Document de travail

ENSEA

Beyond Engineering

Architecture & Protocols

Lab 3

Report Practical Work

3ème année - RTS

PETIT Alexandre
Arthur LAUMY

TP3 REPORT

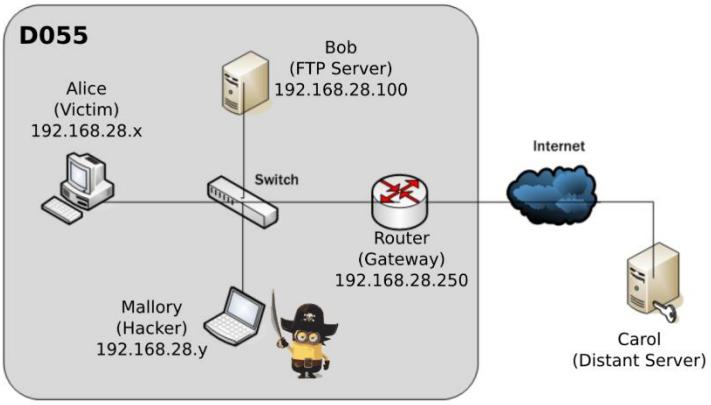


FIG. 1 : Operating diagram

I – Setting up the Layout

```
tpreseau@d055-pc8:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s31f6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 54:bf:64:64:a6:88 brd ff:ff:ff:ff:ff:ff
    inet 192.168.28.8/24 brd 192.168.28.255 scope global enp0s31f6
       valid_lft forever preferred_lft forever
    inet6 fe80::56bf:64ff:fe64:a688/64 scope link
       valid_lft forever preferred_lft forever
3: enp1s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether b4:96:91:2b:69:25 brd ff:ff:ff:ff:ff:ff
4: wlp2s0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether f8:34:41:80:3d:ce brd ff:ff:ff:ff:ff:ff
5: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:3c:05:db brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
6: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel master virbr0 state DOWN group default qlen 1000
    link/ether 52:54:00:3c:05:db brd ff:ff:ff:ff:ff:ff
7: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:75:2f:b7:8f brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
```

We use the ip addr command and find an IP of 192.168.28.8 with a mask of 24. We used the following addresses for our attack:

- Hackeur : 192.168.28.8
- Target 1: 192.168.28.7
- Target 2: 192.168.28.100

II – NMAP

```
tpreseau@d055-pc8:~$ nmap 192.168.28.7

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-09 13:44 CEST
Nmap scan report for 192.168.28.7
Host is up (0.00015s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

The Nmap command is used to map the open and available ports of an IP address. In our case we are looking at two TCP ports: SSH and HTTP, two potential vulnerabilities.

```
tpreseau@d055-pc8:~$ nmap -sP 192.168.28.7

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-09 13:45 CEST
Nmap scan report for 192.168.28.7
Host is up (0.00049s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
tpreseau@d055-pc8:~$ nmap -sP 192.168.28.11

