

ITRI625 - Computer Security II

Metasploit Project Documentation

Affaan Muhammad - 33016763

Joshua Esterhuizen - 30285976

Due: October, 19th 2021

Contents

1	Installation and Setup	2
1.1	Project files	2
1.2	Virtual Environments	2
1.2.1	VirtualBox	3
1.3	Kali Linux	4
1.4	Metasploit on Kali Linux	10

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.

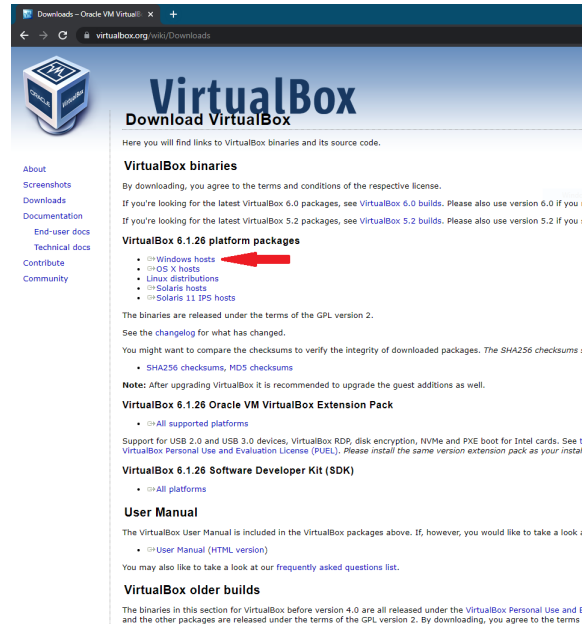


Figure 1.1: Oracle's VirtualBox Download Page

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

