

# ARP SPOOF POISONING

**SUBJECT NAME:** Cryptography and Network Security

**SUBJECT CODE:** CS6008

**MODULE:** 04

**NAME:** R.Aadharsh

**REG.NO.:** 2019103604

**DATE:** 06/06/2022

**AIM:**

Using arpspoof to poison network and detect using Wireshark

**TOOLS INVOLVED:**

ETTERCAP

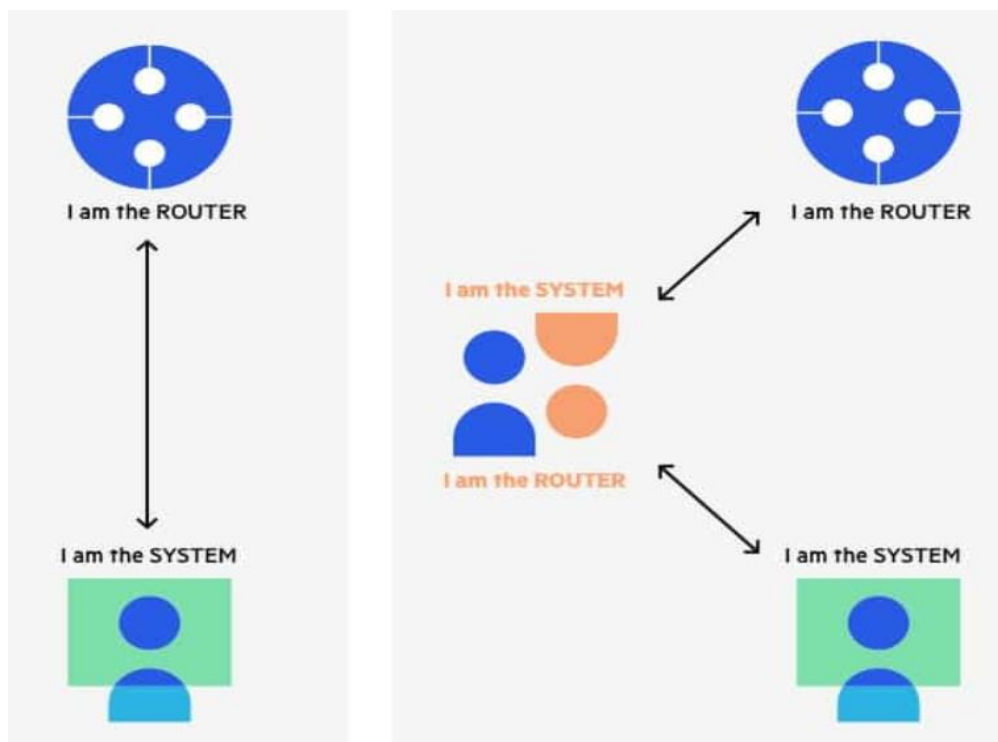
VISUAL STUDIO CODE

KALI LINUX TERMINAL (WSL)

WINDOWS (OPERATION SYSTEM)

**PROBLEM DESCRIPTION:**

Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network. ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address, and vice versa. Most commonly, devices use ARP to contact the router or gateway that enables them to connect to the Internet.



Once the attacker succeeds in an ARP spoofing attack, they can:

Continue routing the communications as-is—the attacker can sniff the packets and steal data, except if it is transferred over an encrypted channel like HTTPS.

Perform session hijacking—if the attacker obtains a session ID, they can gain access to accounts the user is currently logged into.

Alter communication—for example pushing a malicious file or website to the workstation.

Distributed Denial of Service (DDoS)—the attackers can provide the MAC address of a server they wish to attack with DDoS, instead of their own machine. If they do this for a large number of IPs, the target server will be bombarded with traffic.

