1. Define Ethical Hacking and Penetration Testing.

Answer:

- **Ethical Hacking:** It's the act of legally and responsibly **finding security weaknesses** in a system or network with the **permission of the owner**. The goal is to fix vulnerabilities before malicious hackers can exploit them. It's like a controlled attack to improve security.
- **Penetration Testing (Pen Testing):** This is a **specific, structured method** used to perform ethical hacking. Penetration testing is a planned and safe way to test a computer system's security. It acts like a real cyber attack to find weak points, so they can be fixed before hackers can use them.

2. What are the main differences between White Hat, Black Hat, and Gray Hat hackers?

Answer:

Hacker Type	Primary Motivation	Legality	Goal
White Hat	Security, Good	Legal (with permission)	Defend systems, find and fix flaws.
Black Hat	Malicious, Personal gain	Illegal	Steal data, cause damage, profit illegally.
Gray Hat	Curiosity, Ego	Sometimes illegal (no permission)	Find flaws without permission, but may inform the owner (sometimes for a fee).

- **White Hat:** Always acts ethically and legally to help organizations.
- **Black Hat:** Acts maliciously for personal gain or damage.
- **Gray Hat:** Acts without permission but without clear malicious intent; operates in a legal grey area.

3. Explain the five phases of Penetration Testing in sequence.

Answer:

The process is typically divided into five steps:

1. **Reconnaissance (Information Gathering):** In this step, information is collected about the target from public sources like websites and social media. The goal is to understand how the system works and find possible weak areas that can be tested later.
2. **Scanning:** Here, special tools are used to check which computers or servers are active and what ports or services are open. This helps find possible entry points that might be unsafe.
3. **Gaining Access:** the tester tries to enter the system by using weak passwords or software problems found during scanning. This shows how an attacker could get inside the system.
4. **Maintaining Access:** Installing backdoors or configuring the system to ensure the hacker can return later, simulating a long-term threat actor.
5. **Covering Tracks (Analysis & Reporting):** In real hacking, attackers hide their activities. But in a pen test, testers write a report explaining what they did, what they found, and how to fix the issues. The system is then returned to its normal state.

6. What is Digital Forensic ?

Digital Forensics is the scientific method of **preservation**, **collection**, **validation**, **identification, analysis, interpretation, documentation,** and **presentation** (Pretty Cats Visit In An Interesting Dark Place) of digital evidence derived from digital devices.

Purpose :

Digital forensics helps find out what happened during a crime by studying digital evidence. It also helps to prevent or detect any unauthorized activities that could harm normal operations.

☐ What is Digital Evidence ?

Digital Evidence refers to any data that is -

- recorded or stored on a computer system or any digital device.
- can be read, viewed and interpreted by a person or another computer system.
- includes a display, printout or other output of that data.

☐ Characteristics of Digital Evidence

An evidence must be:

- **Admissible :** It must follow the legal rules so it can be used in court.
- **Authentic :** must have a clear connection of specific individuals, devices, or events with data

- **Fragile :** Easily altered, damaged, or destroyed
- **Accurate:** Must be reliable and consistent
- **Complete:** must show the whole story of particular circumstances.
- **Convincing to juries :** It should be strong enough to make judges or juries believe it is true.

☐ Examples of Digital Evidence

- ✓ e-mails,
- ✓ digital photographs,
- ✓ ATM transaction logs,
- ✓ word processing documents,
- ✓ Instant message histories,
- ✓ files saved from accounting program,
- ✓ spreadsheets,
- ✓ internet browser histories,
- ✓ databases,
- ✓ the contents of computer memory,
- ✓ computer backups, computer printouts,
- ✓ Global Positioning System tracks,
- ✓ logs from a hotel's electronic door locks, and
- ✓ digital video or audio files

☐ Types of Digital Evidence :

There are 2 types of digital evidence :

1. **Persistent Data :** it is the type of data that stays intact on a digital device even after it is turned off. It remains stored until it is manually deleted or overwritten. Common examples include data saved on hard drives, disk drives, USB drives, and flash drives.

2. **Volatile Data :** it is temporary data that is lost when a digital device is turned off. It only exists while the system is running. Examples include deleted files, computer history, system registry entries, temporary files, and web browsing history.

☐ Digital Forensic Software Tools

- ***BACKTRACK 5R3*** (Linux operating system)-This OS has **many forensic tools** to analyze any compromised system or find security holes
  - ✓In that a large amount of open source bundled packages are installed in this OS.

- ***Kali Linux*** is a Debian-derived Linux distribution designed for **digital forensics** and **penetration testing**

✓It was developed through the rewrite of Backtrack 5, their previous forensics Linux distribution.