# SUB:- CYBER SECURITY

## UNIT 3:- TOOLS AND METHODS USED IN CYBERCRIME

Prof:- Morade D.S.

## INTRODUCTION:-

Various tools and techniques used to launch attacks against the target These attack goes through certain stages as mentioned below:-

1] Reconnaissance:-

It is an information collecting stage where in the basic information about the victim is being collected by the various social network websites by applying social site engineering.

2] Scanning:

An attackers scan the information received and decided target by applying analytical techniques.

3] Gaining Access:-

After identification of weak victim from the latest stage their credintials & their details are being accessed in this stage include confidential data, personal information etc.,

4] Maintaining Access:-

In which attacker remains connected to victim system's network in order to capture desired information and activities.

5] Covering Tracks :-

After achieving objective of attack , the attackers attempt to erase the footprints and evidences of attack from the network.

## 2. PROXY SERVERS AND ANONYMIZERS:-

### Proxy Server

A **proxy server** is a computer (or system) that acts as a **middleman** between your device and the internet.

When you use a proxy:

- Your device sends a request to the **proxy server**.
- The proxy forwards the request to the website.
- The website sends data to the **proxy**, and the proxy sends it back to **you**.

**Purpose:**

- Hides your real **IP address**.
- Can be used to **access blocked websites**.
- Helps **control and monitor internet use** in schools or offices.

---

**Example:**

You want to visit a website (e.g., www.example.com), but your school has blocked it.

- Normally:
  Your computer → Website (Blocked □)
- Using Proxy:
  Your computer → **Proxy Server** → Website
  Website thinks the request is from **proxy**, not from **you** → Access allowed □

---

### Anonymizer

An **anonymizer** is a tool or service that **completely hides your identity** while you browse the internet.

It's more powerful than a proxy because it hides:

- Your **IP address**
- Your **location**
- Your **browser and device info**

It makes it **very hard** for websites or hackers to track you.

**Example:**

You are in India and want to access a US-only website.

- You use an **anonymizer** like the **Tor browser**.
- Tor changes your IP address to look like you're in the US.
- The website thinks you're a US user and allows access.

You stay anonymous.
The website doesn't know your real location or identity.

## **PHISHING**

Phishing is a **cybercrime** where attackers try to **trick you into giving personal information** like:

- Passwords
- Credit card details
- Bank account numbers
- OTPs (One-Time Passwords)

They usually do this by pretending to be **trusted sources** like banks, government, or known companies.

Phishing is a **cybercrime** where attackers **trick people into giving private information** like passwords, OTPs, or bank details — by pretending to be **trusted companies** or people (like banks, friends, or senior staff).

### **How Does Phishing Work?**

Includes: **Planning, Setup, Attack, Collection, Identity Theft & Fraud**

### **1. Planning**

The attacker decides:

- **Whom to target** (individuals, banks, companies)
- What kind of **data to steal** (passwords, credit card info, etc.)

□ *Example:*
Planning to trick students into giving university portal login details.

### 2. Setup

The attacker creates:

- **Fake websites**, emails, or SMS
- Copies the design of trusted platforms (e.g., SBI, Amazon)

□ *Example:*
Making a fake Gmail login page that looks real.

### 3. Attack (Luring the Victim)

The attacker **sends messages** via:

- Email, SMS, or call
- Makes it look **urgent or important**

□ *Example:*

“Your bank account will be blocked in 24 hours. Click here to update KYC.”

### 4. Data Collection

Once the victim clicks the link and enters info:

- Attacker **captures the sensitive data**
  - Username, password
  - OTP, card details

□ *Example:*
User enters ATM PIN on a fake page thinking it's a real bank website.

### 5. Identity Theft and Fraud

Now the attacker **uses the stolen data** to:

- **Withdraw money**
- **Make online purchases**
- **Access email or banking accounts**
- **Steal identity** to commit further crimes

□ *Example:*
Using your card details to buy expensive items or apply for loans in your name.

- **Phishing Techniques**

**A) Email Phishing**

- Fake emails that look like they're from real banks, apps, or websites.
- Its most common techniques

□ *Example:*

"Your SBI account is blocked. Click here to verify."

**B) SMS Phishing (Smishing)**

- SMS with fake messages and links.
- Tries to scare or lure you to click.

□ *Example:*

"Your bank KYC is incomplete. Click the link to avoid blocking."

---

**C) Voice Phishing (Vishing)**

- Calls pretending to be from banks or authorities.

□ *Example:*

"We are from RBI. Share your OTP to verify your card."