Having a Kali linux box and a windows 10 machine(Target Machine). We are going to intercept the traffic entering and exiting the windows 10 machine by using ARC poisoning attack and Man in the middle attack from the kali linux machine. Here both the machines are guest virtual machines but this attack is

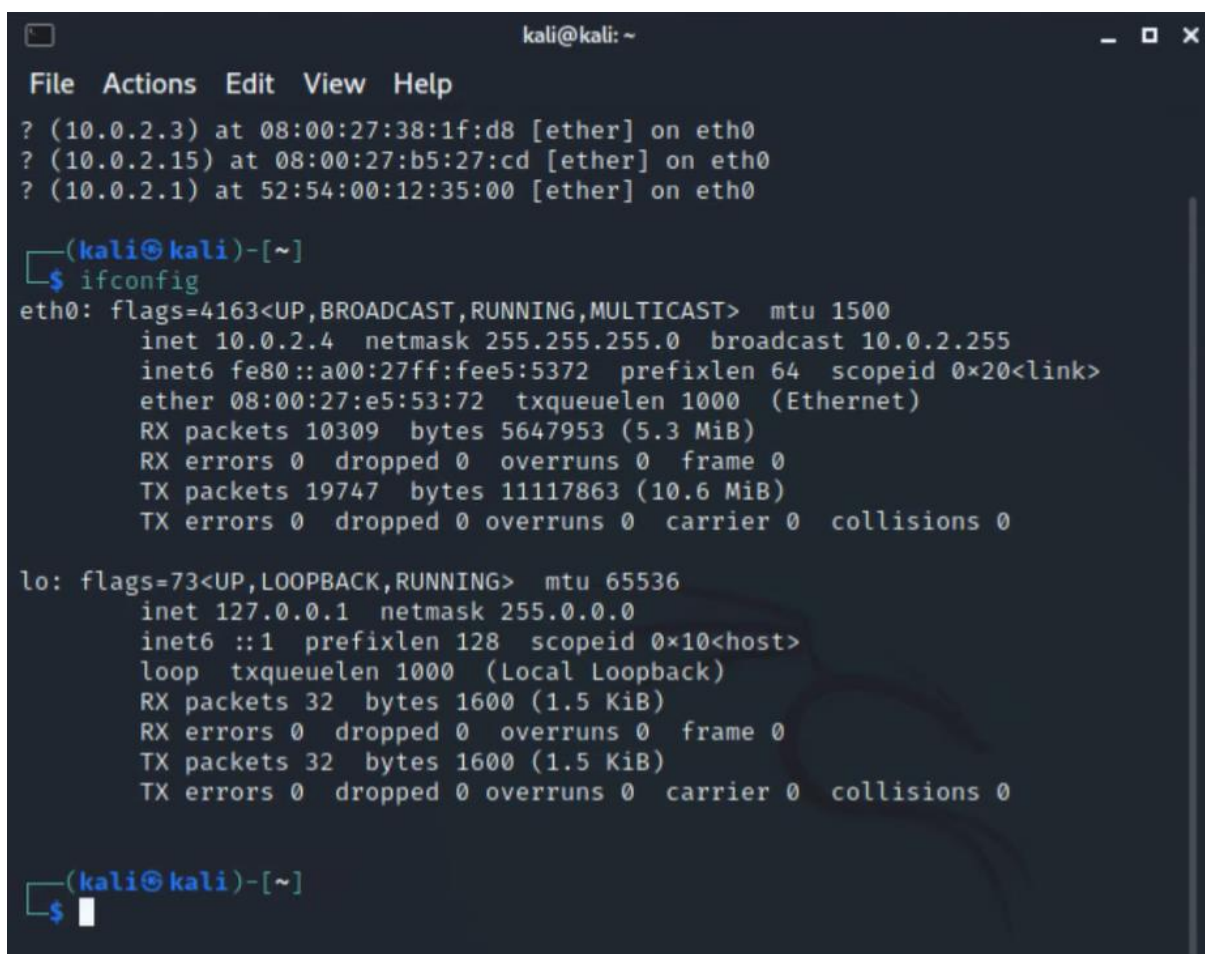
performed in cable connected machines similarly also.

## OUTPUT:

Intercepting the traffic entering and exiting the machine using ARP poisoning attack.