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-09 13:46 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.01 seconds
```

The -sP option is used to check that an IP address is working (if the address exists or if the computer is switched on).

III – ARP Poisoning

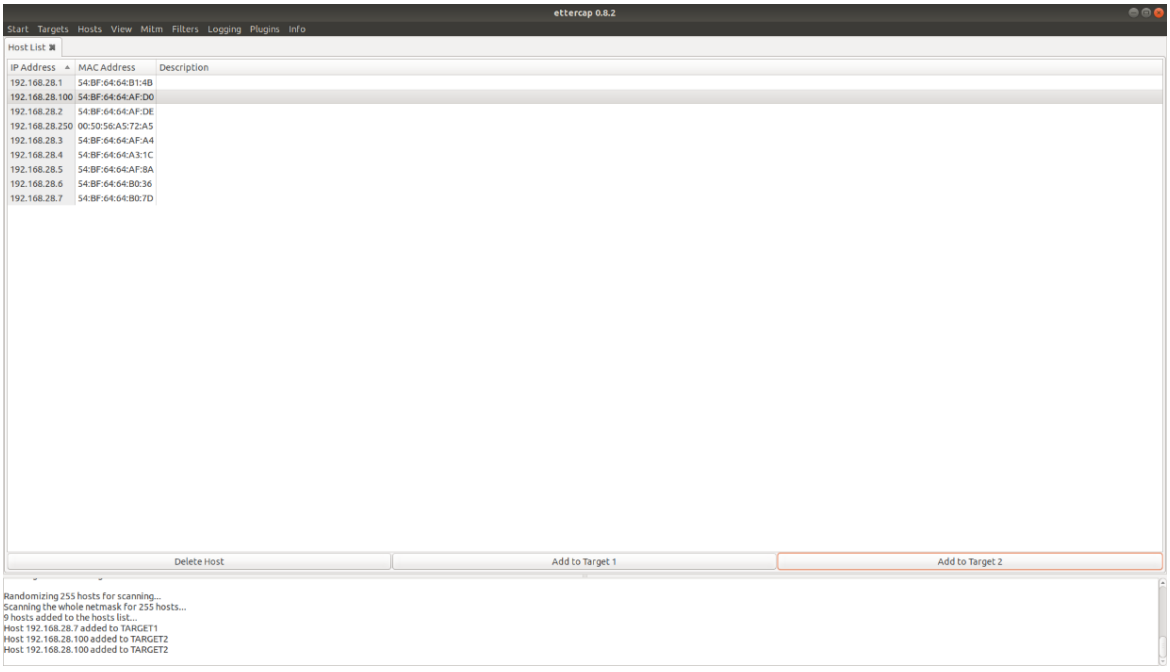
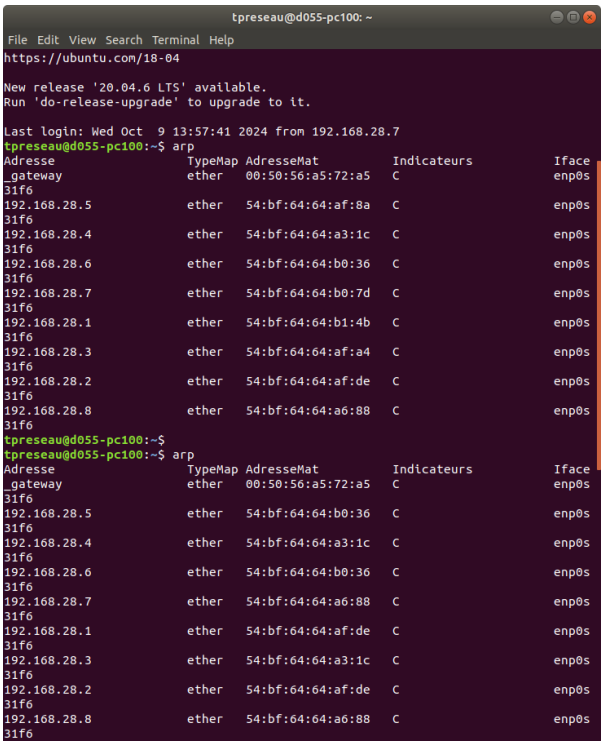


Figure 1 – Ettercap Window



Looking at the ARP table from 192.168.28.100 (retrieved via SSH connection), we can see that the MAC address of our computer (.8) and that of our destination (.7) are the same during ARP poisoning. The station with the IP address 192.168.28.100 therefore thinks it is addressing .7 when it talks to us.

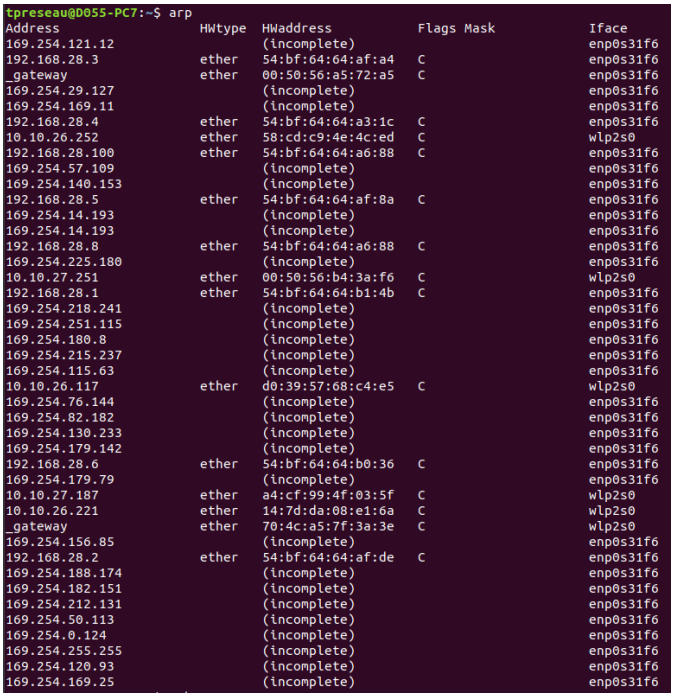


Figure 2 - ARP Table of the First target

