* **Document the IP and MAC addresses of the three PCs.**
  + **ipconfig /all** ( windows)
  + ifconfig ( Ubuntu )

|  |  |  |
| --- | --- | --- |
| PC | IP | MAC |
| Attacker Ubuntu |  |  |
| Victim 1 |  |  |
| Victim 2 |  |  |

**In Ubuntu Terminal**

* **Sudo apt-get update ( you may asked for your password 1234)**
* **Sudo apt-get install Ettercap-graphical** 
  + **Y ( yes )**
  + **Y ( yes)**
* Open wireshaek, type **sudo wireshark**, then start capturing.
* Type sudo **ettercap –G** and press enter.
* On the Ettercap menu bar, choose Sniff | Unified Sniffing.
* In the Ettercap input dialog box, make sure network interface eth0 is selected and click OK.
* Choose Hosts | Scan for Hosts.

This will start an ARP scan to detect what machines are up on the subnetwork. It will add those machines to a host list.

* Choose Hosts | Hosts List.
* Select the Windows 7 and click Add to Target 1.
* Select the Windows 7 (virtual machine) and click Add to Target 2.
* On the Ettercap menu bar, choose Mitm | Arp Poisoning.
* In the MITM Attack dialog box, check Sniff Remote Connections and click OK
* On the menu bar, choose Start | Start Sniffing.
* Check arp table on each victims
  + Arp -a

**Capture an FTP session.**

* **In Windows 7 ( victim 1)**
* **Establish an FTP connection to the server 10.170.14.242 by typing ftp 10.170.14.242 OR telnet 10.170.14.242 21 then ENTER.**
* **Type the username …………. And password ………… ( given by your instructor) then ENTER.**
* **Type dir and then ENTER.**
* **Type bye then ENTER.**
* **Leave the command prompt open.**

**ON Ubuntu:**

* In the Ettercap window, in the bottom pane of the window, notice the captured FTP session with user ID and password.

What is your analysis of what happened?

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

* Stop wireshrak. Try to analyze the capture to see what happened.