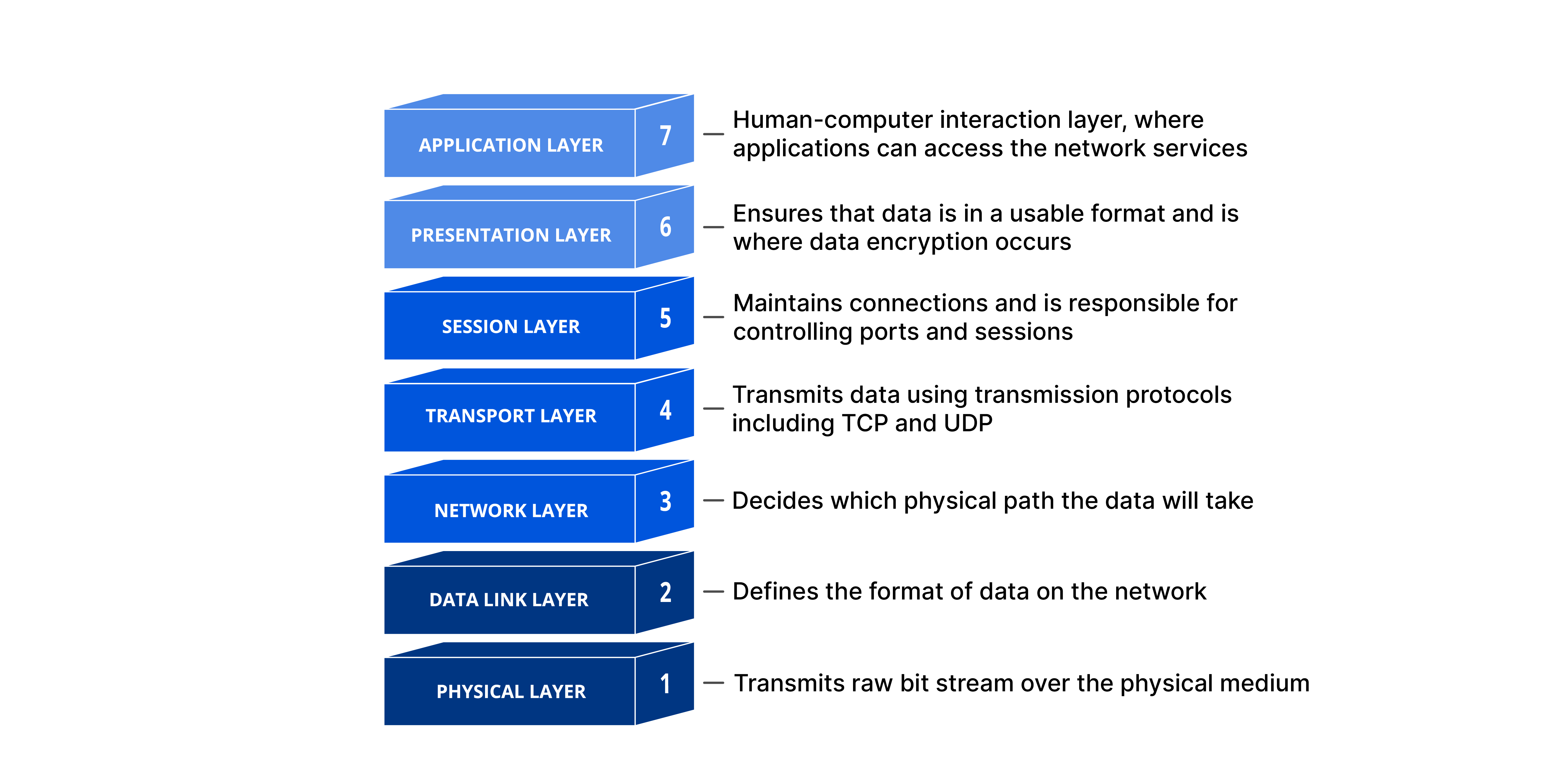
**ATTACKS ON THE OSI MODEL: CASE STUDIES AND REPORT**