On the 192.168.28.7 side, we can see the same phenomenon in the ARP table between our machine (192.168.28.8) and the other target (192.168.28.100). This allows us to verify the man in the middle attack.

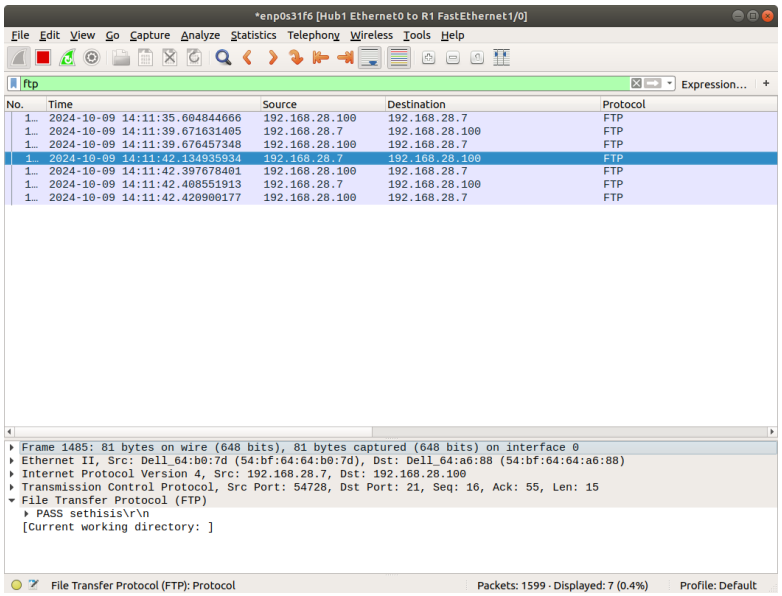


Figure 3 - Wireshark Hacker

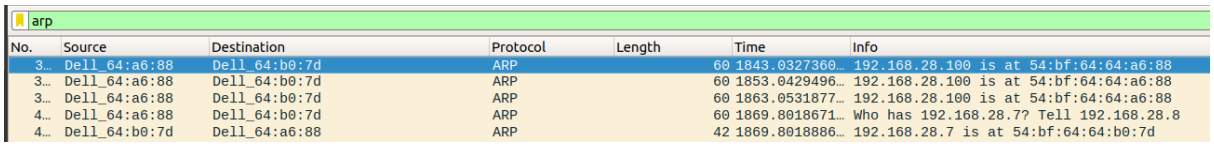
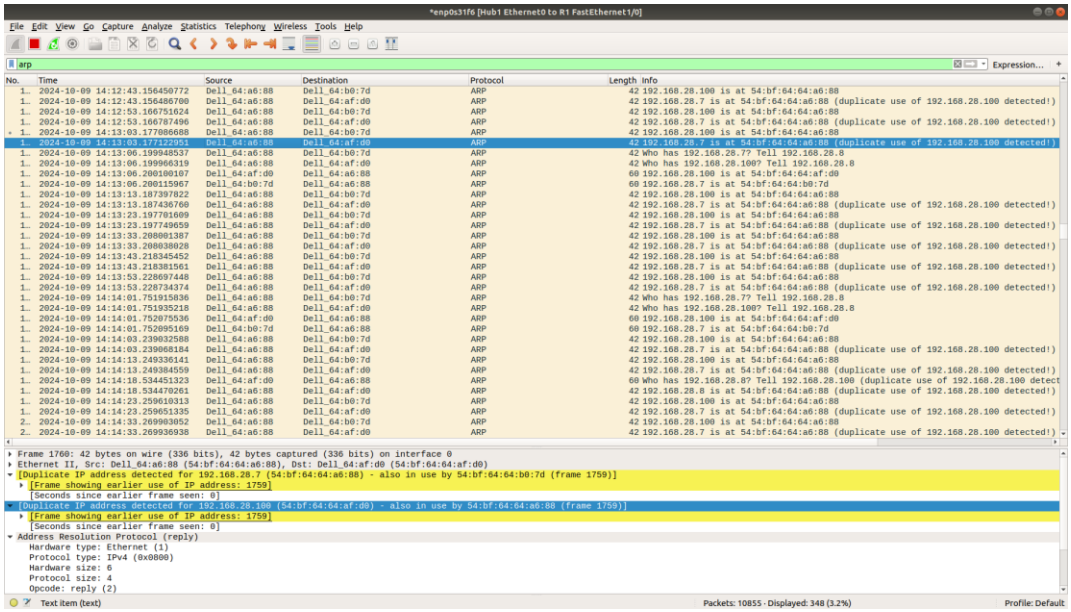
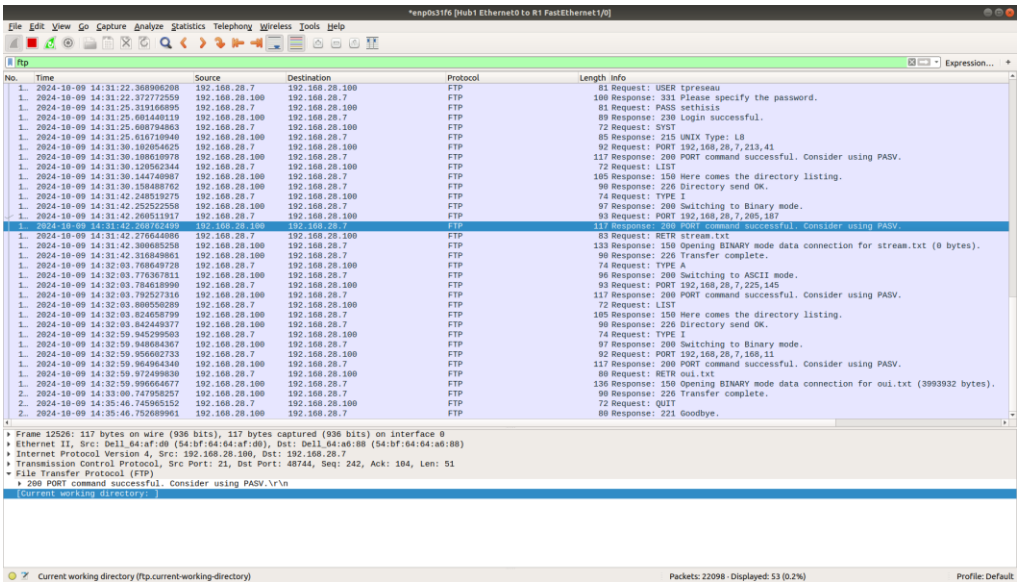


Figure 4 - ARP Traffic

We can see that with ARP poisoning we have managed to recover the FTP network frames during the request and therefore the password. For the ARP traffic, we can see that the MAC addresses have changed as shown above.

Also, the hacker's Wireshark shows that the duplication of the 192.168.28.100 address has been detected.





There are many other things to look out for, such as ls commands and file recovery.

