Lab 1: Lab environment setup

6COSC002W

Ayman El Hajjar

Week 1

PLEASE READ ALL OF THIS DOCUMENT

- **On your own device: You can complete this lab as you will need to only do it once.**
- **In some labs, you need your Kali Linux VM to be connected to the Internet.**
- **The only machine that you possibly need to connect to the Internet is Kali machine, to install some applications or to update your machine.**
- **TO ENSURE CORRECT IP ADDRESS DYNAMIC ALLOCATION, IT IS ESSENTIAL THAT YOU START THE MACHINES IN THE CORRECT ORDER. THE ORDER IS THE FOLLOWING**
  1. **KALI LINUX**
  2. **OWASP VULNERABLE MACHINE**
  3. **WINDOWS Machine**
- **If you are having a problem, check the last section of this document. If this is still not working, check with your lab instructor.**
- You can use either windows or Linux for host.

1 Lab environment

How to download

1. For this course we will be using three different virtual machines.
   (1) The **first** VM will be the attacher machine that contains. This will be a "Kali Linux machine".
   (2) The **second** VM will be the vulnerable machine that contains all the different services (apache, databases,web apps, etc..).
   (3) The **third** VM will be the victim machine. This is a windows 7 virtual machine.. **Download IE8 on Win7**. The platform depends on which Virtual machine software you are using.

- To download them, please choose from below:

2. **ALL links require a password. The password is 6COSC002W**
   - **Kali Linux** You can download this virtual machine from this link
   - **OWASP virtual machine:** You can download this virtual machine from this link
   - **Windows**: You can download this virtual machine from this link

For installing VirtualBox

- Once your files are downloaded, you will need to install a virtual machines manager application
- There are two choices of software you can use. You can either use VMWARE or Oracle VirtualBox.
- For this course we will be using Oracle VirtualBox. You can download Oracle VirtualBox from this link.
  - You need to make sure you are downloading the correct version - **depending on your host Operating system**

- You will then need to import the three VMs you have downloaded.
- You can import in Virtual box by either click on the downloaded file directly and following instructions or by clicking on import to locate the file and import to virtual box as shown below.

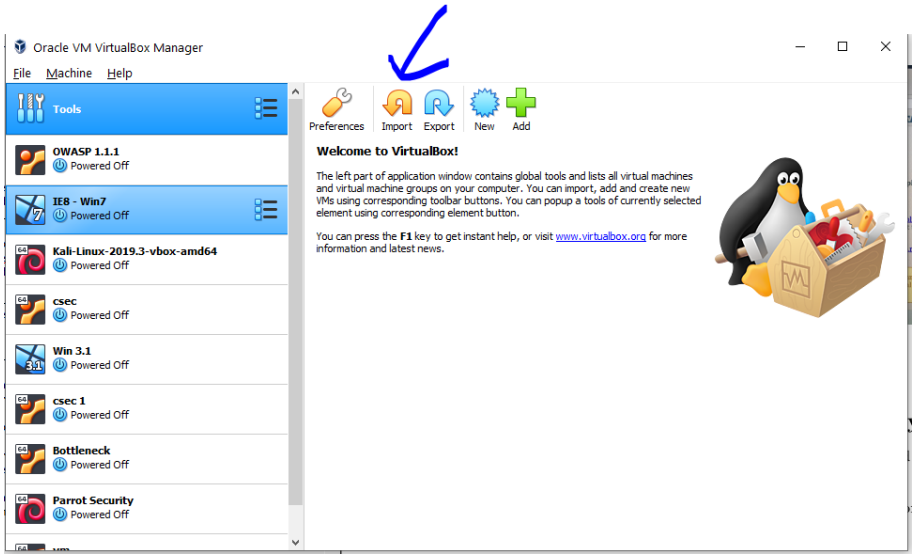

Figure 1: Import VMs into virtualbox

1.1 Virtual machines setup

- Passwords for virtual machines Operating systems are shown below:
  1. Kali Linux
     - username: kali
     - password: kali
  2. owaspbwa linux
     - username: root
     - password: owaspbwa
  3. Windows 7 (If needed)
     - username: admin
     - password: Passw0rd

2 Network Setup

2.1 Internet Connected VM

Internet Connected Network

- In some times, you need your Kali Linux VM to be connected to the Internet.
- You never need to connect the Win7 machine or the OWASP machine to the Internet