---

**D) Spear Phishing**

- **Targeted phishing attack** on a specific person or group.
- Attackers **research the victim** and send **personalized messages** that look real.

□ *Example:*
A hacker sends an email that looks like it's from your **college principal**, asking for your login details for a "portal update".

□ *Used for:*
Employees, students, HR teams, etc.

**E) Whaling**

- A **special type of spear phishing** that targets **high-profile people**:
  - CEOs
  - Bank managers

- Executives

□ *Example:*
A fake email to the CEO saying:

"Here's the confidential board report – login to view."

□ *Goal:*
To gain access to big corporate accounts or financial data.

### 2.4 – Password Cracking

**Password cracking** means trying to **find or break a password** using different tricks and tools.
Hackers or attackers do this to get **unauthorized access** to systems, emails, bank accounts, etc.

**Purpose of Password Cracking:**

1. To recover **lost or forgotten passwords** (legally).
2. To **test the strength** of a password (by security experts).
3. To **hack into systems** and **steal data** (illegally).

- **Examples of Guessable Passwords**

Many people use passwords that are very **easy to guess**. These are called **weak passwords**.

Here are examples:

| Type | Example |
|---|---|
| Blank password | (No password at all) |
| Common words | password, admin, welcome |
| Keyboard patterns | qwerty, asdfgh, 123456 |
| Names | rahul123, mom2021, tommy |
| Birthdays/Dates | 01011999, 19981231 |
| Mobile numbers | 9876543210 |
| Vehicle numbers | MH12AB1234 |
| Celebrities or teams | viratkohli, messi10 |
| Slight modifications | rahul1, rahul@123 |
| Reverse spellings | luhaR (Rahul reversed) |

□ **Example:**
If someone's dog's name is "Rocky", their password might be:
→ rocky123 (Easy to guess!)

- **Types of Password Cracking Attacks**

### 1. Active Online Attacks

- Attacker **tries passwords directly** on login screen.
- If password is weak, it can be cracked easily.

#### a) Dictionary Attack

Tries a list of common words (like a dictionary).

□ *Example:*
Tries: admin, admin123, password, welcome123

#### b) Brute Force Attack

Tries **all possible combinations** of letters, numbers, and symbols.

□ *Example:*
Tries: a1, a2, a3 … z9, until it finds the correct one.

---

### 2. Passive Online Attacks

- Attacker **eavesdrops on network** to steal passwords.

#### a) Wire Sniffing

Monitors data passing through network (like Wi-Fi) and steals login details.

#### b) Man-in-the-Middle Attack

Hacker sits **between you and the website**, sees everything you send.

#### c) Replay Attack

Captures login session, then **reuses** it to log in without needing password again.

### 3. Offline Attacks

- Attacker steals the **password file** (like database) and cracks it **offline**.

-

### a) Rainbow Table Attack

Uses **pre-made tables** of password hashes (encrypted versions) to crack passwords quickly.

### b) Distributed Attack

Uses **many computers** together to speed up cracking.

□ *Example:*
One hacker uses 10 computers together to crack a password faster.

### 4. Non-Electronic Attacks

- No software or hacking needed — just **observe or trick the user**.

### a) Shoulder Surfing

Looking at someone’s screen or keyboard while they type.

□ *Example:*
Standing behind a friend and watching them type their ATM PIN.

### b) Social Engineering

Tricking someone into revealing their password.

□ *Example:*
Pretending to be bank staff and asking,

“Sir, we’re verifying your account. Please tell me your password.”

### c) Dumpster Diving

Searching trash for papers with written passwords.

□ *Example:*
Finding sticky notes in office bins that have passwords written on them.

### ✚ Keyloggers

Keyloggers (also called *Keystroke Logging*) are tools — either **software** or **hardware** — that secretly track and record everything you type on your keyboard.
They are a type of spyware because the victim usually has **no idea** it’s happening.

### ❖ How Keyloggers Work

- The keylogger records your keystrokes (e.g., passwords, messages, credit card numbers).
- The recorded data is stored in a **log file**.
- This log file is sent to the attacker over the internet.
- The attacker can then misuse your personal information.

## ❖ Example

- You log into your **online banking account** at a cybercafé.
- Unknown to you, the computer has a keylogger installed.
- Every key you press (username + password) is recorded and sent to the hacker.
- Within hours, the hacker logs into your account and transfers your money.

## ❖ Methods of Keyloggers

1. **Software Keyloggers**
    - Programs installed in your operating system that run in the background.
    - Capture every keystroke and sometimes screenshots.
    - **Example**: A fake "PDF invoice" email attachment installs a keylogger on your PC.

