CERT Lab 6 – Man in the Middle Attack

Educational Objectives

1. Learn how ARP poisoning is performed and how to detect it

Tools

1. Kali Linux VM

Lab Task 6 – ARP Spoofing using Ettercap

1. Login to Kali Linux machine
2. Open terminal and run as root account `sudo su`

Step 1 – Set up Manual Packet Forwarding

1. Set up Manual Packet Forwarding
   a. In the terminal type in the following commands

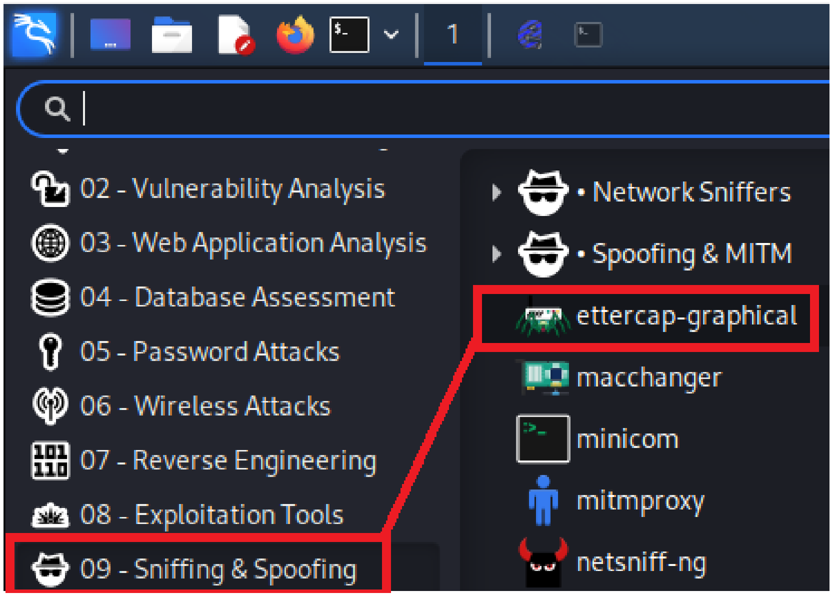
```
cat /proc/sys/net/ipv4/ip_forward
```

   b. If the output returns **1** then you are good to go. However, if the value returns **0**, type the following command:

