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.

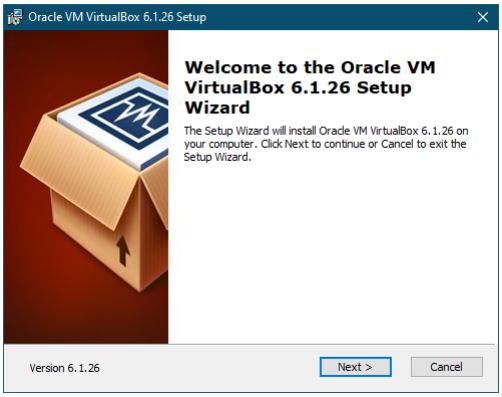


Figure 1.2: Screen 1

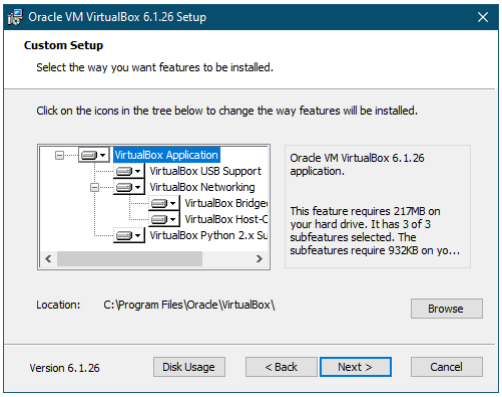


Figure 1.3: Screen 2

Click on **Next** for both above screens

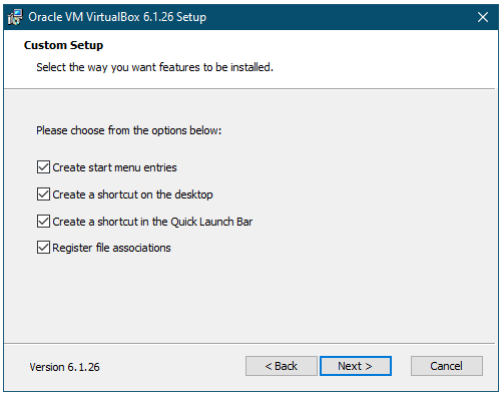


Figure 1.4: Screen 3

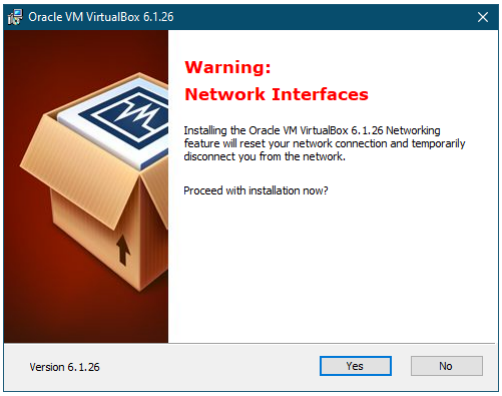


Figure 1.5: Screen 4

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

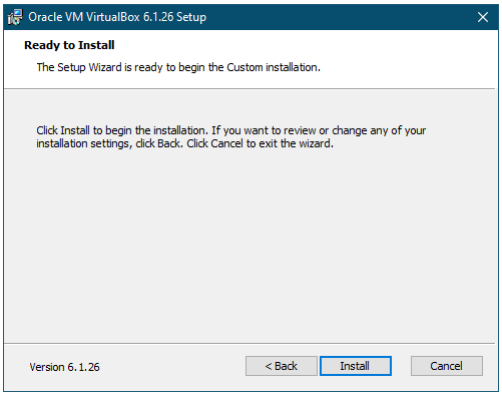


Figure 1.6: Screen 5

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

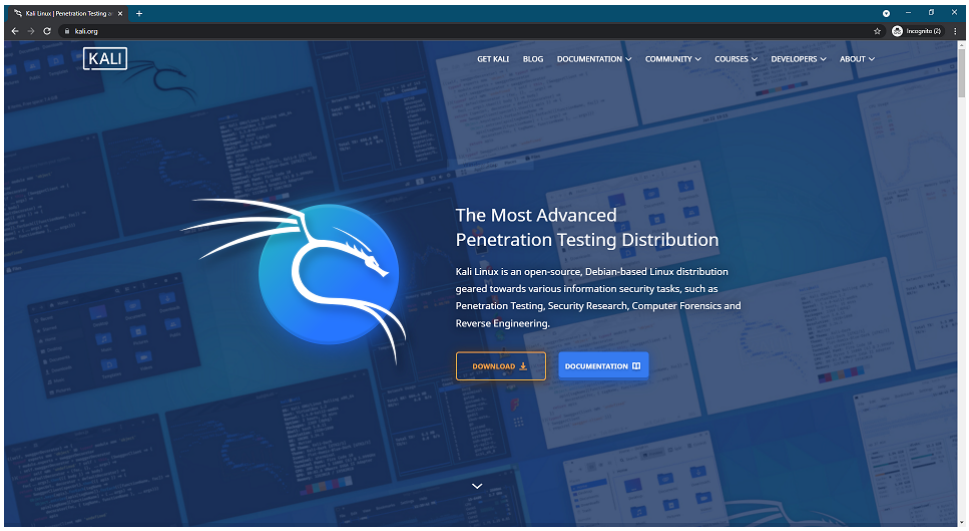


Figure 1.8: Kali Linux's Homepage

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

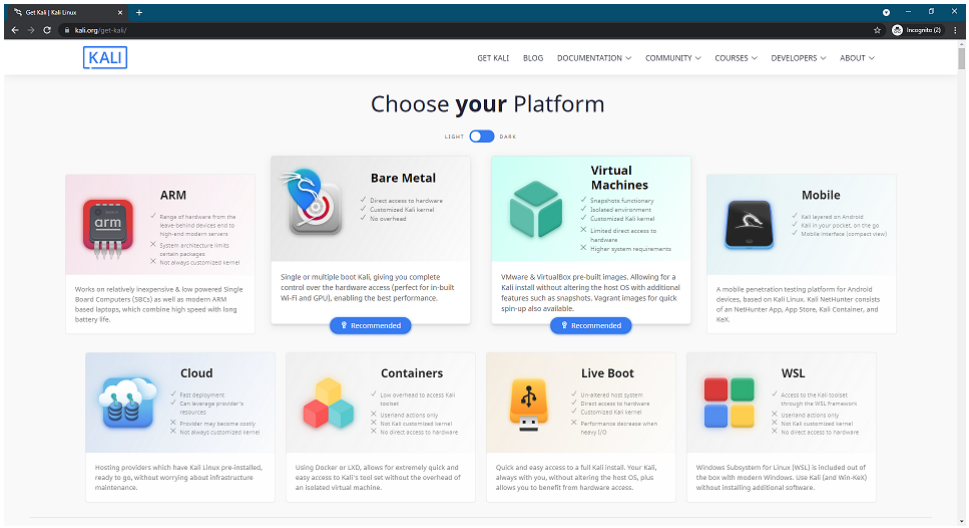


Figure 1.9: Kali Linux's different download options

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

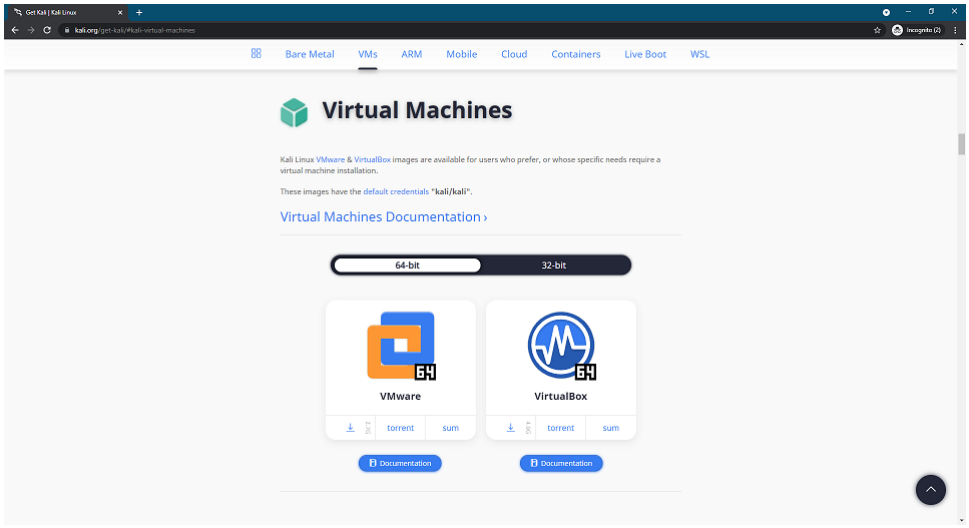


Figure 1.10: The 2 options for Virtual Machines

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. To achieve this open up the file and thereafter change the following settings.

