GROUP TASK :2
OS LAYER 4

A Brief Overview

5

1:Dhairya Khanduja
2:Sanket

Analyze a real-world case study of an attack on Layer 4 (Transport Layer) of the OSI model

TRANSPORT LAYER

The transport layer is the fourth layer of the Open Systems Interconnection (OSI) model. It is responsible for providing communication services to the upper layers of the model. This includes ensuring that data is delivered reliably and in the correct order, and that it is protected from errors.The transport layer does this by breaking up data into smaller units called segments, and adding a header to each segment that contains information such as the source and destination addresses, the sequence number of the segment, and the type of service required. The transport layer then passes these segments down to the network layer for delivery.The transport layer also provides a number of services to the upper layers, such as:

Connection-oriented communication: The transport layer can provide a connection-oriented service, which guarantees that data will be delivered reliably and in the correct order. This is achieved by establishing a connection between the two hosts before any data is sent, and then maintaining that connection until all the data has been transferred.

Connectionless communication: The transport layer can also provide a connectionless service, which does not guarantee that data will be delivered reliably or in the correct order. This is a simpler and faster service than connection-oriented communication, but it is not suitable for all applications.

Flow control: The transport layer can provide flow control, which ensures that the sender does not send data too quickly for the receiver to handle. This is important to prevent the receiver from becoming overloaded and dropping data.

Error control: The transport layer can provide error control, which detects and corrects errors in data that has been transferred. This is important to ensure that data is received correctly.The transport layer is an important layer in the OSI model, as it provides the foundation for reliable and efficient communication between hosts on a network.

CASE STUDY

In this case study, we will analyze a real-world Distributed Denial of Service (DDoS) attack that targeted the Transport Layer (Layer 4) of the OSI model. DDoS attacks overwhelm a target system or network with a flood of traffic, rendering it inaccessible to legitimate users. Layer 4 attacks focus on exploiting vulnerabilities in protocols such as TCP and UDP, causing service disruptions and impacting network availability.

Background: A prominent online gaming company experienced a severe DDoS attack, specifically targeting the Transport Layer of their infrastructure. The attackers aimed to disrupt the gaming services, rendering them unavailable to players and causing financial losses for the company.

In this case study, we will analyze a real-world Distributed Denial of Service (DDoS) attack that targeted the Transport Layer (Layer 4) of the OSI model. DDoS attacks overwhelm a target system or network with a flood of traffic, rendering it inaccessible to legitimate users. Layer 4 attacks focus on exploiting vulnerabilities in protocols such as TCP and UDP, causing service disruptions and impacting network availability.

Background: A prominent online gaming company experienced a severe DDoS attack, specifically targeting the Transport Layer of their infrastructure. The attackers aimed to disrupt the gaming services, rendering them unavailable to players and causing financial losses for the company.

Attack Scenario:

Reconnaissance:
The attackers likely conducted initial reconnaissance to identify the company's gaming servers and associated IP addresses. They may have used various techniques like port scanning, network mapping, or social engineering to gather this information.
Botnet Formation: The attackers employed a botnet, a network of compromised computers or devices, to carry out the attack. The botnet consisted of numerous infected devices, including computers, servers, and Internet of Things (IoT) devices, which were under the control of the attackers.

Attack Launch:
a. Traffic Amplification: The attackers utilized a technique known as "reflection amplification." They spoofed the source IP address to match the target server's IP address and sent requests to publicly accessible UDP-based services that support large responses, such as DNS (Domain Name System) servers or NTP (Network Time Protocol) servers. These services would respond to the spoofed IP address with significantly larger responses, resulting in traffic amplification.
b. Botnet Flood: The attackers instructed the compromised devices in the botnet to flood the target gaming servers with a massive volume of UDP or TCP traffic. The flood targeted specific ports used by the gaming services, overwhelming the Transport Layer and consuming network resources such as bandwidth, processing power, and memory.

Impact:

a. Service Disruption: The DDoS attack saturated the company's network infrastructure, causing a significant increase in traffic and exhausting available resources. As a result, legitimate users were unable to access the gaming services, leading to disrupted gameplay, frustrated players, and potential financial losses for the company.

b. Mitigation Challenges: Detecting and mitigating Layer 4 attacks can be challenging. The attack traffic, originating from a botnet of distributed sources, can make it difficult to distinguish legitimate traffic from the malicious flood. Additionally, attackers continuously evolve their tactics, making it crucial for organizations to implement robust DDoS mitigation strategies.

