CAM (Content Addressable Memory) Table Overflow

CAM Table Overflow is **a type of network attack that targets switches by exploiting their Content Addressable Memory (CAM) table**. **The CAM table is a memory table in network switches that stores the mapping between MAC addresses and the switch's physical ports**. This allows the switch to efficiently forward frames to the correct port based on the destination MAC address, improving network performance.

In a CAM table overflow attack, an attacker floods the switch with a large number of fake MAC addresses, causing the switch's CAM table to become full. **Once the table is full, the switch can no longer store new MAC address mappings, and it starts behaving like a hub, broadcasting incoming traffic to all ports rather than forwarding it to the correct destination**. This behavior compromises network security and performance, allowing the attacker to potentially eavesdrop on network traffic.

How CAM Table Overflow Works

1. CAM Table Function: Normally, when a switch receives a data frame, it checks the CAM table to map the destination MAC address to the appropriate port. If the MAC address is found in the CAM table, the frame is forwarded to that port. If not, the switch floods the frame to all ports (except the source port) to learn the destination MAC address.
2. **Flooding Fake MAC Addresses**: In a CAM table overflow attack, **the attacker sends a large number of packets with randomly generated source MAC addresses to the switch**. This overloads the CAM table by filling it with invalid or fake MAC address entries.
3. **CAM Table Full**: When the CAM table reaches its storage limit, the switch can no longer add legitimate MAC addresses to the table. As a result, **the switch enters a "fail-open" state** where it begins to **act like a hub, broadcasting all frames it receives to all ports**.
4. **Broadcasting and Eavesdropping**: Since the switch is now broadcasting traffic to all ports, **the attacker (or any other device) can capture and eavesdrop on network traffic** that was previously destined for a specific port. This allows the attacker to potentially intercept sensitive data.

Consequences of CAM Table Overflow

- **Network Traffic Eavesdropping**: The attacker can capture network traffic intended for other devices, leading to a potential breach of sensitive data such as passwords, emails, or confidential documents.
- **Degraded Network Performance**: When the switch starts broadcasting frames to all ports, the network becomes congested, which can lead to slower performance and reduced efficiency.
- **Increased Vulnerability**: Once the switch is acting like a hub, the entire network becomes more susceptible to other attacks, such as man-in-the-middle attacks or denial-of-service (DoS).

Mitigation Techniques for CAM Table Overflow

1. **Port Security**: Many switches offer port security features that limit the number of MAC addresses that can be learned on a given port. If the number of MAC addresses exceeds this limit, the switch can either block additional addresses or shut down the port.
2. **MAC Address Aging**: Switches often use a MAC address aging mechanism that **removes inactive entries from the CAM table after a certain period**. This helps to free up space in the table and

prevent it from being overloaded.

3. **VLAN Segmentation**: Using VLANs (Virtual LANs) can limit the impact of a CAM table overflow attack by **segmenting the network into smaller, isolated broadcast domains**.
4. **Monitoring and Alerts**: Network administrators can **monitor the CAM table for unusual behavior**, such as a sudden influx of MAC addresses, and set up alerts to detect possible overflow attacks.
5. **Static MAC Entries**: In environments where devices are known and consistent, static MAC entries can be configured on the switch. These static entries do not expire and are not subject to attacks that rely on flooding the CAM table.

Summary

CAM Table Overflow is **an attack where an attacker floods a switch with fake MAC addresses, causing the switch's CAM table to overflow**. Once the CAM table is full, the **switch behaves like a hub, broadcasting all traffic to every connected device, allowing attackers to eavesdrop on network communications and degrade network performance**. To prevent this, techniques like port security, MAC address aging, and monitoring can be implemented to protect the network.