

Cybersecurity Roadshow - Hands on hacking / The Cyber Kill Chain

Installation Guide

Preface

This guide provides necessary resources for installing Oracle VM VirtualBox and setting up a working guest environment/OS so that a user can complete the provided material. This guest OS will be used as the attacking machine. A virtual instance of Kali Linux has been prepared with all necessary material installed. The image can be downloaded on the link here¹.

Suppose, for some reason, another instance of Kali Linux is preferred. In that case, the Github repository must be cloned, and Docker Compose must be installed on the host to spawn the target application.

Oracle VM VirtualBox installation

Initially, VirtualBox must be installed to spawn a guest OS on the host. Installation packages for the corresponding host (Windows, OS X, Linux) can be found here² along with documentation on how to install the Oracle VM VirtualBox Extension Pack, which allows functionality like USB 2.0 and 3.0 passthrough.

Once VirtualBox has been installed, the provided Kali Linux image must be imported. To import the image, choose File, then Import Appliance, and locate the provided .ova file. Complete the import wizard and you should now be able to start the machine.

¹<https://drive.google.com/drive/folders/1SFFJrhQ1VYwgFkGVwAfFTA1W2vYzDXm-?usp=sharing>

²<https://www.virtualbox.org/wiki/Downloads>



Figure 1: Import Appliance in VirtualBox.

Credentials for the provided Kali Linux:

Username: `kali`

Password: `kali`

If another image is preferred, the user must download it and install it similarly, assuming the preferred image is the VirtualBox one.

Note that virtualization must be enabled in the host's BIOS/UEFI for virtual machines to work. If not, one will have to do so, but this guide will not dive into how due to various ways to achieve this.

Docker Compose installation

Docker Compose is already installed and configured in the provided image. An installation guide and general documentation can be found here³ if another image is used.

Application from Github

The application is already downloaded on the provided image. If another instance is used, it is necessary to download the application from the Github page here⁴, and place it on the Desktop.

Build, start and stop the application

In the provided image, the application will start when the machine is booted.

³<https://docs.docker.com/compose/>

⁴<https://github.com/ABreum95/Cyber-Security-Roadshow>

If using another image, to run the application, open a terminal, navigate to the application's folder, **Cyber-Security-Roadshow**, located on the Desktop, and enter the following commands.

```
sudo docker-compose build
```

```
sudo docker-compose up -d
```

Wait a few minutes to let the SQL server start.

To stop the application from running, execute the following command:

```
sudo docker-compose down
```