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 – Windows.
3. Victim 2 – Ubuntu Linux.

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/

The Lab – Installing Metasploitable

Metasploitable is a vulnerable linux distro, this OS contains a number of vulnerabilities, it is designed for pentesters to try and hack it.

This is going to be one of the victims that we will try to hack.

You can download Metasploitable from the following link:

https://information.rapid7.com/metasploitable-download.html

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 — Snapshots

- Snapshots allow you to save the state of a virtual machine.
- Can be used as bookmarks to go back and forward to different configurations.
- Store stable state, updated state ….etc.