Module 3: CS - Cyber threats & CEH

1. What are the different types of hacking methods?

Hacking is the unauthorized access to a computer system or network. There are various methods used by hackers to achieve their goals. Here are some common types:

- **Phishing:** This involves tricking users into clicking on malicious links or downloading attachments that contain malware.
- **Social engineering:** Hackers exploit human psychology to manipulate users into revealing sensitive information or performing actions that benefit the attacker.
- **Brute force attacks:** This involves trying different combinations of passwords until the correct one is found.
- **Dictionary attacks:** Similar to brute force, but instead of random combinations, the attacker uses a list of common words or phrases.
- **SQL injection:** This attack exploits vulnerabilities in web applications to execute malicious SQL code.
- **Man-in-the-middle attacks:** The attacker intercepts communication between two parties to eavesdrop or modify data.
- **Denial of service (DoS) attacks:** This involves overwhelming a system with traffic to prevent legitimate users from accessing it.

2. Explain Types of Password Attacks

Password attacks are attempts to compromise a user's password to gain unauthorized access to a system. Here are some common types:

- **Brute force attacks:** As mentioned earlier, this involves trying every possible combination of characters.
- **Dictionary attacks:** Uses a list of common words or phrases to guess passwords.
- **Hybrid attacks:** Combines brute force and dictionary attacks to increase the chances of success.
- **Rainbow table attacks:** Pre-computed tables of encrypted passwords are used to quickly crack them.
- **Keylogging:** This involves recording keystrokes to capture passwords and other sensitive information.

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

These tools are used to crack passwords by attempting various combinations or using pre-computed tables.

- **pwdump7:** A Windows password dumper that can extract hashes from the SAM database.
- **Medusa:** A flexible password cracker that supports various protocols and can be used for brute force and dictionary attacks.
- **Hydra:** A similar tool to Medusa, but with a different interface and features.

4. Explain Types of Steganography with QuickStego and Echo

Steganography is the practice of hiding information within other data. Here are some common types:

- **LSB steganography:** This involves modifying the least significant bits of image pixels to hide data.
- **Text steganography:** Data is hidden within text by changing character spacing or using specific words or phrases.
- **Audio steganography:** Data is hidden within audio files by modifying the amplitude or frequency.

QuickStego and **Echo** are examples of steganography tools that can be used to hide data within images or audio files.

5. Perform Practical on key logger tool.

Malware

1. Define Types of Viruses.

Viruses are malicious software that can infect a computer system and cause damage. Here are some common types:

- **Boot sector viruses:** Infect the master boot record of a disk.
- **File infector viruses:** Infect executable files.
- **Macro viruses:** Infect documents that contain macros.
- **Polymorphic viruses:** Change their code to avoid detection.
- **Worms:** Self-replicating malware that spreads through a network.
- **Trojans:** Malicious programs disguised as legitimate software.

2. Create virus using Http Rat Trojan tool.

Http Rat Trojan is a tool that can be used to create remote access trojans (RATs). These trojans allow attackers to control infected systems remotely.

3. Explain any one Antivirus with example

Antivirus software is used to detect and remove malware. One example is **Avast Free Antivirus**. It scans files and systems for viruses and other threats, and provides real-time protection.