Objective:

During our day 4 lab, we sought to learn and perform a MAC flooding attack on a network switch. This means that the switch behaves like a hub when its MAC address table is overloaded thereby enabling the attacker to capture the traffic transmitted across the network.

About what we did in day 4 let’s look at few intro about topics covered:

MAC flooding attack refers to network security attack whereby an attacker sends multiple fake MAC addresses to a switch. This action fills up the switch's MAC address table which has limited space. Consequently, when the table becomes full, there is no longer any possibility of mapping MAC addresses to specific ports by the switch. Hence it floods all incoming traffic to every port like a hub does. Therefore, this allows attackers to access sensitive information.

Materials and Tools used:

GNS3 Network Simulator

Switch

Kali Linux OS

DSNIFF tool (specifically macof command)

Steps followed:

Network Setup:

The network is set according to GNS3 diagram provided.

PC1 and Kali Linux PC are both assigned IP addresses and subnet masks.

Both devices have their default gateways set.

Pre-Attack Observations:

This is checked by using show mac-address-table count command on how many MAC addresses are currently in use within the switches mac address table.

show processes cpu is used for monitoring CPU load on the switch.

Executing the Attack:

On the Kali Linux terminal, the macof command is run to initiate the MAC flooding attack.

The command always sends fake MAC addresses so that the switch’s MAC address table doesn’t get filled quickly.

During the Attack:

Note down the CPU utilization of the switch. It is expected that there will be a significant increase in the load on CPU because of this attack

Once its MAC address table is full, switch starts flooding traffic to all ports.

Packet Capture:

Capture network packets between Kali Linux PC and switch for analyzing traffic and verifying if it is being flooded.

Observations:

After ordering the macof command for initiating a MAC flooding attack, CPU utilization of the switch increased notably

When its MAC address table gets full, this will lead to them switching on all incoming traffic on each single port This act confirmed that MAC flooding was successful.

Protection Against MAC Flooding:

Switch port security should be configured to protect against MAC flooding attacks. The process includes putting a limit on the number of learned MAC addresses or learning actions when this number exceeds certain limit.

Conclusion:

We tried our best after passing through many to demonstrate how exactly a network switch can experience a heavy impact from a mac-flooding attack. Loading up to capacity on its mac-addresses led to an effect where all frames were broadcasted out every interface, making it possible for any person