Helps in risk management
- Ensures compliance with security policies

Marking Scheme:

Point	Marks
Definition of Ethical Hacking	2
Responsibilities of Ethical Hacker	3
Advantages / Conclusion	1

Q.1 A) ii) Differentiate between Hacking, Ethical Hacking, and Cracking with suitable examples. (K2 / CO1) – 06 Marks

Detailed Solution:

Parameter	Hacking	Ethical Hacking	Cracking
Meaning	Accessing systems or networks	Authorized security testing	Illegal breaking of security
Purpose	May be legal or illegal	Improve security	Cause damage or theft
Permission	Not always	Authorized	Unauthorized
Objective	Gain access	Identify vulnerabilities	Steal or destroy data
Legality	Depends on intent	Legal	Illegal
Example	Accessing a network	Penetration testing	Software piracy

Example:

- Ethical Hacker: Security analyst testing company server.
- Cracker: Attacker stealing banking passwords.
- Hacker: Person exploring systems and networks.

Conclusion:

Ethical hacking is beneficial and legal, while cracking is malicious and illegal.

Marking Scheme:

Point	Marks
Definition of terms	2
Comparison table	3
Examples / Conclusion	1

Q.1 B) i) Describe the five stages of hacking with suitable examples. (K2 / CO1) – 06 Marks

Detailed Solution:

The hacking process generally consists of five stages.

1. Reconnaissance

Information gathering about the target.

Example:

Collecting employee emails and IP addresses.

2. Scanning and Enumeration
Identifying open ports, services, and vulnerabilities.
Example:
Using Nmap for port scanning.

3. Gaining Access
Attacker exploits vulnerabilities to enter the system.
Example:
Using SQL Injection to access database.

4. Maintaining Access
Attacker installs malware or backdoors for future access.
Example:
Installing Trojan horse.

5. Covering Tracks
Deleting logs and hiding activities.
Example:
Removing login records from server logs.

Diagram:
Reconnaissance → Scanning → Gaining Access → Maintaining Access → Covering Tracks

Marking Scheme:

Point	Marks
Explanation of stages	5
Examples / Diagram	1

Q.1 B) ii) Describe different categories of hackers and their roles.
(K1 / CO1) – 06 Marks
Detailed Solution:
Hackers are categorized based on their objectives and ethical behavior.

1. White Hat Hackers
Authorized professionals who improve security.
Role:
Conduct penetration testing.

2. Black Hat Hackers
Malicious hackers performing illegal activities.
Role:
Data theft and malware attacks.

3. Grey Hat Hackers
Hackers working between legal and illegal boundaries.

Role:
Identify vulnerabilities without permission.

4. Script Kiddies
Inexperienced hackers using pre-written tools.
Role:
Launch simple attacks.

5. Hacktivists
Hackers motivated by political or social causes.
Role:
Website defacement and protests.

6. State-Sponsored Hackers
Government-supported cyber attackers.
Role:
Cyber warfare and espionage.

Marking Scheme:

Point	Marks
Explanation of categories	5
Roles / Examples	1

Q.2 A) i) Explain password cracking techniques such as brute force and dictionary attacks. (K2 / CO2) – 06 Marks
Detailed Solution:
Password cracking refers to techniques used to recover passwords from stored data.

1. Brute Force Attack
Trying all possible password combinations.
Advantages:
- Guaranteed success if enough time is available.

Disadvantages:
- Time-consuming.

Example:
Trying combinations like:
1234, 12345, abc123 etc.

2. Dictionary Attack
Uses predefined word lists.
Advantages:
- Faster than brute force.

Example:
Trying passwords from common password database.

3. Rainbow Table Attack

Uses precomputed hash values.

Example:

Matching stored password hashes.

Prevention Methods

- Strong passwords
- Multi-factor authentication
- Password salting
- Account lockout policies

Marking Scheme:

Point	Marks
Brute force explanation	2
Dictionary attack explanation	2
Rainbow table / Prevention	2

Q.2 A) ii) Describe privilege escalation and authentication bypass techniques.
(K2 / CO2) – 06 Marks
Detailed Solution:
Privilege Escalation

Privilege escalation occurs when attackers gain higher access rights than originally permitted.

Types:

1. Vertical Privilege Escalation
2. Horizontal Privilege Escalation

Example:

Normal user gaining administrator access.

Authentication Bypass

Authentication bypass allows attackers to access systems without valid credentials.

Techniques:

- SQL Injection
- Session hijacking
- Weak password exploitation

Example:

Using SQL Injection to bypass login page.

Prevention:

- Strong authentication
- Patch management
- Role-based access control

Marking Scheme:

Point	Marks
Privilege escalation	3
Authentication bypass	2

Point	Marks
Prevention methods	1

Q.3 A) i) Explain SQL Injection attacks with suitable examples.
(K4 / CO3) – 06 Marks
Detailed Solution:
SQL Injection is a web application vulnerability where attackers inject malicious SQL queries into input fields.

Working:
Attacker enters SQL code in login form.
Example:
' OR '1'='1
This bypasses authentication.

Types:
1. Union-based SQL Injection
2. Error-based SQL Injection
3. Blind SQL Injection

Effects:
- Data theft
- Database modification
- Unauthorized access

Prevention:
- Prepared statements
- Input validation
- Parameterized queries

Marking Scheme:

Point	Marks
Definition and working	2
Types and examples	2
Prevention methods	2

Q.4 A) i) Explain port scanning and DNS spoofing attacks.
(K4 / CO4) – 06 Marks
Detailed Solution:
Port Scanning
Port scanning identifies open ports and services on target systems.
Tools:
- Nmap
- Angry IP Scanner

Purpose:

Find vulnerabilities.

DNS Spoofing
Attacker modifies DNS responses to redirect users.
Example:
Redirecting bank website to fake website.

Prevention:
- Secure DNS
- Firewalls
- DNSSEC

Marking Scheme:

Point	Marks
Port scanning explanation	3
DNS spoofing explanation	2
Prevention	1

Q.5 A) Explain private key and public key cryptography. Describe digital signatures and digital certificates.
(K2 / CO5) – 12 Marks
Detailed Solution:
1. Private Key Cryptography
Also called symmetric encryption.
Same key is used for encryption and decryption.
Example:
AES, DES
Advantages:
- Fast encryption

Disadvantages:
- Key distribution problem

2. Public Key Cryptography
Uses two keys:
- Public key
- Private key

Example:
RSA
Advantages:
- Better security

Disadvantages:
- Slower than symmetric encryption

3. Digital Signature
Used to verify authenticity and integrity.
Working:

1. Sender creates hash
2. Encrypts with private key
3. Receiver verifies using public key

4. Digital Certificate

Electronic document verifying identity.

Components:

- Owner name
- Public key
- Certificate authority signature

Applications:

- Secure communication
- SSL/TLS
- E-commerce

Marking Scheme:

Point	Marks
Private key cryptography	3
Public key cryptography	3
Digital signature	3
Digital certificate and applications	3