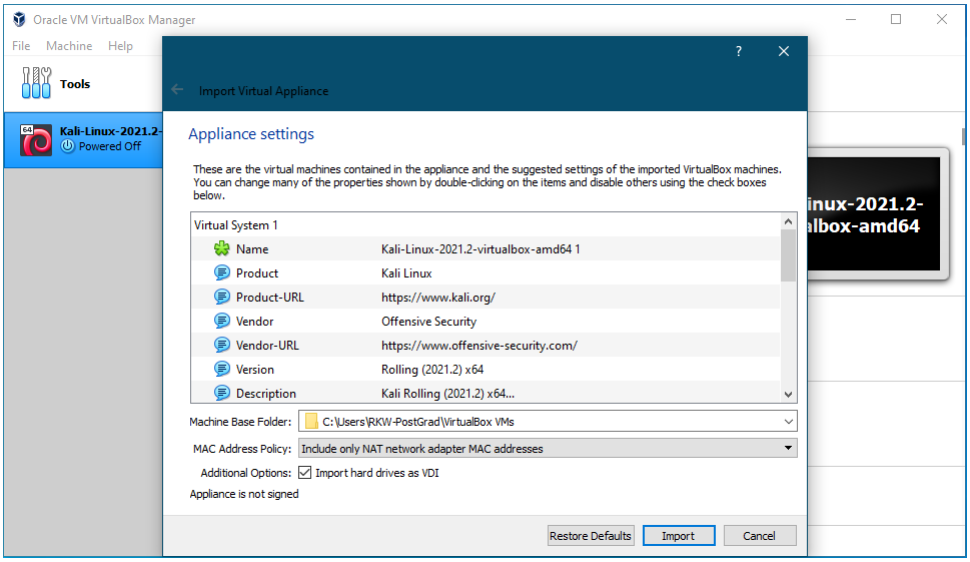


Figure 1.11: The main screen once the file is opened

Click on **Import** thereafter click on **Agree** on the Software Licence Agreement screen. The Kali Linux virtual machine will begin installing. Wait for it to be completed. Depending on the hardware available, it will be done in a few minutes.

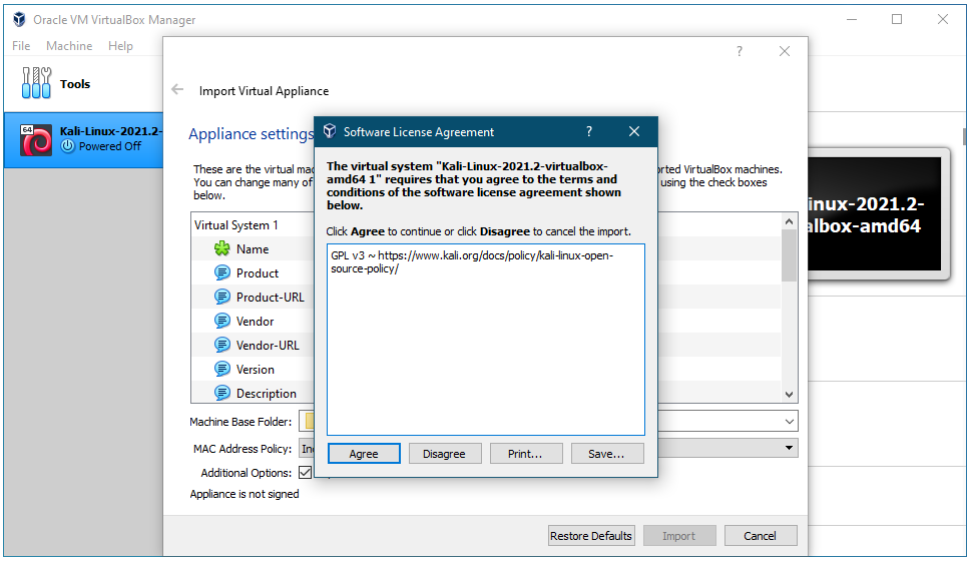


Figure 1.12: Software Licence Agreement screen

Once the installation is completed Oracle's VirtualBox will open to the following main screen. The newly installed Kali Linux is shown on the left of the main screen.

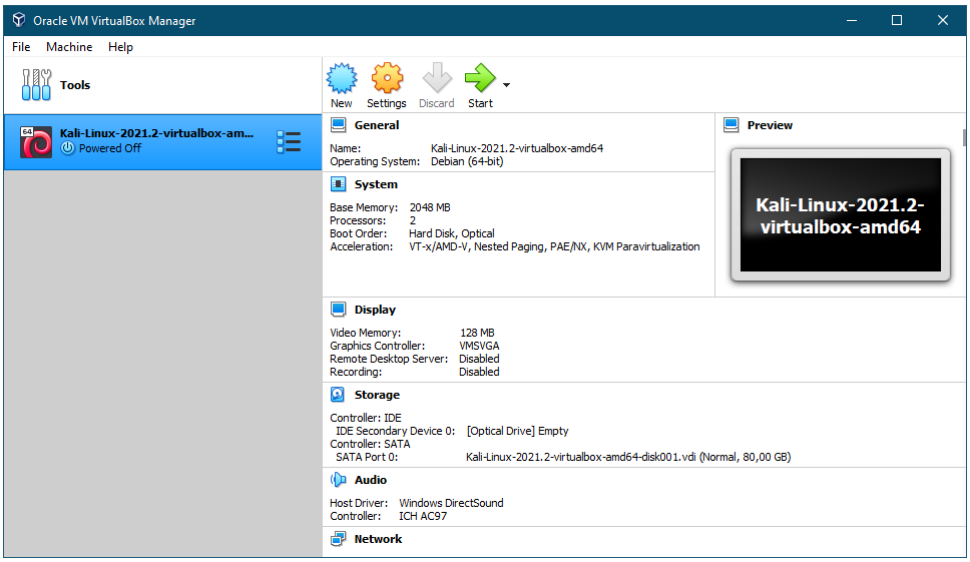


Figure 1.13: VirtualBox's main screen

Before starting up the Kali Linux virtual machine, a few settings have to be changed. Click on the **Settings** icon which is shown by a yellow gear icon. Navigate to **Systems** setting, and thereafter assign the recommended amount of `Base memory` under the `Motherboard` tab.

