

HOW TO SETUP KALI LINUX VIRTUAL MACHINE

Kali Linux is a specialized, Debian-based distribution designed for penetration testing, ethical hacking, and security research. A virtual machine allows you to run Kali Linux on top of your existing operating system without needing to install it directly on your physical hardware.

TOOL: Windows Machine

TASK 1

In this lab, we prefer to use the VirtualBox because of its easy use and because it's also the most popular in the open source world. You can use it in both Linux and Windows PC environments. It is very easy to install in the Windows environment. After installing the actual application, do not forget to download and install the VirtualBox Extension Pack, which is the same version as this.

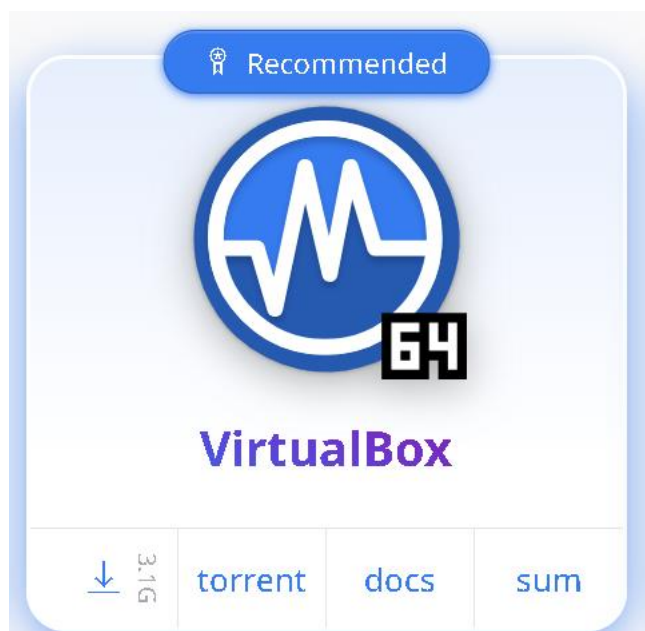


This software will allow us to run the Kali Linux Operating System within our Windows or Linux Desktop Operating System. This means the things we do in the virtual OS will not impact our actual OS.

TASK 2

<https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>

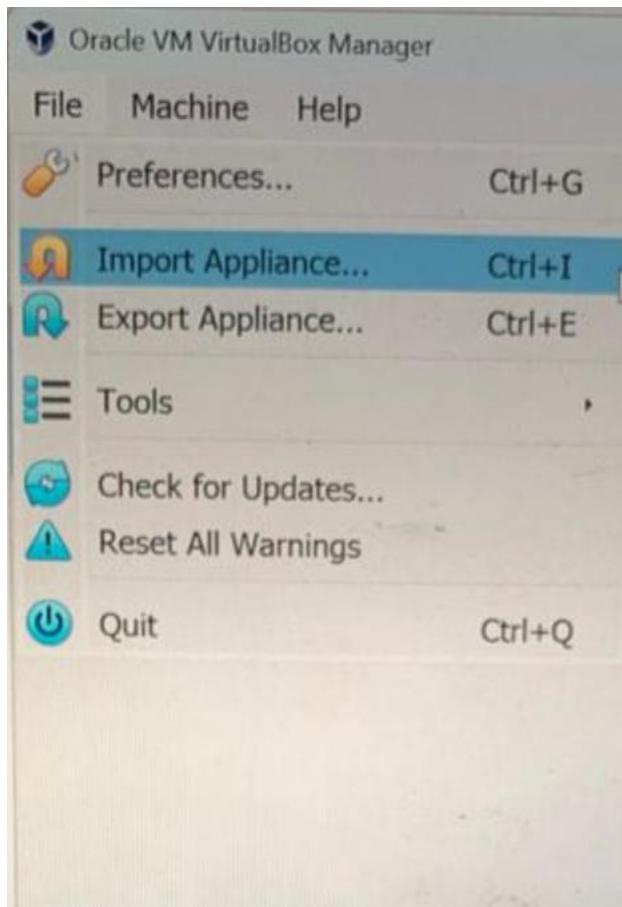
You will see two types of images here, 32bit and 64bit. If your Desktop Operating System supports running a 64bit virtual OS, it is recommended that you download it. Make sure you download for the right virtualization platform.