Mitigation and Countermeasures:

To mitigate and defend against Layer 4 DDoS attacks, the gaming company employed several countermeasures:

- Traffic Analysis and Filtering: The company implemented traffic analysis and filtering mechanisms to identify and block malicious traffic. They used intrusion detection and prevention systems (IDPS) and firewalls to inspect incoming traffic, filter out attack packets, and allow only legitimate traffic to reach the gaming servers.
- Traffic Shaping: The company employed traffic shaping techniques to prioritize legitimate traffic over malicious traffic. By implementing Quality of Service (QoS) policies, they ensured that critical gaming services received higher priority and allocated sufficient resources to handle legitimate requests.
- Rate Limiting and Connection Tracking: The company implemented rate limiting and connection tracking mechanisms to identify and block excessive or suspicious connection requests. This helped to mitigate flooding attacks by limiting the number of connections allowed per source IP address.
- DDoS Mitigation Services: To handle large-scale attacks, the company partnered with a DDoS mitigation service provider. These services employ sophisticated traffic analysis techniques, have extensive bandwidth capacity, and utilize various mitigation methods such as rate limiting, traffic diversion, and intelligent filtering to protect against Layer 4 attacks.

Consequences of the attack:

1. Loss of Revenue: The service disruption caused by the Layer 4 DDoS attack can result in immediate financial losses for the targeted company. In the case of the gaming company, the inability of players to access the gaming services can lead to a decline in in-game purchases, subscription cancellations, and potential loss of new customer acquisitions, directly impacting revenue.
2. Damage to Reputation: The DDoS attack can have a negative impact on the reputation and brand image of the targeted company. Users who experience service disruptions or downtime may perceive the company as unreliable, leading to a loss of trust and potential customers. Negative publicity surrounding the attack can further damage the company's reputation in the industry.
3. Operational Disruption: The attack can disrupt the normal operations of the targeted company. Network infrastructure, servers, and other resources may become overloaded or unavailable due to the flood of malicious traffic, causing a disruption in internal processes and employee productivity. Significant effort and resources may be required to mitigate the attack and restore normal operations.
4. Customer Dissatisfaction and Churn: The inability to access services or experience interrupted gameplay can lead to customer dissatisfaction. Frustrated users may seek alternative solutions or switch to competitor services, resulting in customer churn. Losing customers can have long-term consequences, as acquiring new customers is generally more expensive than retaining existing ones. Additionally, dissatisfied customers may share their negative experiences, further impacting the company's reputation.

Countermeasures:

To mitigate and defend against Layer 4 DDoS attacks, organizations can implement several countermeasures. Here are four common countermeasures:

1. Traffic Analysis and Filtering:
   - Intrusion Detection and Prevention Systems (IDPS): Implement IDPS solutions that can analyze incoming network traffic and identify patterns indicative of a DDoS attack. These systems can detect and block malicious traffic, preventing it from reaching the target network.
   - Firewalls: Configure firewalls to inspect and filter incoming traffic based on predefined rules. Firewalls can block traffic from suspicious or unauthorized sources, reducing the impact of a DDoS attack.
2. Traffic Shaping:
   - Quality of Service (QoS): Implement QoS policies to prioritize critical network traffic over non-essential traffic during a DDoS attack. QoS can ensure that important services, such as web servers or DNS, receive sufficient resources and bandwidth to function properly, mitigating the impact of the attack.

1. Rate Limiting and Connection Tracking:
    - Rate Limiting: Employ rate limiting techniques to restrict the number of connections or requests allowed from a single IP address within a specified time period. By limiting the rate of incoming connections, organizations can mitigate flooding attacks and prevent their network resources from being exhausted.
    - Connection Tracking: Implement connection tracking mechanisms to monitor and track the number of active connections to the network. Unusually high connection rates from individual IP addresses can be identified and blocked, reducing the impact of a DDoS attack.
2. DDoS Mitigation Services:
    - Cloud-based DDoS Protection: Partner with a DDoS mitigation service provider that specializes in handling large-scale attacks. These services utilize advanced traffic analysis techniques and have substantial network capacity to absorb and mitigate DDoS attacks. By diverting traffic through their infrastructure, they can filter out attack traffic and allow legitimate traffic to reach the organization's network.

It's important to note that countermeasures should be implemented in a layered defense approach, combining multiple techniques and solutions to enhance overall resilience against Layer 4 DDoS attacks. Regular testing, incident response planning, and continuous monitoring of network traffic are crucial for effective mitigation and response to such attacks.

THANK YOU