## SCREENSHOTS:

Kali Linux machine:

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~'. The terminal shows the output of the 'ifconfig' command. At the top, there are three lines of text: '? (10.0.2.3) at 08:00:27:38:1f:d8 [ether] on eth0', '? (10.0.2.15) at 08:00:27:b5:27:cd [ether] on eth0', and '? (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0'. Below this, the prompt is '(kali@kali)-[~]' and the command '\$ ifconfig' is entered. The output for 'eth0' shows flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500, inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255, inet6 fe80::a00:27ff:fee5:5372 prefixlen 64 scopeid 0x20<link>, ether 08:00:27:e5:53:72 txqueuelen 1000 (Ethernet), RX packets 10309 bytes 5647953 (5.3 MiB), RX errors 0 dropped 0 overruns 0 frame 0, TX packets 19747 bytes 11117863 (10.6 MiB), TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0. The output for 'lo' shows flags=73<UP,LOOPBACK,RUNNING> mtu 65536, inet 127.0.0.1 netmask 255.0.0.0, inet6 ::1 prefixlen 128 scopeid 0x10<host>, loop txqueuelen 1000 (Local Loopback), RX packets 32 bytes 1600 (1.5 KiB), RX errors 0 dropped 0 overruns 0 frame 0, TX packets 32 bytes 1600 (1.5 KiB), TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0. The prompt is '(kali@kali)-[~]' and the command '\$' is entered with a cursor.

Windows 10 Machine:

```
Command Prompt
(c) Microsoft Corporation. All rights reserved.

C:\Users\tyler>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::74d1:898d:cee3:2748%6
    IPv4 Address. . . . . : 10.0.2.15
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

C:\Users\tyler>arp -a

Interface: 10.0.2.15 --- 0x6
    Internet Address      Physical Address      Type
    10.0.2.1              52-54-00-12-35-00    dynamic
    10.0.2.3              08-00-27-38-1f-d8    dynamic
    10.0.2.4              08-00-27-e5-53-72    dynamic
    10.0.2.255            ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static
    255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

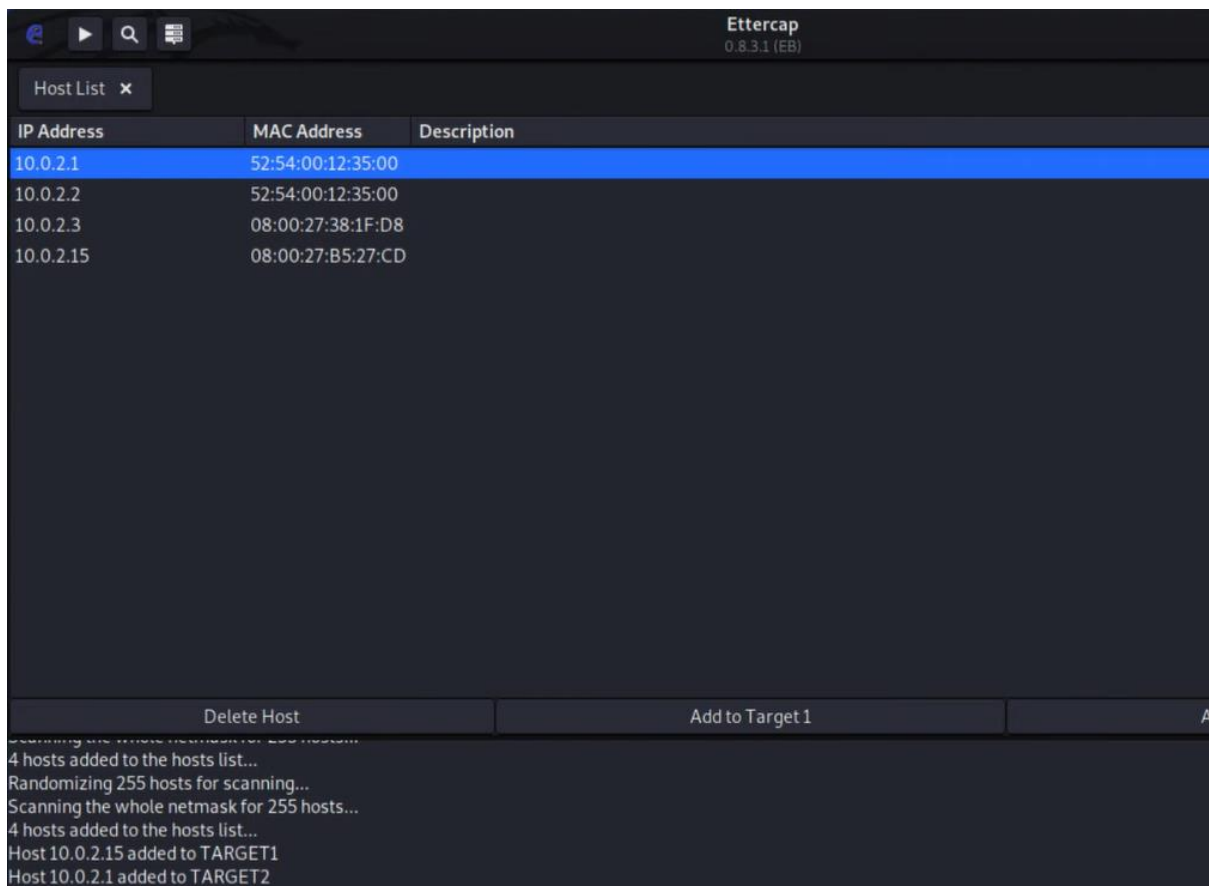
Using Ettercap tool to perform ARP poisoning. And before that forwarding traffic to gateway and start Wireshark to know how the attack changes.

