SecOps Solution

CYBERSECURITY OSI LAYER

Attacks Possibility By OSI Layer Cyber Threat Intelligence

Pallavi Vishwakarma
Member of Technical Staff

Mar 03 2023 | 5 min reading

Figure 1

What is OSI Layer?

OSI (Open Systems Interconnection) Layer is a conceptual model that describes how data is transmitted over a network. It is a standardized reference model for communication between different systems and devices in a network.

The OSI model comprises seven layers, each representing a different stage in the transmission process.

The OSI model is used to help standardize network communication protocols and ensure interoperability between different devices and systems. It also helps troubleshoot network issues by providing a clear and structured way to identify where problems might occur.

How are attacks possible by the OSI layer?

Attacks are possible at each layer of the OSI model because each layer has its own unique vulnerabilities that can be exploited by attackers. These vulnerabilities can arise due to various factors such as design flaws, misconfigurations, software bugs, or weaknesses in the underlying protocols.

Let's discuss what attacks are possible at each layer and how we can mitigate it:

1. **Application Layer**

It provides the interface between the user and the network. Message and packet generation at this layer also contains DB access. End-user networks like Telnet, FTP, SMTP, and RAS function at this layer.

It uses the protocols FTP, HTTP, POP3, & SMTP and its device is a gateway.

Example of DOS technique that can be applied at this layer:

PDF GET requests, HTTP Get, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)

Impact of DOS attack: Resource starvation

When a service exceeds its resource limits, it can lead to resource starvation, which can cause the service to slow down, crash, or stop working altogether. This can have a cascading effect on other services that depend on the affected service, leading to a larger system failure.

Possible mitigation:

Application monitoring is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero-day and application layers. Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDOS attacks

2. **Presentation Layer**

The presentation layer is responsible for ensuring that data exchanged between applications is in a format that both applications can understand. It is also responsible for data encryption and decryption, which is important for maintaining the confidentiality and integrity of data being transmitted over the network.

It uses the protocols Compression and Encryption.

Example of DOS technique that can be applied at this layer:

Malformed SSL Requests -- Inspecting SSL encryption packets as resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server.

Impact of DOS attack: The affected systems could stop accepting SSL connections or automatically restart.

If the SSL service stops accepting SSL connections, it means that clients trying to connect to the affected system using SSL will be unable to establish a secure connection. This can result in various error messages being displayed on the client side. Depending on the severity of the issue, it may also impact other services or applications that rely on SSL for secure communication.

On the other hand, if the affected system automatically restarts, it could potentially interrupt or terminate any ongoing SSL connections. This could result in data loss or other issues, depending on the nature of the connections and the applications involved.

Possible mitigation:

To mitigate, consider options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attack traffic or violations of policy at an application delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in protected memory on a secure bastion host.

3. **Session Layer**

The Session layer is responsible for establishing, maintaining, and ending sessions between applications. A session is a logical connection between two applications that allows them to exchange data over a network.

It uses the protocol logon/logoff.

Example of DOS technique that can be applied at this layer:

Telnet DDos-attacker exploits a flaw in telnet server software running on the switch, rendering Telnet Services unavailable.

Impact of DOS attack: Prevents administrator from performing switch management functions.

The impact of a DoS attack on switch management functions could be significant. Depending on the severity of the attack, administrators may be unable to access the switch, monitor its performance, or perform maintenance tasks. This can result in degraded network performance, increased downtime, and potential security risks. If an attacker exploits vulnerabilities in the switch's firmware or software, they may be able to gain unauthorized access to the switch, preventing legitimate administrators from managing it.

Possible mitigation:

Check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability. You can implement appropriate security measures, such as firewalls, intrusion detection systems, and access controls.

4. **Transport Layer**

It is responsible for providing reliable, end-to-end data delivery and error detection and correction. The Transport layer works by breaking down the data received from the Session layer into smaller packets, or segments, and adding header information to each segment. The header contains information such as the source and destination addresses, sequence numbers, and error-checking codes.

It uses the protocols TCP and UDP.

Example of DOS technique that can be applied at this layer:

SYN flood: The attacker sends a large number of TCP SYN (synchronization) packets to the target system, with the aim of overwhelming the system's ability to process them.

Smurf attack: The attacker sends a large number of ICMP echo request packets to an intermediate network or device, using the spoofed IP address of the victim as the source address.

Impact of DOS attack: Reach bandwidth or connection limits of hosts or networking equipment.

When a host or networking equipment reaches its bandwidth or connection limits, it becomes unable to handle any more requests or traffic and may become unresponsive or even crash. This can lead to disruptions in service, loss of data, and financial losses for businesses and organizations that rely on these systems.

