Module 3: CS – Cyber Threats & CEH

1. What are the different types of hacking methods?

Hacking methods are techniques used to exploit weaknesses in systems or users.

- Phishing: Deceiving users to reveal credentials.
- Malware-based attacks: Using malicious software to gain access.
- SQL Injection: Manipulating database queries.
- Man-in-the-Middle (MITM): Intercepting communications.
- DoS/DDoS: Disrupting service availability.
- Password attacks: Targeting weak or reused passwords.

2. Explain Types of Password Attacks

Password attacks attempt to obtain passwords through various methods.

- Brute Force Attack: Tries all combinations.
- Dictionary Attack: Uses common password lists.
- Rainbow Table Attack: Uses precomputed hashes.
- Credential Stuffing: Reuses leaked credentials.
- Keylogging (conceptual): Capturing keystrokes to learn passwords.

3. Explain Password Cracking Tools: pwdump7, Medusa and Hydra

These tools are discussed at a high level for defensive learning only.

- pwdump7: Extracts password hashes from Windows systems for audit purposes.
- Medusa: Parallel login testing tool supporting multiple protocols.
- Hydra: Network login testing tool supporting services like SSH and FTP.

Ethical use requires written authorization and is performed to assess security.

4. Explain Types of Steganography with QuickStego and Echo

Steganography hides information within other media.

- Image Steganography: Hiding data in images (e.g., QuickStego conceptually).
- Audio Steganography: Hiding data in sound files.
- Text Steganography: Concealing messages in text (e.g., Echo-based concepts).

Used for watermarking and secure communication awareness.

5. Perform Practical on Key Logger Tool

Practical work is explained theoretically for safety and ethics.

Objective: Understand how keylogging threats work and how to defend against them.
Theory: Keyloggers capture keystrokes via malware or compromised software.
Defense: Updated antivirus, OS hardening, application whitelisting, and user awareness.
Outcome: Ability to detect and prevent keylogging threats.

Malware

1. Define Types of Viruses

Computer viruses are malicious programs that replicate and spread.

- File Infector Virus
- Boot Sector Virus
- Macro Virus
- Polymorphic Virus
- Resident Virus

2. Create virus using HTTP RAT Trojan tool

For ethical and legal reasons, this topic is explained conceptually only.

Theory: RAT Trojans allow remote control of infected systems.
Use in CEH: Studied to understand attacker techniques and improve defenses.
Prevention: Network monitoring, endpoint protection, and user training.

3. Explain any one Antivirus with example

Example: Windows Defender Antivirus

Windows Defender provides real-time protection against malware.
Example: If a malicious file is downloaded, Defender scans, quarantines, and alerts the user, preventing system damage.