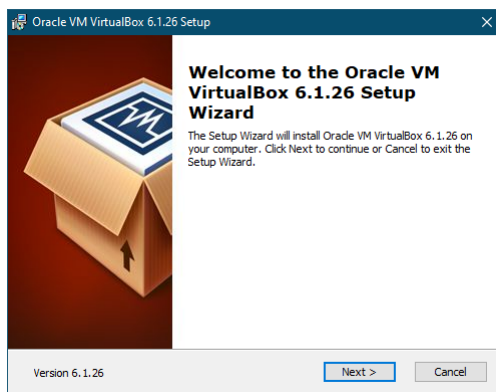


Figure 1.2: Screen 1

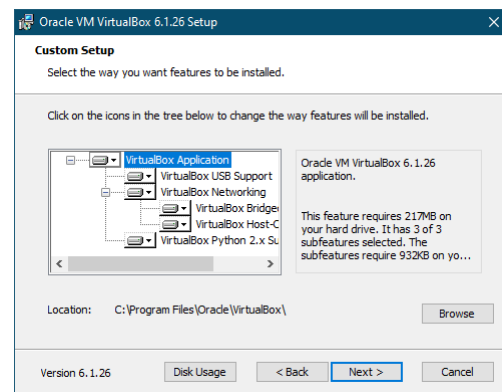


Figure 1.3: Screen 2

Click on **Next** for both above screens

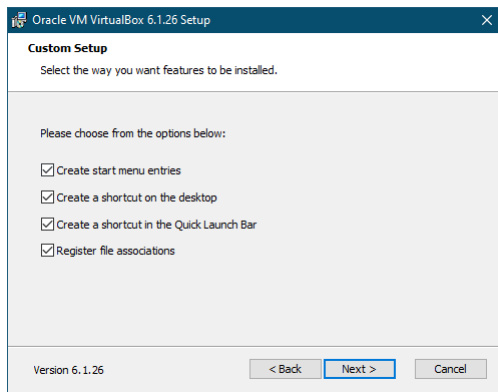


Figure 1.4: Screen 3

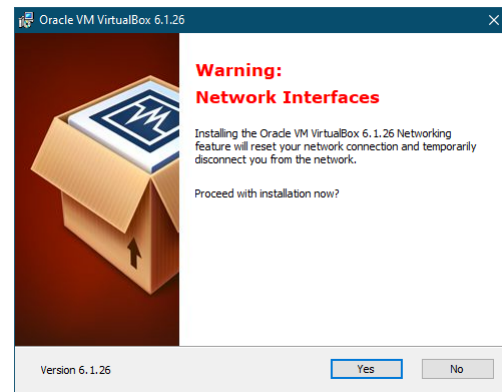


Figure 1.5: Screen 4

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

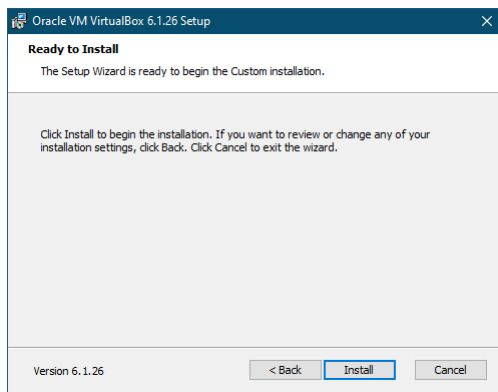


Figure 1.6: Screen 5



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

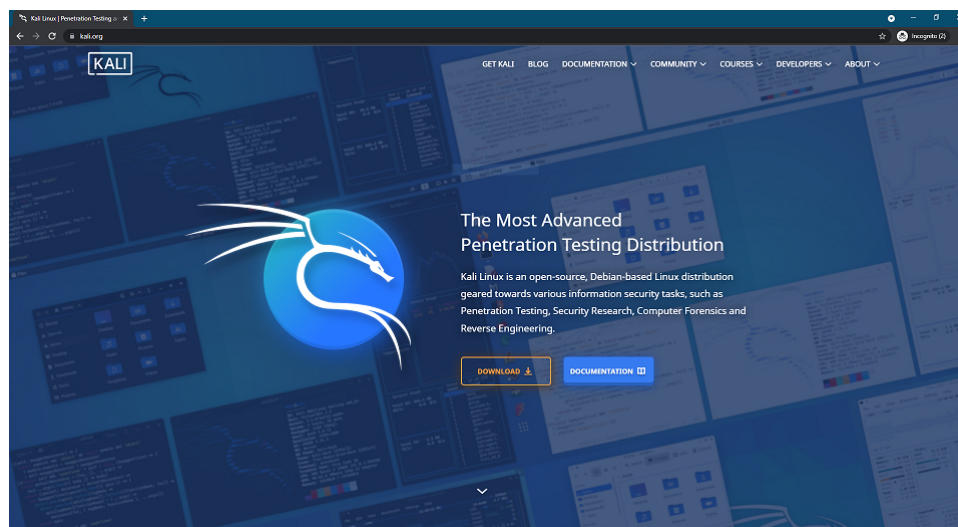


Figure 1.8: Kali Linux's Homepage