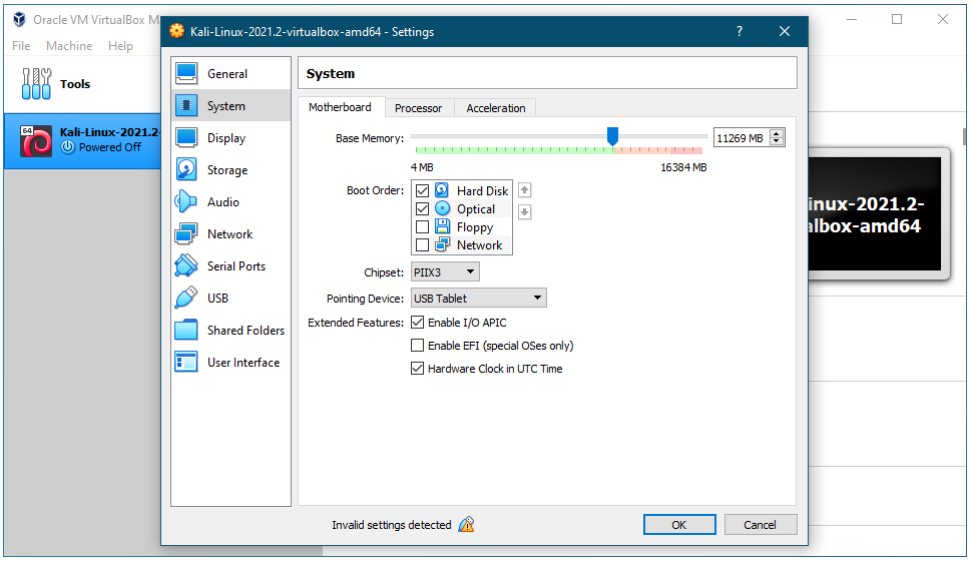


Figure 1.14: Systems settings: Motherboard tab

Under the `Processor` tab assign the recommended amount of `Processor(s)` as well as check the `Enable Nested VT-x/AMD-V` option.

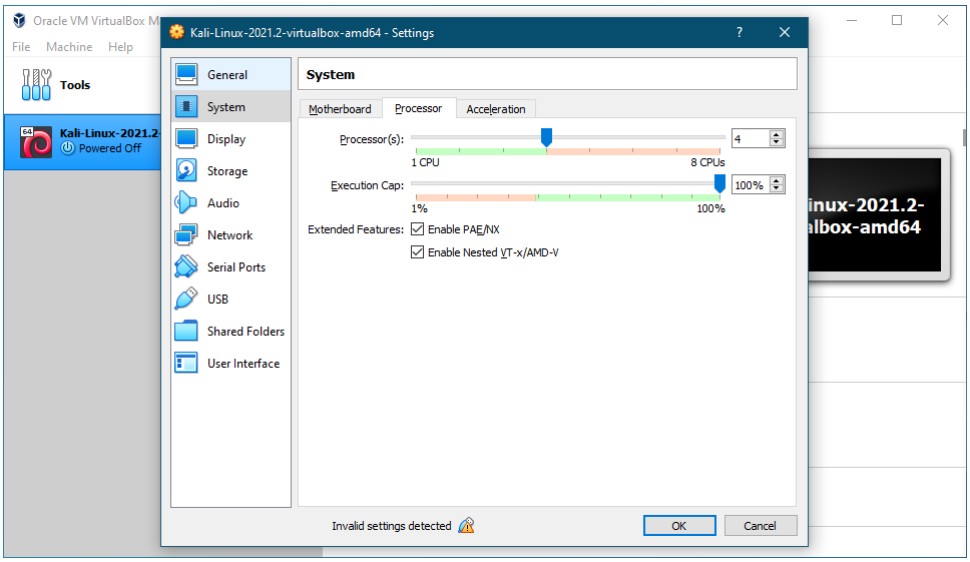


Figure 1.15: Systems settings: Processor tab

If any errors are shown in the Settings for USB, then under the `USB` settings make sure that the `USB 1.1 (OHCI) Controller` option is only selected.

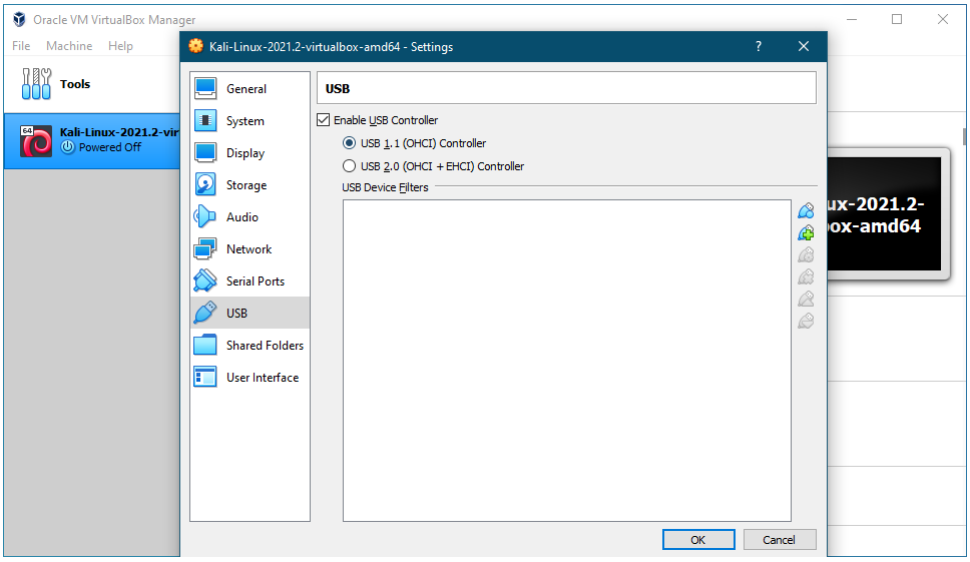


Figure 1.16: USB settings

Click **OK** to save all your settings changes. You should now be able to start up the Kali Linux virtual machine. Click on the `Start` icon which is shown by a green arrow. Once the virtual machine starts up you will be taken to the login screen. enter the following for the username and password:

- Username: `kali`
- Password: `kali`

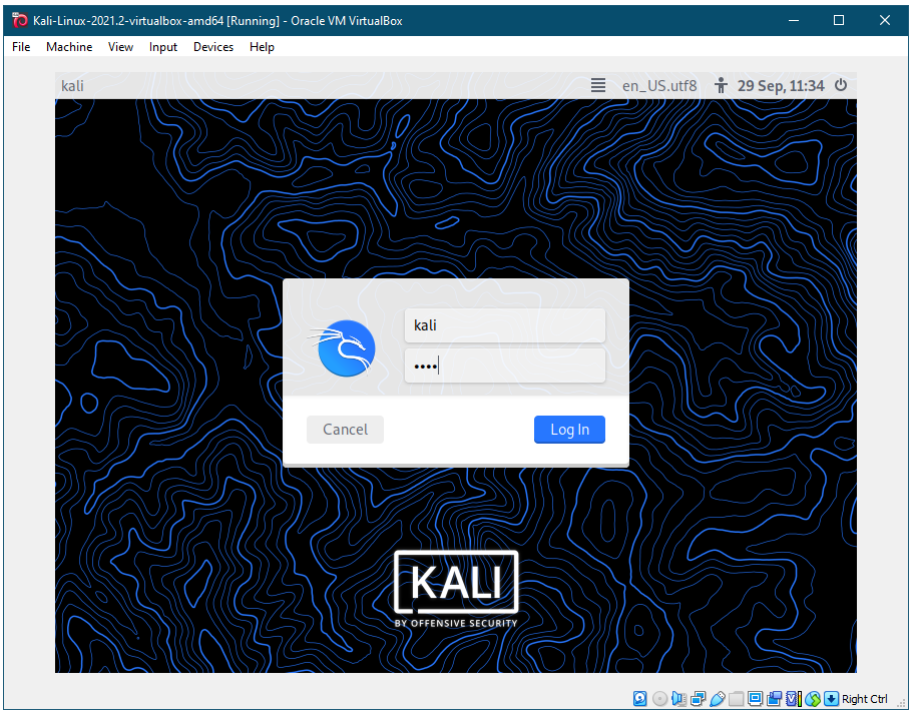


Figure 1.17: Kali Linux login screen

Once you are successful in logging in, you will be greeted by the following splash screen of the Desktop.

