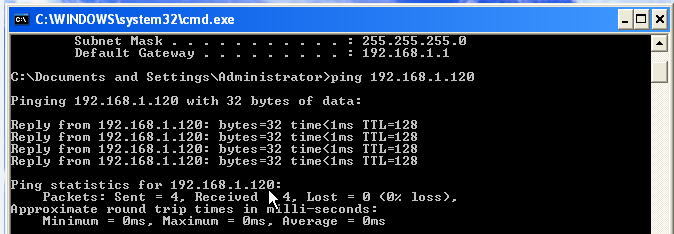
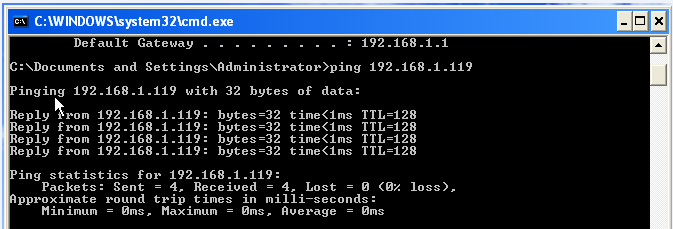
**Practical – 2**

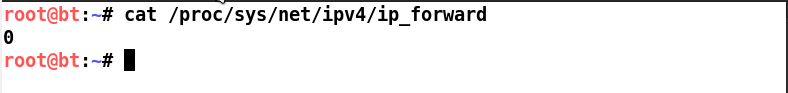
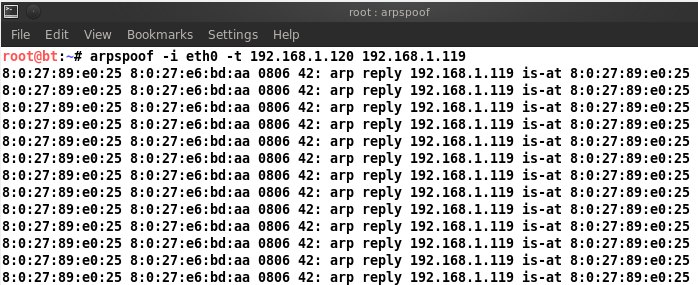
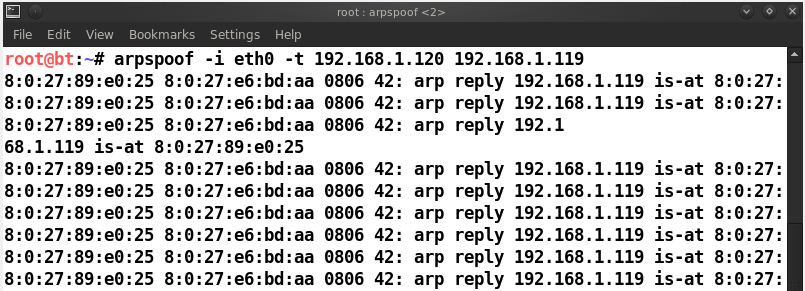
# Aim: Using open port information perform MITM(Man In The Middle) attack using arpspoof, urlsnarf, dsniff, dnsspoof. 1. Interruption, 2. Interception.

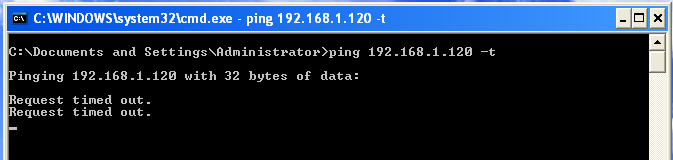
1. **Interruption:**

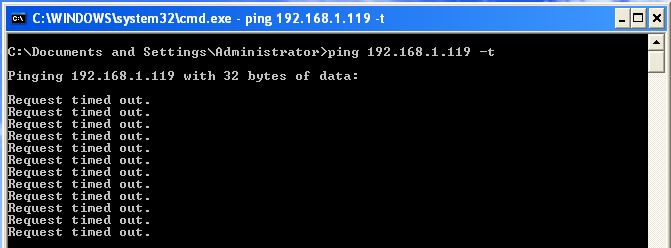
* Initially Before attack Checking the Connection Between Client and Server using ping command at both side.

Client Side:

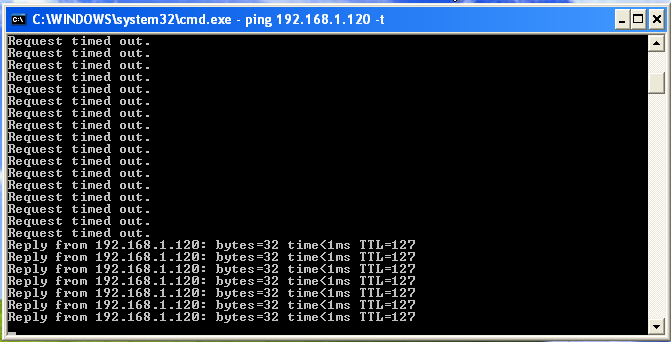
Server Side:

