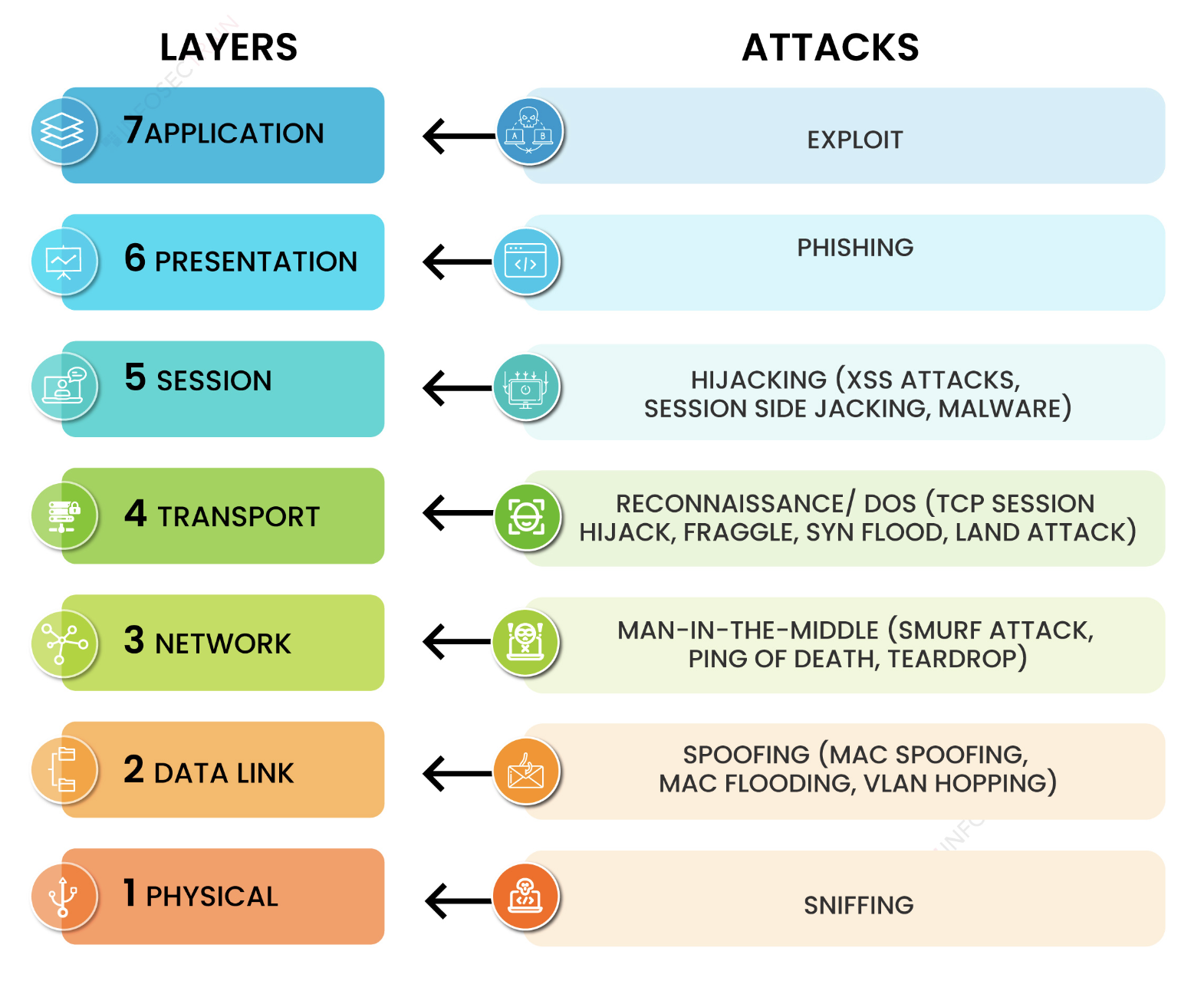
**Analysis of attack at each layer**

Attacks can occur at any layer some of the most common attacks at each layer are as follows:



Physical Layer:

* Denial of service (DoS) attacks: These attacks attempt to disrupt the physical layer by disabling network devices or interrupting the flow of data.
* Eavesdropping: It involves capturing and monitoring data as it travels across the physical layer.
* Man-in-the-middle (MitM) attack: This attack involves an attacker inserting themselves between two communicating parties and intercepting their data.

Data Link Layer:

* Sniffing: In this it involves capturing and monitoring data as it travels across the data link layer.
* Frame modification: This attack involves modifying data frames as they travel across the data link layer.
* MAC flooding: It involves flooding a network with malicious MAC addresses, which can disrupt network traffic.

Network Layer

* Routing attacks: In this attacker attempts to disrupt the routing of data packets across a network.
* Spoofing: This attack involves an attacker sending falsified data packets to a network, which can lead to data theft or denial of service.
* Man-in-the-middle (MitM) attack: This attack involves an attacker inserting themselves between two communicating parties and intercepting their data.

Transport Layer:

* Session hijacking: This attack involves an attacker taking over an existing session between two communicating parties.
* TCP/IP stack overflow: This attack involves exploiting a vulnerability in the TCP/IP stack to gain control of a system.
* SYN flood attack: This attack involves flooding a system with SYN packets, which can exhaust the system's resources and lead to a denial of service.

Session Layer:

* Session hijacking: This attack involves an attacker taking over an existing session between two communicating parties.
* Session replay: This attack involves an attacker capturing and replaying a session between two communicating parties.

Presentation Layer:

* Malformed data: This attack involves sending malformed data to a system, which can lead to system crashes or data corruption.
* Encryption attacks: These attacks attempt to break encryption used to protect data.
* Phishing attacks: These attacks involve sending fraudulent emails or text messages that appear to be from a legitimate source, to trick users into revealing sensitive information, often through fake websites or emails.

Application Layer:

* Injection attacks: These attacks involve injecting malicious code into a system through an application.
* Cross-site scripting (XSS) attacks: These attacks inject malicious code into websites to steal information or manipulate user interactions.

Mitigation Strategies

There are a number of mitigation strategies that can be used to protect against attacks at each layer of the OSI model. Some of the most common mitigation strategies include:

* Using firewalls and intrusion detection systems (IDSs): Firewalls and IDSs can be used to filter traffic and detect malicious activity.
* Encrypting data: Encrypting data can help to protect it from being intercepted and read by unauthorized parties.
* Using strong passwords and security best practices: Using strong passwords and following security best practices can help to protect systems from being compromised.
* Keeping software up to date: Keeping software up to date can help to protect systems from known vulnerabilities.

By implementing these mitigation strategies, organizations can help to protect their networks and data from a variety of attacks.

Reference:

* <https://medium.com/@e.ahmadi/attacks-on-various-osi-model-layers-bd2fac5ab985>
* <https://www.infosectrain.com/blog/common-security-attacks-in-the-osi-layer-model/>