1. Sniffing (physical)

Back in the day when there was no remote home phone, you had to have multiple phones at home anyone can remember the problems that had been occurred when two people wants to speak on the phone someone else could grab another phone and hear the speeches. in the context of network security when packets are not encrypted someone else could intrude to your network and steal those packets with some sniffer applications that work on the **physical** layer of **OSI model** like Wireshark, Tcpdump, WinDump...

some protocols that work on this layer and can be sniffed are:

Examples of protocols that use physical layers include:

- Digital Subscriber Line.
- Integrated Services Digital Network.
- Infrared Data Association.
- Universal Serial Bus (USB.)
- Bluetooth.
- Ethernet.

2. SPOOFING (Data Link)

Spoofing is the act of a person or a program that successfully identifies itself which is from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

IP spoofing and ARP spoofing, in particular, may be used to leverage man-in-the-middle attacks against hosts on a computer network. Spoofing attacks that take advantage of TCP/IP suite protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message.

3. man-in-the-middle (Network)

Many of the protocols in the TCP/IP suite do not provide mechanisms for authenticating the source or destination of a message, leaving them vulnerable cause an attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

4. Reconnaissance (Transport)

In the context of cybersecurity, reconnaissance is the practice of discovering and collecting information about a system. One of the most common techniques involved with reconnaissance is port scanning, which sends data to various TCP and UDP (user datagram protocol) ports on a device and evaluates the response. Some common examples of reconnaissance attacks include packet sniffing, ping sweeping, port scanning, phishing, social engineering, and internet information queries.

5. Hijacking (Session)

sometimes also known as **cookie hijacking** is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many websites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

these explosions can be carried out by these attacks

- **Cross-site scripting: XSS attacks** enable attackers to inject client-side scripts into web pages. It causes running codes, which is treated as trustworthy because it appears to belong to the server, on the victim computer. It allows the attacker to obtain a copy of the cookie or perform other operations.
- **Session side jacking:** where the attacker uses packet sniffing to read network traffic between two parties to steal the session cookie.
- **Malware** and unwanted programs can use browser hijacking to steal a browser's cookie files without a user's knowledge.

6. Phishing (presentation)

Phishing attacks are the practice of sending fraudulent messages that appear to come from a trusted source. It is usually performed through email. The goal is to steal sensitive data like credit card and login information or install malware on the victim's machine. Phishing is a common type of cyber-attack that everyone should learn about in order to protect themselves.

7. Exploit (Application)

An exploit is a program that takes advantage of a bug or vulnerability in other systems. the cause vulnerability may be due to bad system configuration or a bug in a specific version of software installed on the victim system. Many exploits are designed to provide super user-level access to a victim system or are designed to cause DoS (denial of service) or DDoS (distributed denial of service) attacks, in which attackers can bring down a website or critical system without even using an exploit.

for instance, BlueKeep is an exploitable vulnerability in Microsoft Remote Desktop Protocol (RDP) that can allow attackers to log in to a victim's computer remotely.