# Training - Man In The Middle

Loïc Delestra

## A/ Setup the lab

The first part of this training is to setup your lab.

1. Virtualbox.
   For your practical work Virtualbox is already installed.

Computers in A214 have /VM/ folder shared by every system in that machine. Before adding the first VM you need to change the default image directory for /VM.

2. Installing Kali Linux Offensive Security (the company behind Kali) provide a pre-installed VM of Kali.
   The pre-installed VM is already downloaded on your computer in the /VM/ directory.
   Start Virtualbox and click ‘file/import Appliance’ and import the Kali-Linux-2.0.0-vbox-i686.ova file.
   **if you cant found the .ova file in /VM/**, it can be download.
   Download url:
   Kali Linux for VMware and VirtualBox
   https://www.offensive-security.com/kali-linux-vmware-arm-image-download/
   Be sure to download the VirtualBox one (by default it display the VMware) 64bit with PAE.

3. Installing Metaspoitable
   Metasploitable is a vulnerable distribution provided by rapid7 the company behind the Metasploit framework.
   It’s also already downloaded on your computer in /VM/ directory’.
   Unzip it into /VM/ and add this existing VM into VirtualBox.
   Start Virtualbox, click ‘New’ and select ‘use an existing virtual hard disk file’, point to ‘/VM/metasploitable–/–.vmdk’, and create.
   Run it. Use login:msfadmin password:msfadmin
   Check the network interface.
   **if you cant found the metasploitable archive in /VM/**, it can be download.
   Download link:
   http://downloads.metasploit.com/data/metasploitable/metasploitable-linux-2.0.0.zip

4. Installing Lubuntu
   Lubuntu is the client machine (here the victim).
   Do the same as previously with Metasploitable. The existing VDI file must be in /VM/lubuntu/
   Start Virtualbox, click ‘New’ and select ‘use an existing virtual hard disk file’. Use /VM/lubuntu/lubuntu.vdi
   user: osboxes | password:osboxes.org
   **if you cant find the vdi file in /VM/**, you can download it here:
   http://www.osboxes.org/lubuntu/

5. Create an internal network
   Change every existing interface to use the same internal network named ‘lab’.
   Login to every VM to set the IP address.
   Lubuntu: 192.168.0.10 | Metasploitable: 192.168.0.11 | Kali: 192.168.0.20
   **Check all the VMs can ping each other. From every VM. Yes realy, do that, it’s important!**

## B/Start the attack

6. In the lubuntu box

- open the browser and look a http://192.168.0.11
- go to the phpmyadmin page. Everything should be normal
- open a terminal and look at your arp table with `arp -n`

7. In the kali box

- You must allow the packets to be forwarded between the server and the client. `echo 1 > /proc/sys/net/ipv4/ip_forward`
- Open a new terminal. You need to spoof the mac adress of the server (metasploitable) with your own in the client box(lubuntu) `arpspoof -t 192.168.0.10 192.168.0.11`
- Open a new terminal. You need to spoof the mac adress of the client (lubuntu) with your own in the server box(metasploitable) `arpspoof -t 192.168.0.11 192.168.0.10`
- Open Wireshark software and look at your eth0 interface.

8. In the lubuntu box

- go back to your browser and refresh the phpmyadmin page (use ctrl+f5).

9. In the kali box

- In your wireshark… this is where the magic happens! You must see the http request and reply.

10. With your kali and lubuntu.

- Try to login the phpmyadmin page. Find the user and password in your wireshark.
- Try the driftnet tool in your kali `driftnet -i eth0`. In your lubuntu go to the dvwa/login.php page (refresh with ctrl+f5 if needed).