Practical – 4

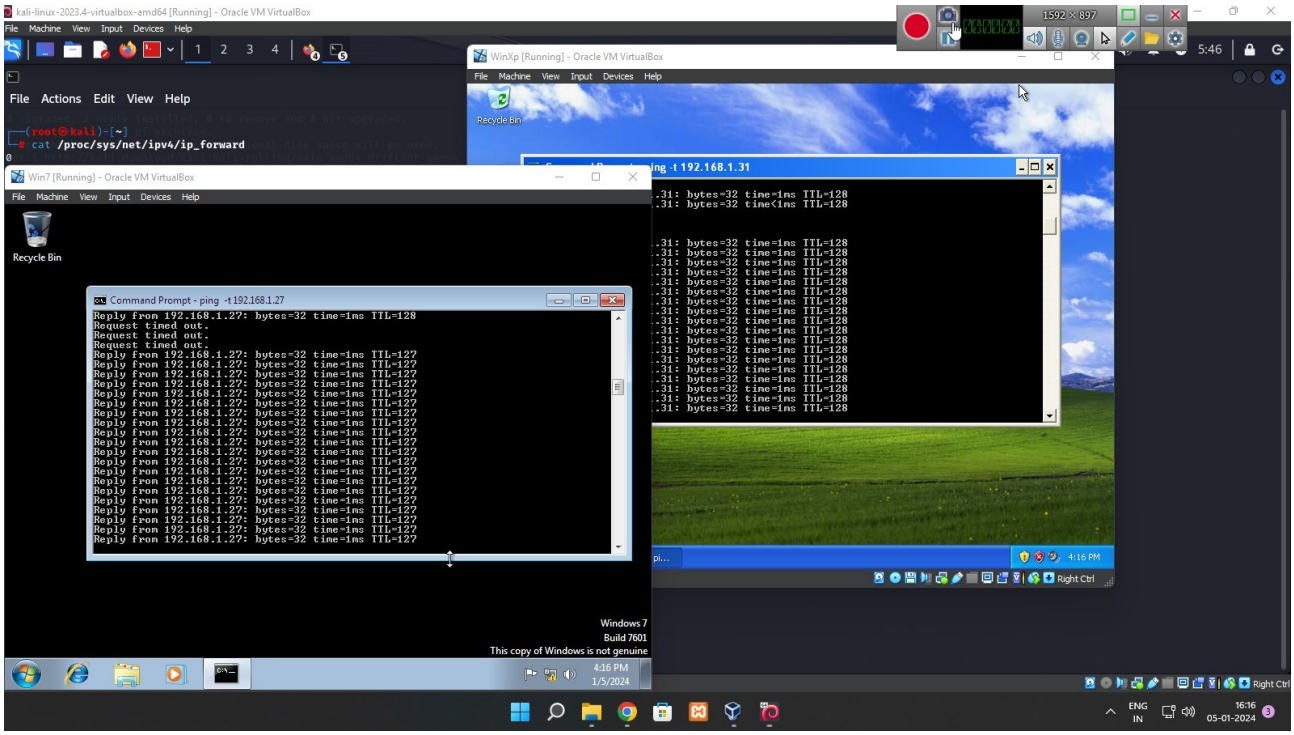
Using open port information perform MITM(Man In The Middle) attack using arpspoof, urlsnarf, driftnet.

1. Interruption
2. Interception

Note :- Here all terminals are Root Terminals

1) Doing Apspoof Attack :

It is an attack that allows attackers to intercept communication between network devices **so** before doing arpspoof attack we need to make sure that client,server & attacker system should be connected in same ethernet(LAN) .It can be checked using **Ping** command