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

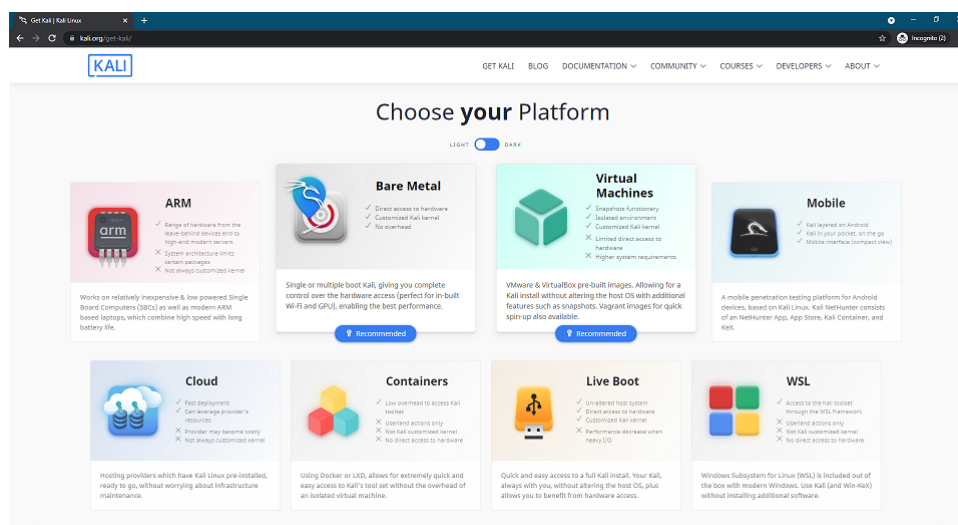


Figure 1.9: Kali Linux's different download options

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

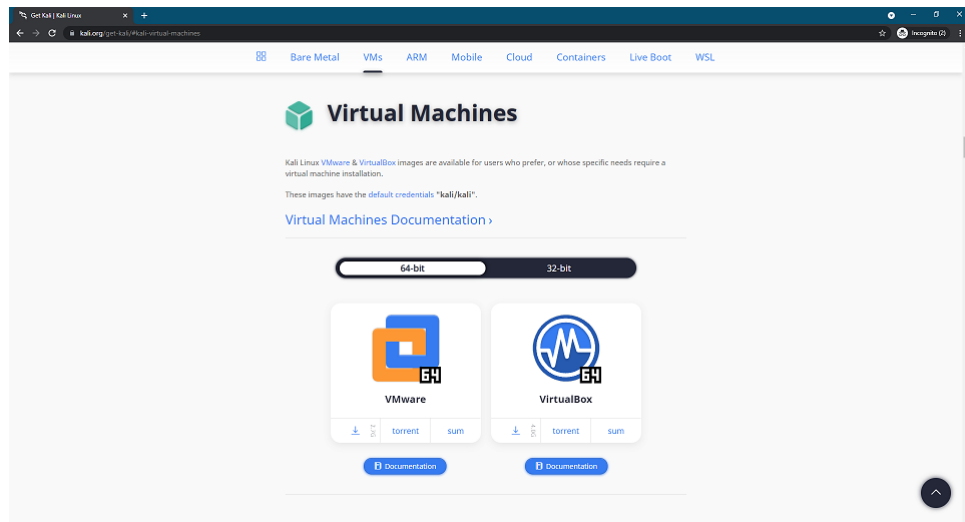


Figure 1.10: The 2 options for Virtual Machines

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.

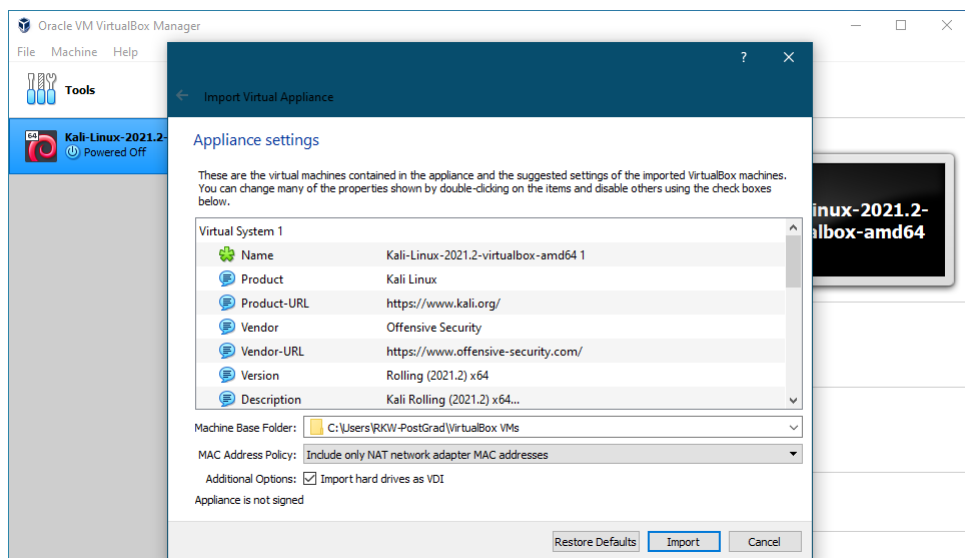


Figure 1.11: The main screen once the file is opened

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.