2. **Hardware Keyloggers**
    - Small devices connected physically between your keyboard and computer.
    - Can also be embedded inside keyboards or ATM machines.
    - **Example**: Criminals attach a tiny keylogging device to an ATM PIN pad to steal card PINs.

3. **Antikeylogger Software**

- Detects and removes keyloggers from a computer.
- Does not need regular updates like antivirus software.
- **Advantage**: Protects against Internet banking fraud, identity theft, and secures email/messaging.

### Advantages for Attackers

- **Stealthy** – Victims usually don't notice them.
- **Continuous Data Capture** – Records every keystroke until removed.
- **Bypasses Security** – Even if you use secure websites (HTTPS), the keylogger captures data before it's encrypted.
- **Low Cost** – Easy to install and maintain for attackers.
-

## Spywares

Spyware is a **malicious program** that secretly gathers information about a user without permission.
It can track browsing history, collect personal files, and monitor online activity.
It often runs silently in the background.

### How Spyware Works

- It installs on your computer (often bundled with free software or through phishing emails).
- It monitors your activity — websites visited, things you type, apps you use.
- Sends this data to hackers, advertisers, or other malicious entities.

### Examples of Spyware

1. **Browser Hijacking** – You install a free video player, but it changes your homepage and search engine to a shady website that tracks your searches.

### Types of Spyware

1. **Adware**
    - Shows unwanted ads on your device, often in pop-up form.
    - Sometimes changes your browser settings or redirects you to ad-filled websites.
    - **Example:**
      You install a free photo-editing app, and suddenly your browser homepage changes, showing ads for products you never searched.
    -
2. **Trojans**
    - Malicious programs disguised as useful software.
    - Once installed, they can steal data, download other malware, or give remote control of your device to hackers.
    - **Example:**
      A fake “antivirus” app claims to remove viruses but instead sends your files and passwords to a hacker.
3. **Keyloggers**
    - Already explained above, but in spyware context, it’s used to track keystrokes without your knowledge.
    - **Example:**
      A keylogger hidden inside a fake PDF reader logs every password you type.

4. **Password Stealers**

  - Specifically made to find and steal saved passwords from browsers, apps, or operating systems.
  - **Example:**
    Malware that scans Google Chrome's stored passwords and sends them to a hacker.

5. **Mobile Spyware**
   - Targets smartphones and tablets.
   - Can read your messages, track GPS location, listen to calls, or activate the camera.
   - **Example:**
     A fake flashlight app on Android that secretly sends your GPS location and WhatsApp messages to the attacker.

- **Viruses and worms**

  - **Virus :**

    1. A computer virus is a harmful program.
    2. It attaches itself* to another file (host), usually executable files like .exe.
    3. It spreads from one computer to another without permission of the user.
    4. Works like a biological virus – spreads from one host to another.

- **Actions viruses can do:**

1. Display messages – Example: A popup that says "You are hacked!"

2. Delete files – Removes your photos, documents, or system files.

3. Scramble data – Makes files unreadable.

4. Cause screen problems – Strange colors, flickering screen.

5. Halt system – Computer freezes or shuts down suddenly.

6. Replicate – Just keep copying itself to spread.

- **How viruses spread:**

Through the Internet* → Downloading infected files, email attachments.

Through removable media* → CD, DVD, pen drives, etc.

A virus needs a host program* to run.

Example: A game .exe file may contain a virus. When you run the game, the virus runs too.

- **Worms**

1. Aworm is also like as  virus but worm does not need host programit is an independent program.
2. A worm spread automatically
3. A computer worm is a type of malicious software (malware) that can self-replicate and spread across networks without needing human help (like clicking a file).
4. Unlike a virus, which usually attaches itself to another program or file, a worm is standalone — it doesn't need a host file.

**How Worms Work**

1. A worm enters a system (through email attachments, downloads, or software vulnerabilities).
2. It exploits security holes or uses network connections to spread.
3. It keeps replicating itself across devices and networks.
4. Depending on design, it may:
    - Just spread (causing network slowdowns)
    - Carry a payload (like ransomware, spyware, or backdoors).

**Example: The** ILOVEYOU Worm (2000)

- Spread via email with the subject "ILOVEYOU" and an attachment "LOVE-LETTER-FOR-YOU.txt.vbs".
- When users opened the attachment, the worm executed and sent itself to all contacts in the victim's address book.
- It overwrote files (images, music, docs) and caused an estimated $10 billion in damages worldwide.