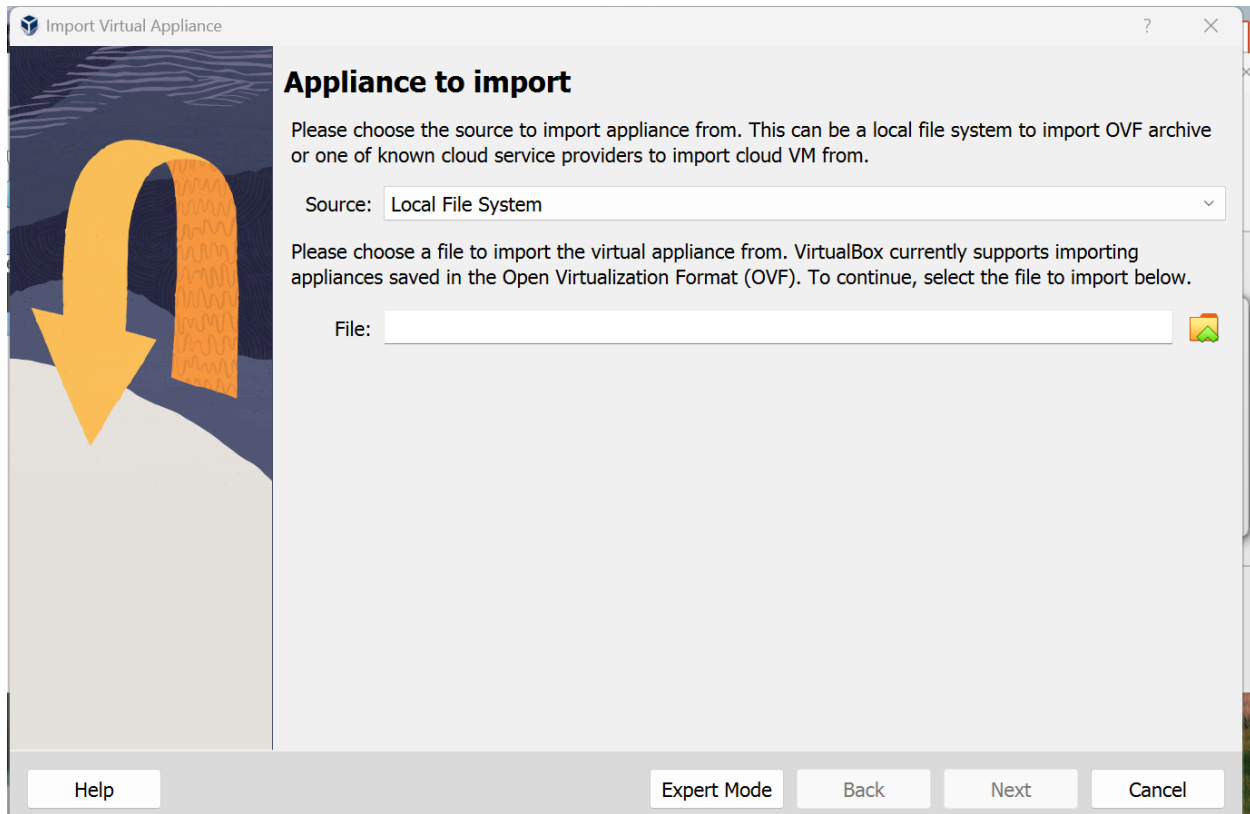
TASK 3

We will import the pre-installed Kali Linux VM machine just downloaded, into the VirtualBox environment.