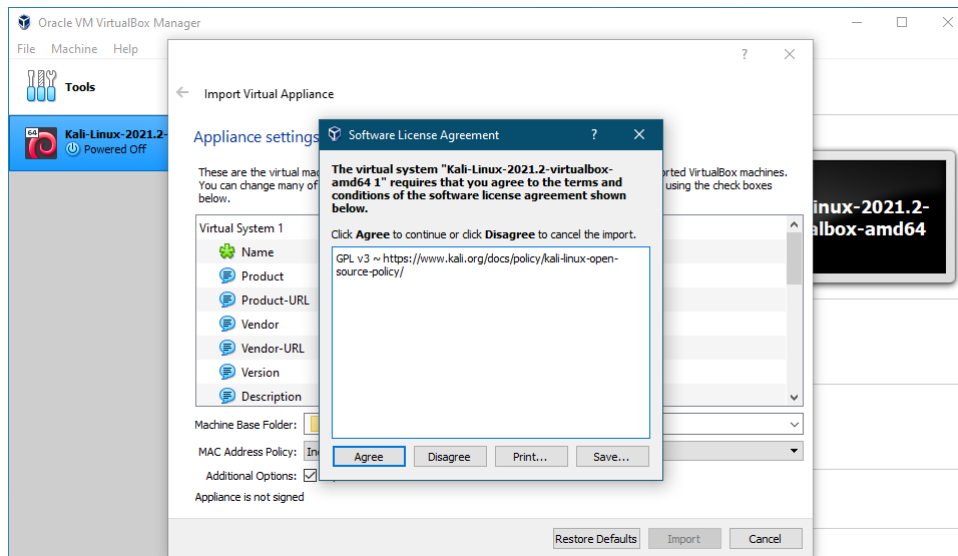


Figure 1.12: Software Licence Agreement screen

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.

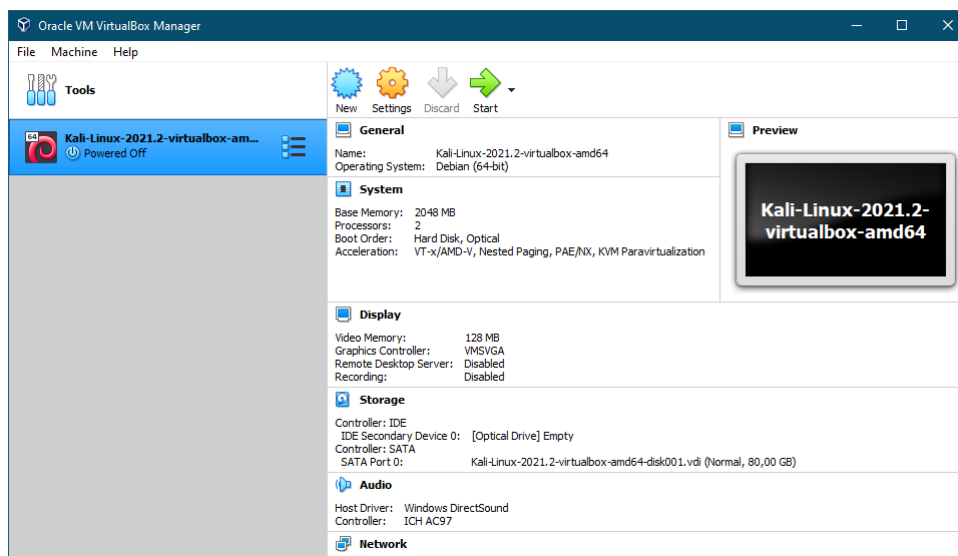


Figure 1.13: VirtualBox's main screen

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.