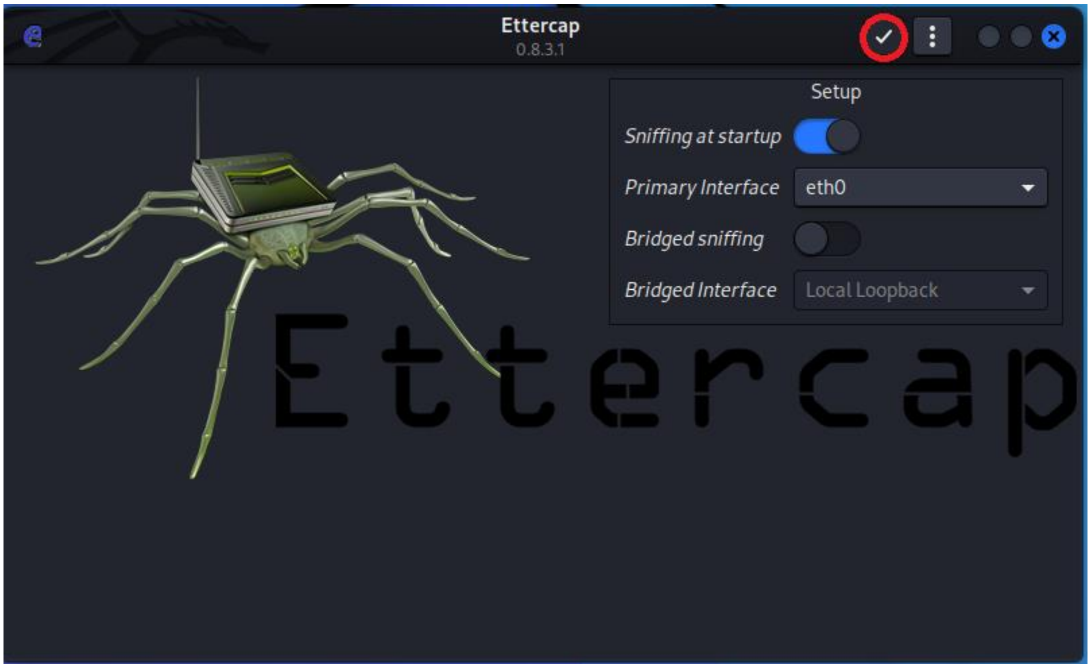
```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Step 2 – Launch Ettercap

1. Click on the Applications button and select 09 - Sniffing & Spoofing>ettercap-graphical



2. The GUI will pop up, leave the default settings, and press the check button on the top right corner



Setup

