TRAINING DAY 22 REPORT:

- ## Spy Any Android Phone

  Definition: Spying on Android phones involves using spyware or monitoring tools to remotely access and monitor activities on a target Android device.

  Purpose:

  - Legitimate: Parental control, employee monitoring (with consent), lost phone tracking.

  - Malicious: Stalking, stealing data, or blackmail.

  Common Features:

  1. GPS location tracking

  2. Call logs and message access

  3. Browsing history

  4. Social media/chat app access (WhatsApp, Facebook, etc.)

  5. Real-time camera/microphone access

  Popular Tools:

  - mSpy

  -FlexiSPY

  - Hoverwatch

  - Spyzie

  Installation: Usually requires physical access to the phone for installation. Some advanced tools can be installed remotely through phishing techniques.

- ## Keylogger

  Definition: A **keylogger** (keystroke logger) is software or hardware that secretly records keyboard inputs.

  Types:

1. Software-based: Installed as malware, often hidden in Trojans or bundled software.

2. Hardware-based: Devices plugged into keyboards to intercept keystrokes.

Uses:

- Password and banking detail theft

- Monitoring user activity

- Forensics and parental control (when used ethically)

Detection/Prevention:

- Use good antivirus software

- Regularly scan for suspicious processes

- Monitor active background applications

- # Adware

Definition: **Adware** is a type of malware or unwanted software that displays ads (pop-ups, banners, redirects) on your device, usually without consent.

Symptoms:

- Sudden browser redirects

- Pop-ups and auto-downloading software

- Ads embedded in system tools

Risks:

- Slows down the system

- Steals browsing behavior and user data

- Installs additional malware

Common Adware:

- Fireball

- DollarRevenue

- CoolWebSearch

Prevention:

1. Avoid downloading cracked/pirated software

2. Use ad-blockers and antivirus tools

3. Don't install unknown browser extensions

- # Introduction to Steganography

Definition: **Steganography** is the practice of hiding secret data within an ordinary file (image, audio, video, etc.) in such a way that no one can detect it.

Difference from Cryptography:

Cryptography: Scrambles the content (encrypted)

Steganography: Hides the content (invisible)

Uses:

- Covert communication

- Digital watermarking

- Malware and spyware (to hide code)

History:

1. Ancient Greece: Wax tablets with hidden messages under wax

2. WW2: Invisible ink

3. Digital era: Hiding data in media files using binary manipulation

- # Steganography - Hide Text File in Images

Concept: Secret text is embedded in an image file using LSB (Least Significant Bit) technique. The image looks the same but contains hidden information.

How it works:

- A .txt file is embedded inside a .jpg or .png file

- Tools modify the image’s binary data without affecting visual quality

Tools:

1. Steghide

2. OpenStego

3. SilentEye

Command example (Linux):

```
steghide embed -cf image.jpg -ef secret.txt
```

- ## Steganography - Hide Text in Video and Audio

Concept: Text or files are hidden in video (`.mp4`) or audio (`.wav`) files using advanced algorithms.

Techniques:

1. LSB: Modify least significant bits of sound frames or video pixels

2. Echo hiding: Uses slight echoes to encode information in audio

3. Phase coding: Modifies phase shifts in audio

Tools:

1. DeepSound

2. Coagula

3. AudioStego

Use case: Secure, undetectable transmission of confidential messages.

- ## Hide Files in Images

Concept: You can hide any file type (like PDFs, zip files, scripts) inside an image without visibly changing the image.

Method (CMD - Windows):

```
copy /b image.jpg + secret.pdf output.jpg
```

Result: `output.jpg` behaves like an image but contains the hidden `secret.pdf`.

Extraction: Open the file using **WinRAR**, **Steghide**, or specific extraction tools.

- ## Convert Images into Sound

  Concept: An experimental method in steganography where an image is converted into audio by converting pixel data into waveforms.

  Process:

  1. Image brightness = sound amplitude

  2. Rows = time progression in the audio file

  3. Specialized tools convert this sound back into an image

  Tools:

  1. Photosounder

  2. Coagula

  3. Sonic Visualiser

  Use:

  - Data art

  - Experimental music

  - Advanced data hiding