```
-rw-------    1 1001     1001         1441 Oct 03  2023 tomcat.gif
-rw-r--r--    1 1001     1001         1317 Apr 20  2019 toto.asc
-rw-r--r--    1 1001     1001          926 Apr 20  2019 toto.gpg
-rw-------    1 1001     1001      1399883 Mar 21  2024 tp_reseau_sujet.pdf
drwxr-xr-x   20 0        0            4096 Jan 13  2020 v8
226 Directory send OK.
ftp> get oui.txt
local: oui.txt remote: oui.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for oui.txt (3993932 bytes).
226 Transfer complete.
3993932 bytes received in 0.73 secs (5.2248 MB/s)
ftp> exit
221 Goodbye.
tpreseau@D055-PC7:~$
```

Figure 5 - FTP of Target 1

IV – Use of an EtterCap Filter

```
tpreseau@D055-PC7:~$ ftp 192.168.28.100
Connected to 192.168.28.100.
220 (RTS's are the best)
Name (192.168.28.100:tpreseau): tpreseau
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Figure 6 - Effect of an Ettercap Filter

By using the filter specified in the statement, we can modify the user's request, as here where we have added a message.

Remark: Be careful when using compiling, it is very case and space sensitive!

V – Spying with DriftNet

Figure 7 - DriftNet of several pictures get during an FTP Protocol

We can recover a picture using Driftnet while the picture is downloaded from an FTP Protocol.