- **Types of Viruses**

1. File-infecting virus

- Attaches itself to .exe or .com files.
- It is also called as parasitic virus

Example: You run a program, virus activates.

2. Macro virus

- Works in MS Word, Excel macros.

Example: An infected Word document spreads the virus when opened.

3. Browser Hijacker

- Changes your browser settings
- It is often called browser redirect virus.

Example: Google Chrome opens unwanted websites automatically.

4. Web Scripting Virus

- Comes from websites → adds malicious code.
- It also steal cookies

Example: Fake login page stealing passwords.

5. Boot Sector Virus

- Infects the boot area of hard disks/USBs.
- Runs every time you start your computer.

6. Polymorphic Virus

- Keeps changing its code→ hard to detect.

Example: Antivirus fails to recognize it because its “signature” keeps changing.

7. Resident Virus

- Stays in computer memory.
- Keeps running even if original infected file is deleted.
- Stores itself on the computer.

8. Multipartite Virus

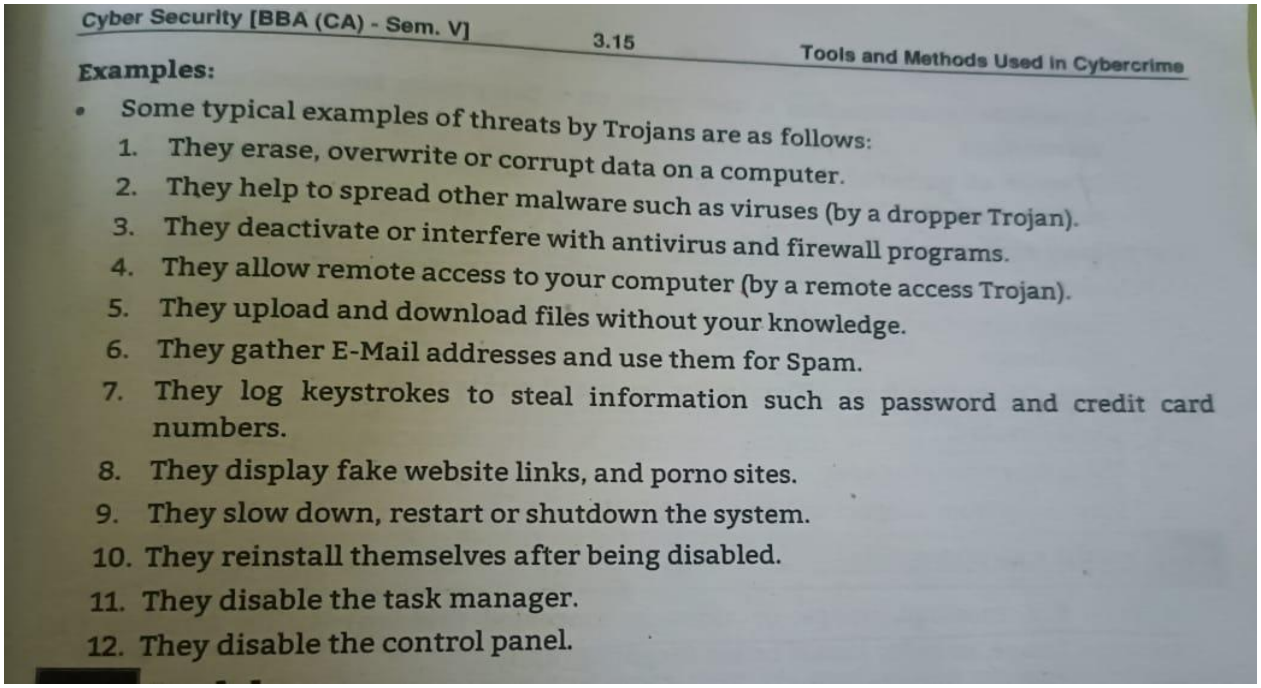
- Infects multiple parts of the system at once (files, boot, memory).
- Easily spread in computer system.

## Trojan Horse (Trojan Virus)

The name comes from **Greek mythology** – the Trojan War, where soldiers hid inside a wooden horse to secretly enter Troy.
Similarly, in computers, a **Trojan looks safe and useful but secretly contains malware.**

### What Trojans Can Do (in Depth):

1. **Change System Settings**
    - Disable your antivirus or firewall.
    - Modify system registry to make itself run at startup.
    - Example: Your PC becomes slower, strange programs start automatically.
2. **Steal Data**
    - Keyloggers inside Trojans record everything you type (passwords, credit card details).
    - They can take screenshots, copy files, or access webcams.
    - Example: A Trojan records your online banking username & password and sends it to a hacker.
3. **Execute Harmful Commands**
    - Delete files, install more malware (like ransomware or spyware).
    - Hackers can even **control your PC remotely** → like they are sitting in front of it.
    - Example: Your system is used to attack another website (DDoS attack).



