**Man in the Middle Attack**

**BE CMPNA**

**Clive Crasto 49**

**Shonil Dabreo 51**

**Onish Dmello 54**

**PROBLEM DEFINITION**

The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

**ABSTRACT**

A man-in-the-middle attack is a type of cyber-attack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. The purpose of this project is to demonstrate ARP spoofing that allows us to demonstrate man in the middle attack. The Basic idea behind Man in the middle attack is to intrude into the existing communications between the end points (hosts) on LAN Network and change the contents or inject false information. This Attack is mainly done in LAN networks .We are implementing this using Linux. ARP Spoofing results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. For implementation of Man-in-the-Middle Attack using ARP spoofing we are using Driftnet and urlsnarf to sniff the images and sites the victim is viewing on the Internet using python script, by using three mobile devices and a laptop ,one of the three mobile acts as a internet access point other two mobiles act as two communicating devices in that network and laptop acts as a middle man i.e. attacker who will access all data which is being transferred between those two mobile devices.