Figure 1.18: Kali Linux's Desktop

1.4 Metasploit on Kali Linux

1.4.1 Installation for the command line

To install Metasploit on Kali Linux the following has to be done. Go to the following GitHub url: https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers Copy the following command:

```
curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/
templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \
  chmod 755 msfinstall && \
  ./msfinstall
```

Open up the terminal and paste the command copied. Thereafter press **Enter** to run it. If a password is required, Enter: `kali`

Once the package has been installed you will see the screen as shown in Figure 1.21

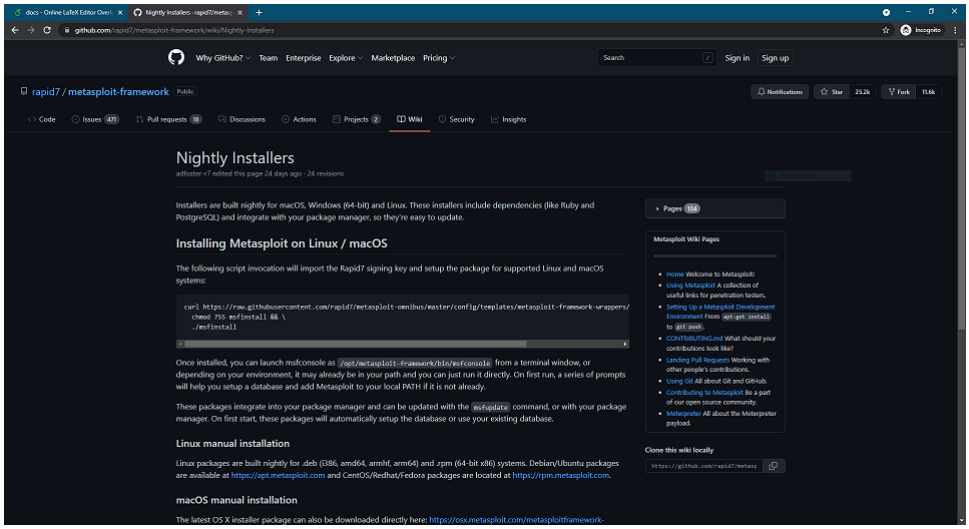


Figure 1.19: Metasploit Framework's GitHub page

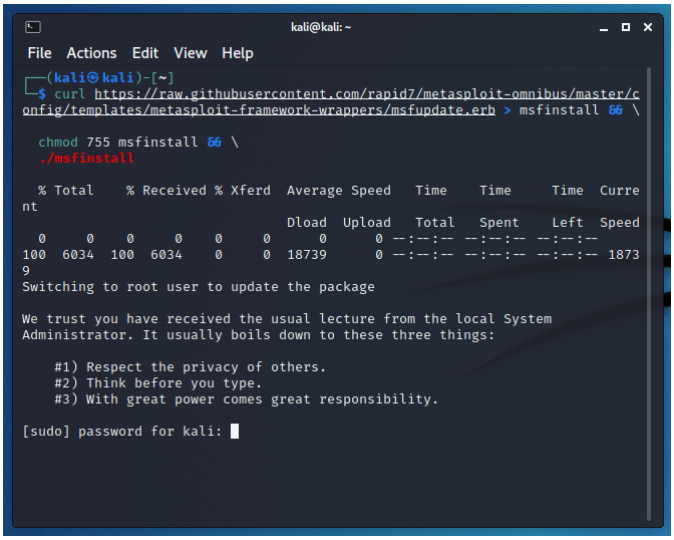


Figure 1.20: Terminal asks for root access

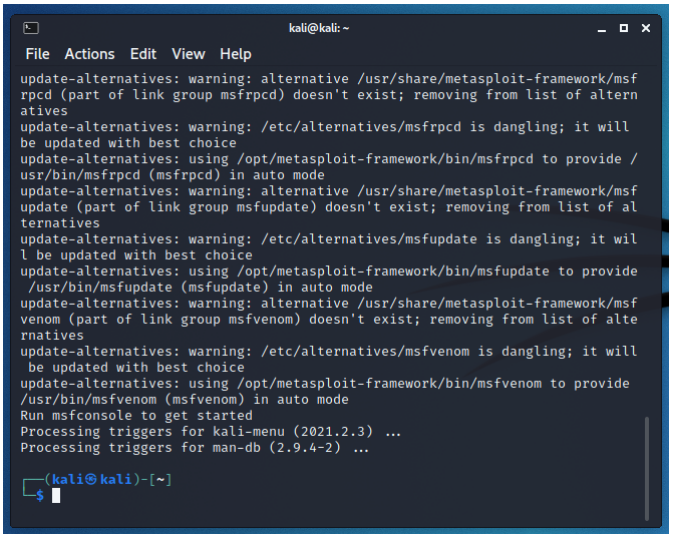


Figure 1.21: Terminal completed installing package

1.4.2 Graphical User Interface (GUI) installation

To install the Graphical User Interface (GUI) go to the following GitHub url: https://github.com/scriptjunkie/msfgui

Thereafter run the following command in the terminal (Preferably change the directory to the Desktop beforehand):

```
cd ~/Desktop
git clone https://github.com/scriptjunkie/msfgui.git
```

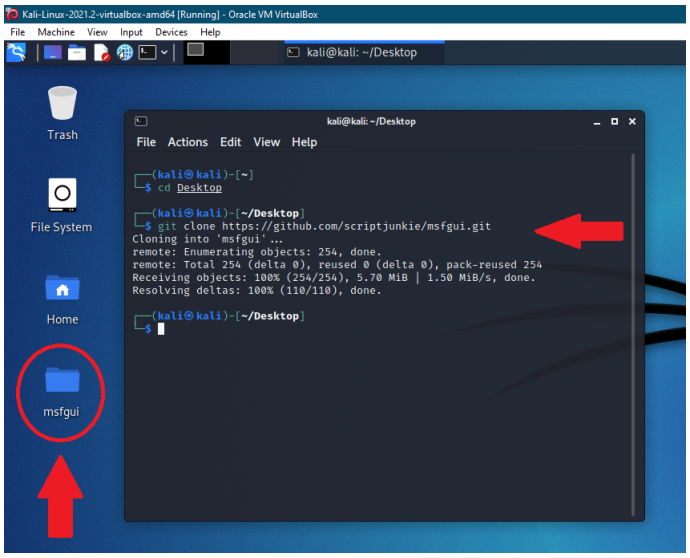


Figure 1.22: GUI folder added to the Desktop

A directory titled `msfgui` will now to added to your Desktop. To run the GUI the following steps have to be carried out.
Firstly change directories to the following: `/opt/metasploit-framework/bin`. This can be done by running the command below in the terminal.

```
cd /opt/metasploit-framework/bin
```

Thereafter run the `msfconsole` shell script. This can be done by running the command below.

```
sudo ./msfconsole
```

If you are prompted for a root password, Enter: `kali`. Thereafter, If you are prompted with the following: *"Would you like to use and setup a new database (recommended)?"*, Type **n** or **no** and press **Enter**.

