****

**CYBERSECURITY INTERNSHIP**

Week 2

**Group Task**

*Team Gentian*

Date: 08/07/2023

**Comprehensive Analysis of Attacks on the OSI Model**

**Introduction:**

The Open Systems Interconnection (OSI) model is a conceptual framework that defines the functions of a network into seven layers. Each layer plays a specific role in transmitting and receiving data.

Unfortunately, attackers can target vulnerabilities at various layers of the OSI model.

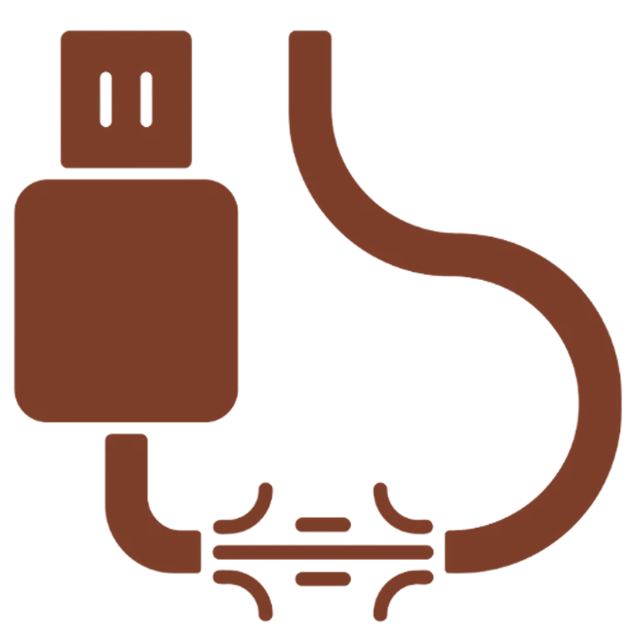
We need security at each layer of OSI model for protecting CIA of the system. Network security includes information security and computer security. It also requires firewalls for protecting systems or data from being attacked and hacked. Cybersecurity threats exist at all OSI-ISO model layers beginning at Layer 7 – the Application Layer because that’s the place where users begin by interfacing with the network. In the table, some common attacks that occur at different layers are shown:

| **LAYERS** | **TYPES OF ATTACKS** | **IMPACT OF ATTACK** |
| --- | --- | --- |
| Application Layer | Possible exploits at the Application Layer include viruses, worms, phishing, keyloggers, backdoors, program logic flaws, bugs, and trojan horses. | No user is able to access the network resources |
| Presentation Layer | SSL Hijacking, Phishing | Affected systems stop accepting SSL requests and automatically restarts |
| Session Layer | Session Hijacking, MITM Attack | Disable Management operations |
| Transport Layer | TCP SYN Flooding | Connection limits of hosts |
| Network Layer | man-in-the-middle | Affects the network BW and overloads the firewall |
| Data Link Layer | IP spoofing, ARP spoofing | Disrupts the flow of data across all the ports |
| Physical Layer | Sniffing | Disconnection of links, data destroyed, access control,Environmental issues |

**Attacks on the OSI Model:**

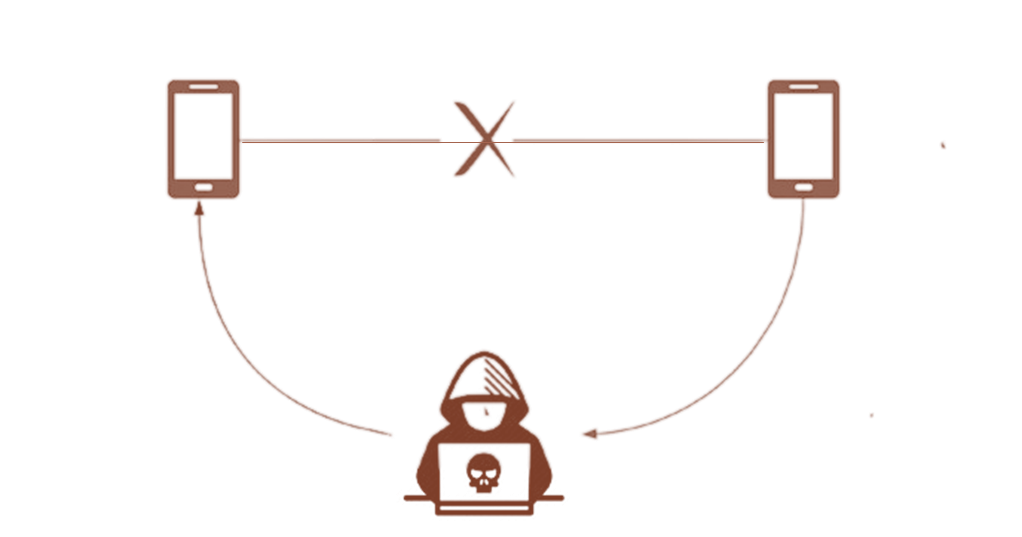
**1. Physical Layer:** This layer deals with the physical transmission of data over the network, including electrical, mechanical, and physical specifications. It defines how bits are transmitted through cables, wireless signals, or other physical media.