**INTRODUCTION**

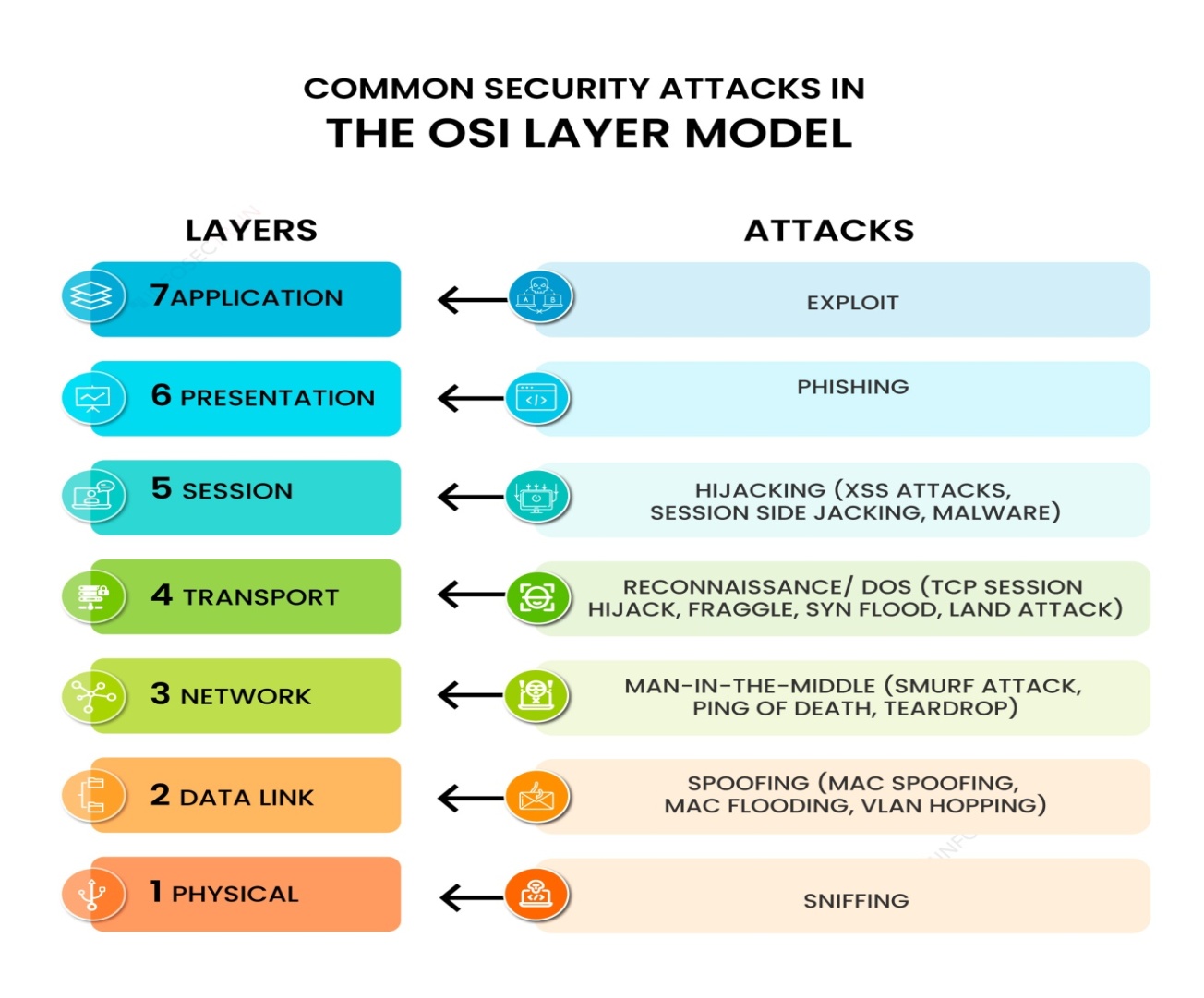
The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard Protocols. The OSI provides a standard for different computer systems to be able to communicate with each other. The OSI (Open Systems Interconnection) model is a framework for describing a networking system’s functionality. The OSI model classifies the computing functions of the various network segments, specifying the rules and requirements necessary to ensure the network’s software and hardware interconnection.