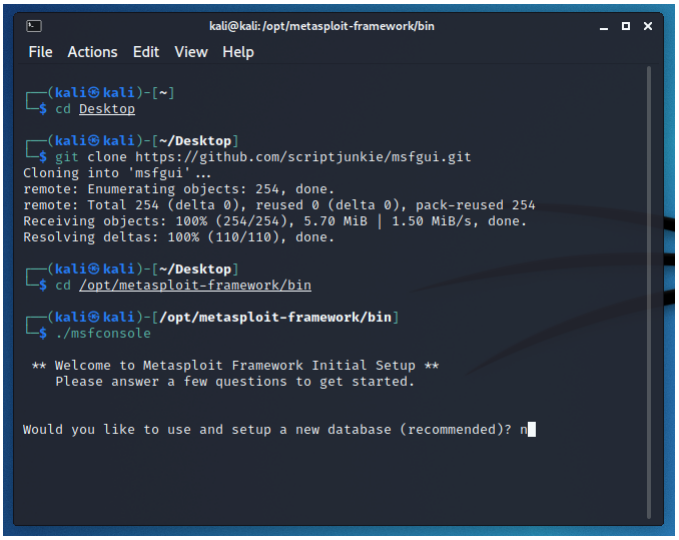


Figure 1.23: Type 'n' for No

Thereafter once ever thing is completed you should see that the terminal now has changed its prompt to the following.

```
msf6 > _
```

This is shown in the picture below. This means that the Metasploit Framework has started up its service in the terminal. With this being done we can now move on to the next step of running the Graphical User Interface (GUI). Firstly you will have to open up a new terminal and change directories to the Desktop. So we can access the directory that was recently created i.e. `msfgui`. The commands are shown after Figure 1.24

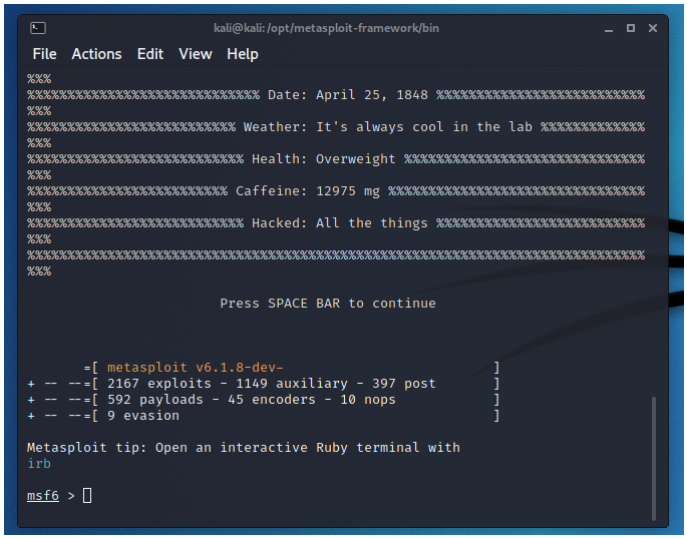


Figure 1.24: Type 'n' for No

```
cd ~/Desktop/msfgui
```

Thereafter run the `msfgui` shell script. This can be done by running the command below.

```
./msfgui
```

Make sure the other terminal that is running the Metasploit command line is also running when the above mentioned command is run. If you are shown the prompt below. Click on **Yes**.

Thereafter another window will pop up. Let it automatically make a choice. If it does not close, then click on the option `Start new msfrpcd` as shown in the figure below.

The Metasploit Framework Grahphical User Interface (GUI) will now be up and running. This is shown in the figure below.

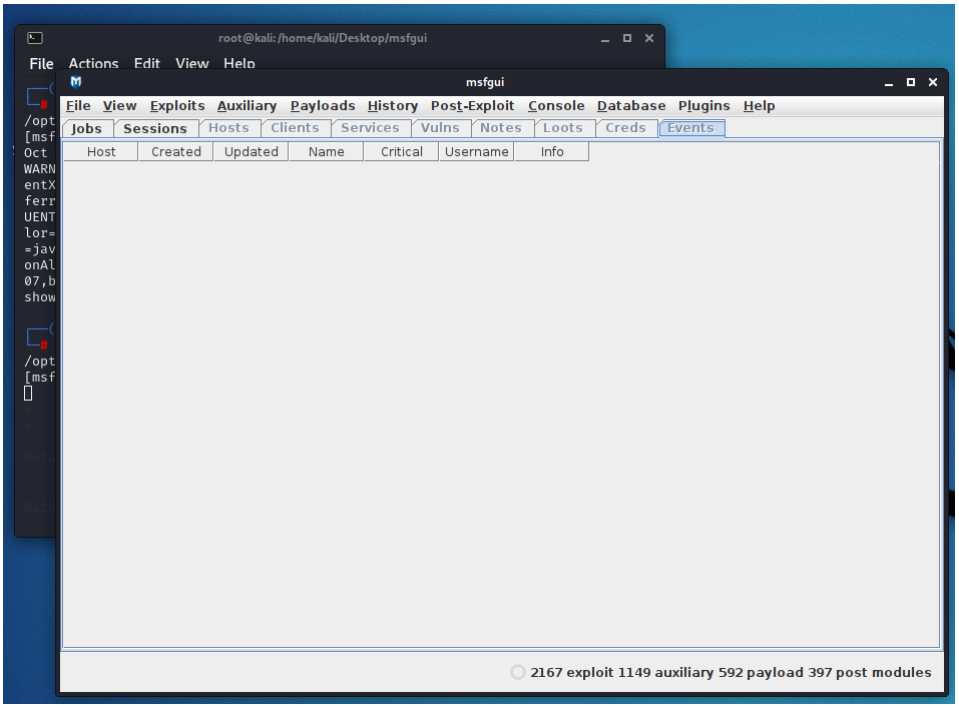


Figure 1.25: The main screen for the Metasploit Framework GUI

1.5 Android Emulator installation

For the first scenario covered in Section 2 we will utilise an Emulator to virtualise an Android phone. This is keeping in line with the topic of virtualisation mentioned in Section 1.2. To emulate such a device you will need the Android Software Development Kit (SDK). This can be downloaded from the following url: `https://developer.android.com/studio`. Below is a screenshot of this page.