```
(kali@kali)-[~]
$ sysctl net.ipv4.ip_forward=1
```

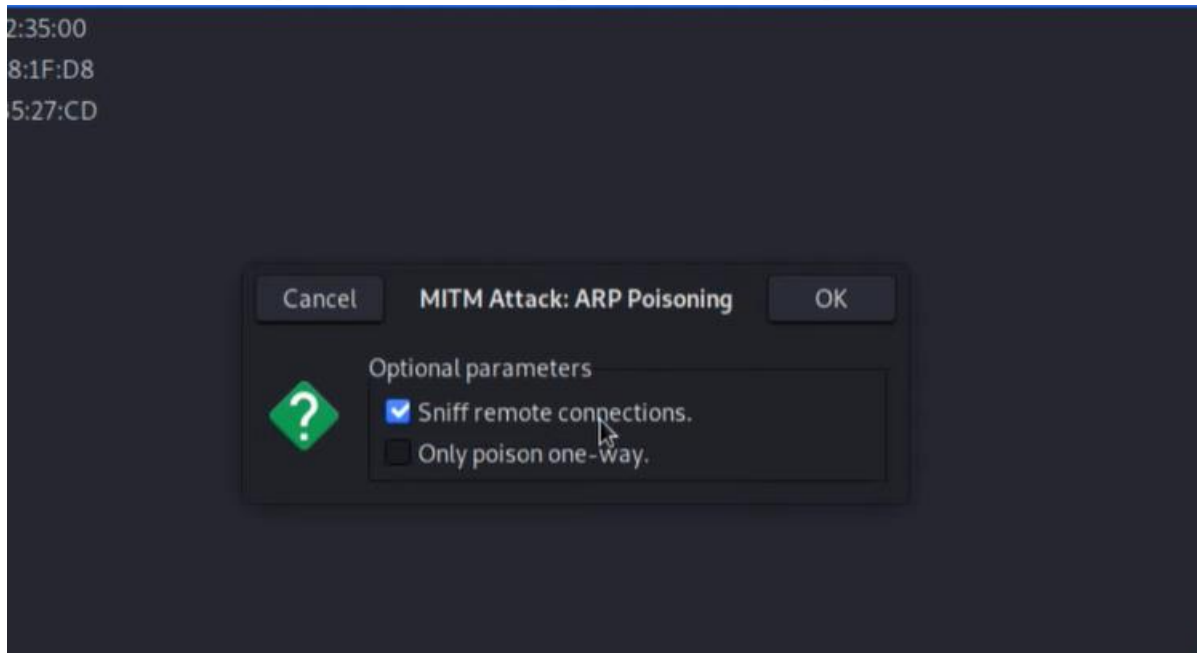
In Ettercap, search for the available machine IPs

The search creates a bunch of ARPs and they send signals to the machines to find out the machines that respond to it to find out the active systems.

After finding out the machines, we set out targets



Initiating the ARP poisoning attack



Now its attacked so the windows thinks that the Ettercap box is the gateway



Interface: 10.0.2.15 --- 0x6

Internet Address	Physical Address	Type
10.0.2.1	08-00-27-e5-53-72	dynamic
10.0.2.3	08-00-27-38-1f-d	dynamic
10.0.2.4	08-00-27-e5-53-72	dynamic
10.0.2.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

## Checking the packets in wireshark

Wireshark packet capture showing ARP request and reply between 10.0.2.1 and 10.0.2.15. The packet list shows several SSDP M-SEARCH requests and two ICMP Echo (ping) requests. The selected packet is an ARP request (Frame 7) from 10.0.2.1 to 10.0.2.15.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
2	1.007903785	10.0.2.15	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
3	2.009176826	10.0.2.15	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
4	3.027536900	10.0.2.15	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
5	51.467644549	10.0.2.1	10.0.2.15	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59262, ttl=64
6	51.468003384	10.0.2.15	10.0.2.1	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59262, ttl=64
7	51.469739820	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	42	10.0.2.1 is at 08:00:27:e5:53:72
8	51.470247096	PcsCompu_e5:53:72	RealtekU_12:35:00	ARP	42	10.0.2.15 is at 08:00:27:e5:53:72 (duplicate use of 10.0.2.1 detected!)
9	52.482543697	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	42	10.0.2.1 is at 08:00:27:e5:53:72
10	52.482590990	PcsCompu_e5:53:72	RealtekU_12:35:00	ARP	42	10.0.2.15 is at 08:00:27:e5:53:72 (duplicate use of 10.0.2.1 detected!)
11	53.493482644	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	42	10.0.2.1 is at 08:00:27:e5:53:72

Frame 7: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0  
 Ethernet II, Src: PcsCompu\_e5:53:72 (08:00:27:e5:53:72), Dst: PcsCompu\_b5:27:cd (08:00:27:b5:27:cd)  