**Examples:**

- Some typical examples of threats by Trojans are as follows:
    1. They erase, overwrite or corrupt data on a computer.
    2. They help to spread other malware such as viruses (by a dropper Trojan).
    3. They deactivate or interfere with antivirus and firewall programs.
    4. They allow remote access to your computer (by a remote access Trojan).
    5. They upload and download files without your knowledge.
    6. They gather E-Mail addresses and use them for Spam.
    7. They log keystrokes to steal information such as password and credit card numbers.
    8. They display fake website links, and porno sites.
    9. They slow down, restart or shutdown the system.
    10. They reinstall themselves after being disabled.
    11. They disable the task manager.
    12. They disable the control panel.

## Backdoors

- A **backdoor** is a secret way for hackers to enter your system without permission.
- Hackers can **bypass login** and access files directly.
- Can be created by malware or even developers for “debugging.”

### Functions of Backdoors:

1. Create, delete, copy, or edit files.
2. Control system settings, registry, and apps.
3. Control hardware (shutdown, restart).
4. Steal information (passwords, browsing history, documents).

□ Example: Back Orifice (famous backdoor used by hackers).

## Steganography

- **Meaning**: It is the practice of hiding secret information (text, image, audio, video, etc.) inside another ordinary file (like an image, audio, video, or document) so that nobody suspects its presence.
- **Goal**: Maintain confidentiality and integrity of data while avoiding detection.
- **Difference from Cryptography**: Cryptography scrambles the message (encryption), while Steganography hides the fact that a message exists at all.

- **Types of Steganography**

### 1. Text / Document Steganography

- Secret data is hidden in **text files or documents**.
- Methods:
  - Adding **whitespace or tabs** at the end of lines.
  - Using **books or newspapers** as cover text (code words/letters).
  - Changing **font or background color** in MS Word.
  - Example : Suppose we want to hide the word **“KEY”** inside a text.
    We take a paragraph and use **extra spaces at the end of sentences**:

This is a secret message.␣ (extra space → K)

Nobody should notice it.␣␣ (two spaces → E)

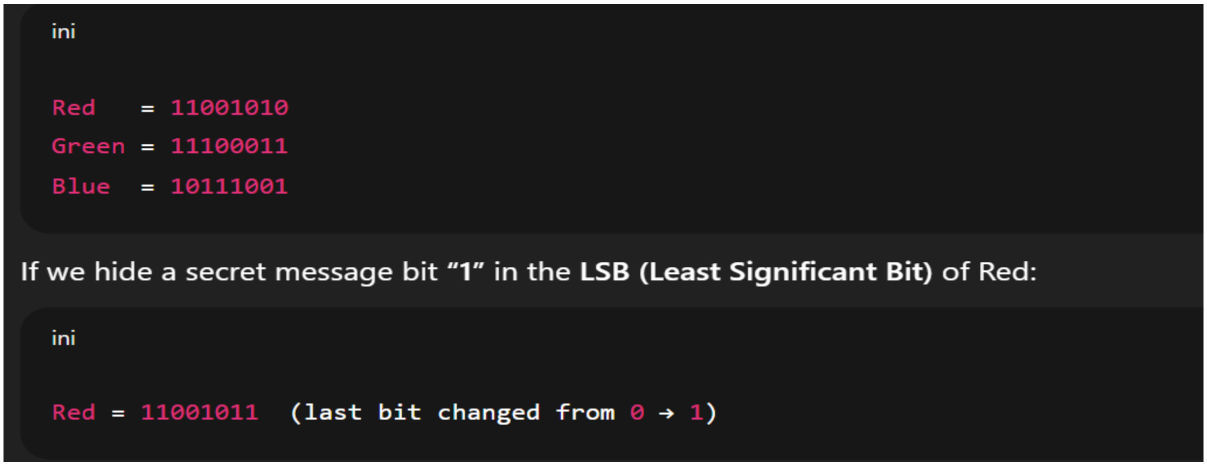
Keep it safe.␣␣␣ (three spaces → Y)

The extra spaces ( ␣ ) at the end of lines represent hidden letters. The normal reader won’t see this, but someone who knows the technique can decode the hidden word.