The steps below will be the same for any VMs that you want it to be connected to the Internet (to the network your host machine is connected to)

- Select the VM you need to change settings for and click on Settings. (Fig.2)
- Select Network (Fig3)
- Choose in the drop down menu of **Attached to** the option NAT. This is network Address Translation. This will give your virtual machine access to the network resources of your host machine. It will use the same IP address of your host machine to connect to the Internet. (Fig3)

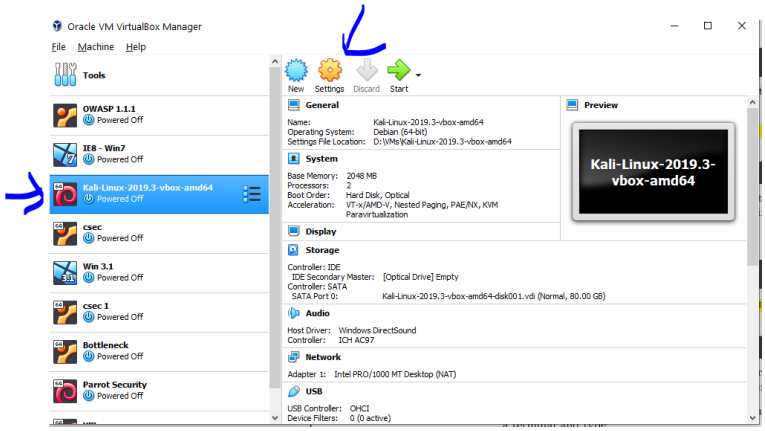

Figure 2: Choose Settings

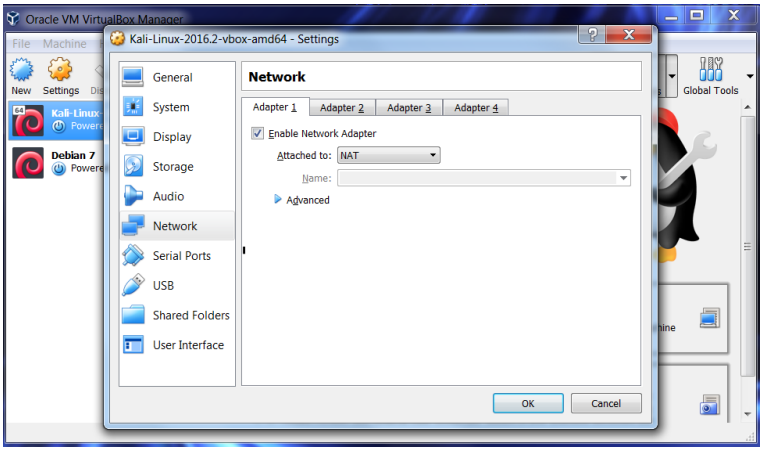

Figure 3: Choose NAT

2.2 Isolated Network

Internet Connected Network

- Most of the labs will need this network setup unless the lab specifies other wise

- There are two methods to configure your lab network environment. We will look at both and how you can set up your network to use any of them.
- For both you will need to first create a Virtual network by following the steps below.
  - Click on File on the Virtual box program and select **Host Network Manager** Fig.4
  - Click on Create Fig.5
    1. If you want to setup your network IP addresses manually for each machine then make sure DHCP is not enabled as in Fig.5
- Now you need to make sure that your VM network settings uses the virtual Network you created.
  - Click on Settings as in (Fig.2)
  - Click on properties after enabling DHCP and select DHCP server. The settings in n (Fig.7) is what I am using for the labs. This will give the first IP 101 to KAli.
  - click on Network as in (Fig.8) and choose **Host Only Adapter**. You should see the Network Name as **Virtual Box host-only adapter.**