 Destination: PcsCompu\_b5:27:cd (08:00:27:b5:27:cd)  
 Source: PcsCompu\_e5:53:72 (08:00:27:e5:53:72)  
 Type: ARP (0x0806)  
 Address Resolution Protocol (reply)  
 Hardware type: Ethernet (1)  
 Protocol type: IPv4 (0x0800)  
 Hardware size: 6  
 Protocol size: 4  
 Opcode: reply (2)  
 Sender MAC address: PcsCompu\_e5:53:72 (08:00:27:e5:53:72)  
 Sender IP address: 10.0.2.1  
 Target MAC address: PcsCompu\_b5:27:cd (08:00:27:b5:27:cd)  
 Target IP address: 10.0.2.15

Here the Ettercap machine pretends to be the kali linux to the windows machine and as the windows machine to the kali linux box. So basically it impersonates the sender and the receiver and performs the man in the middle attack .

Wireshark packet capture showing multiple duplicate ARP requests from 10.0.2.1 to 10.0.2.15. The packet list shows several SSDP M-SEARCH requests and two ICMP Echo (ping) requests. The selected packet is an ARP request (Frame 7) from 10.0.2.1 to 10.0.2.15.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
2	1.007903785	10.0.2.15	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
3	2.009176826	10.0.2.15	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
4	3.027536900	10.0.2.15	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
5	51.467644549	10.0.2.1	10.0.2.15	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59262, ttl=64 (no response found!)
6	51.468003384	10.0.2.15	10.0.2.1	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59262, ttl=64 (no response found!)
7	51.469739820	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	42	10.0.2.1 is at 08:00:27:e5:53:72
8	51.470247096	PcsCompu_e5:53:72	RealtekU_12:35:00	ARP	42	10.0.2.15 is at 08:00:27:e5:53:72 (duplicate use of 10.0.2.1 detected!)
9	52.482543697	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	42	10.0.2.1 is at 08:00:27:e5:53:72
10	52.482590990	PcsCompu_e5:53:72	RealtekU_12:35:00	ARP	42	10.0.2.15 is at 08:00:27:e5:53:72 (duplicate use of 10.0.2.1 detected!)
11	53.493482644	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	42	10.0.2.1 is at 08:00:27:e5:53:72
12	53.493744394	PcsCompu_e5:53:72	RealtekU_12:35:00	ARP	42	10.0.2.15 is at 08:00:27:e5:53:72 (duplicate use of 10.0.2.1 detected!)