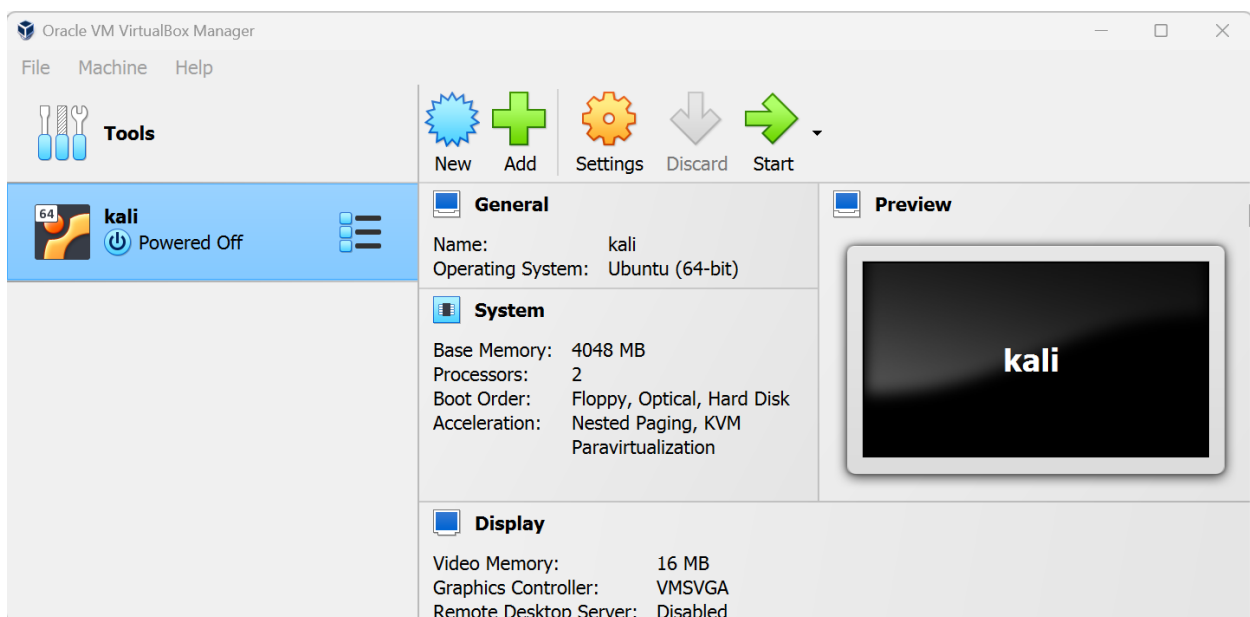
Open Oracle VM VirtualBox Manager, select “File” on the top menu, then click “Import Appliance” from the drop-down menu.



In the “Appliance to import” window, following the numbered steps indicated in the figure, select the Kali Linux VM OVA file we just downloaded. Then, click Next.



