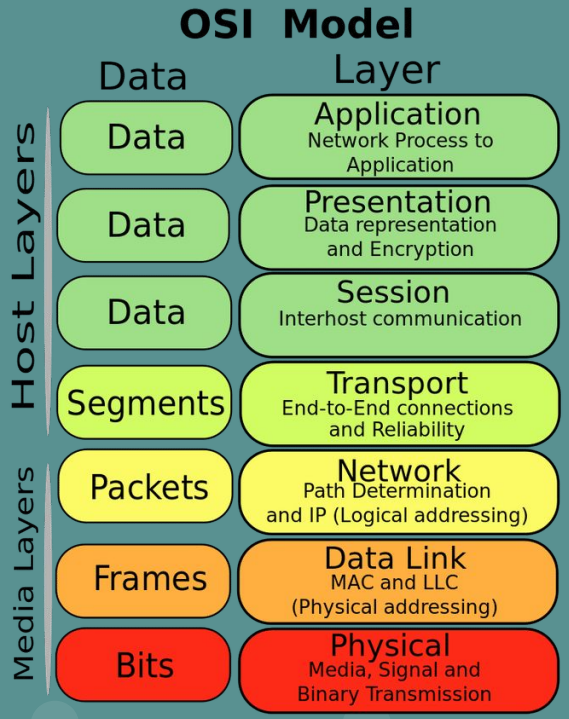
Comprehensive Analysis of Attacks on the OSI Model

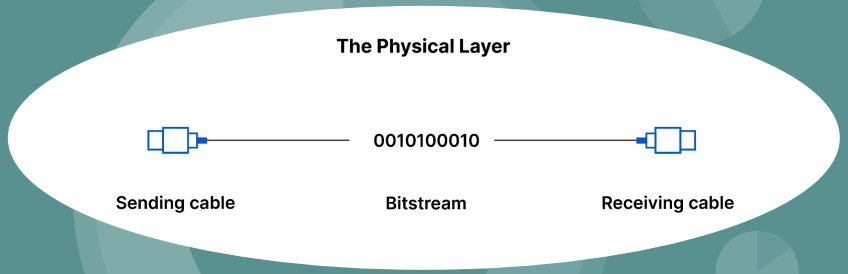
We are representing Nigella Group

OSI - OPEN SYSTEM INTERCONNECTION

The Open Systems Interconnection (OSI) model defines a networking framework to implement protocols in layers, with control passed from one layer to the next. It is primarily used today as a teaching tool. It conceptually divides computer network architecture into 7 layers in a logical progression.



1. Physical Layer



At the bottom of our OSI model we have the Physical Layer, which represents the electrical and physical representation of the system. This can include everything from the cable type, radio frequency link (as in a Wi-Fi network), as well as the layout of pins, voltages, and other physical requirements.

Physical Layer Attack :-

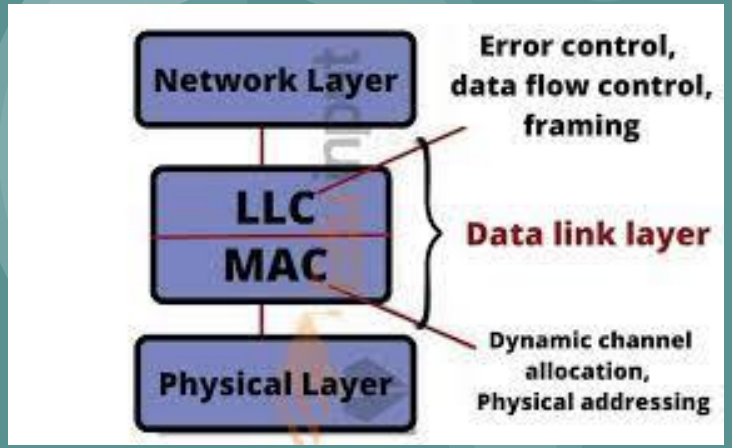
- ★ Denial of Service (DoS): Physically damaging or disrupting network infrastructure, such as cutting cables or overloading network devices.
- ★ Jamming: This is an attack that disrupts the physical transmission of data.
  - ○ For example, an attacker could jam a signal on a network cable or inject corrupted data into a network.

