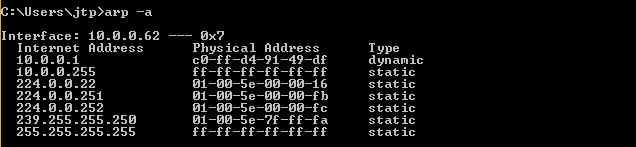
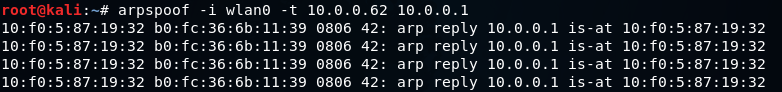
ARP spoofing using arpspoof

Now, we're going to run the actual ARP poisoning attack, redirecting the flow of packets and making it flow through our device. We'll use a tool called arpspoof, which is part of the suite called dsniff. This suite contains a number of programs that can be used to launch MITM attacks. We are going to see how to use **arpspoof tool** to carry out ARP poisoning, which redirects the flow of packets through our device.

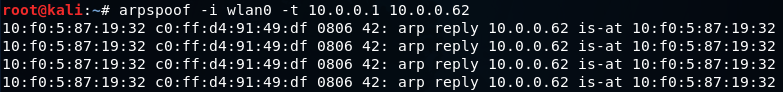
Now, let's see, at the target, Windows is the target device, and we are going to the ARP table. So, we will run **arp -a** on the **Windows** machine to see the ARP table. In the following screenshot, we can see that the IP address for the access point is 10.0.0.1, and we can see its MAC address is **c0-ff-d4-91-49-df**. It is stored in the ARP table:



So, we are connected now to the target network. We're going to use a tool **arpspoof** -i to choose our internet card which is **wlan0**. Then we are going to put the IP address of the target Window device which is **10.0.0.62**. Then we are going to put the IP address for the access point, which is **10.0.0.1**. We will tell the access point that the client IP address has our MAC address, so basically, we're going to tell the access point that we are the target client:

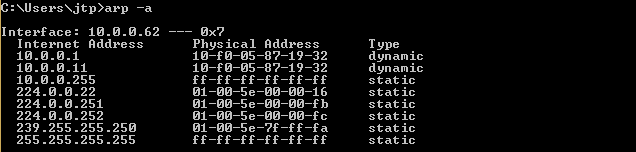


After this, we're going to run arpspoof again, and instead of telling the access point that we are the target client, we are going to tell the client that we are the access point, so we're just going to flip the IPs:



So, by running both the preceding command we are going to fool the client and the access point, and we're going to let the packets flow through our device.

Now, once we do the attack, we will see that the MAC address of the target access point is changed. In the following screenshot, we can see that the MAC address of access point is changed from **c0-ff-d4-91-49-df** to **10-f0-05-87-19-32** which is the MAC address of Kali machine.



Now, we're going to enable the IP forwarding. We do that so that when the packets flow through our device, they don't get dropped so that each packet that goes through our device gets actually forwarded to its destination. So, when we get a packet from the client, it goes to the router, and when a packet comes from the router, it should go to the client without being dropped in our device. So, we're going to enable it using this command:

ARP spoofing using arpspoof

The window device now thinks that the attacker device is the access point, and whenever the window device tries to communicate with the access point, it is going to send all these requests to the attacker device. This will place our attacker device in the middle of the connection, and we will be able to read all the packets, modify them, or drop them.

## **ARP Poisoning − Exercise**

In this exercise, we have used **BetterCAP** to perform ARP poisoning in LAN environment using VMware workstation in which we have installed **Kali** Linux and **Ettercap** tool to sniff the local traffic in LAN.

For this exercise, you would need the following tools −

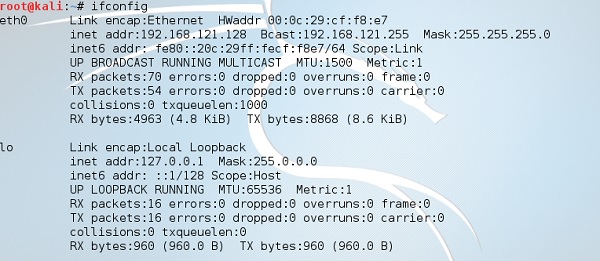
* VMware workstation
* Kali Linux or Linux Operating system
* Ettercap Tool
* LAN connection

**Note** − This attack is possible in wired and wireless networks. You can perform this attack in local LAN.

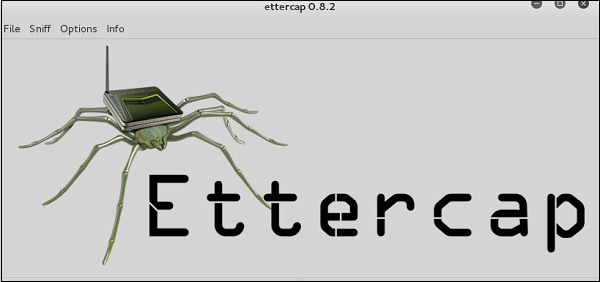
**Step 1** − Install the VMware workstation and install the Kali Linux operating system.

**Step 2** − Login into the Kali Linux using username pass “root, toor”.

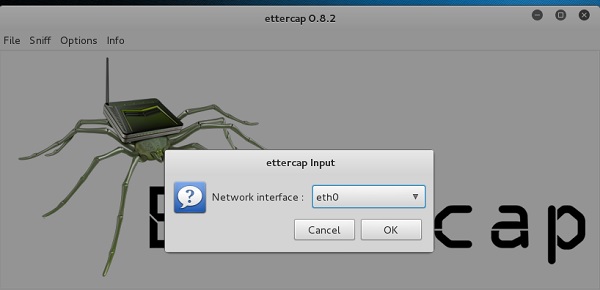
**Step 3** − Make sure you are connected to local LAN and check the IP address by typing the command **ifconfig** in the terminal.