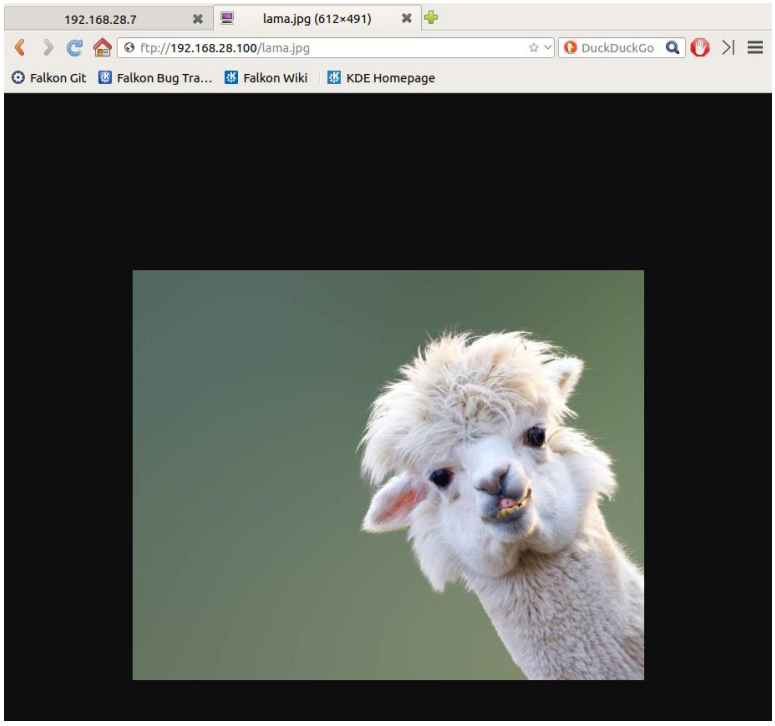


Figure 8 - Standard Web Access

Figure 9 - Driftnet during standard web access

Similarly, with a web access standard, it is possible to retrieve the image using Driftnet.

Remark: jpg appears once, jpeg appears twice on the hacker's screen (even if we open the picture on the internet). With Driftnet the hacker can see the file that the victim retrieved from her ftp connection with Bob.

VI – DNS Poisoning

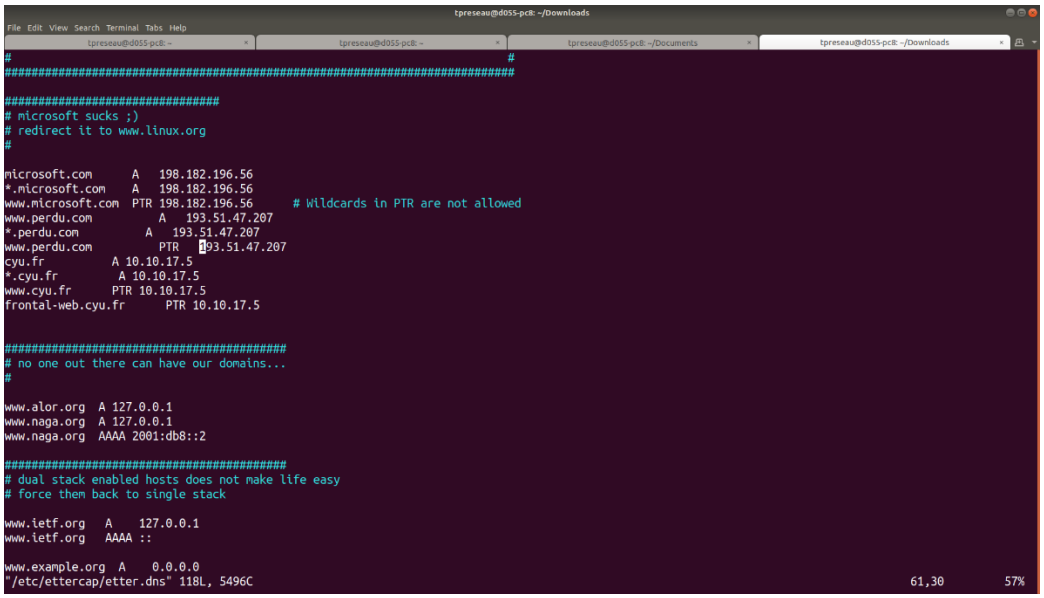


Figure 10 - Edit of /etc/ettercap/etter_dns

We modify the /etc/ettercap/etter_dns file to redirect the address to www.ensea.fr (10.10.17.5).

