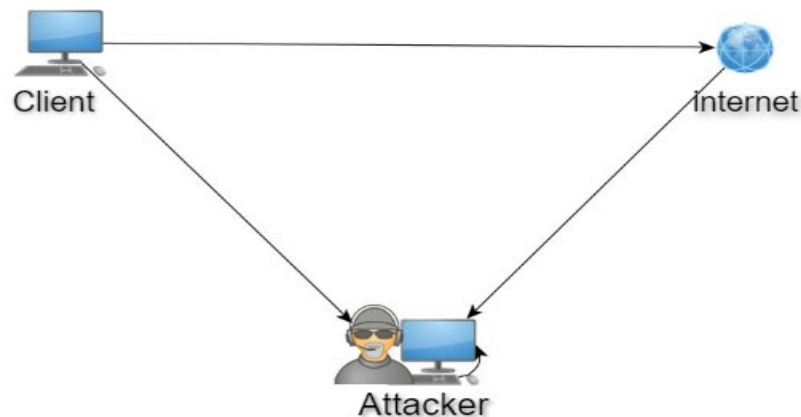


Main in the middle lab

The lab introduces to students the Man in The Middle (MIM) attack. A man-in-the-middle attack is a type of eavesdropping attack, where attackers interrupt an existing conversation or data transfer. After inserting themselves in the "middle" of the transfer, the attackers pretend to be both legitimate participants. This enables an attacker to intercept information and data from either party while also sending malicious links or other information to both legitimate participants in a way that might not be detected until it is too late.

This lab consists of three virtual machines which are a client computer, a server, and an attacker computer. These computers are all connected to the same network.



jane is an administrator at Shifa hospital, when she comes to her desk first in the morning, she always opens a browser to access the hospital system. Attack the hospital system using the Ettercap tool installed in the attacker's machine and prevent jane from accessing any browser from her machine.

In this lab, a Wireshark tool is installed in the attacker's machine. Run the Wireshark tool to analyze the traffic on jane's computer after you conduct an ARP poisoning attack on her computer.

On the attacker machine run

`Sudo Wireshark &.` Analyze the traffic on ethernet 0

Then run `sudo Ettercap -G` to conduct the ARP poisoning attack Firefox is installed and run

Firefox is installed on jane's computer. Run this command Firefox & to run the Firefox browser then browse www.shifahospital.com

The goal of this lab is to prevent jane from accessing the Firefox browser. Analyze the traffic on the Wireshark.

After successfully conducting this attack. Write a paragraph about how to mitigate this type of attack if this happens in your organization.