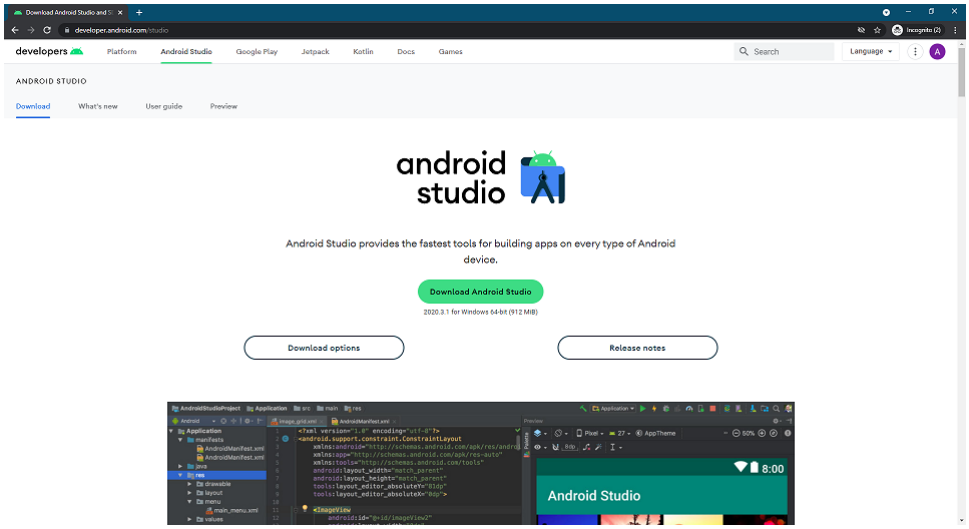


Figure 1.26: Homepage of Android Studio

Therefore open up the link in the browser of Kali Linux and click on button **Download Android Studio**. Thereafter Agree to the Terms and Conditions and click on the **Download Android Studio** button once again.

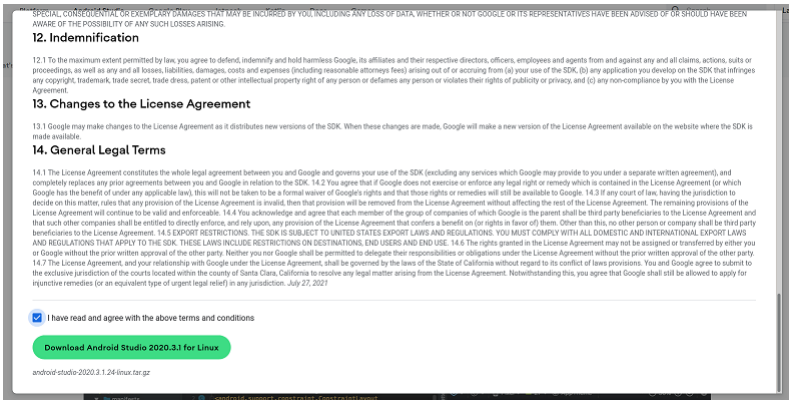


Figure 1.27: Agree to the terms and conditions

After the file has been downloaded you will see it is a `tar.gz` file. You can extract it to the Desktop either using the command line or the File Explorer. Below both options are shown. Run the following command in a terminal where the file was downloaded.

```
tar -xf filename.tar.gz -C /home/kali/Desktop
```

The figure below shows a folder named `android-studio` created on the Desktop.

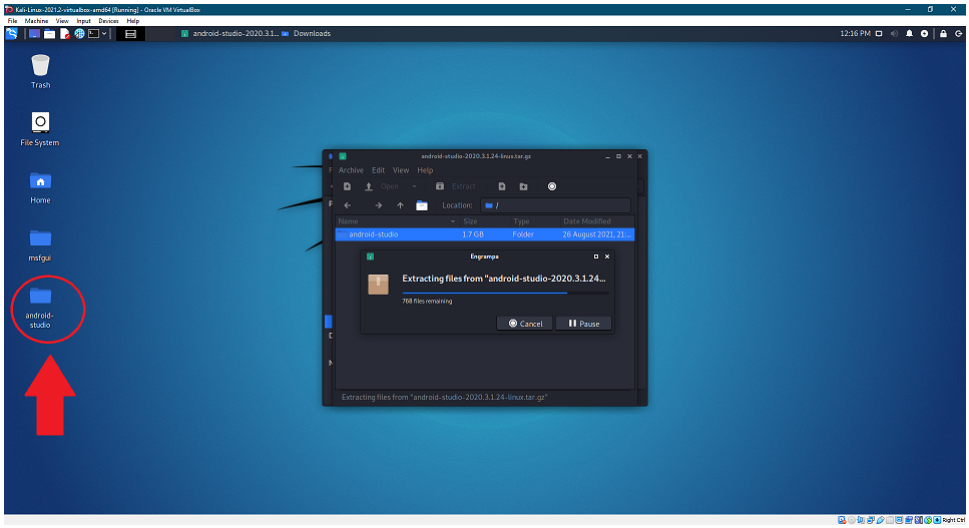


Figure 1.28: File extracted with the File Explorer

We can now start up Android Studio and thereafter create an Android phone emulator. You will have to run the `studio` shell script inside the Android Studio folder. This can be done by running the commands below.

```
cd ~/Desktop/android-studio
```

Thereafter,

```
./studio
```

You will be prompted with `Import Android Studio Settings`. Choose the **Do not import settings** and click **Ok**.

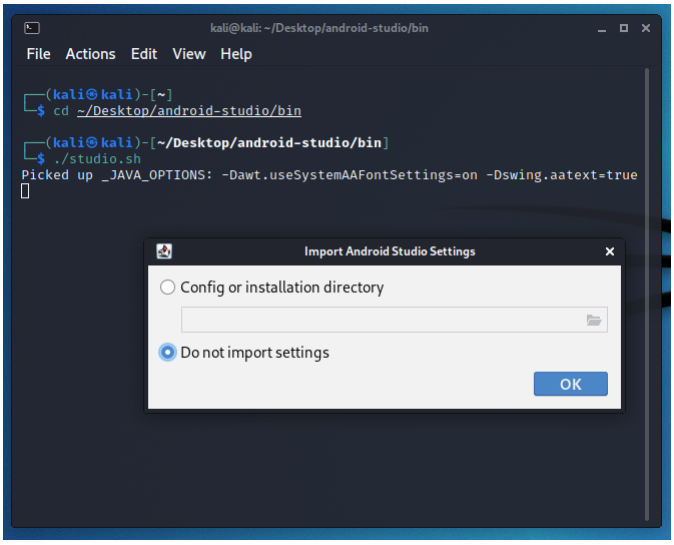


Figure 1.29: Do not import settings

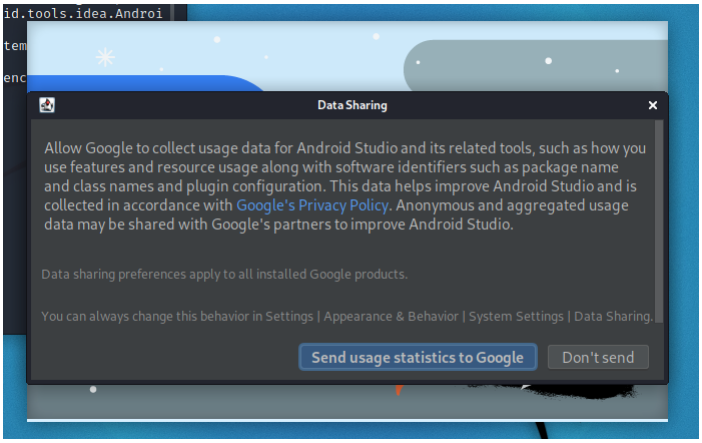
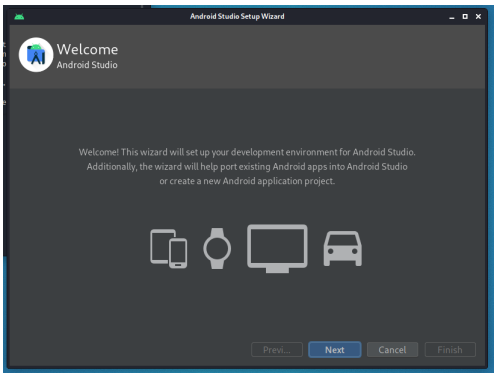
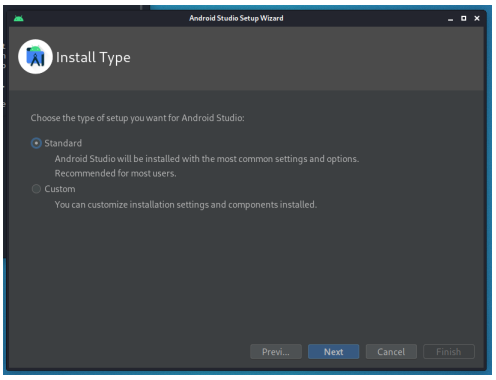