Physical Layer Attack Impact :-

- ★ Denial of Service (DoS) attacks disrupt or overwhelm a network or server, rendering it inaccessible to legitimate users.
- ★ Jammer devices emit radio frequency interference, disrupting wireless communications, such as cell phones or Wi-Fi signals, causing service disruptions or preventing communication in a targeted area.

2. Data Link Layer

The Data Link Layer provides node-to-node data transfer (between two directly connected nodes), and also handles error correction from the physical layer. Two sublayers exist here as well--the Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. In the networking world,



Data Link Layer Attack :-

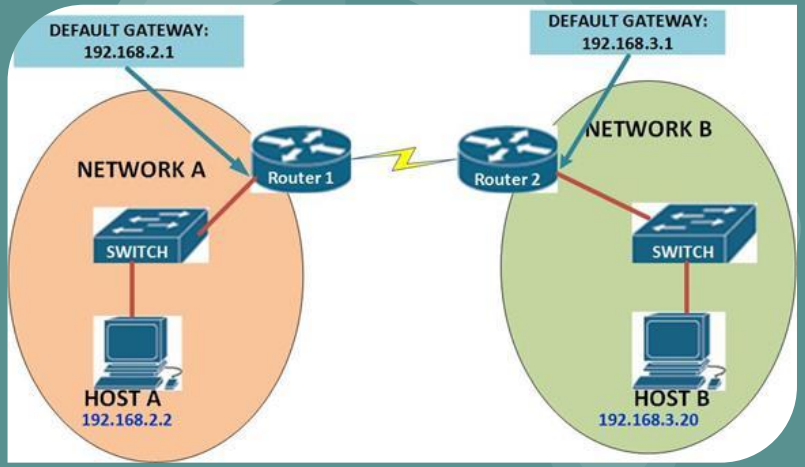
- ★ MAC Spoofing: Forging or impersonating Media Access Control (MAC) addresses to gain unauthorized access to a network.
- ★ ARP Poisoning: Manipulating Address Resolution Protocol (ARP) tables to redirect network traffic or perform man-in-the-middle attacks.

Data Link Layer Attack mitigation strategies :-

- ★ Network administrators can implement measures such as port security, MAC address filtering, MAC address whitelisting, network access control (NAC) solutions, and regular monitoring of network logs to detect and respond to suspicious MAC address activities.
- ★ Network administrators can implement techniques like ARP inspection, dynamic ARP inspection (DAI), or use secure ARP protocols like ARPSEC to detect and prevent ARP spoofing attacks.

3. Network Layer

Here at the Network Layer is where you'll find most of the router functionality that most networking professionals care about and love. In its most basic sense, this layer is responsible for packet forwarding, including routing through different routers.



Network Layer Attack :-

★ IP Spoofing: Forging or impersonating IP addresses to deceive network devices and gain unauthorized access. For Example- an attacker could send a packet with a forged IP address, which would cause the victim's computer to think that the packet came from a trusted source.

Attack Impact :-

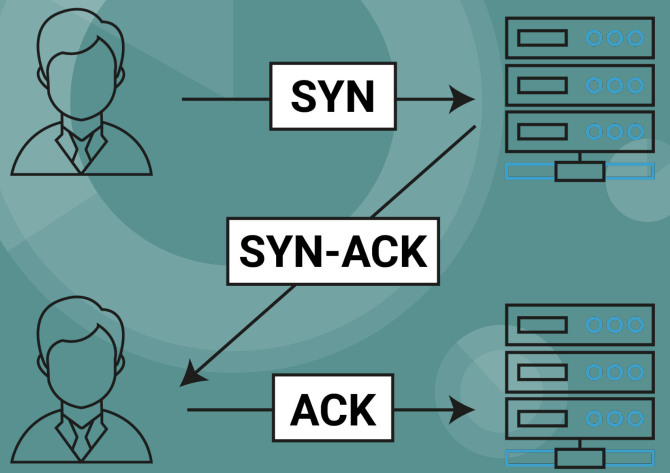
★ IP spoofing allows attackers to falsify the source IP address of network packets, making it difficult to trace the origin of the attack or enabling impersonation, facilitating various malicious activities such as DDoS attacks or unauthorized access.