Now we can start the attack using arpspoof

1. Open Terminal 1 and write the following :

> arpspoof -i eth0 -t 192.168.1.31 192.168.1.27

2. Open Terminal 2 and write the following :

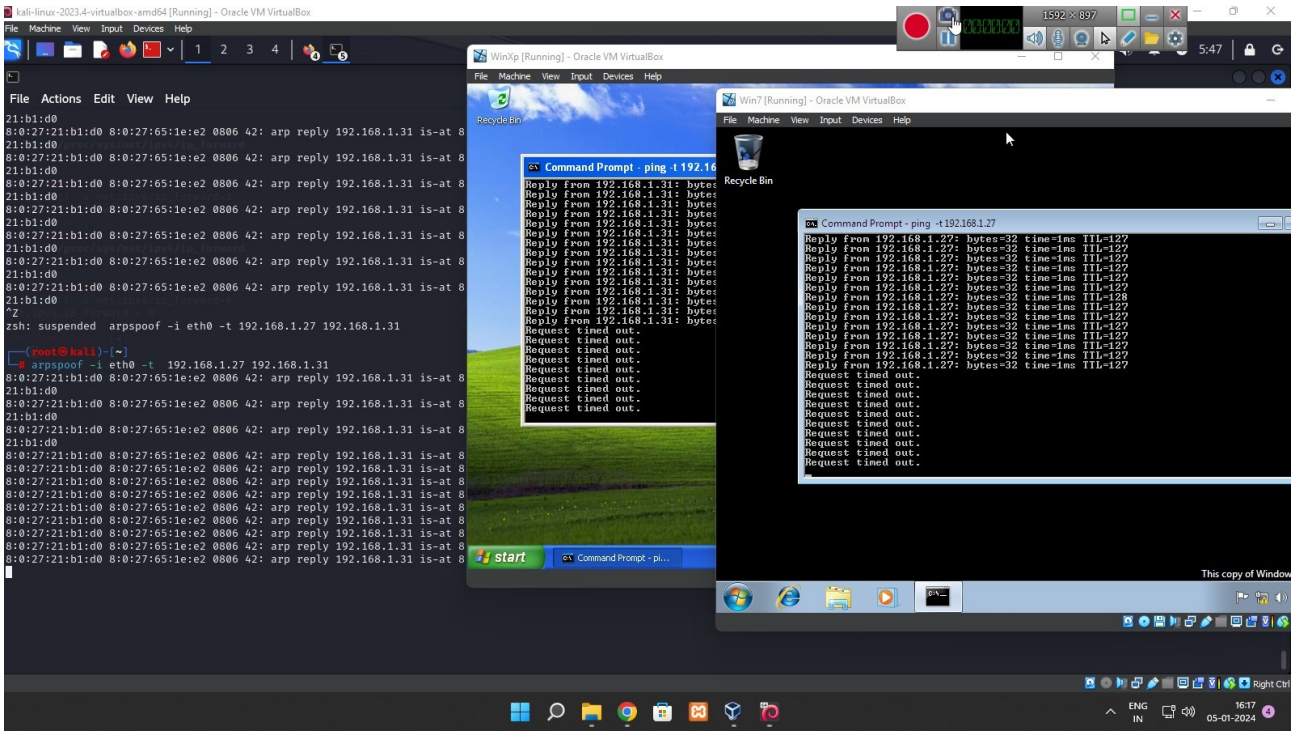
> arpspoof -i eth0 -t 192.168.1.27 192.168.1.31

Here **192.168.1.27 & 192.168.1.31** are **IP address of Client & Server machines**

-i option in arpspoof is used to define our interface i.e. **Ethernet** defined as **eth0**

-t option is used to define **target machines**.