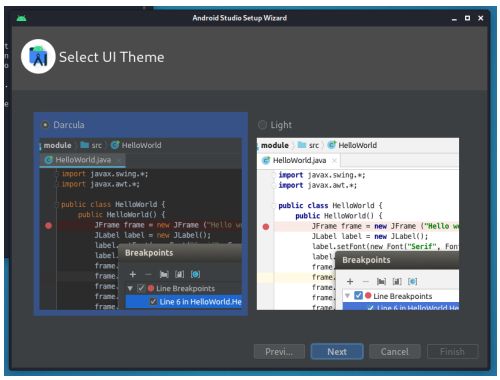
Figure 1.30: Data Sharing screen

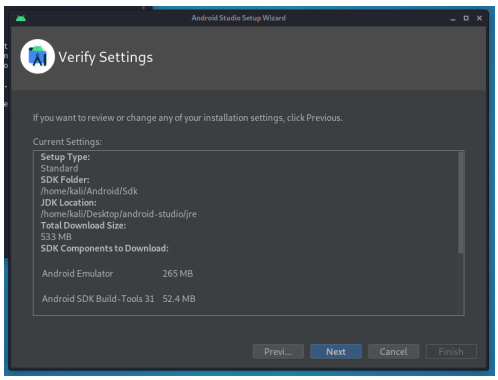
Choose any option for the Data Sharing screen





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





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

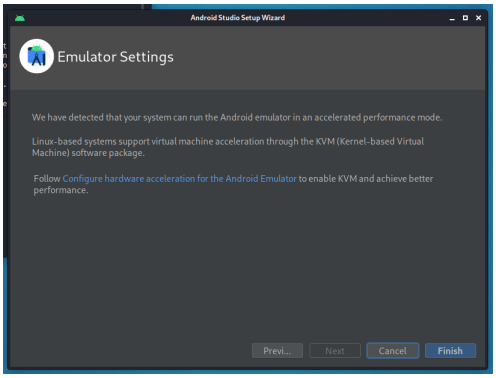
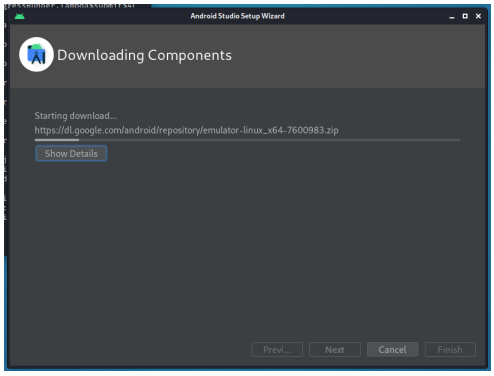
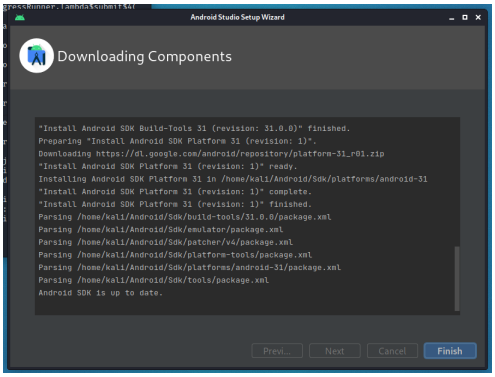


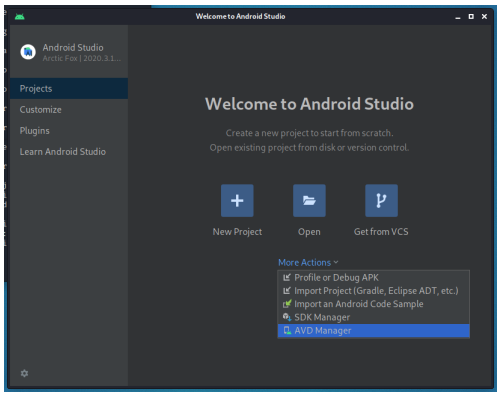
Figure 1.31: Final Screen

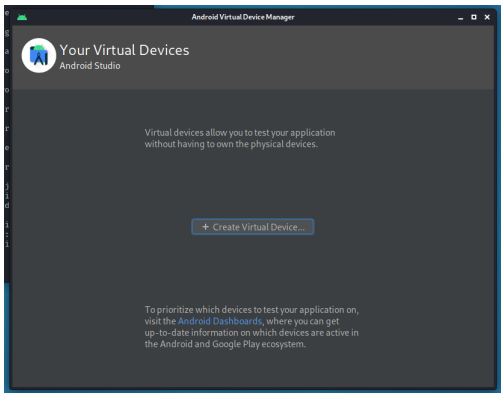
Click on **Finish**. Thereafter you will see that the Components will begin downloading as seen in the figure below.



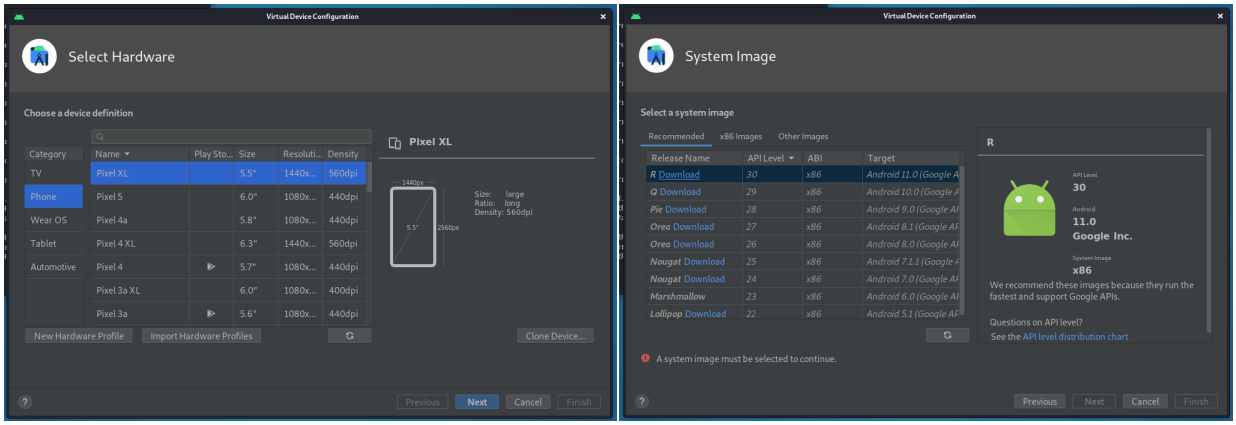


Click on **Finish** after everything is completed. Thereafter you will see the `Welcome to Android Studio` screen.





Click on **More actions** and then select the **AVD Manager** option. You will be lead to the `Android Virtual Device Manager` screen. Click on the **+ Create Virtual Device...** option.