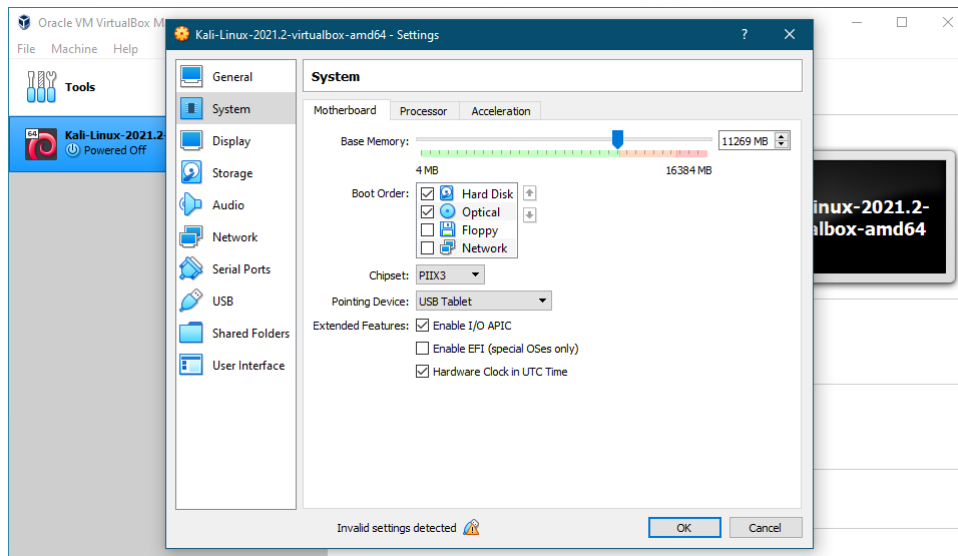


Figure 1.14: Systems settings: Motherboard tab

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

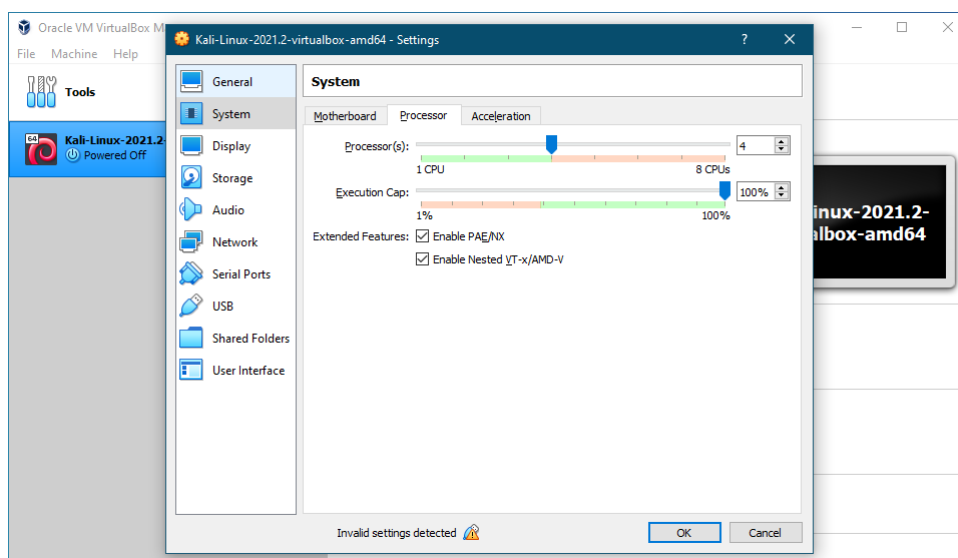


Figure 1.15: Systems settings: Processor tab

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.