## 2. Image Steganography

- Digital images are commonly used since they have huge storage of bits (pixels).
- **Techniques:**
  - **LSB (Least Significant Bit) Insertion** → Replace the last bit of pixels with secret message bits.
  - **Masking & Filtering** → Hide data in significant areas of the image.
  - **Redundant Pattern Encoding** → Embed patterns in the image.
  - **Encrypt & Scatter** → Encrypt data first, then scatter across the image.

Example : Take a **24-bit image**. Each pixel has 3 color channels (Red, Green, Blue).
Let’s say the pixel color is:



ini

```
Red   = 11001010
Green = 11100011
Blue  = 10111001
```

If we hide a secret message bit “1” in the **LSB (Least Significant Bit)** of Red:

ini

```
Red = 11001011  (last bit changed from 0 → 1)
```

The human eye cannot see this tiny change in color, but over thousands of pixels, we can hide an entire text or file.

## 3. Video Steganography

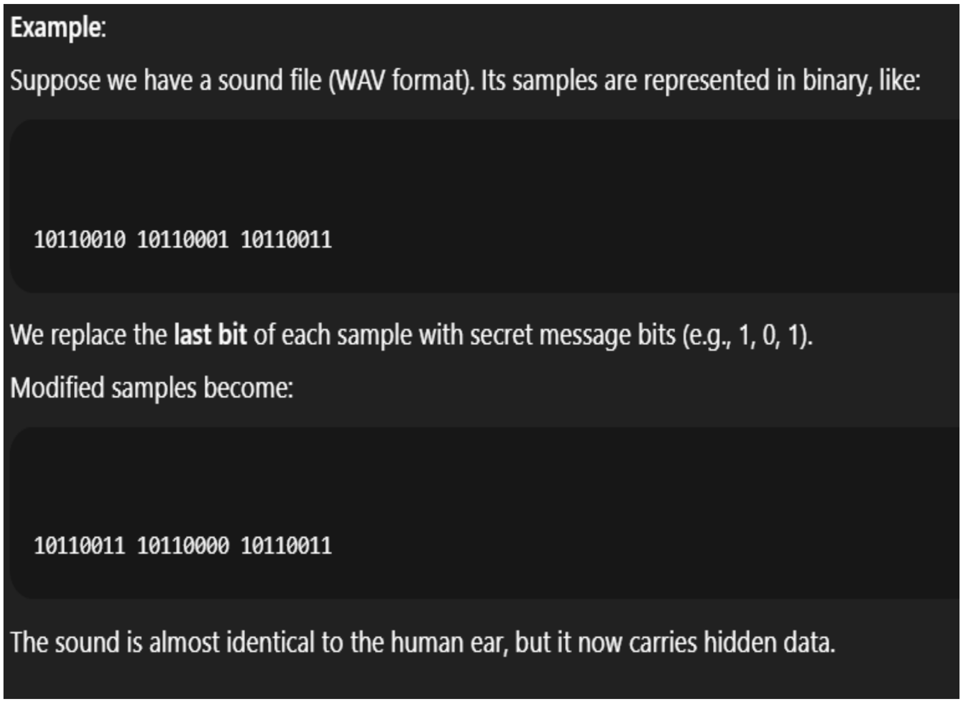
- Uses video files as carriers for secret data.
- Since video = frames of images + sound, both can be used for hiding information.
- **Approaches**:
  - LSB Insertion in video frames.
  - Real-time embedding (used in streaming).

Example : in a 10-minute video with 30 frames per second = **18,000 frames**.
If we hide 1 byte in each frame, we can store **18 KB of secret data** without being noticed.

**Explanation**:
Because video has a lot of redundancy (many frames + sound), it’s one of the best carriers for secret communication.

### 4. Audio Steganography

- Secret message is hidden in **sound files**.
- Difficult because the **human ear** is very sensitive.
- **Techniques**:
  - **Parity coding**
  - **LSB coding**
  - **Echo hiding** (adding faint echoes that carry data).



**Example**:

Suppose we have a sound file (WAV format). Its samples are represented in binary, like:

```
10110010 10110001 10110011
```

We replace the **last bit** of each sample with secret message bits (e.g., 1, 0, 1).

Modified samples become:

```
10110011 10110000 10110011
```

The sound is almost identical to the human ear, but it now carries hidden data.

### 5. Network Steganography

- Information is hidden in **network protocols** like TCP, UDP, ICMP.
- Example: Modify fields in a packet header to carry hidden data.
- Used in **covert channels** of the OSI model.

