Module 3: CS - Cyber threats & CEH

1. What are the different types of hacking methods?

Ans:

- **Phishing**
  Tricking people into giving personal info by fake emails or websites.
- **Malware**
  Using malicious software like viruses or ransomware to damage or control computers.
- **Brute Force Attack**
  Trying many passwords quickly until the right one is found.
- **SQL Injection**
  Injecting harmful code into websites to steal or change data.
- **Man-in-the-Middle (MITM) Attack**
  Intercepting communication between two parties to steal information.
- **Denial of Service (DoS) Attack**
  Overloading a website or server to make it stop working.
- **Password Cracking**
  Using tools to guess or decrypt passwords.
- **Social Engineering**
  Manipulating people to reveal confidential info, like pretending to be someone trustworthy.

2. Explain Types of Password Attacks ?

Ans:

1. **Brute Force Attack**

- Trying every possible password combination until the right one is found.
- It’s like guessing every key on a keychain until one opens the lock.

2. **Dictionary Attack**

- Using a list of common words and passwords to guess the password.
- Instead of random guesses, it tries words like "password," "123456," or "admin."

3. **Credential Stuffing**

- Using stolen username and password pairs from one site to try logging into other sites.

- Happens because many people reuse passwords.

4. **Phishing**

- Tricking people into giving their passwords by fake emails or websites.
- Example: A fake bank email asking you to enter your password.

5. **Keylogger Attack**

- Installing software or hardware that records everything you type, including passwords.
- The attacker then collects these keystrokes secretly.

6. **Password Spraying**

- Trying a few common passwords on many accounts to avoid account lockouts.
- Unlike brute force, it tries fewer passwords but on many users.

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

Ans:

1. pwdump7

- **What it does:**
  It extracts (dumps) **password hashes** from **Windows systems**.
- **Used for:**
  Getting password data from the Windows **SAM (Security Account Manager)** database.
- **Example Use:**
  Ethical hackers use it to test if Windows systems store passwords securely.

2. Medusa

- **What it does:**
  It is a **fast, parallel, and modular brute-force tool**.
- **Used for:**
  Cracking **remote login passwords** over various protocols like **SSH, FTP, HTTP, Telnet**, etc.
- **Features:**
  - Fast and supports multiple targets
  - Tries many passwords on many user accounts
- **Example Use:**
  To test the strength of login credentials on a network.

3. Hydra (THC-Hydra)

- **What it does:**
  Hydra is one of the **most powerful password cracking tools** for **online login services**.
- **Used for:**
  Cracking usernames and passwords over **network protocols** like **FTP, HTTP, SSH, SMTP, Telnet, RDP**, and more.
- **Features:**
  - Supports many protocols
  - Flexible and fast
  - Can run attacks using **wordlists** (dictionary attack)
- **Example Use:**
  To test login security on a company's web server.

4. Explain Types of Steganography with QuickStego and Echo

Ans:

Types of Steganography:

1. **Image Steganography**
   - Hiding text or data inside an image file (like .jpg or .png) by changing pixels slightly.
2. **Audio Steganography**
   - Hiding data in audio files by modifying sound waves in a way that the human ear can't detect.
3. **Video Steganography**
   - Hiding information in video files by altering frames or sound.
4. **Text Steganography**
   - Hiding messages inside text by using spaces, special characters, or letter patterns.
5. **Network Steganography**
   - Hiding data in network traffic like IP headers or unused bits in packets.

QuickStego:

- **Type:** Image Steganography Tool
- **What it does:** Hides text inside **image files (like .bmp or .jpg)**.
- **Use:** Easy to use — just insert the text, choose an image, and save it. No one can see the hidden message in the image.
- **Purpose:** For beginners to learn how data can be hidden in images.

Echo:

- **Type:** Audio Steganography Tool
- **What it does:** Hides secret messages inside **audio files** using small echo delays.
- **Use:** You can hide a message in a song or sound file, and it will sound the same to human ears.
- **Purpose:** To secretly transmit information through audio.

6. Perform Practical on key logger tool

Ans:

A keylogger **secretly saves what you type**, like usernames, passwords, and messages. It is often used by **hackers** to steal information, but it can also be used legally by parents or companies to monitor computer activity.

Example:

If you type your password into a login page, a keylogger running in the background can **record and save that password** without you knowing.

Malware

1. Define Types of Viruses.

Ans:

A **computer virus** is a type of **malicious software (malware)** that spreads from one computer to another and can damage files, steal data, or slow down the system.

Common Types of Viruses:

1. **File Infector Virus**
   Attaches itself to files (like .exe) and spreads when the file is opened.
   Example: Infects games or apps.
2. **Macro Virus**
   Targets programs like **MS Word or Excel**, using macros (scripts).
   Example: Opens when you view a Word document with the virus.
3. **Boot Sector Virus**
   Infects the boot sector of hard drives or USBs and loads before the operating system.
   Effect: Hard to remove, can stop the system from booting.
4. **Polymorphic Virus**
   Changes its code every time it runs, making it hard for antivirus to detect.
5. **Resident Virus**
   Hides in the computer's memory and infects files as they open or close.
   Effect: Keeps running even after removing infected files.
6. **Direct Action Virus**
   Activates when the infected file is run, then spreads quickly and stops.
   Example: Less harmful and easier to remove.
7. **Multipartite Virus**
   Attacks in multiple ways (boot sector + files), making it dangerous and fast-spreading.
8. **Web Scripting Virus**
   Infects through websites using malicious scripts (JavaScript, HTML).
   Example: Can steal cookies or redirect users.
9. **Overwrite Virus**
   Deletes or replaces the content of a file completely.
   Effect: File becomes unusable.
10. **Logic Bomb**
    Activates only when certain conditions are met (like a date or action).
    Example: Deletes data on a specific date.

2. Create virus using Http Rat Trojan tool.

3. Explain any one Antivirus with example.

Ans:

An **antivirus** is a software program designed to **detect, prevent, and remove** malicious software like viruses, worms, trojans, spyware, and ransomware from your computer or device.

It acts like a **security guard** for your system, watching for any suspicious activity and blocking it before damage is done.

Example: Quick Heal Antivirus

Quick Heal is a popular antivirus software developed in India. It provides **real-time protection** and regularly scans your system for threats.

Features:

- Real-time virus and malware protection
- Web security to block unsafe websites
- Email protection from spam and phishing
- Firewall to block unauthorized access
- Ransomware protection

Example Use:

If you download a file from the internet, Quick Heal will automatically **scan it**. If the file contains a virus, it will **alert you** and **quarantine or delete** the threat.