* Physical layer attacks involve tampering with the physical components of the network, such as cutting cables, unauthorized access to network equipment, or intercepting electromagnetic signals. These attacks can disrupt network connectivity and compromise data confidentiality.



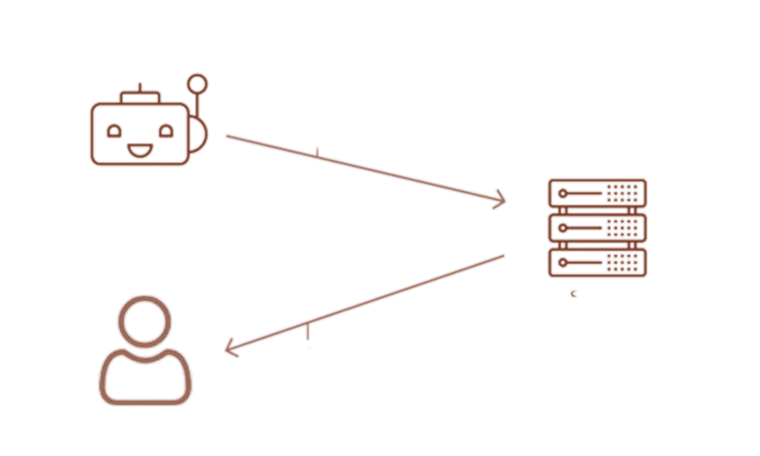
**2. Data Link Layer:** The data link layer provides reliable point-to-point data transfer between devices on the same network segment. It deals with framing, error detection and correction, and flow control. Ethernet is an example of a data link layer protocol.

* Mac Address Spoofing Attacks: This layer includes MAC address spoofing, where an attacker impersonates the MAC address of a trusted device to gain unauthorized access. It can also involve attacks on the data link layer protocols to intercept or modify network traffic.



**3. Network Layer:** This layer handles the routing of data packets between different networks. It determines the best path for data transmission based on logical network addresses (IP addresses) and is responsible for logical addressing, routing, and fragmentation.

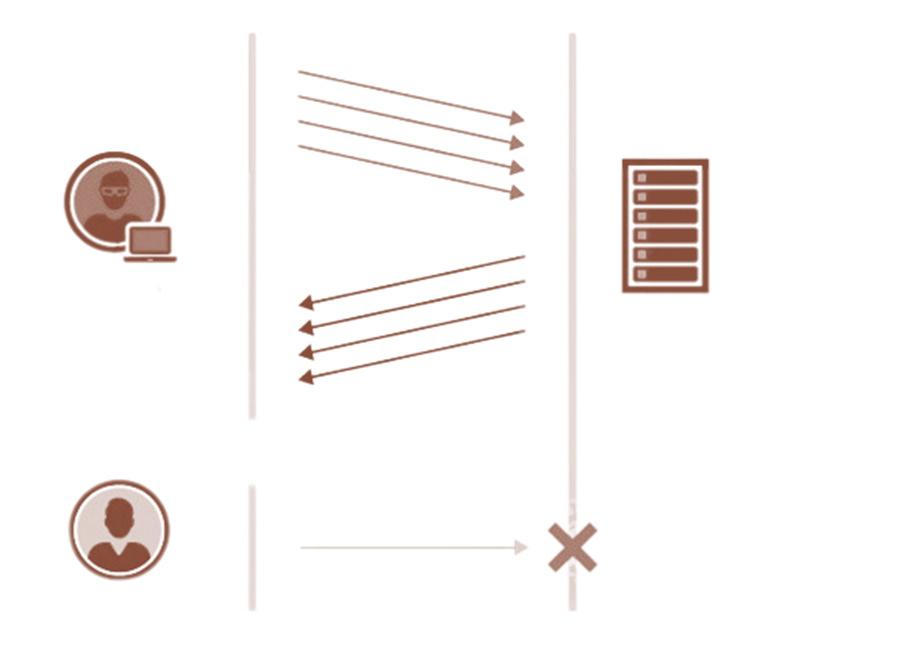
* IP spoofing: Network layer attacks can include IP spoofing, where an attacker falsifies the source IP address to deceive or impersonate another system. Network layer attacks can also involve network scanning, denial-of-service (DoS) attacks, or routing protocol attacks to manipulate routing tables.