Possible mitigation:

DDoS attack blocking commonly referred to as blackholing is a method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. Blocking holding is typically deployed by the ISP to protect other customers on its network from the adverse effects of DDoD attacks such as slow

network performance and disrupted services.

5. **Network Layer**

The network layer is responsible for the delivery of data between devices across different networks. Its primary function is to provide logical addressing and routing services, allowing data to be transmitted from a source device to a destination device even if they are on different networks.

It uses the protocols IP, ICMP, ARP, & RIP and uses routers as its device.

Example of DOS technique that can be applied at this layer:

ICMP Flooding - A Layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth.

Impact of DOS attack: Network bandwidth and impose extra load on the firewall.

When a network reaches its bandwidth limit, it becomes unable to handle any more traffic and may become unresponsive or even crash. This can lead to disruptions in service, loss of data, and financial losses for businesses and organizations that rely on the network for their operations. Additionally, the extra load on the firewall can cause it to slow down or even crash, allowing malicious traffic to bypass its protections and reach the network.

Possible mitigation:

Rate-limit ICMP traffic and prevent the attack from impacting bandwidth and

firewall performance.

6. **Data Link Layer**

The primary function of the data link layer is to provide reliable communication over a physical link between two devices on a network. This is achieved by dividing the data into frames and transmitting them over the physical link. The data link layer provides mechanisms to ensure that frames are transmitted without errors and in the correct order. It also handles the flow control of data between the devices, to prevent the receiver from being overwhelmed with too much data at once.

It uses the protocols 802.3 & 802.5 and its devices are NICs, switches bridges & WAPs.

Example of DOS technique that can be applied at this layer:

MAC flooding - inundates the network switch with data packets.

Impact of DOS attack: Disrupts the usual sender-to-recipient flow of data - blasting across all ports.

Possible mitigation:

Many advanced switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations; allow discovered MAC addresses to be authenticated against an authentication, authorization, and accounting (AAA) server and subsequently filtered.

7. **Physical Layer**

The primary function of the Physical layer is to transmit raw bits over a communication channel, such as copper wires, optical fibers, or wireless signals.

It uses the protocols 100Base-T & 1000 Base-X and uses Hubs, patch panels, & RJ45 Jacks as devices.

Example of DOS technique that can be applied at this layer:

Physical destruction, obstruction, manipulation, or malfunction of physical assets.

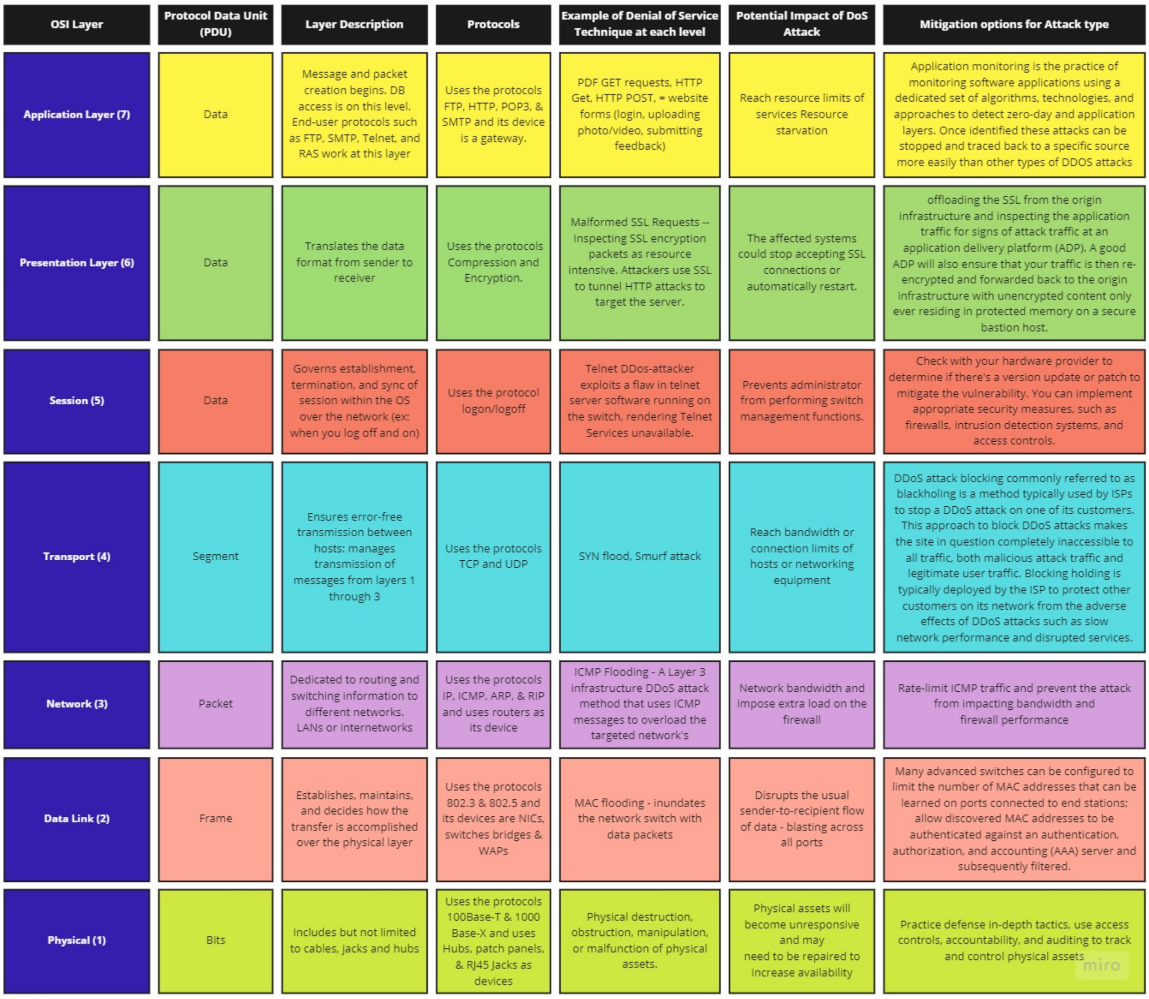
Impact of DOS attack: Physical assets will become unresponsive and may

