# ITRI625 - Computer Security II

# Metasploit Project Documentation

Affaan Muhammad - 33016763

Joshua Esterhuizen - 30285976

Due: October, 19th 2021

# Contents

# Section 1

# Installation and Setup

## 1.1 Project files

The project files can be found on the following GitHub link:
https://github.com/AM-ops/MetasploitProject/

This was our main code repository. We both have been updating the code as we went along and added details and bug fixes to the project.

To copy the code to your own machine, follow the following steps:

1. Make sure Git is installed. If not it can be downloaded from here:
   https://git-scm.com/
2. Create an empty directory where the code can be copied to
3. Run the following command:

```
git clone https://github.com/AM-ops/MetasploitProject.git
```

## 1.2 Virtual Environments

There are multiple advantages of using virtual environments when testing for vulnerabilities and exploits in computer security. The primary reason being we create a layer of separation and abstraction between our host machine and our virtual environments. This 'sand-boxing' allows for analysis of threats in a contained environment.

### 1.2.1 VirtualBox

We made use of Oracle's VirtualBox software for the virtualisation. This can be downloaded from the following link: https://www.virtualbox.org/wiki/Downloads
Below is a screenshot of the site. We also chose the `Windows hosts` option to download. Other hosts can also be utilised such as Linux hosts, or OS X hosts.


Figure 1.1: Oracle's VirtualBox Download Page

Once the file has been downloaded, open it. Thereafter follow the default prompts of the installation. Below are some figures illustrating this.

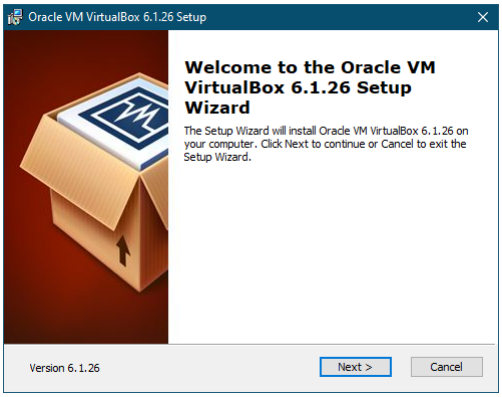


Figure 1.2: Screen 1

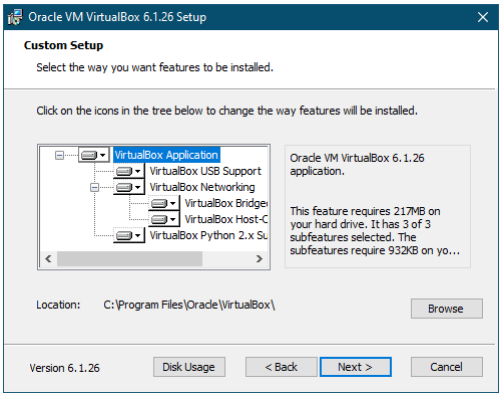


Figure 1.3: Screen 2

Click on **Next** for both above screens

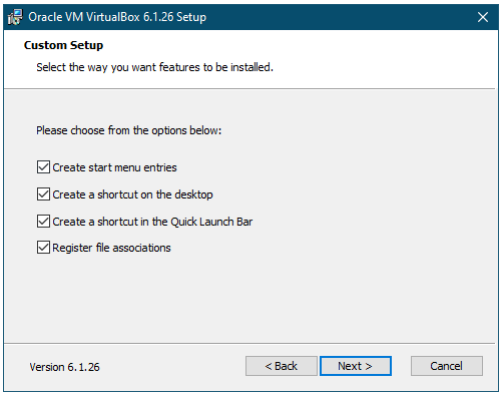


Figure 1.4: Screen 3

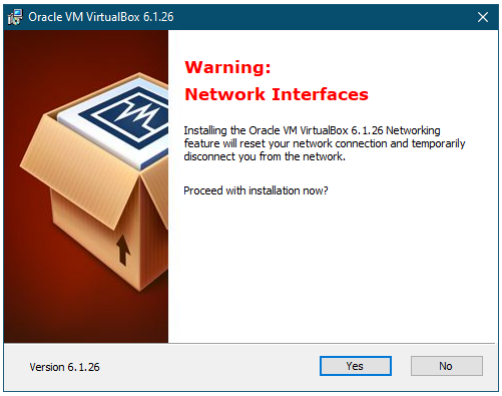


Figure 1.5: Screen 4

Click on **Next** for both of the above screens

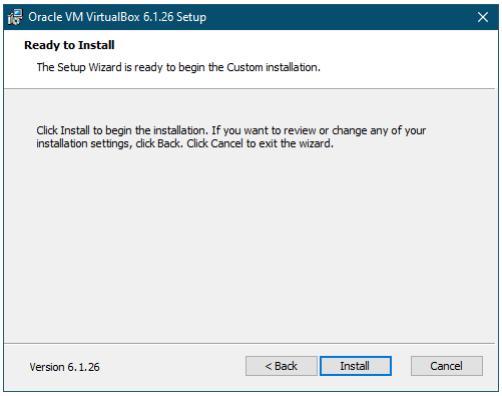


Figure 1.6: Screen 5


Figure 1.7: Screen 6

Click on **Next** and then **Finish**

## 1.3 Kali Linux

The next step is to acquire an Operating System for carrying out our Penetration Testing. For this purpose we utilised `Kali Linux`. The main site for this OS is: https://www.kali.org/

According to them they quote the following:

> "**The Most Advanced Penetration Testing Distribution**
> *Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.*"