### □ Examples of Steganography

1. Playing audio backwards to reveal hidden message.
2. Playing video at a faster frame rate to hide data.
3. Inserting message into RGB channels of an image.
4. Encrypting image inside another photo (with noise).
5. Hiding info in file headers or metadata.

### □ Steganalysis (Opposite of Steganography)

- **Definition**: The science of detecting hidden messages inside files.
- **It is opposite process of stegnography**.
- While steganography hides data, **steganalysis** tries to **detect and extract** it.
- Used by cyber forensic experts to check if files contain hidden data.

### DoS Attacks

1. **What it is**:
   - A DoS attack happens when a criminal sends a huge amount of traffic (requests, data, signals) to a victim's system.
   - This overloads the system and **shuts it down** or makes it too slow to respond.
2. **Effect**:
   - The attack makes the server of a website **unavailable** for normal users.
   - Example: When too many fake requests are sent to a bank's website, genuine users can't access their accounts.
3. **Target**:
   - Usually aimed at **high-profile websites and services** like:
     - Banks
     - Credit card payment gateways
     - Large companies
     - Mobile phone networks

□ **Example:** Imagine you order 100 pizzas using a fake phone number. The shop keeps waiting for payment but cannot serve real customers → shop is blocked.

### □ Signs of DoS Attacks

1. Internet or websites open **very slowly**.
2. A **particular website** stops working.
3. **No website** can be accessed.
4. Sudden flood of **spam emails** (called **Email Bomb**).

### □ Functions of DoS Attacks

A DoS attack may:

1. **Flood a network** with too much traffic.
2. **Break connections** between two systems.
3. **Block a person** from using a service.
4. **Disrupt services** of a website or company.

□ **Example:** A college exam portal crashes when too many students try to log in at the same time (intentional or unintentional).

### □ Classification of DoS Attacks

1. **Bandwidth Attacks:**
    - Overloads the network bandwidth → websites take too long to load.
      □ Like a road jammed with traffic so no car can move.
2. **Logic Attacks:**
    - Exploit **software weaknesses** in web servers or TCP/IP rules.
      □ Like finding a loophole in exam rules to cheat.
3. **Protocol Attacks:**
    - Misuse the **rules of communication (protocols)** to overload the system.
      □ Like following rules in a twisted way to confuse others.
4. **Unintentional DoS Attack:**
    - A sudden spike in visitors makes a website crash (not always malicious).
      □ Example: When train booking opens, IRCTC website slows down or crashes.

---

### □ Types / Levels of DoS Attacks

1. **Flood Attack:**
    - Attacker uses the **ping command** to send many packets to victim.
    - Victim receives more traffic than it can handle → system slows/crashes.
      □ Example: Like hundreds of people keep pressing your doorbell nonstop.
2. **Ping of Death Attack:**
    - Hacker sends **oversized ICMP packets** (error messages) to victim.
    - Victim system cannot handle large packets → crashes.
      □ Example: Giving a computer a book with **10,000 pages at once**, it cannot read and breaks down.
3. **SYN Attack:**
    - Uses the **TCP handshake process** (SYN → SYN-ACK → ACK).
    - Attacker sends **SYN requests** but **never completes** with ACK.
    - Victim keeps waiting and its resources get locked.
      □ Example: Many people book seats in a theater but never pay → real customers can't book tickets.

4. **Teardrop Attack**

- **Meaning:**
  In this attack, hackers send **broken (fragmented) packets** that **overlap each other** when the computer tries to join them back.
- Since the packets are damaged, the victim's system gets **confused** and may **hang or crash**.

□ **Example:**
Imagine you receive a puzzle but some pieces **don't fit properly**. When you try to force

them together, the puzzle breaks. Similarly, the victim computer cannot rebuild the packets and stops working.

### 2. DoS vs DDoS Attack

- **DoS (Denial of Service):**
  Attack comes from **one computer** → keeps sending requests → victim system gets **overloaded**.
- **DDoS (Distributed Denial of Service):**
  Attack comes from **many computers** (hacked and controlled by hacker) → victim system receives **huge traffic from multiple sources** → much faster and harder to stop.

□ **Example:**

- DoS = One person continuously ringing your doorbell → you can stop them easily.
- DDoS = Hundreds of people ringing at once → impossible to manage.

**Botnet =** A group of hacked computers controlled by hacker to launch DDoS attacks.

### Types of DDoS Attacks

#### (i) Volumetric Attacks

- Flood the network with **tons of fake traffic** (like ICMP ping requests).
- Result → **No internet bandwidth left** for real users.

□ **Example:**
Think of a road filled with thousands of fake cars → **real cars cannot pass**.