**4. Transport Layer:** The transport layer ensures reliable and transparent transfer of data between end systems. It provides mechanisms for segmentation, reassembly, error recovery, and flow control. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)

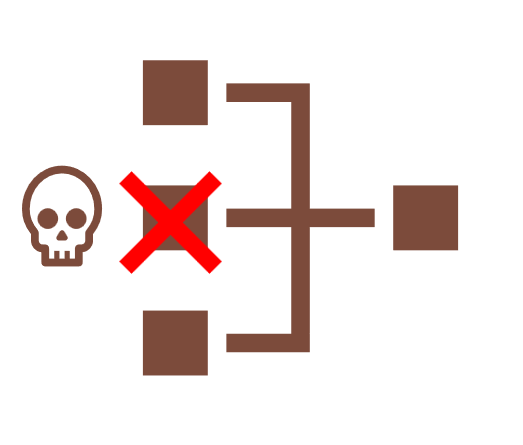
operate at this layer.

* In TCP SYN Flooding attack, the attacker floods a target server with a large number of TCP SYN requests, consuming server resources and exhausting its ability to handle legitimate connection requests. By overwhelming the server with incomplete connections, the attacker aims to disrupt or disable the target system, rendering it unable to respond to legitimate user requests.



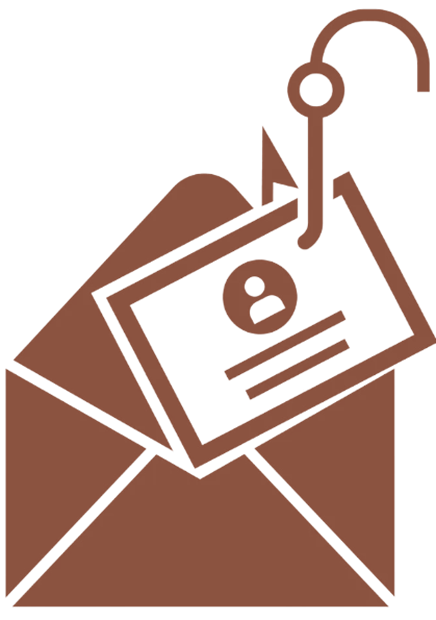
**5. Session Layer:** The session layer establishes communication channels between devices, known as sessions. It starts sessions, keeps them open and effective while data is transferred, and closes them after communication is completed.

* Hijacking 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.



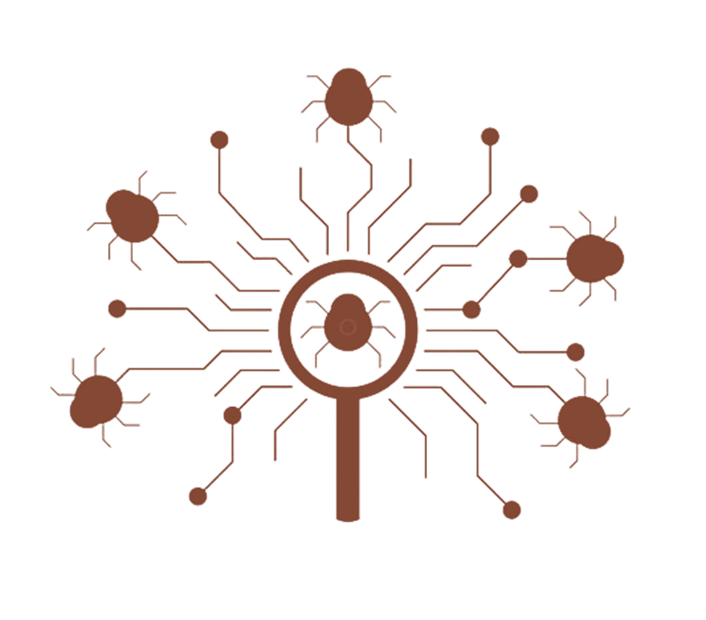
**6. Presentation Layer:** The presentation layer specifies the two devices’ encoding, encryption, and compression methods for proper communication. Anything sent from the application layer is received by the presentation layer, which is transformed into a format suitable for transmission via the session layer.