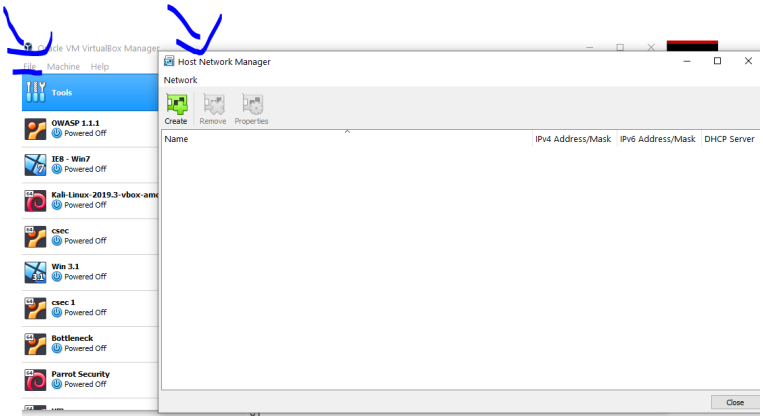

Figure 4: Enter into Host Network manager Setup window

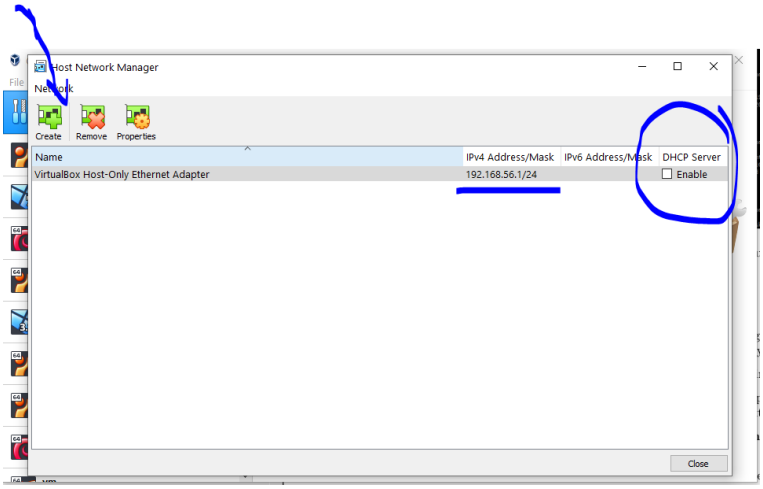

Figure 5: Create Network

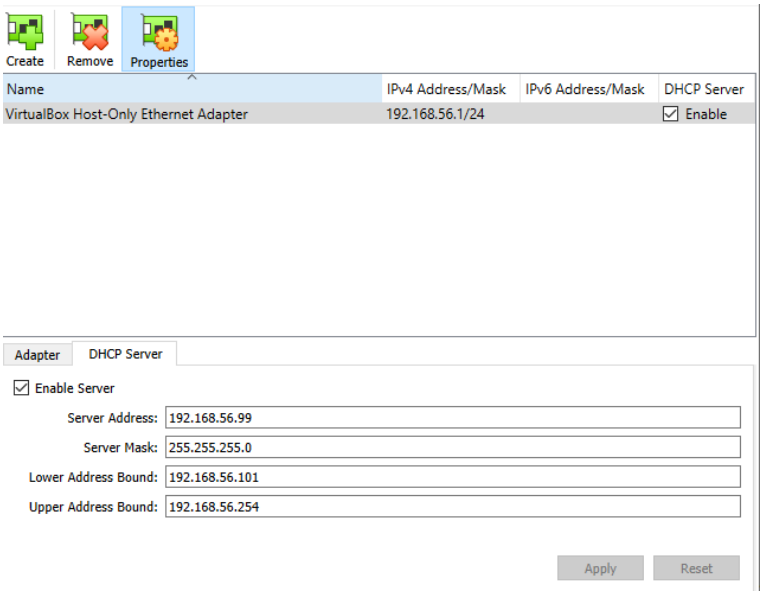

Figure 7: DHCP settings

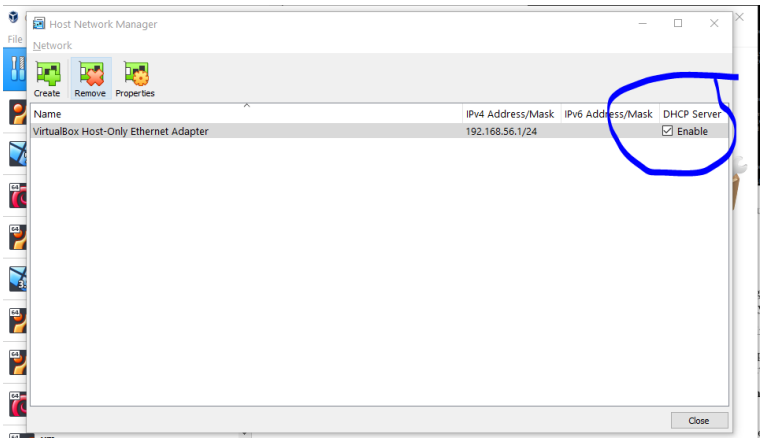

Figure 6: Enable DHCP

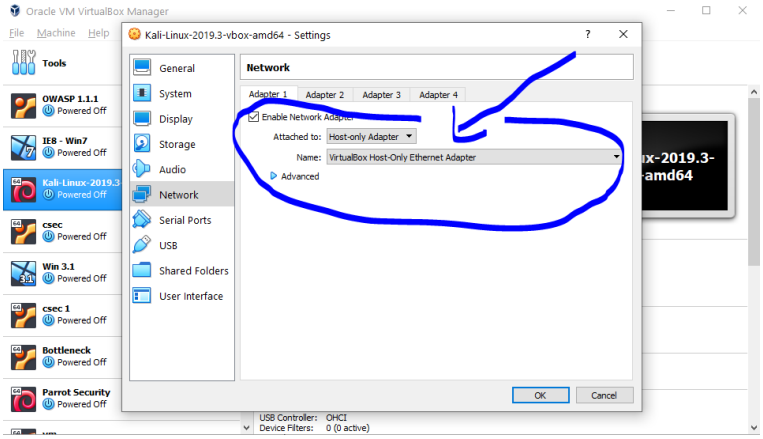

Figure 8: Host Only Adapter Settings

- To check your ip address, in any of those virtual machine devices you open a terminal and type:
  - **ifconfig**
- In Windows you can open a command line Interface by clicking on start and typing cmd.
  - **ipconfig**
- **The step shown in Fig.8 needs to be repeated for all the VMs to ensure that all of them are on the same network.**

3 Test connectivity

- You can test connectivity between machines on the terminal by using **ping** command.
  - To ping the vulnerable machine from kali **ping 192.1268.56.102**
  - To ping the kali machine from the vulnerable machine **ping 192.1268.56.101**
  - To ping the windwows machine from the kali machine **ping 192.1268.56.103**
    - If the ping to windows does not work, disable the firewall on windows control panel.
- when we selected host only network we created a private network between our VMs that is completely isolated from the external world.

4 Update Kali Linux and install app

For our labs, we will need a browser attachment called **owasp mantra**

- Kali linux needs to be on the internet (NAT). Check (Fig3). You will only need to connect KALI VM to the internet.
- THE OTHER MACHINES SHOULD NOT BE CONNECTED TO THE INTERNET
- **Update repositories for Linux** by typing
  - sudo apt-get update
- **Install OWASP mantra** and dependencies by typing
  - sudo apt-get install owasp-mantra-ff
  - sudo apt-get isntall xterm

Access OWASP Mantra

- To run OWASP Mantra you need to type **sudo owasp-mantra-ff**
- We will be using OWASP mantra at a later stage in the term

IF update fails

- **"check the update Kali error" section at the end of the document (6)**

5 Getting to know web applications on a vulnerable VM

OWASP-bwa contains many web applications, intentionally made vulnerable to the most common attacks. Some of them are focused on the practice of some specific technique while others try to replicate real-world applications that happen to have vulnerabilities.