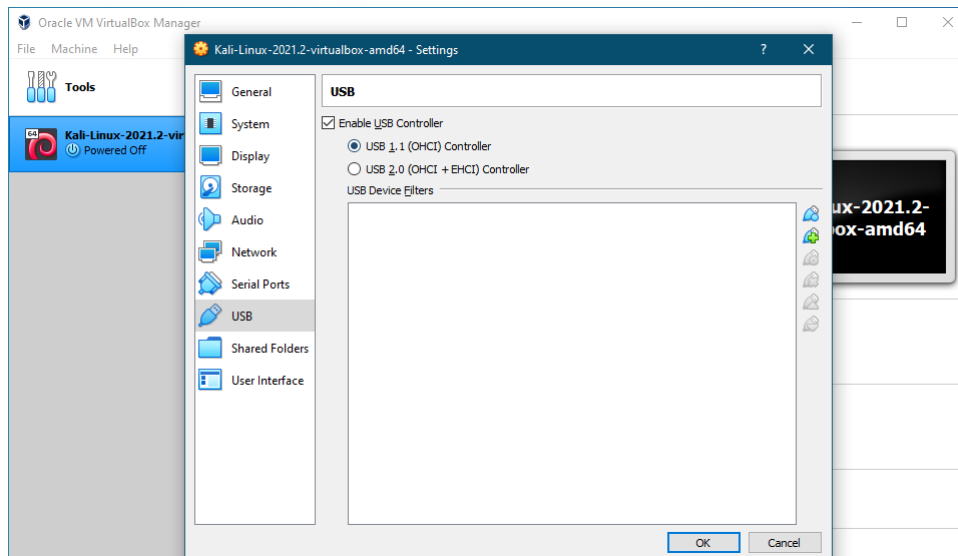


Figure 1.16: USB settings

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`

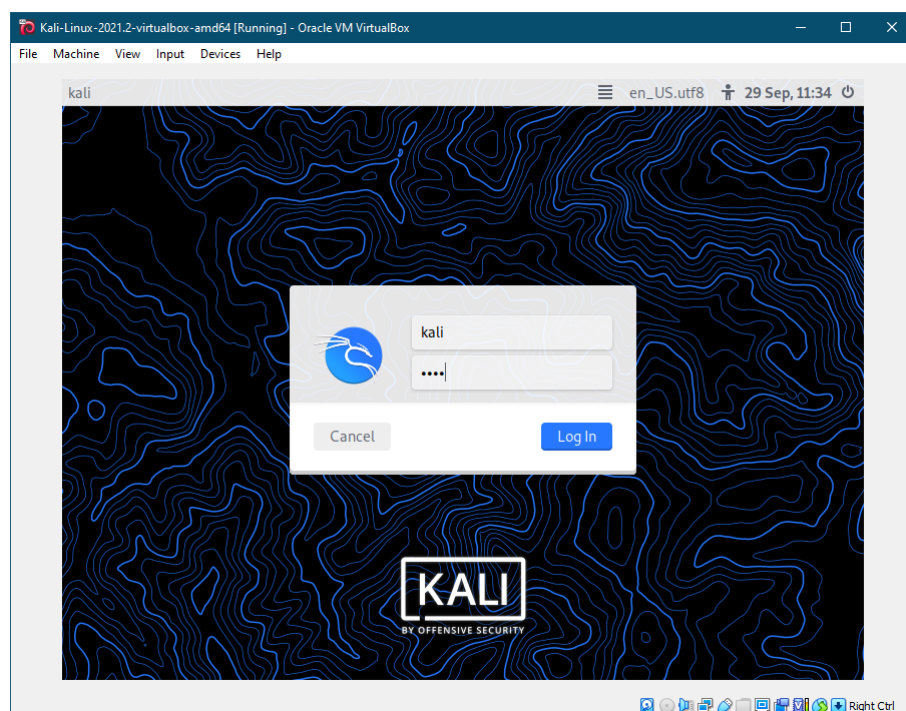


Figure 1.17: Kali Linux login screen

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

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

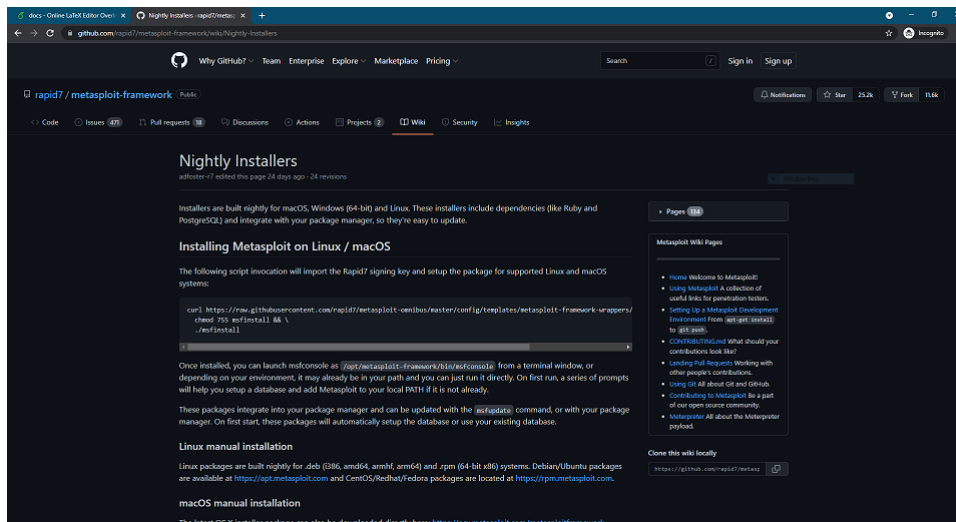


Figure 1.19: Metasploit Framework's GitHub page

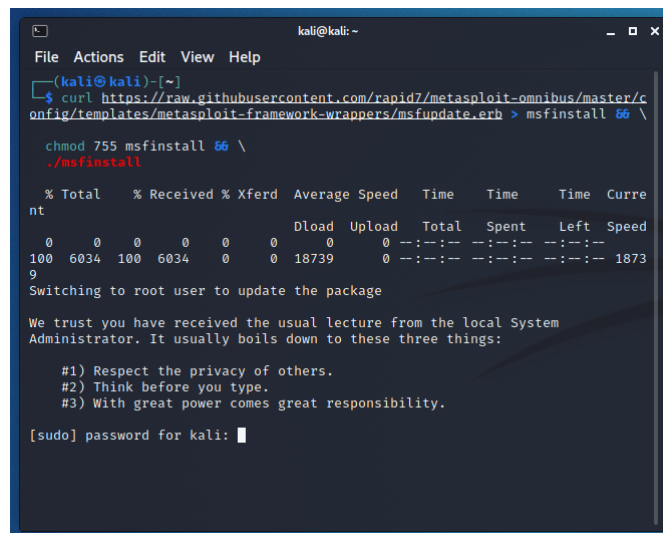
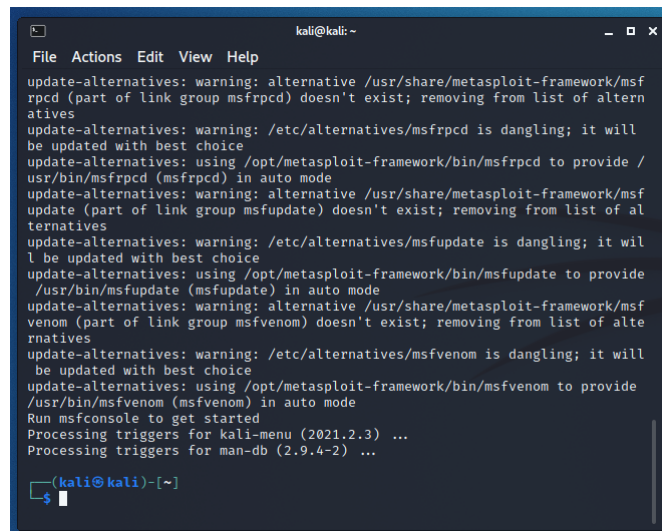


Figure 1.20: Terminal asks for root access

A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). It displays several warning messages from 'update-alternatives' regarding missing or dangling links for 'msfrpcd', 'msfupdate', and 'msfvenom'. It then shows the installation of these packages using the best choice from the alternatives. The terminal ends with the prompt '(kali@kali)-[~]' and a '\$' symbol.

```
kali@kali: ~
File Actions Edit View Help
update-alternatives: warning: alternative /usr/share/metasploit-framework/msfrpcd (part of link group msfrpcd) doesn't exist; removing from list of alternatives
update-alternatives: warning: /etc/alternatives/msfrpcd is dangling; it will be updated with best choice
update-alternatives: using /opt/metasploit-framework/bin/msfrpcd to provide /usr/bin/msfrpcd (msfrpcd) in auto mode
update-alternatives: warning: alternative /usr/share/metasploit-framework/msfupdate (part of link group msfupdate) doesn't exist; removing from list of alternatives
update-alternatives: warning: /etc/alternatives/msfupdate is dangling; it will be updated with best choice
update-alternatives: using /opt/metasploit-framework/bin/msfupdate to provide /usr/bin/msfupdate (msfupdate) in auto mode
update-alternatives: warning: alternative /usr/share/metasploit-framework/msfvenom (part of link group msfvenom) doesn't exist; removing from list of alternatives
update-alternatives: warning: /etc/alternatives/msfvenom is dangling; it will be updated with best choice
update-alternatives: using /opt/metasploit-framework/bin/msfvenom to provide /usr/bin/msfvenom (msfvenom) in auto mode
Run msfconsole to get started
Processing triggers for kali-menu (2021.2.3) ...
Processing triggers for man-db (2.9.4-2) ...

(kali@kali)-[~]
$
```

Figure 1.21: Terminal completed installing package

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):

```
git clone https://github.com/scriptjunkie/msfgui.git
```