You will have to **Select Hardware**, and thereafter the **System Image**. For the purposes of this project the following specifications were utilised:

- *Hardware*: Pixel 3a
- *System Image*:
  - *Release name*: R
  - *API Level*: 30
  - *Target*: Android 11.0

You will have to download the System Image if it is not installed.

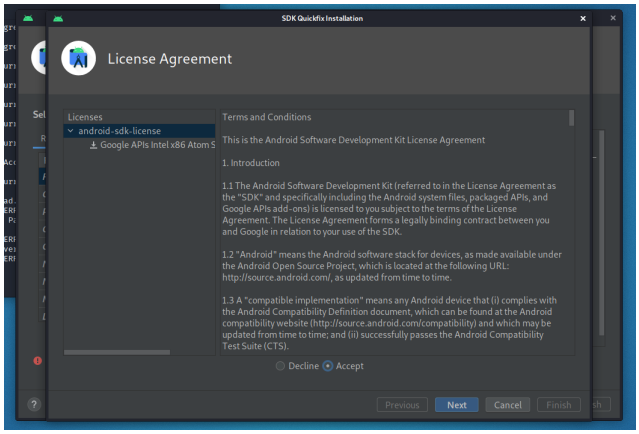
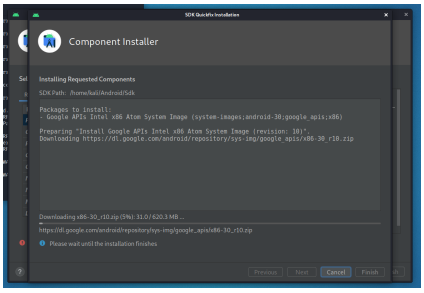
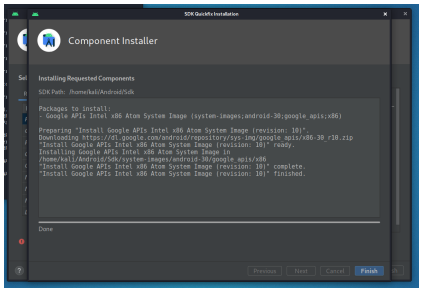


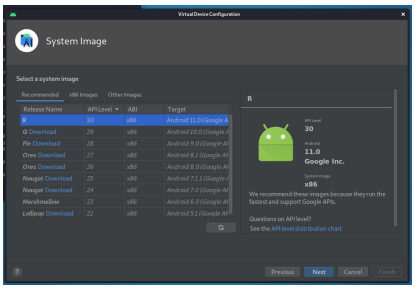
Figure 1.32: License Agreement screen

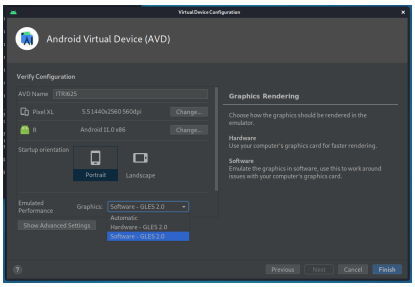
Make sure to agree to the License Agreement before downloading the System Image and then click **Next**.





Click on **Finish** after the install is done.





You should be able to select the newly installed System Image and click on **Next**. Thereafter under the **Emulated Performance -> Graphics** settings. Choose the **Software - GLES 2.0** option if you do not have a GPU on your host machine. If a GPU is present you can select the **Hardware - GLES 2.0** option. Thereafter click on **Finish**. Click on **Finish** after the download is completed.

You should see the following in your **AVD Manager** now as shown below.

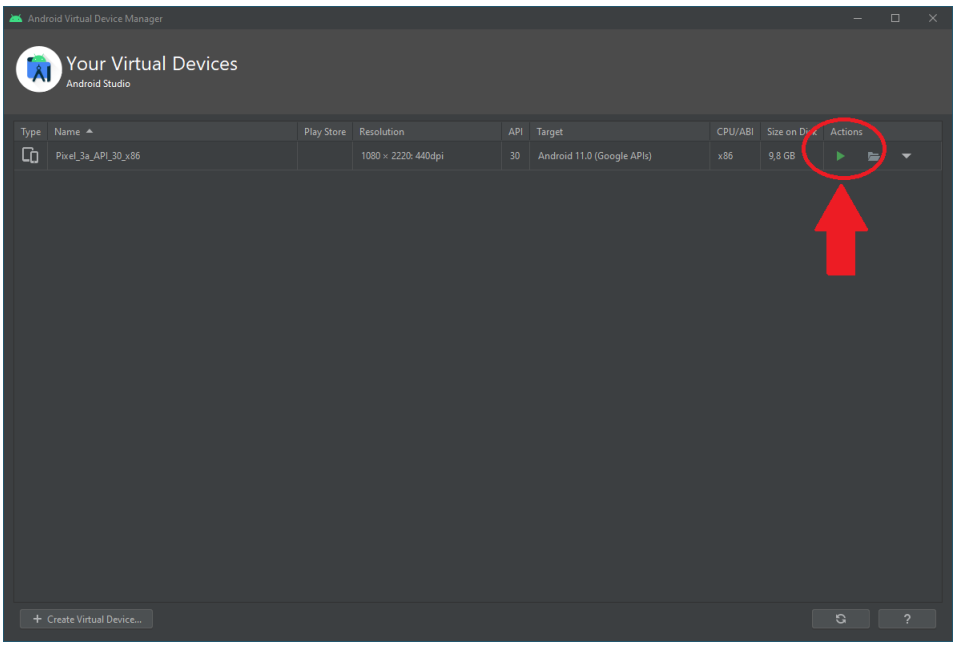


Figure 1.33: Android Emulator listed under the AVD Manager

Click on the green arrow to start up the newly created Android Emulator.

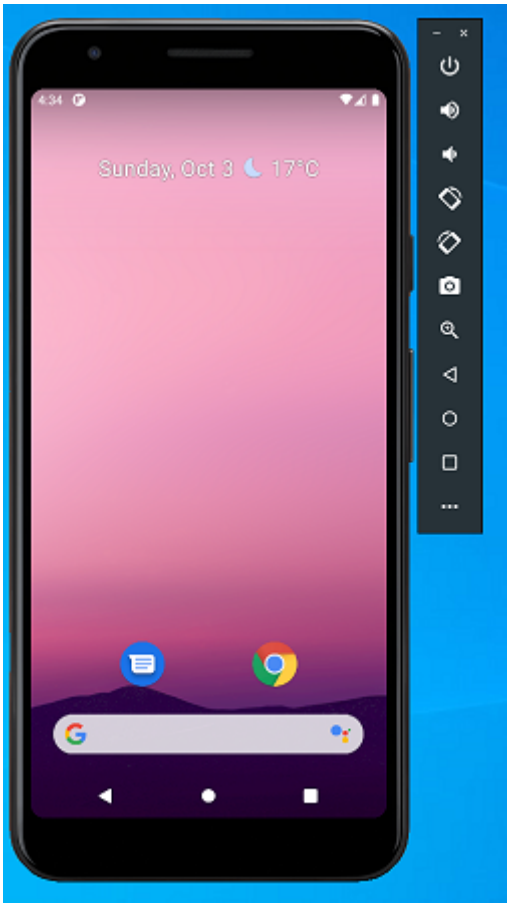


Figure 1.34: The Android Emulator running

Section 2

Scenario 1: Android exploit

Section 3

Scenario 2: Windows exploit

Section 4

Additional readings and miscellaneous information

https://citizenlab.ca/