need to be repaired to increase availability.

Possible mitigation:

Practice defense in-depth tactics, use access controls, accountability, and auditing to track and control physical assets.

Let's see the summary of Attacks Possibilities by OSI Layer:



OSI Layer	Protocol Data Unit (PDU)	Layer Description	Protocols	Example of Denial of Service Technique at each level	Potential Impact of DoS Attack	Mitigation options for Attack type
Application Layer (7)	Data	Message and packet creation begins. DB access is on this level. End-user protocols such as FTP, SMTP, Telnet, and RAS work at this layer	Uses the protocols FTP, HTTP, POP3, & SMTP and its device is a gateway.	PDF GET requests, HTTP Get, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)	Reach resource limits of services Resource starvation	Application monitoring is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero-day and application layers. Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDOS attacks
Presentation Layer (6)	Data	Translates the data format from sender to receiver	Uses the protocols Compression and Encryption.	Malformed SSL Requests -- Inspecting SSL encryption packets as resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server.	The affected systems could stop accepting SSL connections or automatically restart.	offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attack traffic at an application delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in protected memory on a secure bastion host.
Session (5)	Data	Governs establishment, termination, and sync of session within the OS over the network (ex: when you log off and on)	Uses the protocol logon/logoff	Telnet DDos-attacker exploits a flaw in telnet server software running on the switch, rendering Telnet Services unavailable.	Prevents administrator from performing switch management functions.	Check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability. You can implement appropriate security measures, such as firewalls, intrusion detection systems, and access controls.
Transport (4)	Segment	Ensures error-free transmission between hosts: manages transmission of messages from layers 1 through 3	Uses the protocols TCP and UDP	SYN flood, Smurf attack	Reach bandwidth or connection limits of hosts or networking equipment	DDoS attack blocking commonly referred to as blackholing is a method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. Blocking holding is typically deployed by the ISP to protect other customers on its network from the adverse effects of DDoS attacks such as slow network performance and disrupted services.
Network (3)	Packet	Dedicated to routing and switching information to different networks. LANs or internetworks	Uses the protocols IP, ICMP, ARP, & RIP and uses routers as its device	ICMP Flooding - A Layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's	Network bandwidth and impose extra load on the firewall	Rate-limit ICMP traffic and prevent the attack from impacting bandwidth and firewall performance
Data Link (2)	Frame	Establishes, maintains, and decides how the transfer is accomplished over the physical layer	Uses the protocols 802.3 & 802.5 and its devices are NICs, switches bridges & WAPs	MAC flooding - inundates the network switch with data packets	Disrupts the usual sender-to-recipient flow of data - blasting across all ports	Many advanced switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations; allow discovered MAC addresses to be authenticated against an authentication, authorization, and accounting (AAA) server and subsequently filtered.
Physical (1)	Bits	Includes but not limited to cables, jacks and hubs	Uses the protocols 100Base-T & 1000 Base-X and uses Hubs, patch panels, & RJ45 Jacks as devices	Physical destruction, obstruction, manipulation, or malfunction of physical assets.	Physical assets will become unresponsive and may need to be repaired to increase availability	Practice defense in-depth tactics, use access controls, accountability, and auditing to track and control physical assets

***SecOps Solution** is an agent-less Risk-based Vulnerability Management Platform that helps organizations identify, prioritize and remediate security vulnerabilities and misconfigurations in seconds.*

To schedule a demo, drop us a note at hello@secopsolution.com