THE OSI REFERENCE MODEL VS. TCP/IP MODEL

Before the 1980s, computers from different vendors could only communicate within their network, which meant that a Cisco computer, for example, could only communicate with another Cisco computer.

To tackle this challenge, two groups of engineers came up with the OSI and TCP/IP models. These models are now incorporated into devices, enabling computers from different companies to connect and communicate across networks. The TCP/IP Model, created by the U.S. Department of Defense, has four layers and is the most widely used model in practice. On the other hand, the OSI Reference Model was developed by the International Organization for Standardization (ISO) and consists of seven layers. Although the modern internet does not strictly follow the OSI model, network engineers still use this model as a reference and to troubleshoot network issues.

The **TCP/IP model** consists of four (4) layers, called the Internet Protocol Suite, which are:

Layer 4: Application Layer.

Layer 3: Transport Layer.

Layer 2: Internet Layer.

Layer 1: Network Access Layer.

The **OSI Model consists** of seven (7) layers, called the Protocol Stack, which are:

Layer 7: Application Layer.

Layer 6: Presentation Layer.

Layer 5: Session Layer.

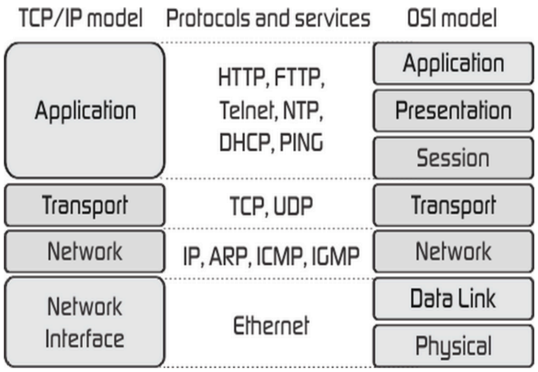
Layer 4: Transport Layer.

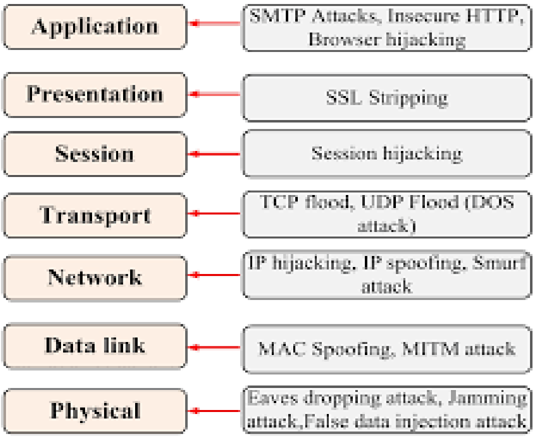
Layer 3: Network Layer.

Layer 2: Data-link Layer.

Layer 1: Physical Layer.

The diagrams below illustrate how the TCP/IP model maps to the OSI model, the protocols on each layer, and the attacks on each layer.




Application
SMTP Attacks, Insecure HTTP, Browser hijacking
Presentation
SSL Stripping
Session
Session hijacking
Transport
TCP flood, UDP Flood (DOS attack)
Network
IP hijacking, IP spoofing, Smurf attack
Data link
MAC Spoofing, MITM attack
Physical
Eaves dropping attack, Jamming attack,False data injection attack

In this report, I will base my references on the OSI model for an in-depth understanding.

Application Layer: This layer enables network applications and determines their behavior. It uses protocols to provide the basic functions and services when data is transmitted between devices over the internet. For example, Kate transfers files across the internet to a file server.

Presentation Layer: This layer receives data from the Application Layer on the sending device, and translates it into machine language. It also encrypts and compresses the data to reduce its size for faster delivery. The data is encapsulated in a layer 6 header.

Session Layer: It manages communication sessions with the receiving device for data transfer, performs authentication and authorization, and establishes a checkpoint used by the transport layer. It encapsulates the layer 6 data in a layer 5 header.

Transport Layer: This layer is responsible for error control, flow control, and segmentation. It divides the data into segments and encapsulates them in a layer 4 header consisting of the source port number, destination port number, and sequence number.

Network Layer: This layer receives segments and divides them into packets. It encapsulates the packets in a layer 3 header containing the IP addresses of the source and destination devices and determines the fastest path to deliver the IP packets.

Data-link Layer: This layer divides the packets into frames and encapsulates them in a layer 2 header and trailer. The header includes the MAC address of the sending device and router. A frame check sequence is included in the trailer for error correction. This layer also uses framing to allow upper layers to access the media.

Physical Layer: This layer receives the frames, converts them into signals (in the form of bitstream), and transmits them across the media to the destination device.

At the receiving device, the physical layer converts the bit stream into frames, then, each frame, packet, segment, and data are de-encapsulated in the layer by which they were encapsulated, and reassembled, and the data is received in the application layer of the receiving device.

Routing: This refers to the process of transmitting packets from the source device to the intended destination device. This is accomplished at Layer 3 utilizing the IP Protocol, which is a connectionless protocol. The routing process employs a routing table comprising a list of IP addresses that correspond to the path towards the destination. Once a match for the path to the destination is determined, the packet is forwarded to the router, and the process continues until it reaches the destination using the shortest available distance.

Flow Control: TCP (Transmission Control Protocol) uses flow control at the Transport Layer to manage the amount of data sent. The window size (the maximum amount of data that can be sent before an ACK (acknowledgment) is received) is communicated to the sending device by the receiving device. The sequence number is used to reorder segments. If no acknowledgment is received, the sender will resend the segments. The window size can be increased or decreased based on the state of the connection. This is done to prevent overwhelming the receiver, which could lead to data loss or device failure. This doesn't apply to UDP (User Datagram Protocol).

Error correction: This is performed at layer two. When a packet arrives at layer two of the sending device, it is divided into frames and encapsulated using a header and a trailer (the trailer contains the Frame Check Sequence (FCS) field). The sending device uses a mathematical function to compute a value, which is then stored in the FCS field. The receiving device receives the frame and performs the same mathematical function. It compares the result with the value in the FCS field. The frame is de-encapsulated and sent to the network layer if the results match. However, if the results don't match, there's an error and the frame is discarded. Retransmission of the packet is dependent on the TCP protocol in layer 4.

References:

Fig.1: https://fiberbit.com.tw/tcpip-model-vs-osi-model/ - Fiberbit website.
Fig.2: https://www.mdpi.com/1996-1073/16/12/4573 - MDPI website.