13	54.503988422	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	42	10.0.2.1 is at 08:00:27:e5:53:72
14	54.504030607	PcsCompu_e5:53:72	RealtekU_12:35:00	ARP	42	10.0.2.15 is at 08:00:27:e5:53:72 (duplicate use of 10.0.2.1 detected!)
15	55.514254078	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	42	10.0.2.1 is at 08:00:27:e5:53:72

Here wireshark finds out duplicates also.

Apply a display filter ... <Ctrl-/>					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	10.0.2.15	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1
2	1.007903785	10.0.2.15	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1
3	2.009176826	10.0.2.15	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1
4	3.027536900	10.0.2.15	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1
5	51.467644549	10.0.2.1	10.0.2.15	ICMP	42 Echo (ping) request id=0x7ee7, seq=32487/59262, tt
6	51.468003384	10.0.2.15	10.0.2.1	ICMP	42 Echo (ping) request id=0x7ee7, seq=32487/59262, tt
7	51.469739820	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	42 10.0.2.1 is at 08:00:27:e5:53:72
8	51.470247096	PcsCompu_e5:53:72	RealtekU_12:35:00	ARP	42 10.0.2.15 is at 08:00:27:e5:53:72 (duplicate use of
9	52.482543697	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	42 10.0.2.1 is at 08:00:27:e5:53:72
10	52.482590990	PcsCompu_e5:53:72	RealtekU_12:35:00	ARP	42 10.0.2.15 is at 08:00:27:e5:53:72 (duplicate use of
11	53.493482644	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	42 10.0.2.1 is at 08:00:27:e5:53:72

Frame 8: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0  
 Ethernet II, Src: PcsCompu\_e5:53:72 (08:00:27:e5:53:72), Dst: RealtekU\_12:35:00 (52:54:00:12:35:00)  
 Destination: RealtekU\_12:35:00 (52:54:00:12:35:00)  
 Source: PcsCompu\_e5:53:72 (08:00:27:e5:53:72)  
 Type: ARP (0x0806)  
 Address Resolution Protocol (reply)  
 Hardware type: Ethernet (1)  
 Protocol type: IPv4 (0x0800)  
 Hardware size: 6  
 Protocol size: 4  
 Opcode: reply (2)  
 Sender MAC address: PcsCompu\_e5:53:72 (08:00:27:e5:53:72)  
 Sender IP address: 10.0.2.15  
 Target MAC address: RealtekU\_12:35:00 (52:54:00:12:35:00)  
 Target IP address: 10.0.2.1  
 Duplicate IP address detected for 10.0.2.15 (08:00:27:e5:53:72) - also in use by 08:00:27:b5:27:cd (frame 7)  
