Module : 30 Malware And Threat Detection

1) 8 are the different types of hacking methods.

- Phishing
- Malware Attacks
- SQL Injection
- Man-in-the-Middle (MITM) Attacks
- Denial of Service (DoS) Attacks
- Brute Force Attacks
- Social Engineering
- Zero-Day Exploits

2) 10 Types of Password Attacks

- Brute Force Attack
- Dictionary Attack
- Credential Stuffing
- Keylogger Attack
- Phishing
- Rainbow Table Attack
- Shoulder Surfing
- Man-in-the-Middle (MITM) Attack
- Password Spraying
- Social Engineering

3) pwdump7

- Purpose: Extracts password hashes from the Security Account Manager (SAM) database on Windows systems.
- How It Works: It retrieves hashed passwords stored in the SAM file, which can then be cracked using tools like Ophcrack or rainbow tables.
- Use Case: Often used in penetration testing to assess password strength.
- Key Feature: Requires administrative privileges to access the SAM file.
- Medusa
- Purpose: A fast, multi-threaded brute-force tool for cracking passwords across various protocols.
- Supported Protocols: FTP, SSH, HTTP, RDP, MySQL, and more.
- How It Works: Medusa attempts multiple username-password combinations in parallel, making it efficient for large-scale testing.
- Use Case: Used by security professionals to identify weak or default passwords in systems.
- Key Feature: Modular design allows easy addition of new protocols.
- Hydra
- Purpose: A highly flexible and parallelized login cracker for network services.

- Supported Protocols: Over 50 protocols, including Telnet, FTP, HTTP, HTTPS, SMB, and databases.
- How It Works: Hydra performs rapid dictionary or brute-force attacks to crack login credentials.
- Use Case: Commonly used in penetration testing to demonstrate vulnerabilities in authentication systems.
- Key Feature: Supports both single-target and multi-target attacks.

4) Types of Steganography

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Network Steganography
- QuickStego
- QuickStego is a tool specifically designed for image steganography. It allows users to hide text within image files. The hidden text is imperceptible to the human eye, and the image can still be shared or uploaded like any normal picture.
- Echo Steganography
- Echo steganography is a technique used in audio steganography. It embeds secret messages by introducing echoes into an audio signal. The delay and amplitude of the echoes encode the hidden data.

5) Types of Viruses

- File Infector Virus
- Macro Virus
- Boot Sector Virus
- Polymorphic Virus
- Resident Virus
- Multipartite Virus
- Ransomware (a type of virus)
- Email Virus
- Logic Bomb
- Worms (closely related to viruses)

6) Antivirus Software: Avast Antivirus

- Avast Antivirus is a popular cybersecurity tool designed to detect, prevent, and remove malware, viruses, and other malicious threats. It provides real-time protection for individuals and businesses.