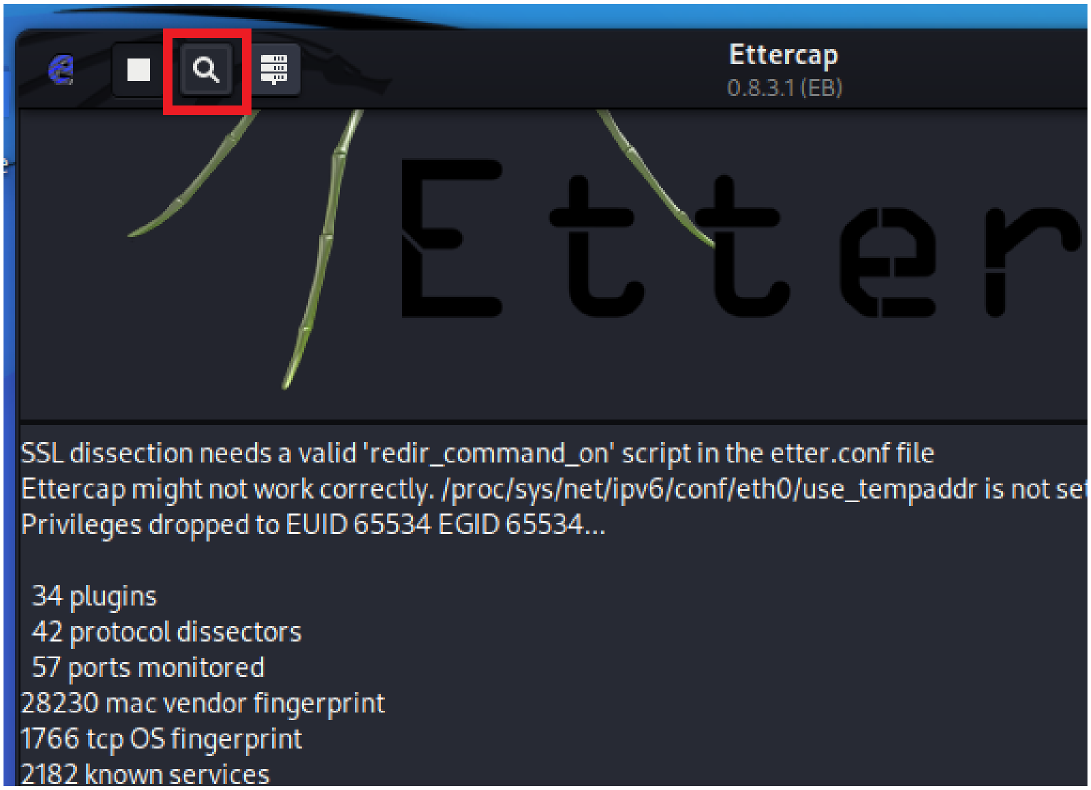
Sniffing at startup: on

Primary Interface: eth0

Bridged sniffing: off

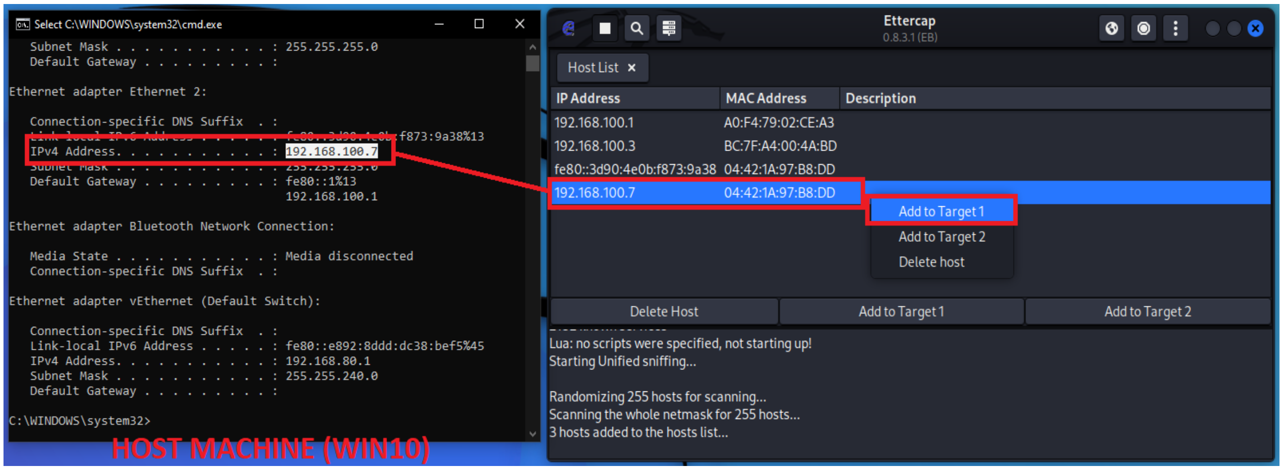
Bridged Interface: Local Loopback

3. First thing that we need to do is to scan for host, click on the magnifying glass button on the top left corner of the Ettercap window