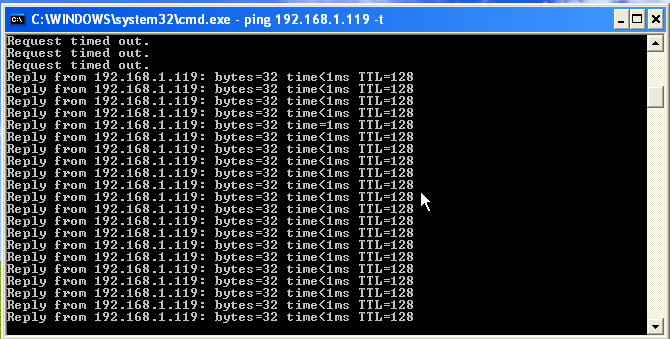
* Configuring machine to allow packet forwarding, because act as man in the middle attacker machine must act as router between "real router" and the victim.
* Without Change the value in /proc/sys/net/ipv4/ip\_forward from 0 to 1.
* The next step is setting up arpspoof between victim and router.
* Further setting up arpspoof from to capture all packet from router to victim.
* The Reply between Client and Server are stopped because we had not changed the value in /proc/sys/net/ipv4/ip\_forward from 0 to 1.

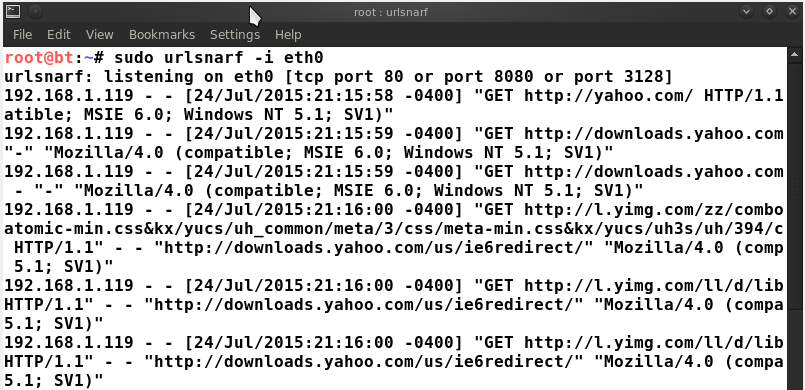
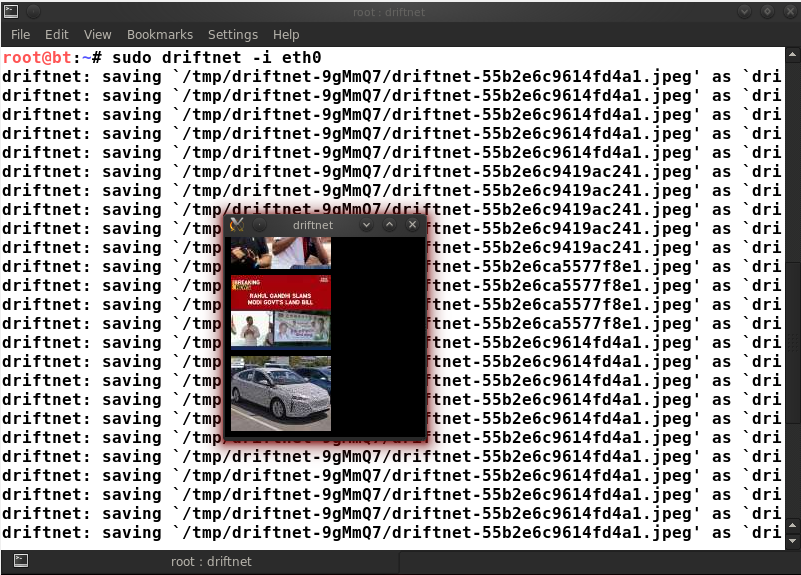
Client Side:

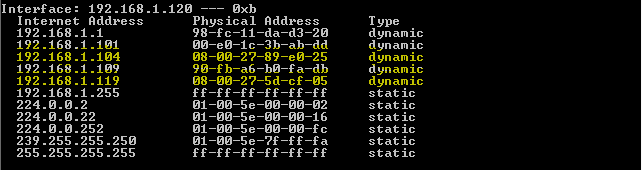
Server Side:

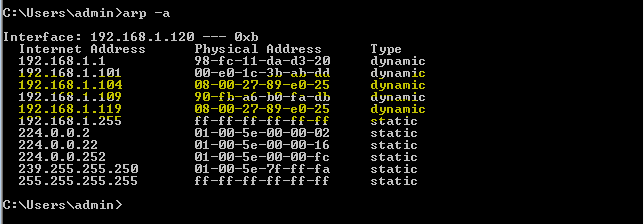
* Changing the value in /proc/sys/net/ipv4/ip\_forward from 0 to 1.
* After changing the value in /proc/sys/net/ipv4/ip\_forward from 0 to 1 server and client both are further able to communicate with each other and started ping reply.

Client Side:

Server Side:

* Now performing urlsnarf from the attackers machine which capture the packets from both Client and Server side and gives output as bellow.
* Now performing driftnet from the attackers machine which capture the packets from both Client and Server side and gives output as bellow.
* Checking Interfaces before and after attack on server Machine using command arp –a.

Before Attack: It shows that physical addresses of attacker and client both are different.

After Attack: It shows that physical addresses of attacker and client both are same.