**Step 4** − Open up the terminal and type “Ettercap –G” to start the graphical version of Ettercap.

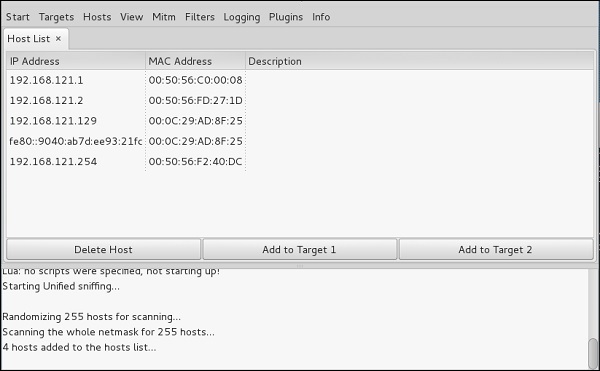


**Step 5** − Now click the tab “sniff” in the menu bar and select “unified sniffing” and click OK to select the interface. We are going to use “eth0” which means Ethernet connection.



**Step 6** − Now click the “hosts” tab in the menu bar and click “scan for hosts”. It will start scanning the whole network for the alive hosts.

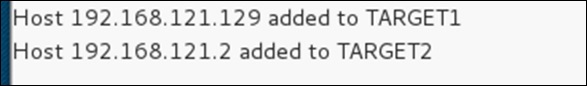
**Step 7** − Next, click the “hosts” tab and select “hosts list” to see the number of hosts available in the network. This list also includes the default gateway address. We have to be careful when we select the targets.



**Step 8** − Now we have to choose the targets. In MITM, our target is the host machine, and the route will be the router address to forward the traffic. In an MITM attack, the attacker intercepts the network and sniffs the packets. So, we will add the victim as “target 1” and the router address as “target 2.”

In VMware environment, the default gateway will always end with “2” because “1” is assigned to the physical machine.

**Step 9** − In this scenario, our target is “192.168.121.129” and the router is “192.168.121.2”. So we will add target 1 as **victim IP** and target 2 as **router IP**.



**Step 10** − Now click on “MITM” and click “ARP poisoning”. Thereafter, check the option “Sniff remote connections” and click OK.



**Step 11** − Click “start” and select “start sniffing”. This will start ARP poisoning in the network which means we have enabled our network card in “promiscuous mode” and now the local traffic can be sniffed.

**Note** − We have allowed only HTTP sniffing with Ettercap, so don’t expect HTTPS packets to be sniffed with this process.

**Step 12** − Now it’s time to see the results; if our victim logged into some websites. You can see the results in the toolbar of Ettercap.



This is how sniffing works. You must have understood how easy it is to get the HTTP credentials just by enabling ARP poisoning.

ARP Poisoning has the potential to cause huge losses in company environments. This is the place where ethical hackers are appointed to secure the networks.

Like ARP poisoning, there are other attacks such as MAC flooding, MAC spoofing, DNS poisoning, ICMP poisoning, etc. that can cause significant loss to a network.

## **How To Perform A TCP SYN Flood Attack With Kali Linux & Hping3**

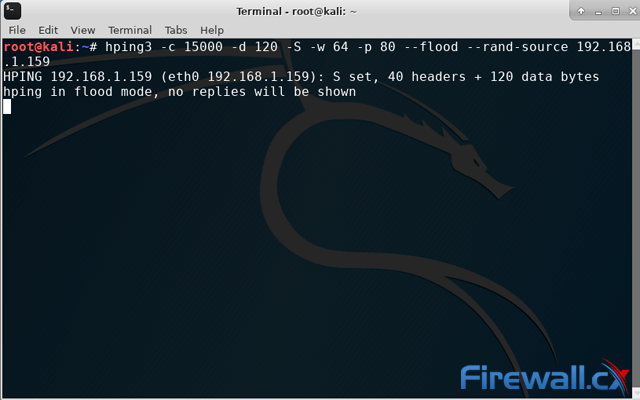
However, to test if you can **detect** this type of a **DoS attack**, you must be able to perform one. The simplest way is via a [Kali Linux](https://www.kali.org/) and more specifically the [hping3](https://www.kali.org/tools/hping3/), a popular **TCP penetration testing tool** included in Kali Linux.

Alternatively Linux users can install **hping3** in their existing Linux distribution using the command:

# **sudo apt-get install hping3**

In most cases, attackers will use **hping** or another tool to spoof IP random addresses, so that’s what we’re going to focus on.  The line below lets us start and **direct the SYN flood attack** to our target (192.168.1.159):

#**hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.159**



Let’s explain in detail the above command:

We’re sending **15000 packets** (**-c 15000**) at a size of **120 bytes** (**-d 120**) each. We’re specifying that the **SYN Flag** (**-S**) should be enabled, with a [**TCP window size**](https://www.firewall.cx/networking/network-protocols/tcp-udp-protocol/tcp-window-size-checksum.html) of **64** (**-w 64**). To direct the attack to our victum’s HTTP web server we specify **port 80** (**-p 80**) and use the **--flood** flag to send packets as fast as possible. As you’d expect, the **--rand-source** flag generates spoofed IP addresses to disguise the real source and avoid detection but at the same time stop the victim’s **SYN-ACK reply packets** from reaching the attacker.