Module 3: CS - Cyber threats & CEH

1.  **Social Engineering**: Phishing, pretexting, baiting.

 **Exploiting Vulnerabilities**: SQL Injection, XSS, Zero-Day Exploits.

 **Malware**: Ransomware, Trojans, Spyware, viruses.

 **Interception & Eavesdropping**: Man-in-the-Middle, packet sniffing, DNS spoofing.

 **Denial of Service**: DDoS, DoS.

 **Privilege Escalation**: Gaining higher access privileges.

2.Brute Force Attack

Rainbow table Attack

Phishing

Keylogging

Dictionary Attack

3.Pwdump7:Pwdump7 is a tool used to extract password hashes from Windows systems.

Medus: Medusa is a powerful, multi-threaded brute force password-cracking tool used for testing the strength of remote authentication services.

Hydra: Hydra is another well-known brute-force cracking tool designed to perform rapid password cracking for various network services.

4.Types of Steganography

Image Steganography

AudioSteganography

VideoSteganography

TextSteganography

Network Steganography

File system Steganography

QuickStego is a simple and user-friendly tool designed for hiding text messages inside image files (specifically BMP files). It allows users to embed a secret message into the image without affecting its appearance significantly.

Echo is an audio-based steganography tool used to hide messages within audio files. It primarily uses an **echo hiding** technique, where an inaudible echo is added to the audio file to encode hidden data.

● Malware

1. File Infector Virus

Description: This type of virus attaches itself to executable files (such as .exe, .com, or .bat files) and spreads when the infected file is executed.

Macro Virus

Description: Macro viruses infect documents that contain macros (such as Word or Excel files). These viruses exploit the macro functionality of office programs to execute malicious code when the document is opened.

Boot Sector Virus

Description: This type of virus infects the boot sector of a computer's hard drive or USB drive. The boot sector is a part of the drive that contains the information necessary to start the operating system.

Polymorphic Virus

Description: Polymorphic viruses are designed to change their code each time they infect a new system. This makes it harder for antivirus software to detect the virus using traditional signature-based detection.

Metamorphic Virus

Description: Similar to polymorphic viruses, metamorphic viruses change their code every time they infect a system. However, unlike polymorphic viruses, they completely rewrite themselves each time, making them even harder to detect.

Resident Virus

Description: A resident virus infects a computer's memory and can remain active even after the original program or file has been closed.

Non-Resident Virus

Description: A non-resident virus does not stay in the system’s memory. Instead, it attaches itself to a file or program and becomes active when that file or program is executed.

Multipartite Virus

Description: Multipartite viruses combine multiple infection strategies, making them versatile and hard to defend against. They may infect the system through file infectors, boot sector viruses, and more.

2. **Kaspersky Anti-Virus**

**Overview:** Kaspersky Anti-Virus is a popular and widely used antivirus software developed by **Kaspersky Lab**, a Russian cybersecurity company. It provides real-time protection against various types of malware, including viruses, worms, trojans, ransomware, spyware, and other malicious software. Kaspersky is known for its high detection rates, advanced threat protection, and minimal system impact.