**Module : 5 Information Gathering And Malware**

1. What Are the Different Types of Hacking Methods?

1. Phishing: Deceiving users into revealing sensitive information via fake websites or emails.
2. Man-in-the-Middle (MITM): Intercepting and altering communication between two parties.
3. SQL Injection: Injecting malicious SQL queries to manipulate databases.
4. Cross-Site Scripting (XSS): Injecting scripts into web pages to steal user data.
5. Denial of Service (DoS) and Distributed DoS (DDoS): Overloading servers to disrupt services.
6. Brute Force Attack: Guessing passwords through exhaustive attempts.
7. Social Engineering: Manipulating individuals to divulge confidential information.
8. Keylogging: Recording user keystrokes to capture credentials.

2. Explain Types of Password Attacks

1. Brute Force Attack: Trying every possible combination of characters.
2. Dictionary Attack: Using a pre-defined list of commonly used passwords.
3. Credential Stuffing: Using leaked username-password pairs from previous breaches.
4. Keylogger Attack: Capturing keystrokes to steal passwords.
5. Phishing: Tricking users into entering passwords on fake websites.
6. Rainbow Table Attack: Using precomputed hash values to find passwords.
7. Shoulder Surfing: Observing someone entering their password physically.

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

1. pwdump7:
   * Extracts hashed passwords from the Windows SAM (Security Account Manager) file.
   * Useful for recovering lost passwords.
2. Medusa:
   * A fast, parallel, and modular brute-forcing tool.
   * Supports multiple protocols, such as SSH, HTTP, and FTP.
3. Hydra:
   * A powerful and widely used brute-forcing tool.
   * Can crack passwords over multiple services like Telnet, SSH, and RDP.

4. Explain Types of Steganography with QuickStego and Echo

Types of Steganography:

1. Text Steganography: Hiding data in text files.
2. Image Steganography: Embedding data in images by altering pixel values.
3. Audio Steganography: Hiding data within audio files.
4. Video Steganography: Embedding data into video streams.

Tools:

* QuickStego:
  + Simple tool for hiding text inside images.
  + Example: Embed confidential information in a .jpg file.
* Echo:
  + A tool for audio steganography that hides data in sound files.

5. Perform Practical on Keylogger Tool

Steps Using a Keylogger Tool (e.g., Spyrix Free Keylogger):

1. Install the tool on the target system (requires physical access or social engineering).
2. Configure the tool to start on boot.
3. Enable logging and specify storage location for logs.
4. Retrieve captured keystrokes from the logs.  
   *Note:* Only perform practicals ethically in controlled environments.

Malware

1. Define Types of Viruses

1. File Infector Virus: Attaches to executable files and spreads when the file is run.
   * Example: Melissa Virus.
2. Boot Sector Virus: Infects the boot sector of storage drives.
   * Example: Michelangelo Virus.
3. Macro Virus: Targets files with macros, like MS Word documents.
   * Example: Concept Virus.
4. Polymorphic Virus: Alters its code to evade detection.
   * Example: Storm Worm.
5. Resident Virus: Resides in memory and infects files when executed.
   * Example: Randex Virus.

2. Create Virus Using HTTP RAT Trojan Tool

1. Download and install a Remote Access Trojan (RAT) tool, like HTTP RAT.
2. Configure the server by setting up the listening port and attacker IP address.
3. Generate a malicious executable or link.
4. Deliver the payload to the target through phishing.
5. Access the victim’s system remotely once the payload is executed.  
   *Note:* Use only in a virtual lab or testing environment, as malicious use is illegal.

3. Explain Any One Antivirus with Example

* Antivirus Example: Norton Antivirus
  + Detects and removes malware like viruses, worms, and ransomware.
  + Uses signature-based and behavior-based detection methods.
  + Example Use Case: Preventing the spread of the WannaCry ransomware by detecting its payload.