* Phishing 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 or install malware on the victim’s system.



**7. 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.

* 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. Without employing an exploit, attackers can take down a website by using DoS (Denial-of-Service) or DDoS (Distributed Denial-of-Service) cyberattacks.



**Impact of Attacks and Consequences:**

1. **Impacts on Physical Layer:**

* Data corruption: If the physical transmission of data is disrupted, it can lead to data corruption. This can make data unreadable or unusable and can cause significant problems for applications that rely on this data.
* Eavesdropping: An attacker can also use a physical layer attack to eavesdrop on network traffic. This allows them to steal sensitive data, such as passwords or credit card numbers.

1. **Impacts on Data Link Layer:**

* Unauthorized Access and Data Breaches: Attacks targeting Layer 2 can enable unauthorized access to the network. By exploiting vulnerabilities in protocols like Ethernet or Wi-Fi, attackers can gain entry into the network infrastructure. This can lead to data breaches, as the attackers can intercept, modify, or steal sensitive information flowing through the network.
* Compromised Network Infrastructure: Attacks on Layer 2 can compromise the integrity and security of network infrastructure devices such as switches and routers. If attackers gain control over these devices, they can manipulate network traffic, redirect data to malicious destinations, or launch further attacks on higher layers of the OSI model.
* Operational Disruptions: An attack on Layer 2 can cause operational disruptions for organizations. For example, if a network switch is compromised, it may result in network outages, loss of connectivity, or impaired network performance. These disruptions can lead to financial losses, productivity loss, and business reputation damage.

1. **Impacts on Network Layer:**

* Network Disruption: Attacks targeting Layer 3 can disrupt network connectivity and cause service outages. For example, a Distributed Denial of Service (DDoS) attack at Layer 3, such as a SYN flood attack, can flood a target network with an overwhelming amount of traffic, exhausting its resources and rendering it unable to handle legitimate traffic. This can result in network downtime and a loss of connectivity for users.
* Routing Manipulation: Layer 3 attacks can target routing protocols and manipulate the routing tables, causing traffic to be redirected or misrouted. This can result in data packets being sent to unauthorized destinations or falling into malicious hands, compromising data confidentiality and integrity. Routing manipulation attacks can also lead to network congestion and suboptimal performance.
* Network Resource Exhaustion: Certain Layer 3 attacks, such as ICMP flood attacks or ICMP redirect attacks, can consume network resources, such as bandwidth, processing power, and memory. This can lead to performance degradation, reduced network efficiency, and increased operational costs as organizations need to invest in additional resources to handle the attack traffic.

1. **Impacts on Transport Layer:**

* Degraded Performance: Attacks on the Transport Layer can degrade network performance by introducing delays, packet loss, or high latency. For example, a SYN flood attack, which overwhelms a host with a large number of incomplete connection requests, can exhaust network resources and cause delays in establishing connections, resulting in slow response times and degraded performance for legitimate users.
* Impaired Data Integrity: Attacks targeting the Transport Layer can manipulate or tamper with the integrity of transmitted data. By intercepting or altering data packets, an attacker can modify information, insert malicious code, or execute man-in-the-middle attacks. This compromises the integrity of the data, leading to potential data corruption, unauthorized access, or unauthorized modifications.
* Unauthorized Access and Data Theft: Certain attacks on the Transport Layer, such as session hijacking or TCP/IP hijacking, can enable unauthorized access to sensitive information transmitted over the network. By exploiting vulnerabilities in the transport protocols, attackers can gain access to confidential data, login credentials, or financial transactions, potentially leading to identity theft, data breaches, or financial losses.