```
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set
Privileges dropped to EUID 65534 EGID 65534...

 34 plugins
 42 protocol dissectors
 57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
```

4. Once the hosts are detected, click on Host List button, then find out your host machine's IP address, right click on the host and select "Add to Target 1"

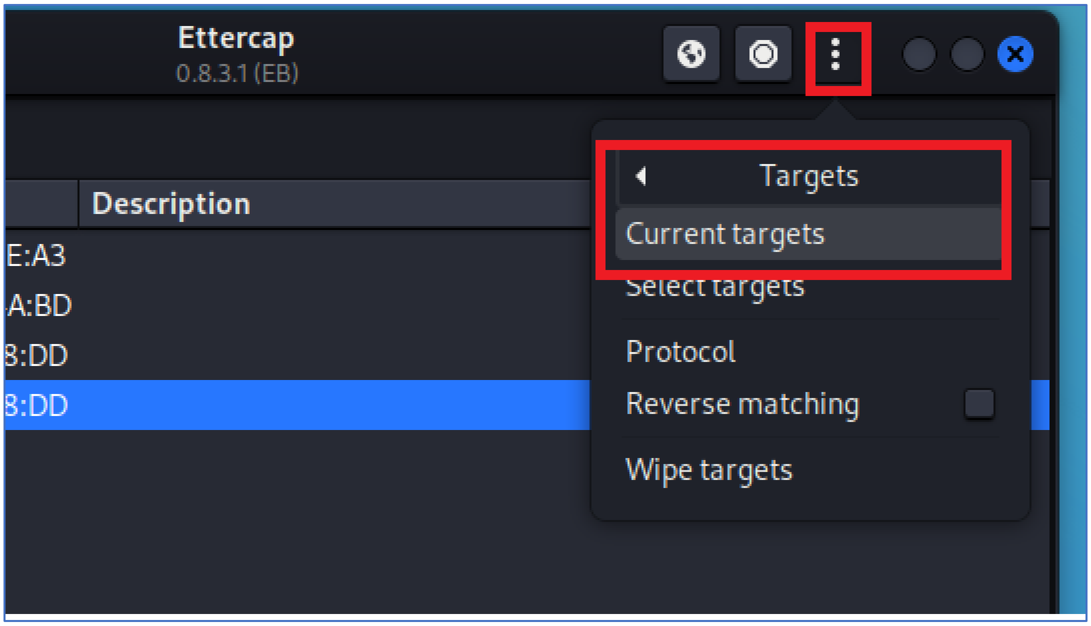


```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3d90:4e0b:f873:9a38%13
   IPv4 Address. . . . . . . . . . . : 192.168.100.7
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%13
                                       192.168.100.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e892:8ddd:dc38:bef5%45
   IPv4 Address. . . . . . . . . . . : 192.168.80.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