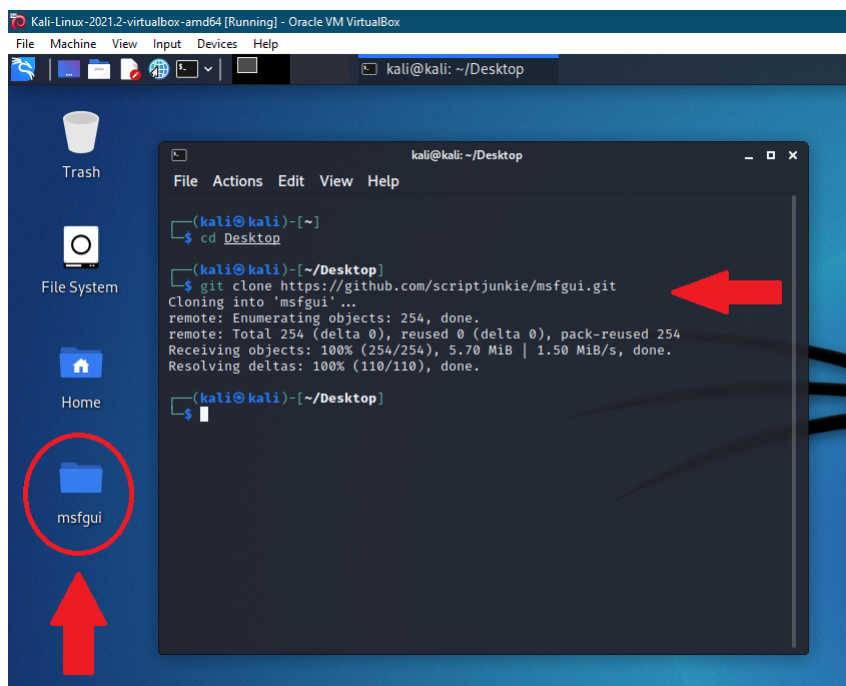
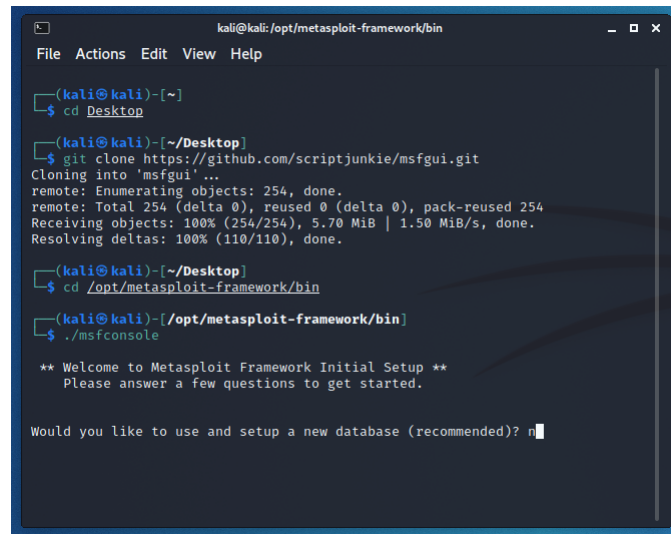


Figure 1.22: GUI folder added to the Desktop

A directory titled `msfgui` will now be added to your Desktop. To run the GUI the following steps have to be carried out.



```
kali@kali: /opt/metasploit-framework/bin
File Actions Edit View Help

(kali@kali)-[~]
$ cd Desktop

(kali@kali)-[~/Desktop]
$ git clone https://github.com/scriptjunkie/msfgui.git
Cloning into 'msfgui'...
remote: Enumerating objects: 254, done.
remote: Total 254 (delta 0), reused 0 (delta 0), pack-reused 254
Receiving objects: 100% (254/254), 5.70 MiB | 1.50 MiB/s, done.
Resolving deltas: 100% (110/110), done.

(kali@kali)-[~/Desktop]
$ cd /opt/metasploit-framework/bin

(kali@kali)-[/opt/metasploit-framework/bin]
$ ./msfconsole

** Welcome to Metasploit Framework Initial Setup **
Please answer a few questions to get started.

Would you like to use and setup a new database (recommended)? n
```

Figure 1.23: Type 'n' for No

<https://citizenlab.ca/>