1. **Impacts on Session Layer:**

* Disruption of Communication Sessions: Attacks on the Session Layer can result in the disruption or termination of established communication sessions. By interfering with session establishment or injecting malicious data into ongoing sessions, an attacker can render the sessions ineffective or non-operational. This can lead to interruptions in communication and loss of productivity.
* Session Data Manipulation or Tampering: Attacks on Layer 5 can involve tampering with session-related data, such as session identifiers or session parameters. By manipulating this data, attackers can attempt to gain unauthorized access to resources or inject malicious code into the session, potentially leading to the compromise of system integrity or unauthorized data modifications.

1. **Impacts on Presentation Layer:**

* Loss of Data Format Compatibility: The Presentation Layer is responsible for translating data formats between the application layer and the lower layers. An attack on this layer can disrupt the data format conversion process, leading to compatibility issues. This may result in data transmission errors, loss of data integrity, and difficulties in interpreting and using the transmitted information.
* Impact on Application Functionality: The Presentation Layer also plays a role in data compression and decompression. An attack targeting this functionality can disrupt the compression algorithms, resulting in inefficient or incorrect data compression. This can lead to increased bandwidth usage, slower data transmission, and reduced application performance.

1. **Impacts on Application Layer:**

* Service Disruptions: Attacks targeting the Application Layer can render applications or services inaccessible or unavailable to legitimate users. This can result in significant disruptions to business operations, leading to financial losses, reduced productivity, and negative customer experiences
* Data Breaches and Information Exposure: Attacks on Layer 7 can exploit vulnerabilities in applications to gain unauthorized access to sensitive information. This can include user credentials, personal data, financial information, or confidential business data. Data breaches can result in severe consequences, including financial penalties, legal ramifications, damaged reputation, and loss of customer trust.
* Impact on User Trust and Reputation: Attacks on Layer 7 can erode user trust in the affected organization or application. Users may become hesitant to use the compromised service or share their personal information, resulting in a loss of customers and a damaged reputation. Rebuilding trust can be a lengthy and challenging process.

**Attack Mitigation Techniques:**

1. **Physical Layer (Layer 1)**

**•Attacks:** Sniffing and Eavesdropping

**•Mitigation:**

* Physical Security: Securing physical access to network infrastructure is a fundamental aspect of mitigating physical layer attacks. This includes Restricting access to network equipment rooms, server rooms, and data centers through the use of access control systems, such as keycards, biometric scanners, or security guards, monitoring facilities using video surveillance and intrusion detection systems to identify unauthorized entry attempts or suspicious activities, conducting regular security audits to ensure compliance with security policies and to identify potential vulnerabilities.
* Endpoint Protection: Securing the devices connected to the network is another critical aspect of mitigating physical layer attacks. This can be achieved through:
* Installing antivirus software, firewalls, and intrusion detection systems on devices to detect and prevent malware and unauthorized access attempts.
* Regularly updating device software, firmware, and security patches to address known vulnerabilities and reduce the risk of exploitation.
* Implementing strong authentication mechanisms, such as two-factor authentication (2FA), to protect against unauthorized access.
* Employee Awareness and Training: Educating employees about the risks associated with physical layer attacks and the importance of maintaining secure practices is an essential component of an effective mitigation strategy. This includes:
* Conducting regular training sessions to inform employees about potential threats, warning signs, and best practices for maintaining physical security.
* Encouraging employees to report any suspicious activities, unauthorized access attempts, or security incidents.
* Implementing a clear and comprehensive security policy that outlines the organization’s expectations and requirements for maintaining physical security.