 Duplicate IP address detected for 10.0.2.1 (52:54:00:12:35:00) - also in use by 08:00:27:e5:53:72 (frame 7)

Apply a display filter ... <Ctrl-/>					
No.	Time	Source	Destination	Protocol	Length Info
152	232.336984551	10.0.2.4	10.0.2.15	ICMP	102 Redirect
153	232.337000825	10.0.2.15	142.250.191.68	ICMP	74 Echo (pi
154	232.370301570	142.250.191.68	10.0.2.15	ICMP	74 Echo (pi
155	232.370318130	142.250.191.68	10.0.2.15	ICMP	74 Echo (pi
156	234.469136095	PcsCompu_e5:53:72	RealtekU_12:35:00	ARP	42 Who has
157	234.469177396	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	42 Who has
158	234.469385202	RealtekU_12:35:00	PcsCompu_e5:53:72	ARP	60 10.0.2.1
159	234.469498599	PcsCompu_b5:27:cd	PcsCompu_e5:53:72	ARP	60 10.0.2.1
160	235.702092439	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	42 10.0.2.1
161	235.702160122	PcsCompu_e5:53:72	RealtekU_12:35:00	ARP	42 10.0.2.1

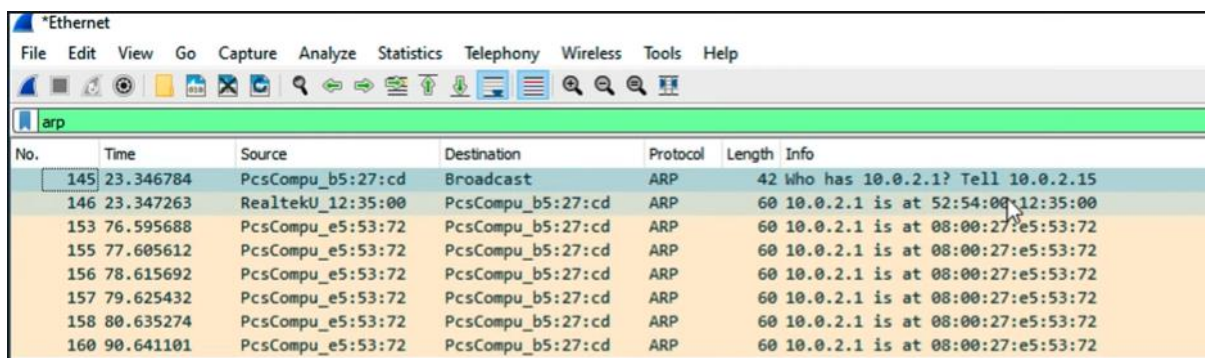
Frame 7: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0  
 Ethernet II, Src: PcsCompu\_e5:53:72 (08:00:27:e5:53:72), Dst: PcsCompu\_b5:27:cd (08:00:27:b5:27:cd)  
 Destination: PcsCompu\_b5:27:cd (08:00:27:b5:27:cd)  
 Source: PcsCompu\_e5:53:72 (08:00:27:e5:53:72)  
 Type: ARP (0x0806)  
 Address Resolution Protocol (reply)  
 Hardware type: Ethernet (1)  
 Protocol type: IPv4 (0x0800)  
 Hardware size: 6  
 Protocol size: 4  
 Opcode: reply (2)  
 Sender MAC address: PcsCompu\_e5:53:72 (08:00:27:e5:53:72)  
 Sender IP address: 10.0.2.1  
 Target MAC address: PcsCompu\_b5:27:cd (08:00:27:b5:27:cd)  
 Target IP address: 10.0.2.15

Packets being transferred from sender to man in the middle and then to the receiver.

Here we are able to capture the information but the information is encrypted so it is pretty hard to decrypt the information to get the actual information .



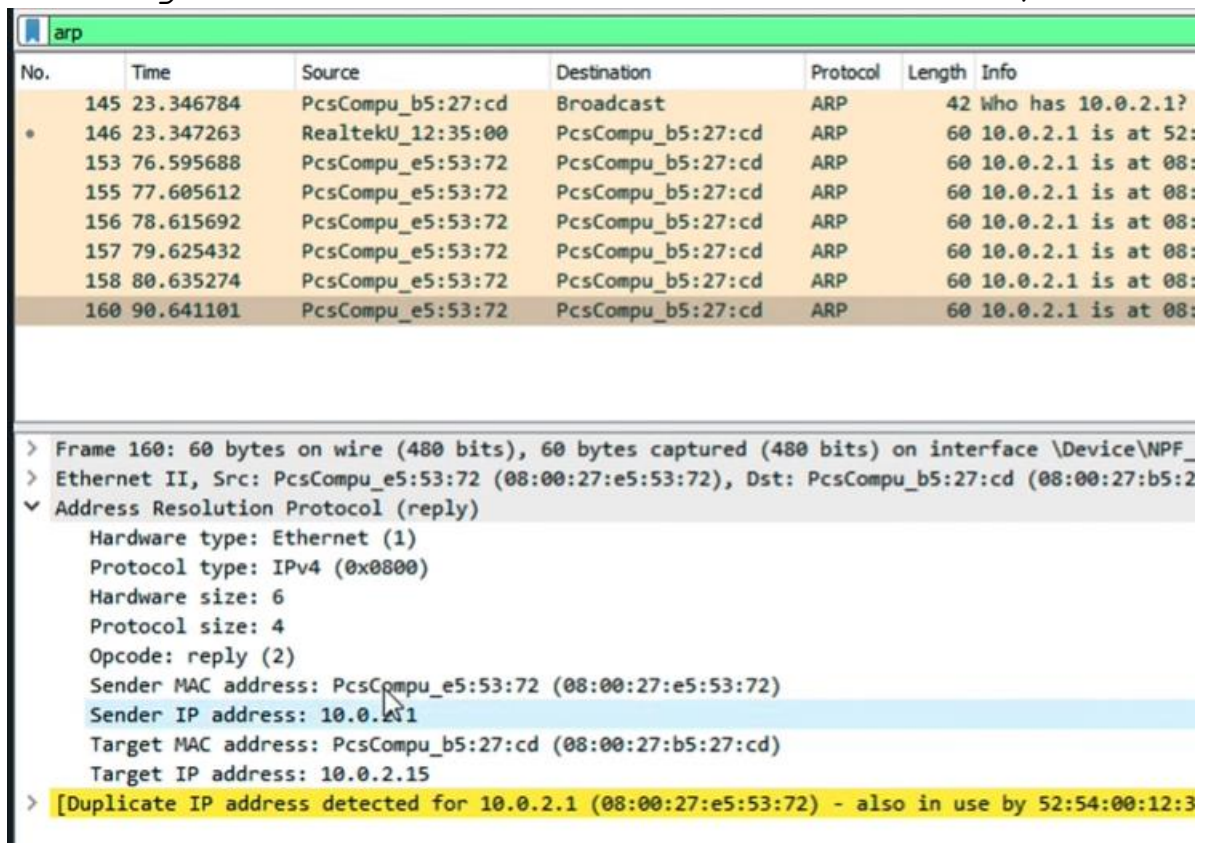
In wireshack



No.	Time	Source	Destination	Protocol	Length	Info
145	23.346784	PcsCompu_b5:27:cd	Broadcast	ARP	42	Who has 10.0.2.1? Tell 10.0.2.15
146	23.347263	RealtekU_12:35:00	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
153	76.595688	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
155	77.605612	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