---

#### (ii) Fragmentation Attacks

- Hacker sends **packets with wrong header information**.
- When the system tries to **join them back**, it **fails** and crashes.

□ **Example:**
Like sending puzzle pieces that are **too big to fit together** → puzzle cannot be completed.

---

#### (iii) Application Layer Attacks

- Directly target **applications or websites** (e.g., login page, online shopping cart).
- Attackers send **too many fake requests**, making the app **slow or crash**.

 **Example:**
Thousands of people pressing "Buy Now" button on an online store at the same time, so the server cannot handle it.

## How to Protect from DoS/DDoS Attacks?

1. **Use Router Filters**
   - Block suspicious or fake traffic before it enters your network.
     Like a **security guard at the gate** stopping unwanted visitors.
2. **Install Patches for TCP SYN Flooding**
   - Keep systems updated with **security patches** to handle common DDoS tricks (like SYN flooding).
     Like **fixing weak doors** so thieves cannot break in easily.

## 3.11 – SQL Injection (SQLi)

###  What is SQL?

- **SQL (Structured Query Language)** is used to talk to a **database**.
- Databases store important data like:
  - usernames, passwords
  - bank account numbers
  - personal info (e.g., credit card numbers)
  - website content (blogs, comments, etc.)

 Example: When you log in, the website runs a query like:

```
SELECT * FROM users WHERE username = 'dipali' AND password = '12345';
```

###  What is SQL Injection?

- SQL Injection (SQLi) happens when a hacker **inserts malicious SQL code** into a website’s input fields (like login forms, search bars, or URLs).
- This tricks the database into running **extra commands**.
- Hackers can then **see, edit, or delete confidential data**.

 **Example Attack:**
URL:

```
http://teachers.com?teacherId=117 or 1=1;--
```

SQL Query becomes:

```
SELECT * FROM teachers WHERE teacherId=117 OR 1=1;
```

- OR 1=1 is **always true**, so the database returns **all teacher records**, not just teacherId=117.
- Hacker gains **unauthorized access**.

---

### □ Why SQL Injection is Dangerous?

- Hackers can:
  1. Steal data (passwords, bank details).
  2. Modify or delete database records.
  3. Gain admin access to websites.
  4. Run harmful system commands.

---

### □ Types of SQL Injection

1. **In-band SQLi:**
   - Hacker uses normal SQL queries (like UNION) to get database info.
     □ Example: Extracting usernames and passwords directly.
2. **Blind SQLi:**
   - Database doesn't show error messages.
   - Hacker asks the database **true/false questions** to guess the data.
     □ Example: Checking if a user exists by sending AND 1=1 vs AND 1=2.
3. **Out-of-band SQLi:**
   - Data is sent through different channels (like email or DNS requests).
   - Rare but powerful.

---

### □ Real-World Example

- In a login form:

```
SELECT * FROM users WHERE username = 'admin' AND password = '123';
```

Hacker enters this in the **username field**:

```
' OR '1'='1
```

Query becomes:

```
SELECT * FROM users WHERE username = '' OR '1'='1' AND password = '123';
```

- '1'='1' is always true → hacker **bypasses login** without password.

### Methods to Prevent SQL Injection Attack

1. **Use of Prepared Statements / Queries**
    - SQL statements are **pre-compiled** with placeholders for inputs.
    - User data is passed separately, so the database can **clearly distinguish** between code and data.
    - Prevents malicious SQL injection.

□ Example:

```
PreparedStatement stmt = con.prepareStatement(
 "SELECT * FROM users WHERE username=? AND password=?");
```

2. **Escape All User-Supplied Input**
    - Apply **character-escaping functions** before passing user input.
    - Each DBMS (MySQL, Oracle, SQL Server) provides its own escaping methods.
    - Ensures database does not confuse input with SQL code.

---

3. **Use of Stored Procedures (SP)**
    - A **Stored Procedure** is a group of SQL statements stored in the database.
    - Automatically parameterized, reducing chances of SQL injection.
    - Can be **reused** multiple times securely.

□ Example:

```
CREATE PROCEDURE GetUser(IN userId INT)
BEGIN
  SELECT * FROM users WHERE id = userId;
END;
```

---

4. **Apply Least Privilege**
    - Each application should have its **own database credentials**.
    - Only minimum rights should be given (e.g., read-only if needed).
    - Limits damage even if the database is attacked.

---

5. **Isolate Database Server from Web Server**
    - Keep **database servers separate** from web servers.
    - Adds extra layers of security to protect against:
        - Vulnerabilities
        - Human errors
        - Bad or insecure code