



## THE LAB

We will use a program called Virtual Box to setup our pentesting lab. Virtual Box allows us to create virtual machines inside our current OS. We will create the following machines in our lab (for now):

1. Attacker machine – Kali Linux
2. Victim 1 – Metasploitable.
3. Victim 2 – Windows.

First of all download and install Virtual Box from <https://www.virtualbox.org/wiki/Downloads>



## THE LAB – KALI LINUX

Kali Linux is a linux distribution based on Debian, Kali is especially made for pentesters, it contains most of the tools that we need, installed and configured correctly.

This is going to be the attacker machine.

1. You can download Kali Pre Built machines from the following link:

<https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/>

2. Or use the iso image:

<https://www.kali.org/downloads/>



KALI LINUX™

“the quieter you become, the more you are able to hear”



## THE LAB – INSTALLING WINDOWS

We will also install a normal windows machine as a victim, we will be running our attacks against this machine.

Microsoft has released a number of windows virtual machines that can be downloaded from the following link (**make sure you select windows 10 stable and virtual box**)

<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>



## THE LAB – CONFIGURING KALI LINUX

1. Update the source list  
    > `apt-get update`
2. Install terminator  
    > `apt-get install terminator`
3. Install needed updates  
    > `apt-get upgrade`

