Networking Models

Two networking models describe the communication and transfer of data from one host to another, called ISO/OSI model and the TCP/IP model. This is a simplified representation of the so-called layers representing transferred Bits in readable contents for us.

Comparison of OSI and TCP/IP Models

- **OSI Model** has 7 layers:

    - Application
    - Presentation
    - Session
    - Transport
    - Network
    - Data-Link
    - Physical

- **TCP/IP Model** has 4 layers:

    - Application
    - Transport
    - Internet
    - Link

The OSI Model

The OSI model, often referred to as ISO/OSI layer model, is a reference model that can be used to describe and define the communication between systems. The reference model has seven individual layers, each with clearly separated tasks.

The term OSI stands for **Open Systems Interconnection** model, published by the **International Telecommunication Union (ITU)** and the **International Organization for Standardization (ISO)**.

The TCP/IP Model

TCP/IP (**Transmission Control Protocol/Internet Protocol**) is a generic term for many network protocols. The protocols are responsible for the switching and transport of data packets on the Internet.

TCP/IP is used as a **generic term** for the protocol family, including:

- TCP
- IP
- ICMP (Internet Control Message Protocol)
- UDP (User Datagram Protocol)

These protocols provide necessary functions for transporting and switching data packets in both private and public networks.

ISO/OSI vs. TCP/IP

- **TCP/IP** is a communication protocol allowing hosts to connect to the Internet. It is more flexible in its rules.
- **OSI** is more of a communication **reference model** between the network and end-users, known for its strict protocols and limitations.

Packet Transfers

In a layered system, devices in a layer exchange data using **Protocol Data Units (PDUs)**.

- When browsing a website, data is passed down through each layer (Application → Physical) on the sender's side.
- Each layer **adds a header** (encapsulation).
- On the receiving end, headers are **stripped away** (decapsulation) as data travels back up.

PDU Representation

OSI Layer	TCP/IP Layer	PDU
Application	Application	Data
Presentation		
Session		
Transport	Transport	Segment
Network	Internet	Packet
Data-Link	Link	Frame
Physical		Bit

Encapsulation and Decapsulation

- Each layer **adds a header** during transmission (encapsulation).
- Each layer **removes the header** during reception (decapsulation).
- Process ensures data integrity and structured communication.

Summary

As penetration testers:

- Use **TCP/IP** to understand high-level communication.
- Use **OSI** to break down and analyze data in detail.

- Both models are essential for **network traffic analysis**.

Understanding both models is crucial for mastering network analysis and developing strong cybersecurity skills.