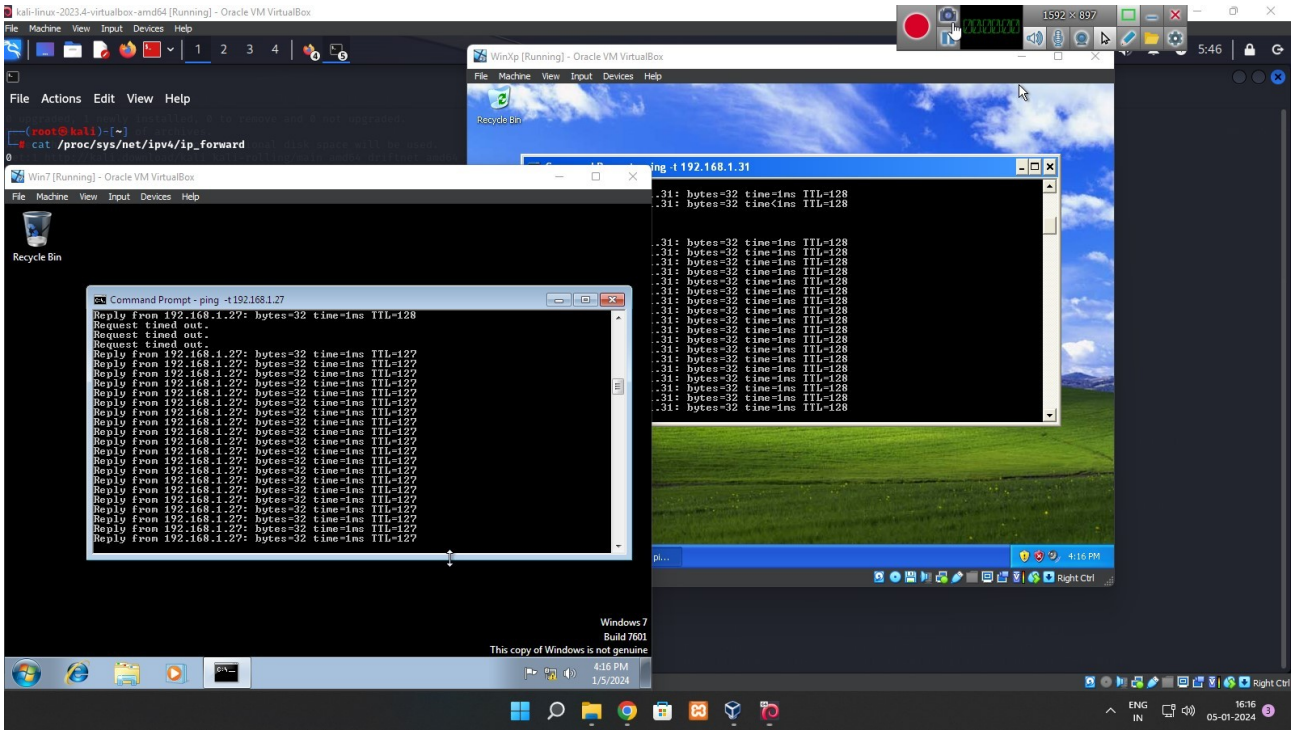
After doing so we see connection is **interrupted** between client and server machines



But we don't want to interrupt connection we just want to intercept it so for doing this we need to capture packet and forward it.

But our machine is not capable for forwarding packets we can see it by following command:

> cat /proc/sys/net/ipv4/ip_forward



Hence the output is 0 which means our machine is not capable of forwarding packets

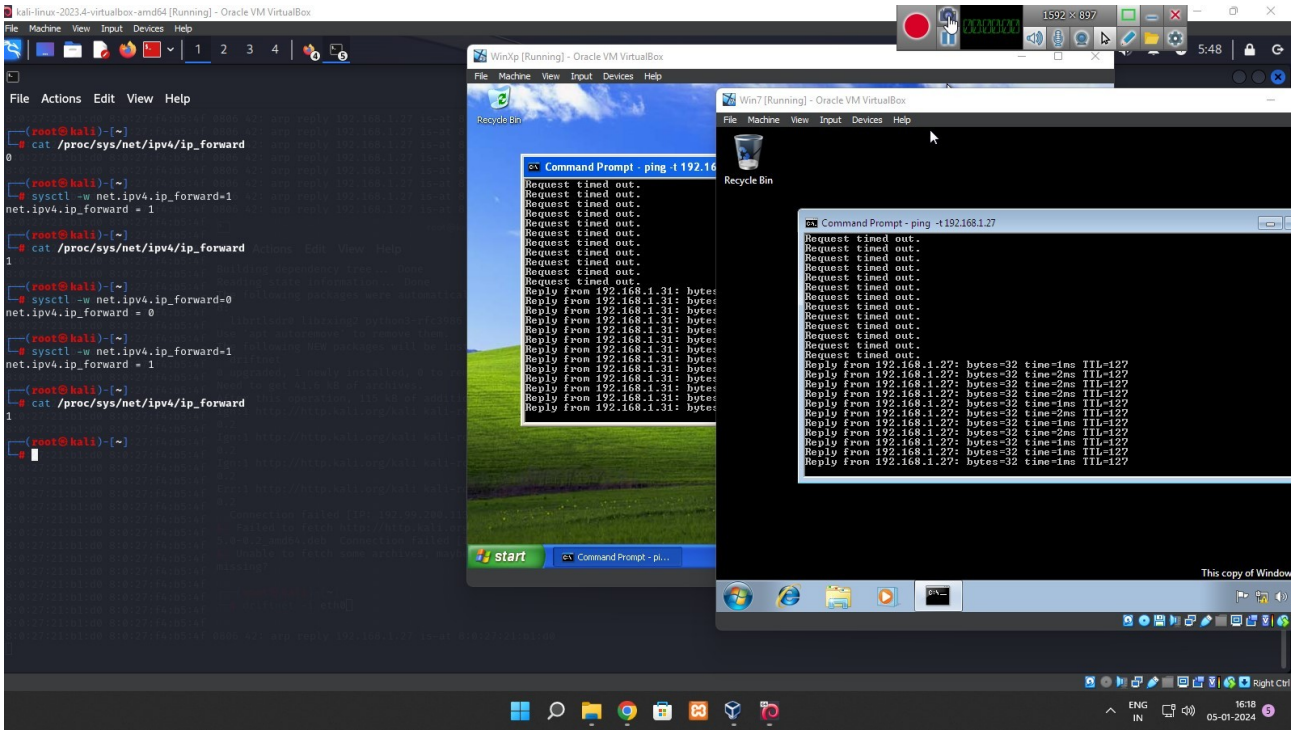
We need to configure it to 1 to make it capable for forwarding packets by doing this we can **intercept** packets and not interruption .