The OSI Model can be seen as a universal language for computer networking. It is based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last. 

Each layer of the OSI Model handles a specific job and communicates with the layers above and below itself. DDOS attacks target specific layers of a network connection ;application layer attacks target layer 7 and protocol layer attacks target layers 3 and 4.

**7 Layers of the OSI Model and Common Security Attacks in Each Layer**

The OSI model comprises seven layers of abstraction. The layer establishes communication between one user to another from layers 7 to 1. Each layer carries out a particular function before sending data to the subsequent layer.

****

**Application layer**

The application layer is the closest to users in the OSI layer model and establishes the communication between the user and applications with which they interact individually. The common security attack on this layer is an exploit.

**Attack: Exploit**

Exploit means taking advantage of a software vulnerability. An exploit in the application layer refers to a type of cyber attack that targets vulnerabilities in software applications. These attacks take advantage of bugs or weaknesses in the code of the application to gain unauthorized access or perform malicious actions. This indicates that the target of an attack includes a software vulnerability that allows attackers to build the means to access and exploit it. Without employing an exploit, attackers can take down a website or important system by using DoS (Denial-of-Service) or DDoS (Distributed Denial-of-Service) cyberattacks. Many exploits are designed to enable super user-level access to a victim system.

**2. Presentation layer**

The presentation layer specifies the two devices’ encoding, encryption, and compression methods for proper communication. Anything sent from the application layer is received by the presentation layer, which is transformed into a format suitable for transmission via the session layer. Phishing is one of the common security attacks carried out by attackers in this layer.

**Attack: Phishing attack**

Phishing attacks in the presentation layer comprise using social engineering tactics to trick users into providing personal and sensitive information or clicking on a malicious link. This is often done by creating fake websites or email messages that appear to be from a legitimate source. This attack aims to steal sensitive information such as login credentials and credit card information or install malware on the victim’s system by disguising the attack as a legitimate request.

**3. Session layer**

The session layer establishes communication channels between devices, known as sessions. It starts sessions, keeps them open and effective while data is transferred, and closes them after communication is completed. Hijacking is one of the common security attacks that occurs in this layer.

**Attack: Hijacking**

Hijacking in the session layer occurs when an attacker intercepts and takes control of an established communication session between two parties. This can be carried out by exploiting vulnerabilities in the protocol used to establish the session or using the tools to intercept and manipulate network traffic. Once the attackers hijack the session, they can access sensitive information or gain unauthorized access. There are two types of session hijacking:

* **Active session hijacking**: In this, the attacker takes control of an active user session on a network and intercepts and alters network traffic in real time.

**Passive session hijacking**: In this, attackers monitor network traffic and wait for users to log into a website; at that point, the attackers take over the session

**Attack: Man-in-the-Middle (MITM) attack**

In the network layer, a man-in-the-middle attack occurs when an attacker intercepts and modifies communication between two parties without their knowledge. The attackers become a man in the middle of the communication, able to read, modify, or inject new information into the communication. Attackers also intercept and alter communication by manipulating the routing of packets between the two sources. This can be done by using a technique such as ARP spoofing, where attackers send fake ARP messages to a target system, tricking it into sending packets to the attacker’s device instead of the intended source.

**6. Data link layer**

The data link layer establishes and terminates communication between two technically connected network nodes. It divides packets into frames and transmits them from source to destination. In this layer, attackers use spoofing attacks to target the network system.

**Attack: Spoofing attack**

A spoofing attack in the data link layer occurs when an attacker alters a device’s Media Access Control (MAC) address to impersonate another device in the network. This can allow the attackers to gain access to network resources or intercept and modify network traffic intended for the legitimate source. There are different ways that attackers carry out MAC spoofing.

**Transport layer**

The transport layer performs flow control, transmitting data at a frequency corresponding to the receiving device’s connection speed and error control, determining whether data was received wrongly and requesting it if necessary. The most common security attack that is carried out in this layer is reconnaissance.