1. **Data Link Layer (Layer 2)**

**•Attacks:** MAC Spoofing, Address Resolution Protocol (ARP) Spoofing

**•Mitigation:**

* MAC Address Filtering: Implement MAC address filtering on switches and routers to control access to the network. By allowing only authorized devices to connect, organizations can reduce the risk of unauthorized devices gaining access to sensitive data or launching attacks.
* Encryption: Employ encryption techniques, such as Wi-Fi Protected Access (WPA) or WPA2, to protect data transmitted across wireless networks. This can help prevent eavesdropping and Man-in-the-Middle (MITM) attacks.
* Port Security: Enable port security features on network switches to limit the number of devices that can connect to a specific port or disable ports that are not in use. This can help prevent unauthorized devices from connecting to the network and launching attacks.
* Robust Authentication: Implement strong authentication mechanisms, such as 802.1X, for devices connecting to the network. This can help ensure that only authorized devices are granted access and reduce the risk of unauthorized access.
* Intrusion Detection and Prevention Systems (IDPS): Deploy IDPS solutions that can monitor the network for signs of malicious activity and take action to block or mitigate attacks in real time.
* Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify potential weaknesses in the data link layer and implement necessary patches or updates to address them.
* Regular Software Updates: Keep network devices, such as switches and routers, up-to-date with the latest firmware and security patches to address known vulnerabilities and reduce the attack surface.

1. **Network Layer Attacks (Layer 3)**

**•Attacks:** IP Spoofing, Routing Protocol Attacks

**•Mitigation:**

* Firewalls: Deploy firewalls at the network perimeter to filter and control incoming and outgoing traffic. Properly configured firewalls can help prevent unauthorized access and block known malicious traffic, including network layer attacks.
* Intrusion Detection and Prevention Systems (IDPS): Implement IDPS solutions to monitor network traffic for signs of suspicious activity and automatically block or mitigate detected threats.
* Network Segmentation: Divide the network into smaller, isolated segments to limit the scope of potential attacks and restrict lateral movement within the network.
* Access Control Lists (ACLs): Use ACLs on routers and switches to control and filter traffic based on specific criteria, such as IP addresses, protocols, or ports. This can help prevent unauthorized access and mitigate the impact of network layer attacks.
* Rate Limiting: Implement rate limiting on routers and firewalls to control the amount of traffic allowed from specific sources. This can help mitigate the impact of DoS and DDoS attacks by limiting the amount of traffic that can reach the target.
* Traffic Analysis: Regularly analyze network traffic for signs of abnormal activity or patterns that may indicate an ongoing attack. Network monitoring tools and threat intelligence feeds can help identify potential threats and take appropriate action.
* Security Patches and Updates: Keep network devices, such as routers, switches, and firewalls, updated with the latest security patches and firmware updates to address known vulnerabilities and reduce the attack surface.
* Redundancy and Load Balancing: Implement redundancy and load balancing techniques to distribute network traffic and reduce the impact of DoS and DDoS attacks on critical infrastructure.
* Security Awareness Training: Educate employees and users about the risks associated with network layer attacks and provide guidance on how to recognize and report potential security incidents.
* Incident Response Plan: Develop and maintain an incident response plan to ensure a swift and effective response to network layer attacks. Regularly review and update the plan, and conduct training exercises to ensure all relevant personnel are familiar with their roles and responsibilities.

1. **Transport Layer (Layer 4)**

**•Attacks**: DoS

**•Mitigation:**

* Rate Limiting: Implementing rate limiting can help mitigate SYN flood and UDP flood attacks by restricting the number of incoming connections or packets per second to a manageable level.
* Firewalls: Implementing firewalls with proper rules and filtering can help block unauthorized traffic and limit the exposure of open ports and services on the network.
* Monitoring and Logging: Monitoring network traffic and maintaining detailed logs can help identify signs of transport layer attacks, allowing for a quicker response to potential threats.
* Intrusion Detection/Prevention Systems (IDS/IPS): Utilize IDS/IPS systems to monitor network traffic for signs of TCP/IP hijacking. These systems can identify suspicious activities, such as unexpected modifications to TCP headers, and trigger alerts or block malicious traffic.
* Traffic filtering and blacklisting: Employ traffic filtering mechanisms to detect and block malicious traffic associated with DDoS attacks. Use techniques such as IP blacklisting, rate limiting, or traffic pattern analysis to identify and block malicious traffic sources.
* Content Delivery Networks (CDNs): Utilize CDNs to distribute and absorb traffic during DDoS attacks. CDNs help mitigate DDoS attacks by distributing the traffic across multiple servers and data centers, reducing the impact on the targeted network.