C:\WINDOWS\system32>
```

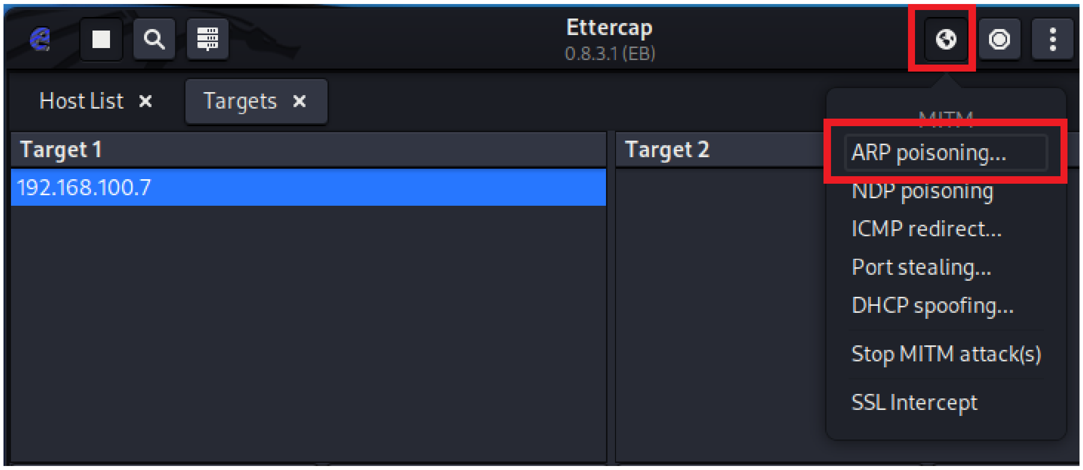
IP Address	MAC Address	Description
192.168.100.1	A0:F4:79:02:CE:A3	
192.168.100.3	BC:7F:A4:00:4A:BD	
fe80::3d90:4e0b:f873:9a38	04:42:1A:97:B8:DD	
192.168.100.7	04:42:1A:97:B8:DD	

```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
```

5. Ettercap will display Host 192.168.100.7 added to TARGET1, next click on the three-dot button on the top right and select Targets > Current Target

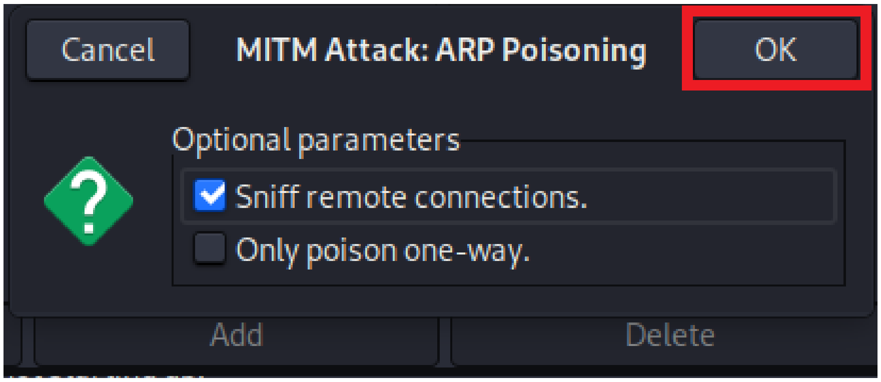


6. When the target window shows, click on MiTM menu button , and select ARP Poisoning



Target 1	Target 2
192.168.100.7	

7. Leave the option as is and click on OK

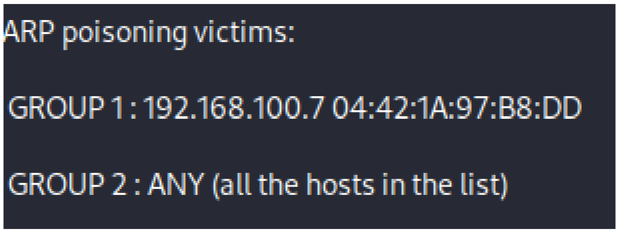


Optional parameters

☑ Sniff remote connections.

□ Only poison one-way.

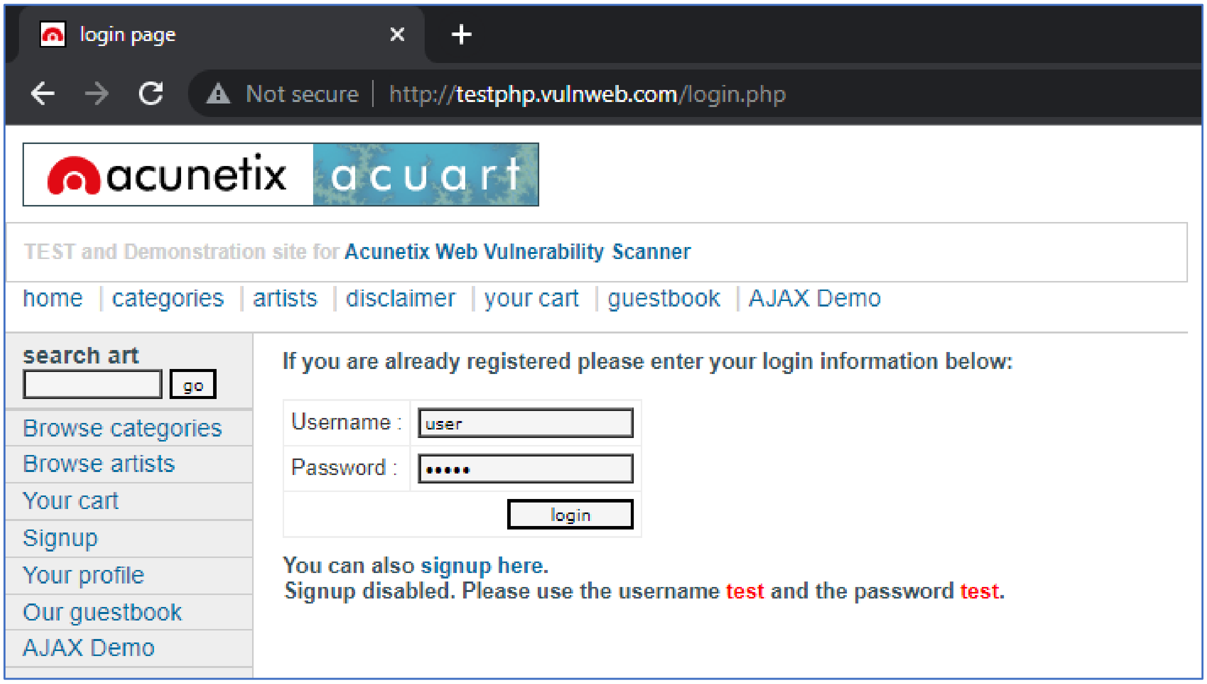
8. The host machine is sniffed (ARP Poisoning) as shown in the log and the log does not show much output. However, once our target visits a page that sends unencrypted usernames and passwords, it will print