**Attack: Reconnaissance**

A reconnaissance attack in the transport layer typically involves an attacker attempting to gather information about a target system or network by actively probing the transport layer protocols, such as TCP or UDP. This can include techniques such as port scanning, which involves sending messages to various ports on the target system to determine which ports are open and potentially vulnerable to attack. Additionally, an attacker may use tools such as packet sniffers to capture and monitor network traffic to gather information.

**5. Network layer**

There are two primary jobs that the network layer does. One breaks up the segments into network packets and then puts the packets back together at the other end. The other is sending packets through a physical network by finding the best route. One of the most common security attacks in this layer is a man-in-the-middle attack.

* Address Resolution Protocol (ARP) spoofing
* DHCP spoofing
* MAC flooding

**7. Physical layer**

The physical layer is responsible for adequately connecting network nodes via wired or wireless means. Sniffing is the most common security attack used by attackers to target the data link layer.

**Attack: Sniffing attacks**

A sniffing attack in the data link layer occurs when an attacker captures and analyzes network traffic to gather sensitive information. This is done using a packet sniffer tool, which captures and decodes all the packets passing through a particular network segment. Sniffing attacks steal sensitive information such as login details, credit card numbers, and other personal and sensitive information.

**REAL WORLD CASE STUDIES**

* **The Mirai botnet attack** in 2016 used a vulnerability in the Data Link Layer to infect and control millions of IoT devices. The botnet then used these devices to launch a distributed denial-of-service (DDoS) attack against Dyn, a domain name system (DNS) provider. The attack caused widespread disruption to websites and online services.
* **The WannaCry ransomware attack** in 2017 used a vulnerability in the Network Layer to spread to computers running unpatched versions of Microsoft Windows. The ransomware encrypted files on the infected computers and demanded a ransom payment in exchange for the decryption key. The attack affected hundreds of thousands of computers in over 150 countries.
* **The Heartbleed bug** in 2014 was a vulnerability in the Transport Layer of the OpenSSL cryptographic library. The bug allowed attackers to read the memory of servers running OpenSSL, including sensitive data such as passwords and encryption keys. The bug was exploited by attackers to steal data from a number of high-profile organizations, including Yahoo, Facebook, and Google.
* **The SQL injection attack** is a type of attack that targets the Presentation Layer of a web application. The attack involves injecting malicious code into a web form or query string. When the victim submits the form or query, the malicious code is executed on the server, which can then be used to steal data or take control of the server.

**MITIGATION STRATEGIES**

**Physical Layer**

* Use strong physical security measures to protect network devices and infrastructure.
* Implement intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) to detect and prevent unauthorized access to physical network components.
* Use encryption to protect sensitive data in transit and at rest.

**Data Link Layer**

* Implement port security on switches to prevent unauthorized access to network segments.
* Use MAC filtering to restrict access to network devices based on their MAC addresses.
* Implement VLANs to isolate different networks from each other.

**Network Layer**

* Use firewalls to filter traffic between different networks.
* Implement IPsec to encrypt traffic between different networks.

**Transport Layer**

* Use TCP/IP with the SYN cookies option to mitigate SYN flood attacks.
* Use UDP with the checksum option to detect and prevent corrupted data packets.
* Use stateful inspection firewalls to track the state of connections and prevent unauthorized traffic.

**Session Layer**

* Implement authentication and authorization mechanisms to control access to network resources.
* Use encryption to protect sensitive data in transit and at rest.

**Presentation Layer**

* Use data encoding and decoding mechanisms to protect sensitive data from unauthorized access.
* Use encryption to protect sensitive data in transit and at rest.

**Application Layer**

* Implement input validation and output filtering to prevent cross-site scripting (XSS) and other attacks.
* Use encryption to protect sensitive data in transit and at rest.
* Keep software up to date with the latest security patches.

It is important to note that no single mitigation strategy can protect against all attacks. A layered approach that combines multiple security measures is the best way to protect your network from attack.