Attack mitigation strategy :-

★ Network administrators can implement measures such as ingress and egress filtering, implementing anti-spoofing rules, and deploying network-based intrusion detection systems (IDS) or intrusion prevention systems (IPS).

4. Transport Layer

The Transport Layer deals with the coordination of the data transfer between end systems and hosts. How much data to send, at what rate, where it goes, etc. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are the most common examples of Transport Layer protocol.



techopedia

Transport Layer Attack :-

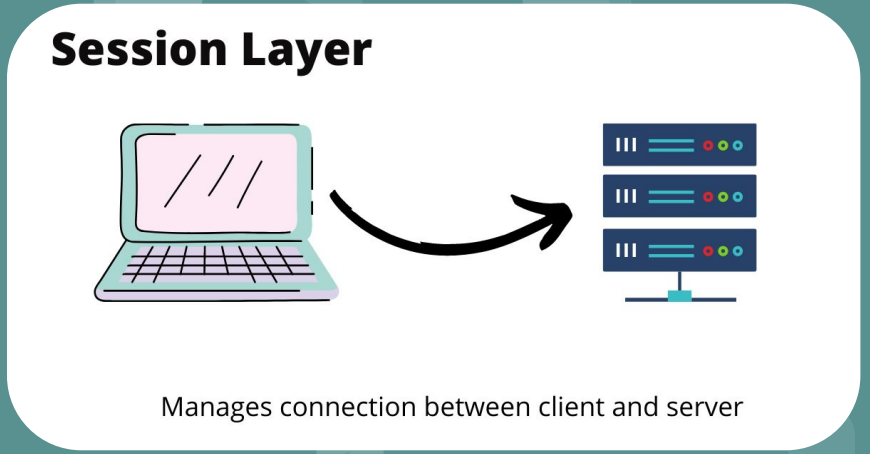
- ★ SYN flooding: This is an attack that floods a server with SYN requests. This can cause the server to become overloaded and unable to respond to legitimate requests.
- ★ TCP/IP Hijacking: Attackers intercept and manipulate TCP/IP packets to hijack an established TCP connection, allowing them to eavesdrop on or modify the communication, or perform session hijacking.

Mitigation strategies :-

- ★ network administrators can implement techniques like SYN cookies, rate limiting, or deploying firewalls and intrusion prevention systems (IPS) to detect and block suspicious SYN flood traffic.
- ★ Mitigation techniques for transport layer attacks include implementing rate limiting, traffic monitoring, access control lists (ACLs), firewall rules, Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS), and configuring network devices to drop or mitigate abnormal traffic patterns associated with these attacks.

5. Session Layer

The Session Layer manages the sequence and flow of events that initiate and tear down network connections. At layer 5, it is built to support multiple types of connections that can be created dynamically and run over individual networks.When two computers or other networked devices need to speak with one another, a session needs to be created, and this is done at the Session Layer.



Session Layer Attack :-

★ Session hijacking: This is an attack that allows an attacker to take control of an existing session. For example- an attacker could intercept a session cookie and use it to gain access to the victim's account.

Impact :-

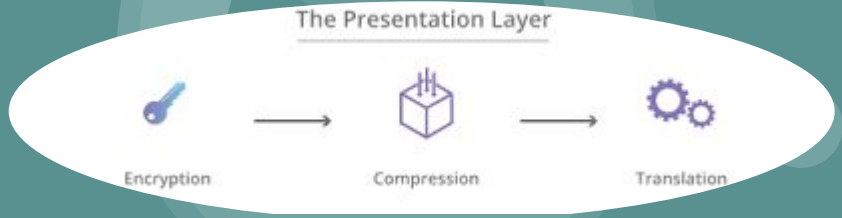
★ Session hijacking allows attackers to gain unauthorized access to a user's session, enabling them to impersonate the user, access sensitive information, perform unauthorized actions, and potentially compromise the entire system.

mitigation strategies :-

★ Session hijacking allows attackers to gain unauthorized access to a user's session, enabling them to impersonate the user, access sensitive information, perform unauthorized actions, and potentially compromise the entire system.