1. With OWASP vm running, open your Kali Linux host's web browser and go to http://192.168.56.102. You will see a list of all applications the server contains.
2. For **Damn vulnerable Web Application**. Use username **admin** and password **admin**. We can see a menu on the left; this menu contains links to all the vulnerabilities that we can practice in this application: Brute Force, Command Execution, SQL Injection, and so on.
3. **OWASP WebGoat.NET**. This is a .NET application where we will be able to practice file and code injection attacks, cross-site scripting, and encryption vulnerabilities. It also has a WebGoat Coins Customer Portal that simulates a shopping application and can be used to practice not only the exploitation of vulnerabilities but also their identification

The applications in the home page are organized in the following six groups:

- **Training applications:** These are the ones that have sections dedicated to practice-specific vulnerabilities or attack techniques; some of them include tutorials, explanations, or other kind of guidance.
- **Realistic, intentionally vulnerable applications:** Applications that act as real-world applications (stores, blogs, and social networks) and are intentionally left vulnerable by their developers for the sake of training.
- **Old (vulnerable) versions of real applications:** Old versions of real applications, such as WordPress and Joomla are known to have exploitable vulnerabilities; these are useful to test our vulnerability identification skills.
- **Applications for testing tools:** The applications in this group can be used as a benchmark for automated vulnerability scanners.
- **Demonstration pages / small applications:** These are small applications that have only one or a few vulnerabilities, for demonstration purposes only. OWASP demonstration application: OWASP AppSensor is an interesting application, it simulates a social network and could have some vulnerabilities in it. But it will log any attack attempts, which is useful when trying to learn; for example, how to bypass some security devices such as a web application firewall.