```
ARP poisoning victims:

 GROUP 1 : 192.168.100.7 04:42:1A:97:B8:DD

 GROUP 2 : ANY (all the hosts in the list)
```

Step 3 - Capturing login credentials on ARP spoofed machine

1. On the host (victim) machine, open a browser and go to http://testphp.vulnweb.com/login.php
2. Type any username and password on this page and click login



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

If you are already registered please enter your login information below:

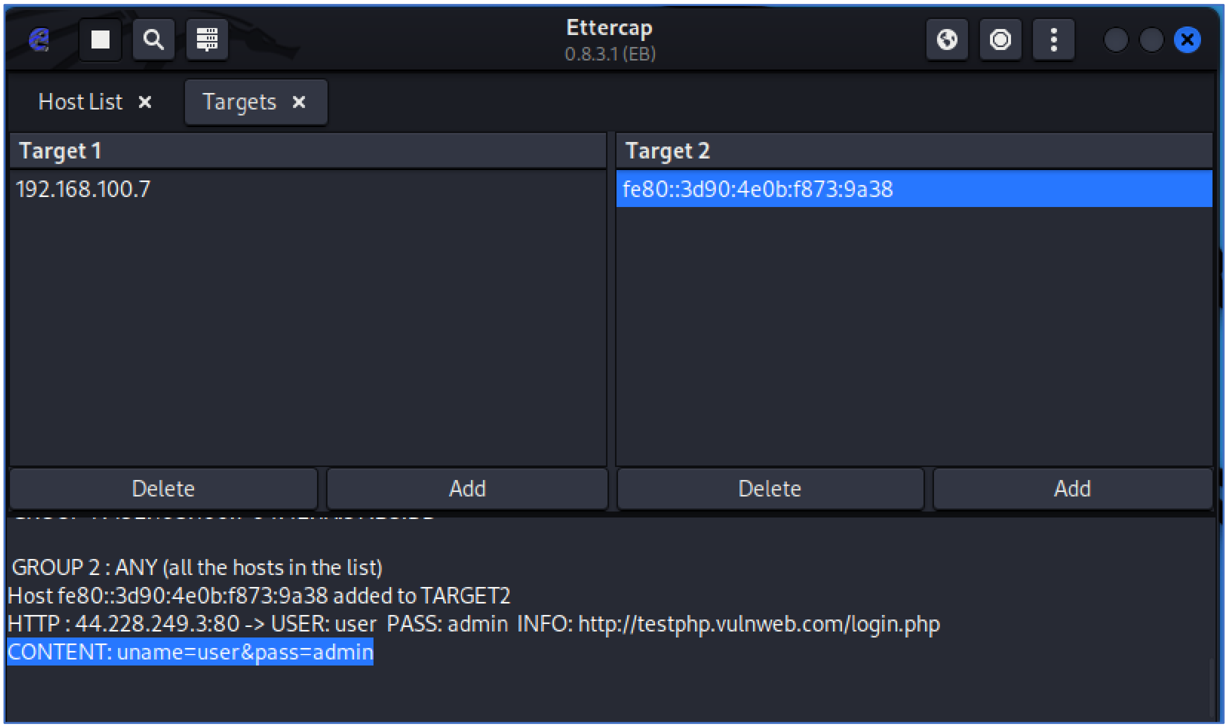
Username : user

Password : •••••

login

You can also signup here.
Signup disabled. Please use the username test and the password test.

3. Go back to the Kali Linux machine and check on Ettercap's captured login



Target 1	Target 2
192.168.100.7	fe80::3d90:4e0b:f873:9a38

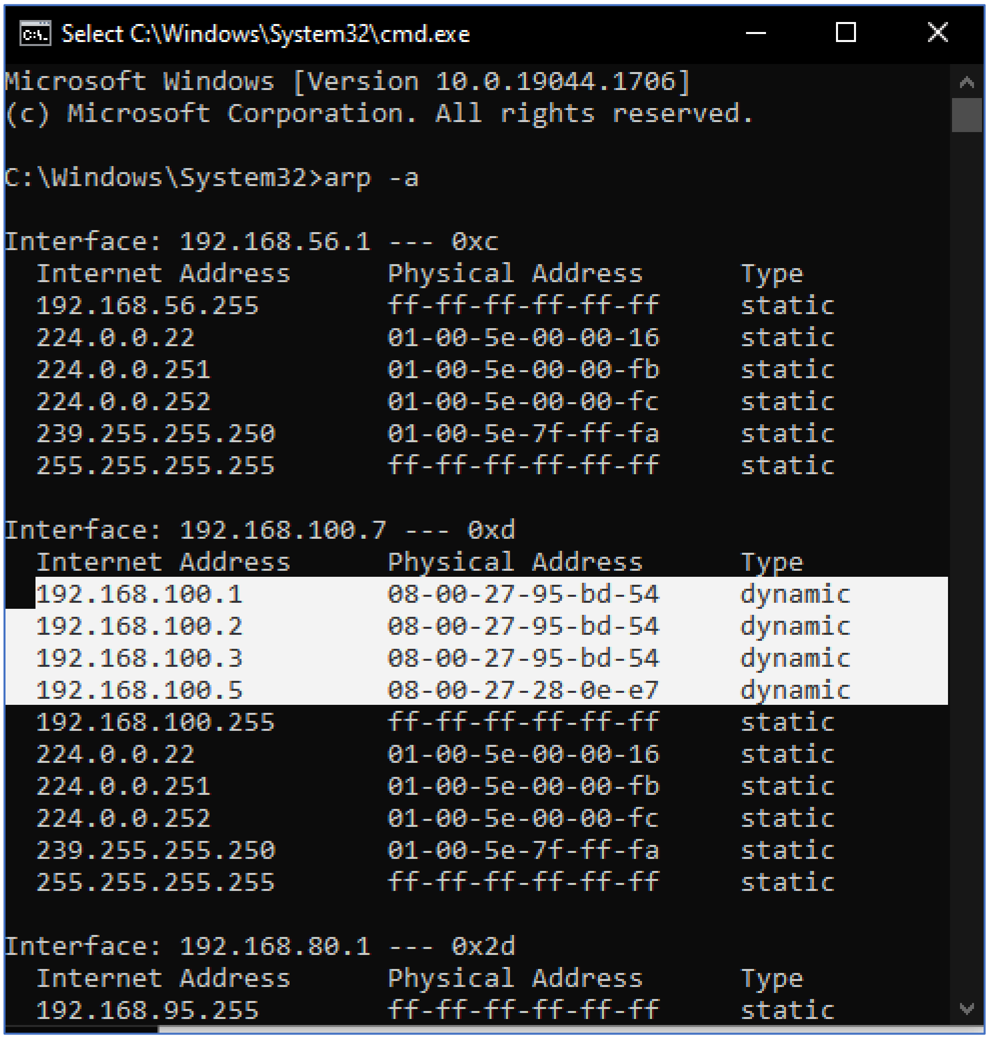
```
GROUP 2 : ANY (all the hosts in the list)
Host fe80::3d90:4e0b:f873:9a38 added to TARGET2
HTTP : 44.228.249.3:80 -> USER: user  PASS: admin  INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=user&pass=admin
```

Step 4 - Detecting if your machine is being sniffed

1. On the host (victim) machine, open cmd and type the following command