For doing this we can use following command in Terminal 3

> sysctl -w net.ipv4.ip_forward=1

or

> sudo echo 1 >> /proc/sys/net/ipv4/ip_forward



Now we can do other man in the middle attacks .

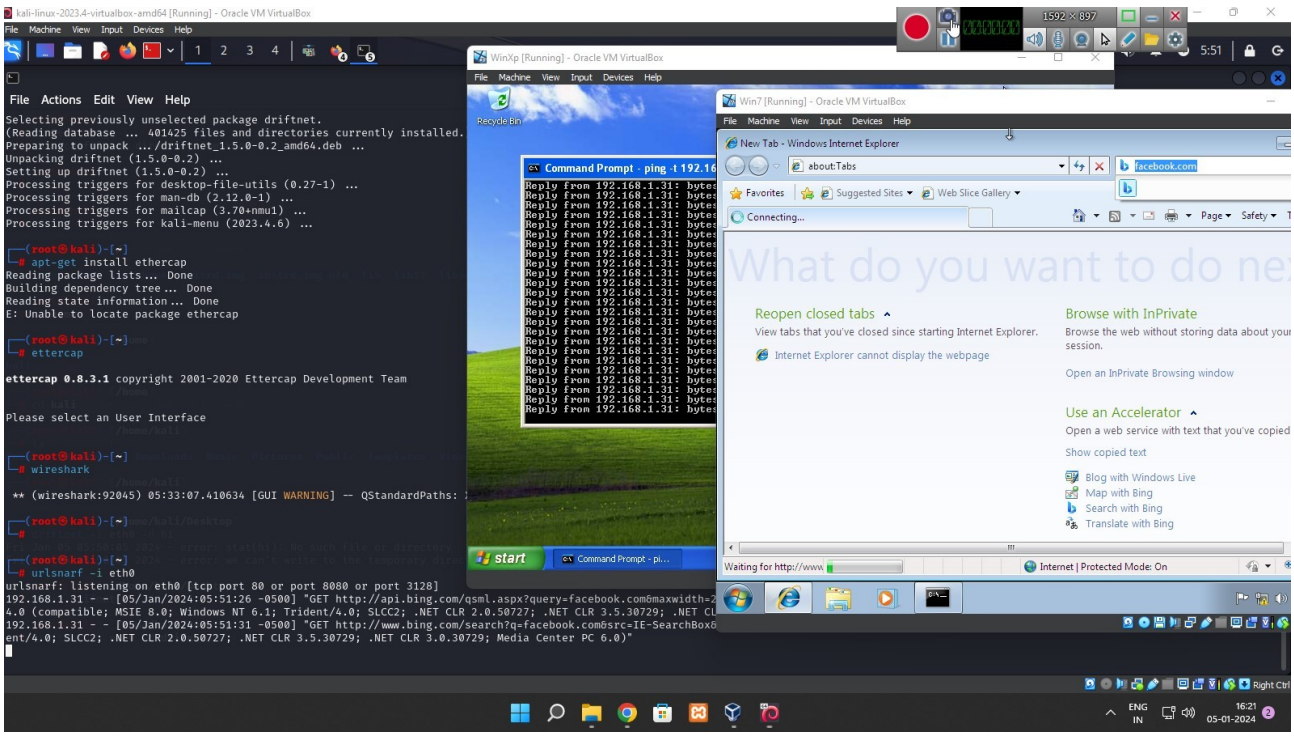
2) Doing Urlsnarf Attack :