156	78.615692	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
157	79.625432	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
158	80.635274	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
160	90.641101	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72

We initially have the legitimate Ips but following it we have a series of random ARPs generated.

Having a more detailed look over it,



No.	Time	Source	Destination	Protocol	Length	Info
145	23.346784	PcsCompu_b5:27:cd	Broadcast	ARP	42	Who has 10.0.2.1?
146	23.347263	RealtekU_12:35:00	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
153	76.595688	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
155	77.605612	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
156	78.615692	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
157	79.625432	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
158	80.635274	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
160	90.641101	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72

Frame 160: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{...}
Ethernet II, Src: PcsCompu_e5:53:72 (08:00:27:e5:53:72), Dst: PcsCompu_b5:27:cd (08:00:27:b5:27:cd)
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: PcsCompu_e5:53:72 (08:00:27:e5:53:72)
Sender IP address: 10.0.2.1
Target MAC address: PcsCompu_b5:27:cd (08:00:27:b5:27:cd)
Target IP address: 10.0.2.15

[Duplicate IP address detected for 10.0.2.1 (08:00:27:e5:53:72) - also in use by 52:54:00:12:35:00]

Wireshark tells that there is a duplicate ip configured.

So we can use this as a filter and find out all the bad ARPs .

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
arp.duplicate-address-detected						
No.	Time	Source	Destination	Protocol	Length	Info
153	76.595688	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
155	77.605612	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
156	78.615692	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
157	79.625432	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
158	80.635274	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72
160	90.641101	PcsCompu_e5:53:72	PcsCompu_b5:27:cd	ARP	60	10.0.2.1 is at 08:00:27:e5:53:72

This is how we use wireshark to detect the ARP poisoning attack .