1. **Session Layer (Layer 5)**

**•Attacks:** Session Hijacking, MITM Attack.

**•Mitigation:**

* Secure Session Management: Using secure methods for generating, storing, and transmitting session tokens or cookies can help prevent session hijacking attacks. Ensure that session identifiers are sufficiently long and random to make guessing them more difficult. Set the secure flag on session cookies to ensure they are transmitted over encrypted channels only. This helps protect against session hijacking through the interception of unsecured cookies.
* Use SSL/TLS: Employ secure communication protocols like SSL (Secure Sockets Layer) or its successor TLS (Transport Layer Security) to encrypt the session data exchanged between the client and server. Encryption prevents attackers from intercepting and reading sensitive information.
* Validate and Sanitize User Input: Implement strict input validation and sanitization techniques to prevent common attacks like cross-site scripting (XSS) and SQL injection. Proper input handling reduces the risk of attackers injecting malicious code into the application.
* Session Timeout: Implementing short session timeouts and automatically terminating sessions after a period of inactivity can help reduce the risk of session hijacking and fixation attacks. Additionally, require users to re-authenticate for sensitive actions or after a certain period of time.
* Intrusion Detection and Prevention Systems (IDPS): Implementing an intrusion detection and prevention system can help identify and block potential session layer attacks, such as man-in-the-middle, replay, or denial of service attacks, in real-time.
* Verify Server Certificates: Implement robust certificate validation mechanisms to ensure that the server’s SSL/TLS certificate is valid, trusted, and issued by a recognized certificate authority. This helps prevent attackers from impersonating legitimate servers.
* Educate Users: Promote security awareness among users to recognize potential signs of a MitM attack, such as invalid certificates, unexpected warnings, or sudden changes in the website’s appearance. Encourage users to be cautious while connecting to public Wi-Fi networks or accessing sensitive information over insecure channels.

1. **Presentation Layer (Layer 6)**

**•Attacks:** SSL/TLS Vulnerabilities, Phishing.

**•Mitigation:**

* Regularly Update SSL/TLS Protocols: Keep up to date with the latest SSL/TLS protocols and configurations to ensure that known vulnerabilities are patched. Disable outdated or weak encryption algorithms and ciphers, and regularly update certificates.
* Implement Secure Coding Practices: Developers should follow secure coding practices to avoid introducing vulnerabilities related to data parsing and processing. Regular code reviews, static and dynamic analysis, and thorough testing can help identify potential issues before they become exploitable.
* Use Strong Encryption Algorithms: Employ strong, widely-accepted encryption algorithms and key management practices to protect sensitive data. Avoid using outdated or weak encryption methods, and regularly review and update cryptographic implementations as new threats emerge.
* Employ Content Filtering and Validation: Implement strict content filtering and validation mechanisms for data streams and file uploads to prevent the execution of malicious payloads. Scan incoming files and data for known malware signatures and disallow uploads of potentially harmful file types.
* Educate Users: Train employees to recognize and report suspicious content, files, or communications. Educating users on the risks associated with opening unexpected or unsolicited files can help prevent the spread of malware or the execution of malicious payloads.
* Regularly Update and Patch Software: Keep software and systems up to date with the latest patches and updates. This includes operating systems, web browsers, PDF readers, and other applications that may process or display data at the presentation layer.
* Monitor Network Traffic: Employ network monitoring tools to detect and analyze unusual traffic patterns or behaviors, which may indicate a potential attack at the presentation layer. Investigate and respond to such incidents promptly.
* Implement Intrusion Detection and Prevention Systems (IDPS): Use IDPS solutions to detect and prevent potential presentation layer attacks. These systems can identify and block suspicious traffic or activities, helping to safeguard your network and data.