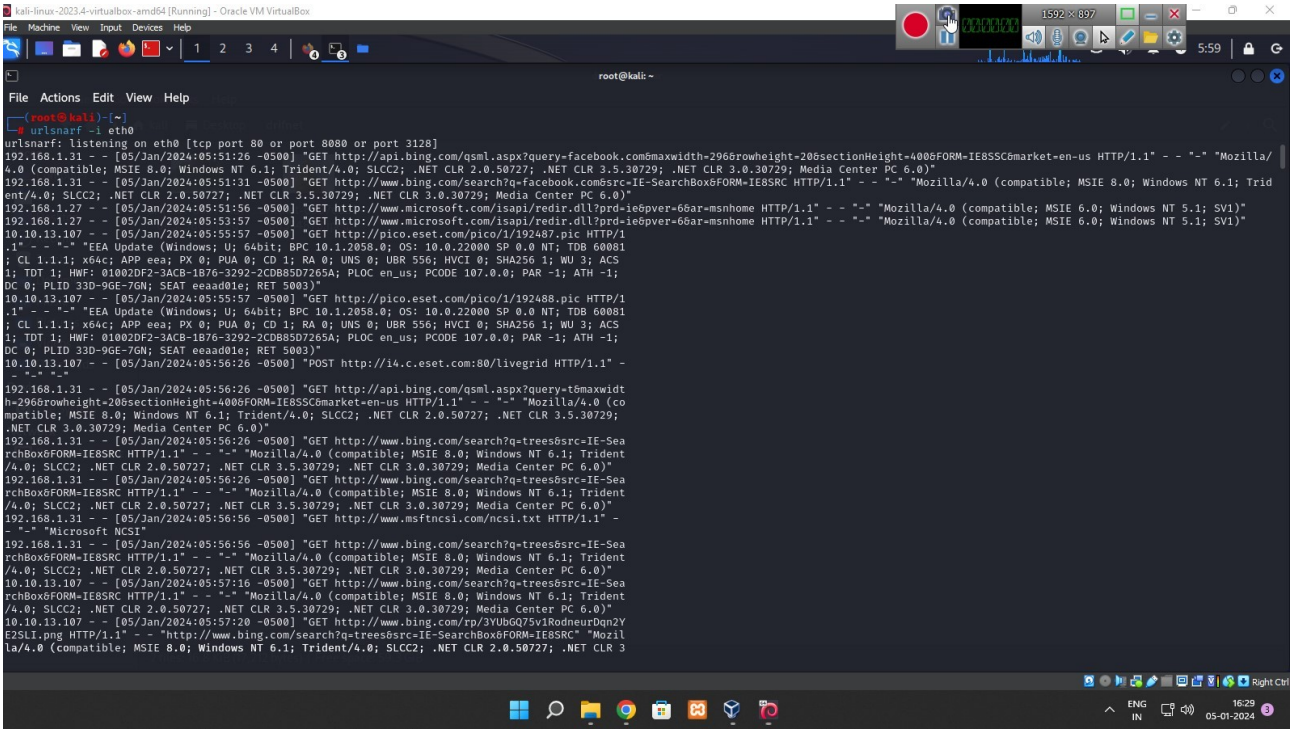
By doing this attack we can capture url of client machine it can be done by following way after doing arpspoof attack

Urlsnark is used to sniff HTTP requests from live network traffic and even offline `.pcap` files. This tool can help us determine which websites were visited by the clients on a network

Continue arpspoof atack and open Terminal 3 ad type the following:

> urlsnarf -i eth0





3) Doing Driftnet attack

Driftnet is a program which listens to network traffic and picks out images from TCP streams it observes.
Capture images from network traffic and display them in an X window; optionally, capture audio streams and play them.
This attack is used to capture images & videos that client watches .

Continue arpspoofing and open a new terminal and write the following command in it :

> mkdir drifnet

This is temporary directory used to store captured media.

> driftnet -i eth0 -d driftnet -g

-d here is used to specify temperorary diectory name which we will store media.
-g is used to enable GUI of drifnet if it is not working by default