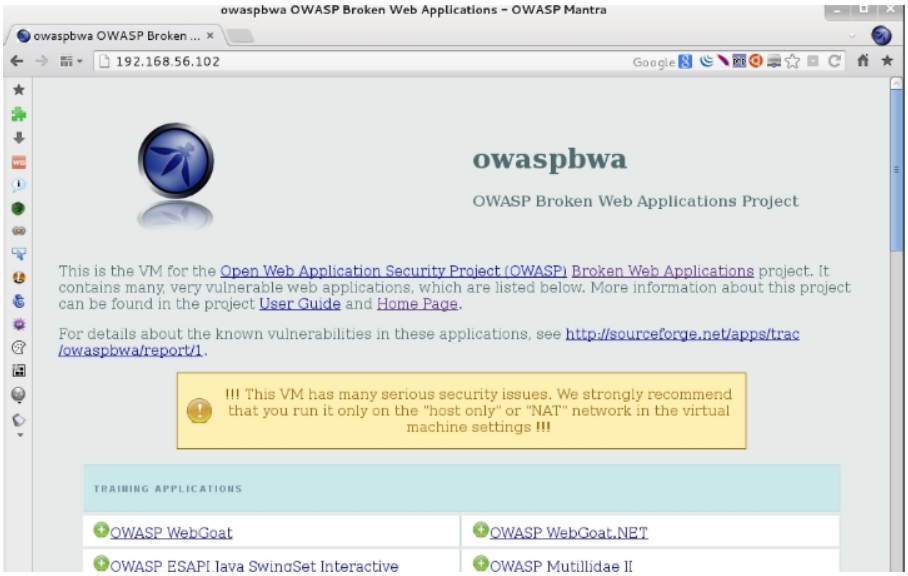

Figure 9: OWASP Web Interface

6 Problems that you can possibly face

We faced some problems in the class. I want to avoid having those problems every week as it will take away from our lab time.

1. on vmware, make sure your virtual network is connected as in (virtually connected)
2. on Vbox, you need to create a virtual box network interface first
3. If you cannot see any virtual interface on your computer and you are using vmware type **sudo systemctl restart vmware**.
4. On Kali Linux, changes you made in your network interface were not taking effects until the network manager service was restarted by using **sudo service network-manager restart**
5. In some machines, you need to change the USB setting for the VM to USB 1.1 as shown in fig below. This applies for any machines that throw the USB error.

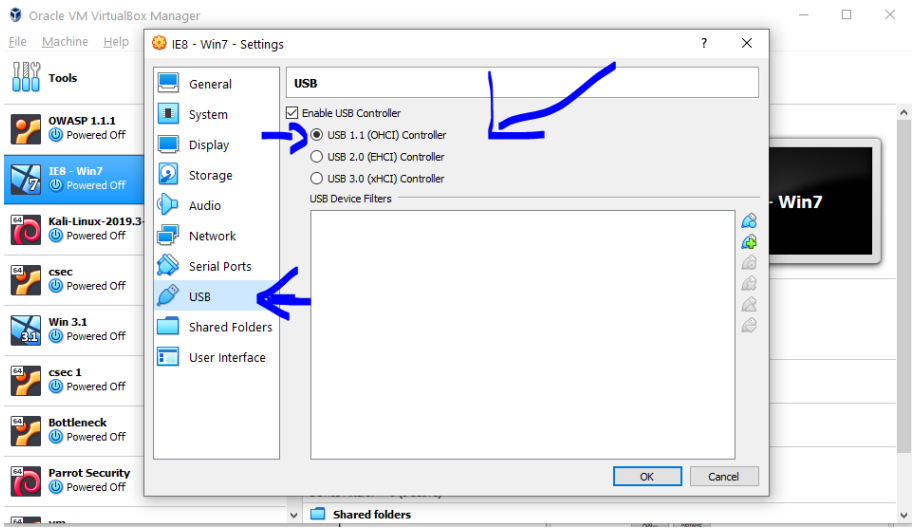

Figure 10: USB error