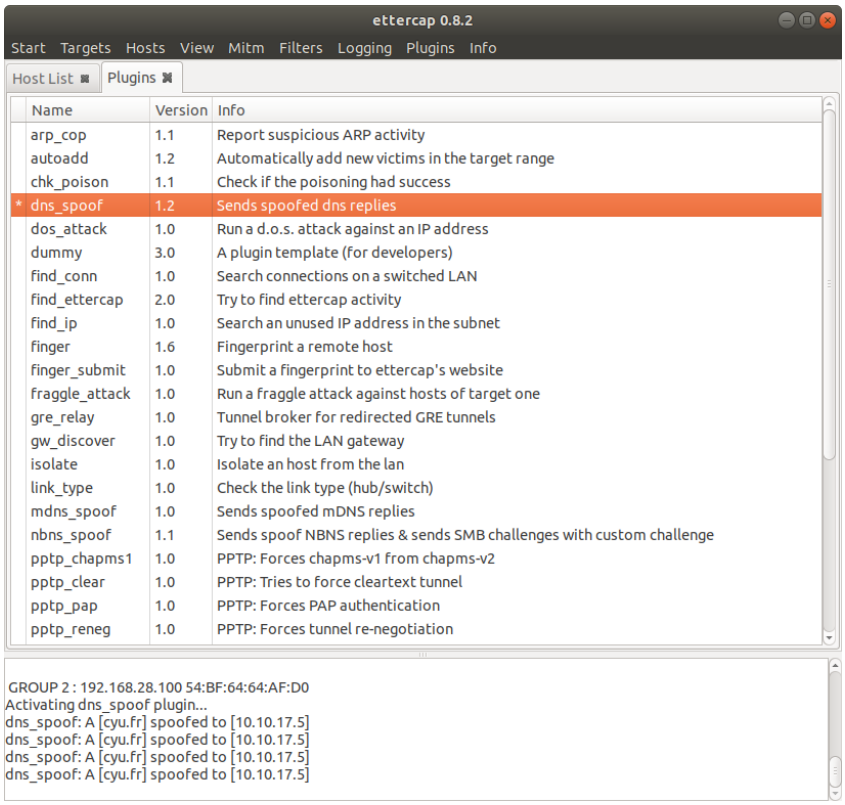


Figure 11 - DNS Spoofing

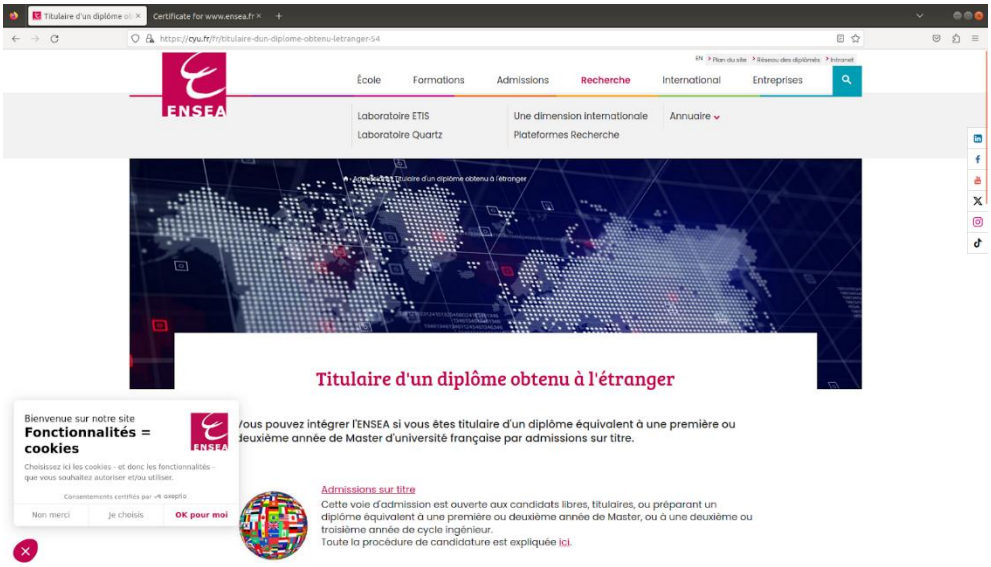


Figure 11 -12 Result of the web page

For the cyu.fr address, we therefore get the home page of www.ensea.fr with its associated pages, which clearly shows another vulnerability.