1. **Application Layer (Layer 7)**

**•Attacks:** Exploiting.

**•Mitigation:**

* Regular software updates and patch management: Keep software, operating systems, and applications up to date with the latest security patches to address known vulnerabilities and reduce the risk of exploitation.
* Antivirus and antimalware software: Deploy antivirus and antimalware solutions on all devices to detect, prevent, and remove malicious software. Regularly update virus definitions and perform routine system scans.
* Strong authentication and access control: Implement multi-factor authentication (MFA), strong password policies, and role-based access control to limit unauthorized access to sensitive data and systems.
* Employee training and awareness: Educate employees about common application layer attacks, such as phishing and social engineering, and train them to recognize and report suspicious activity. Regularly conduct security awareness training and simulated phishing exercises.
* Secure software development practices: Follow secure coding practices to minimize vulnerabilities in application code. Implement security testing and vulnerability scanning throughout the development lifecycle to identify and remediate potential weaknesses.
* Web application firewalls (WAFs): Deploy WAFs to protect web applications from common attacks, such as SQL injection, cross-site scripting, and session hijacking. Regularly update WAF rules and configurations to address emerging threats.
* Network segmentation: Isolate sensitive systems and data from other parts of the network to limit the potential impact of a successful attack. Implement strong access controls and monitoring to detect unauthorized activity.
* Regular monitoring and incident response: Continuously monitor network and system activity for signs of intrusion or malicious behavior. Develop and maintain a comprehensive incident response plan to quickly detect, contain, and remediate security incidents.

**Real-World Case Studies**

**Case Study 1: The Equifax Data Breach *(Application Layer)***

In 2017, the Equifax credit reporting agency was the victim of a data breach that was carried out using a SQL injection attack. The attack resulted in the theft of sensitive personal information from over 143 million people, including names, Social Security numbers, and birthdates.

The SQL injection attack was carried out by an attacker who exploited a vulnerability in Equifax's website. The attacker was able to inject malicious code into the website, which allowed them to steal data from the company's database.

Impact: The impact of the data breach was significant. The affected individuals were at risk of identity theft and other financial crimes. Equifax also faced significant financial losses, as it had to pay millions of dollars in fines and settlements. The attack also highlighted the need for organizations to implement security measures to protect their websites from SQL injection attacks.

Recommendations for Mitigation:

To defend against SQL injection attacks, organizations can implement a number of mitigation strategies, including:

* Using a web application firewall (WAF): A WAF can be configured to block SQL injection attacks.
* Using secure coding practices: Developers should use secure coding practices to minimize the risk of SQL injection vulnerabilities in their code.
* Deploying web applications in a secure environment: Web applications should be deployed in a secure environment, such as a cloud environment with a robust security posture.
* Monitoring web application traffic: Organizations should monitor web application traffic for signs of malicious activity. This can help to identify and respond to attacks quickly.

In addition to these mitigation strategies, organizations can also take steps to improve the security of their databases. This includes:

* Using strong passwords: Database passwords should be strong and unique.
* Encrypting sensitive data: Sensitive data, such as credit card numbers, should be encrypted at rest and in transit.
* Regularly backing up databases: Databases should be regularly backed up to prevent data loss in the event of an attack.

By implementing these mitigation strategies and best practices, organizations can reduce their risk of being targeted by SQL injection attacks.

**Case Study 2: Distributed Denial of Service (DDoS) Attack on a Session Border Controller (SBC) *(Session Layer)***

In this case study, an organization experienced a distributed denial of service (DDoS) attack targeting their Session Border Controller (SBC). The SBC is responsible for managing and securing session initiation and termination for Voice over IP (VoIP) and other real-time communication services.

Impact: During the DDoS attack, a massive volume of traffic was directed toward the SBC, overwhelming its processing capabilities. As a result, legitimate communication sessions were disrupted, leading to service unavailability and a significant loss of productivity. The attack rendered the SBC incapable of handling legitimate traffic, effectively blocking access to the organization's communication services.

Recommendations for Mitigation:

To mitigate the impact of the DDoS attack, the organization implemented the following strategies:

* Traffic Filtering: The organization set up traffic filtering mechanisms to distinguish legitimate traffic from malicious traffic. By implementing traffic filtering rules, they could block or limit the incoming traffic that exhibited suspicious patterns or originated from known malicious sources.
* Rate Limiting: The organization imposed rate limits on incoming traffic to prevent the SBC from being overwhelmed by a sudden surge in requests. Rate limiting allowed them to control the number of session initiation requests and manage the traffic flow effectively.
* Collaboration with Service Provider: The organization collaborated with their Internet service provider (ISP) to divert and mitigate the attack traffic before it reached their network. By leveraging the ISP's network infrastructure and expertise, they were able to filter out the DDoS traffic and restore normal communication services.