```
arp -a
```

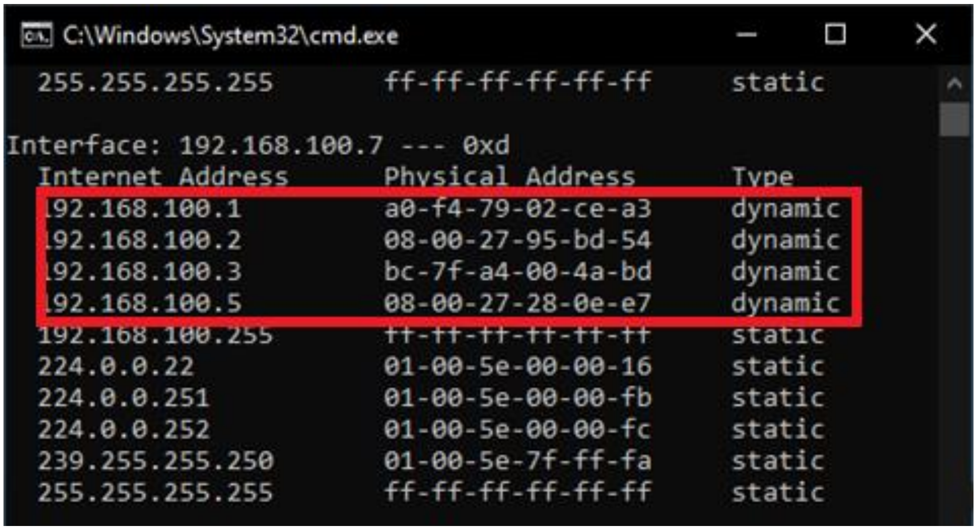
2. This will list out the ARP cache, which is, the IP addresses of the local machine on the network and their corresponding MAC addresses



```
Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>arp -a

Interface: 192.168.56.1 --- 0xc
  Internet Address      Physical Address      Type
  192.168.56.255        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

Interface: 192.168.100.7 --- 0xd
  Internet Address      Physical Address      Type
  192.168.100.1         08-00-27-95-bd-54     dynamic
  192.168.100.2         08-00-27-95-bd-54     dynamic
  192.168.100.3         08-00-27-95-bd-54     dynamic
  192.168.100.5         08-00-27-28-0e-e7     dynamic
  192.168.100.255       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

Interface: 192.168.80.1 --- 0x2d
  Internet Address      Physical Address      Type
  192.168.95.255        ff-ff-ff-ff-ff-ff     static
```

a. If we observe the first 4 IP addresses in this list, they appear to have the same MAC (physical) address and that is a sign that the machine is ARP spoofed.

3. Switch to Kali Linux machine and close the Ettercap main window.
4. Go back to the cmd in host machine and enter `arp -a` again
5. When the Man in the Middle attack is stopped, we can now see that the previous IP addresses are back to having different MAC addresses



```
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.100.7 --- 0xd
  Internet Address      Physical Address      Type
  192.168.100.1         a0-f4-79-02-ce-a3     dynamic
  192.168.100.2         08-00-27-95-bd-54     dynamic
  192.168.100.3         bc-7f-a4-00-4a-bd     dynamic
  192.168.100.5         08-00-27-28-0e-e7     dynamic
  192.168.100.255       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
```