Module 3: CS - Cyber threats & CEH

1. **What are the different types of hacking methods?**

   Ans: -

   - Phishing:
   - Malware (viruses, trojans, worms):
   - Ransomware:
   - Brute-force attacks:
   - Social engineering:
   - SQL Injection:
   - Cross-Site Scripting (XSS):
   - Man-in-the-Middle (MitM):
   - Zero-day exploits:
   - DDoS (Distributed Denial of Service):

2. **Explain Types of Password Attacks**

   Ans: -

   - Brute-force attack
   - Dictionary attack
   - Credential stuffing
   - Password spraying
   - Rainbow table attack
   - Offline hash cracking
   - Keylogging
   - Phishing (credential theft)
   - Shoulder surfing
   - Man-in-the-Middle (credential interception)

3. **Explain Password Cracking Tools: pwdump7,Medusa and Hydra**
   Ans: -
   - pwdump7
     - A Windows tool that extracts password hashes from the local SAM/LSA storage for analysis.
     - Used by admins for offline auditing and by attackers to obtain hashes — protect by enforcing least privilege and patching systems.

   - Medusa
     - A speedy, modular network login brute-forcer that tests credentials across many protocols.
     - Valuable for penetration testers checking weak accounts, but dangerous if misused — mitigate with rate-limiting and strong passwords.

   - Hydra (THC Hydra)
     - A popular parallelized login cracker that supports many services and authentication methods.
     - Common in security assessments to find weak credentials; defend against it with MFA, account lockouts, and monitoring.
     -

4. **Explain Types of Steganography with QuickStego and Echo**
   Ans: -
   - **Image steganography**
     - **Hides data inside images by subtly altering pixels or metadata so changes aren't visible.**
   - **Audio steganography**
     - **Embeds information in sound files by altering imperceptible audio samples or metadata.**
   - **Video steganography**
     - **Hides data across frames or in the container metadata of videos for large-capacity covert channels.**
   - **Text steganography**
     - **Conceals messages using formatting, spacing, synonyms, or intentional typos in plain text.**

- **QuickStego (tool)**
  - **A simple Windows application that embeds small text messages into image files for basic steganography.**
- **Echo (tool)**
  - **A steganography utility (often command-line or lightweight GUI) that hides data inside files or containers using common encoding methods.**

5. Perform Practical on key logger tool

● Malware

1. Define Types of Viruses.

Ans: -

1. File Infector Virus
   - Definition: Infects executable files (like .exe, .com) by attaching malicious code.
2. Boot Sector Virus
   - Definition: Infects the boot sector of storage devices (like hard drives or USB drives).
3. Macro Virus
   - Definition: Written in macro languages (like MS Word or Excel macros) and infects documents.
4. Polymorphic Virus
   - Definition: Changes its code each time it infects a new file, making it hard to detect.
5. Resident Virus
   - Definition: Loads itself into a computer's memory and remains active even after the infected file is closed.
6. Stealth Virus
   - Definition: Hides its presence by intercepting system requests and showing clean data to antivirus software.
7. Worm (Self-replicating Virus)
   - Definition: Replicates itself without needing to attach to files.

8. Trojan Horse

- Definition: Disguised as a legitimate program but performs malicious actions.

2. Create virus using Http Rat Trojan tool.

Ans: -

3. Explain any one Antivirus with example.

Ans: -

1. Definition:

Antivirus software is a program designed to detect, prevent, and remove malicious software (viruses, worms, trojans, etc.) from a computer or device.

2. Example: Avast Antivirus

Avast Antivirus is one of the most popular antivirus programs developed by Avast Software.
It provides real-time protection against various types of malware, phishing attacks, and network threats.

3. Features of Avast Antivirus:

1. 🛡️ Real-Time Protection:
   Continuously monitors your computer for viruses and suspicious activities.
2. 🧠 Smart Scan:
   Scans the entire system for malware, outdated software, and network issues.
3. 🌐 Web Shield:
   Protects users from harmful websites, fake downloads, and phishing links while browsing.

4. Example of Use:

Suppose you download a file from the internet that contains a Trojan virus.
When you open the file, Avast Antivirus automatically detects and blocks the threat, showing a warning message and moving the infected file to the Virus Chest (a quarantine area).

5. Conclusion:

Avast Antivirus helps users keep their systems safe by detecting and removing malicious software in real-time, providing strong protection against modern cyber threats.