The main site looks as follows

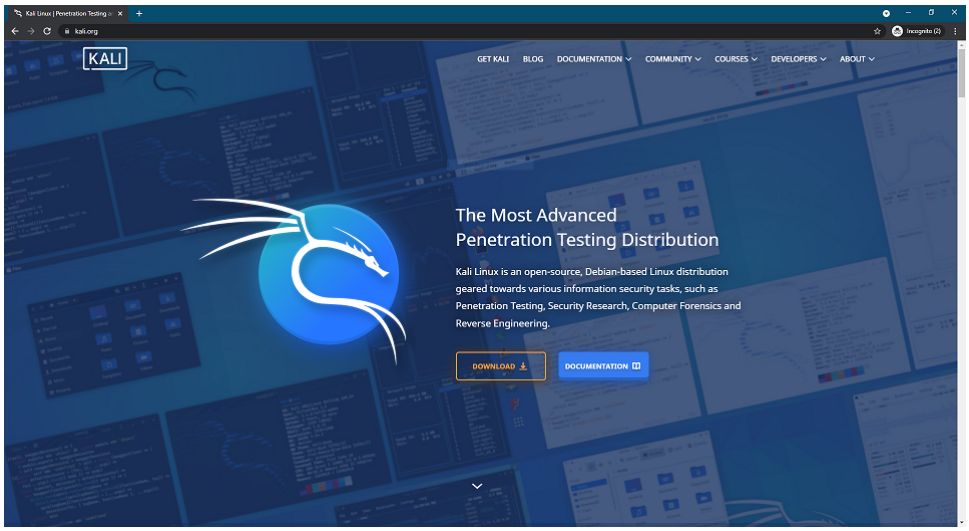


Figure 1.8: Kali Linux's Homepage

Click on the `Download` button to see the different options available. Below the options are shown.

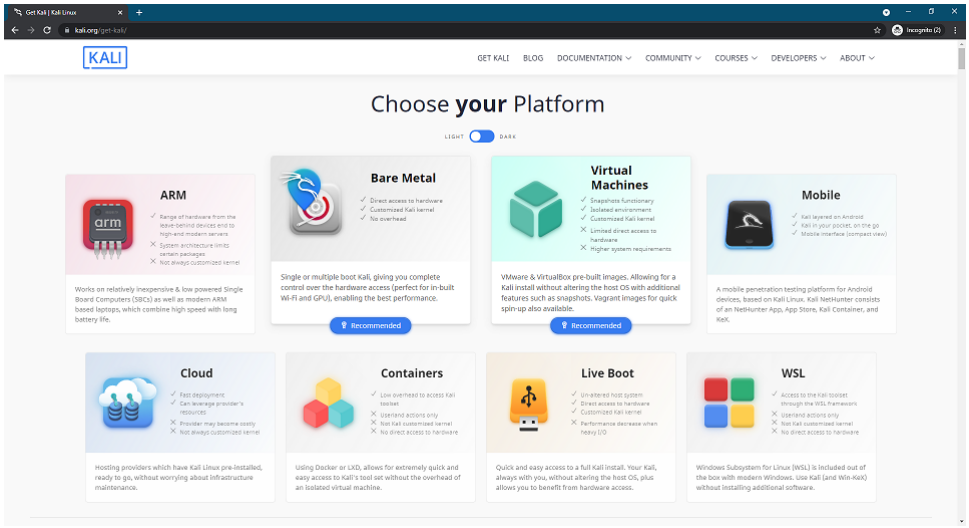


Figure 1.9: Kali Linux's different download options

The option we chose is the `Virtual Machines` one. Thereafter you are presented with the two options available.

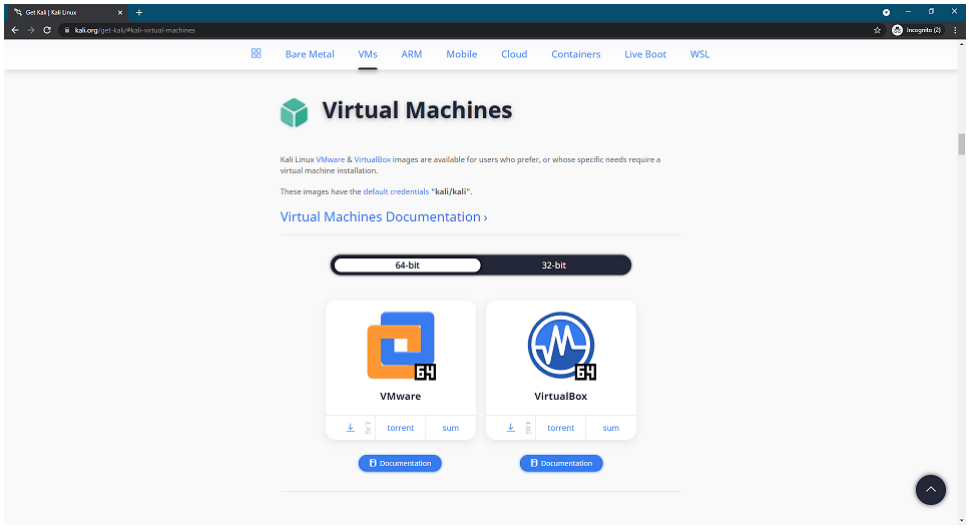


Figure 1.10: The 2 options for Virtual Machines

Select the `VirtualBox` option and click on the direct download link.

After the download is completed it is time to set up Kali Linux inside VirtualBox. https://citizenlab.ca/