6. Presentation Layer

The Presentation layer has the simplest function of any piece of the OSI model. At layer 6, it handles syntax processing of message data such as format conversions and encryption/decryption needed to support the Application layer above it.



Presentation Layer attack :-

★ Code injection: Embedding malicious code or commands into data streams to exploit vulnerabilities in the receiving system.

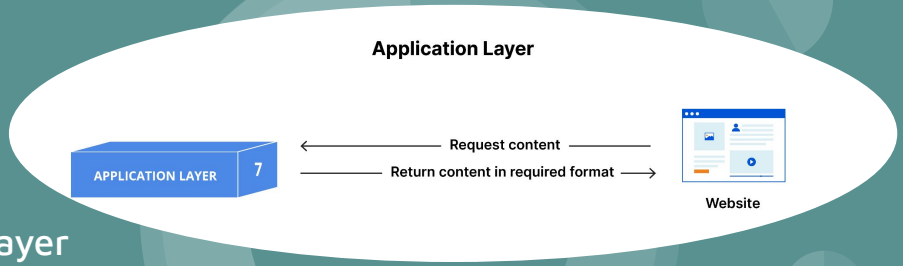
Impact :-

★ Code injection allows attackers to execute malicious code within an application, leading to unauthorized access, data breaches, system compromise, or the manipulation of the application's behavior and functionality.

mitigation strategies :-

★ developers should employ secure coding practices, input validation, and parameterized queries, and utilize web application firewalls (WAFs) to detect and block malicious code injection attempts.

7. APPLICATION LAYER



The Application Layer in the OSI model is the layer that is the “closest to the end user”. It receives information directly from users and displays incoming data to the user.Network services are protocols that work with the user's data.the Application layer protocol HTTP packages the data needed to send and receive web page content.Web browsers (Google Chrome, Firefox, Safari, etc.) TelNet, and FTP, are examples of communications that rely on Layer 7.

Application Layer Attack :-

- ★ Cross-Site Scripting (XSS): Injecting malicious scripts into web applications, which are then executed by unsuspecting users visiting the compromised page.
- ★ SQL injection: Inserting malicious SQL statements into input fields of a web application to manipulate the underlying database or gain unauthorized access.

mitigation strategies :-

- ★ developers should implement input validation, output encoding, and use security libraries or frameworks that provide protection against XSS vulnerabilities.
- ★ developers should use parameterized queries or prepared statements, input validation, and implement strict access controls to prevent unauthorized database access and manipulation.

Case Study 1: The Morris Worm

The Morris worm was a computer worm that infected Unix systems in 1988. The worm exploited a buffer overflow vulnerability in the sendmail program, which allowed it to gain control of the victim's system. The worm then spread to other systems by sending itself to random IP addresses.

The Morris worm had a significant impact on the Internet. It infected over 6,000 systems and caused millions of dollars in damage. The worm also caused widespread disruption to the Internet, as many systems were taken offline to prevent the worm from spreading.

The Morris worm was a significant event in the history of computer security. It highlighted the vulnerability of Unix systems to buffer overflow attacks and led to the development of new security measures, such as stack protection.

Case Study 2: The Stuxnet Worm

The Stuxnet worm was a computer worm that targeted Iranian nuclear facilities in 2010. The worm exploited a vulnerability in the Siemens Step 7 software, which is used to control industrial control systems. The worm then spread to other systems by sending itself to random IP addresses.

The Stuxnet worm had a significant impact on the Iranian nuclear program. It caused significant damage to the centrifuges used to enrich uranium and forced Iran to shut down its nuclear program for several months. The worm also caused widespread fear and uncertainty in the international community, as it demonstrated the ability of cyber attacks to disrupt critical infrastructure.

The Stuxnet worm was a sophisticated attack that took advantage of vulnerabilities in both the physical and cyber worlds. It was a wake-up call for the international community, as it showed that cyber attacks could have a real-world impact

Thank You