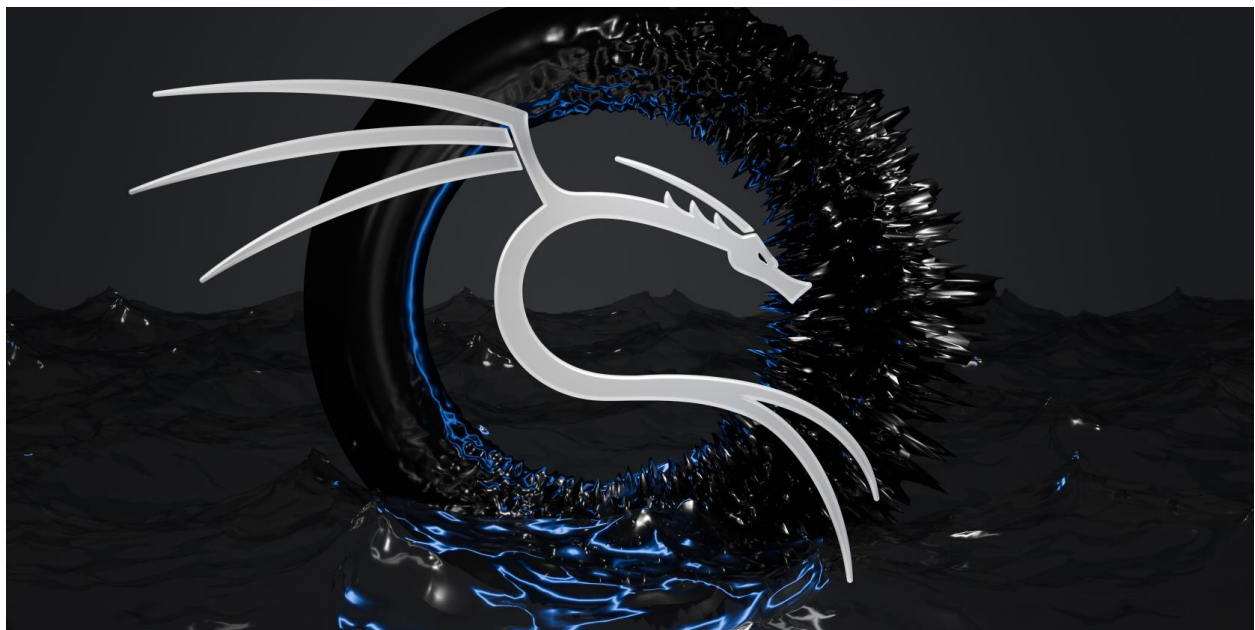
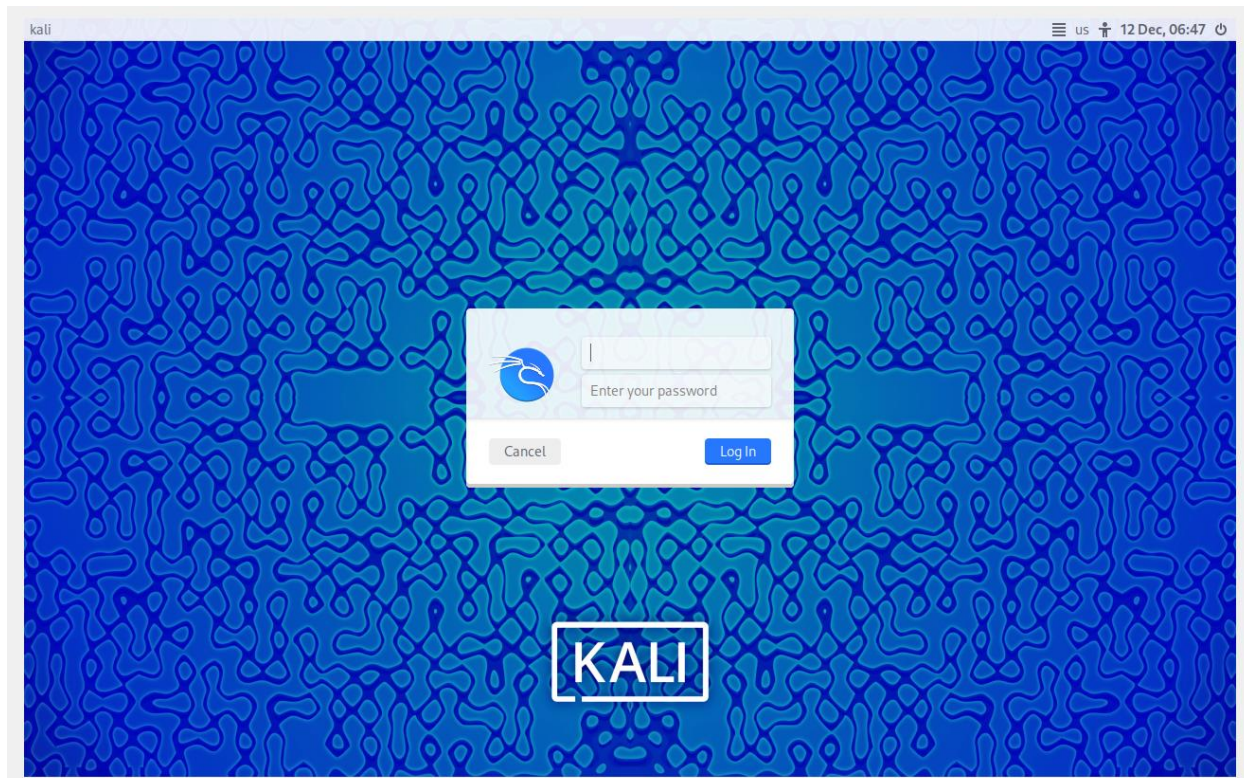
After the import is done, the Kali Linux VM is ready for use. Click the green “Start” button to boot virtual machine.



TASK 4

Once the importer is finished, boot up the virtual machine. It may take a few minutes to load. Once loaded, enter “kali” as both username and password.

By default, a password is not defined for the root user, so you cannot log in directly as that user.

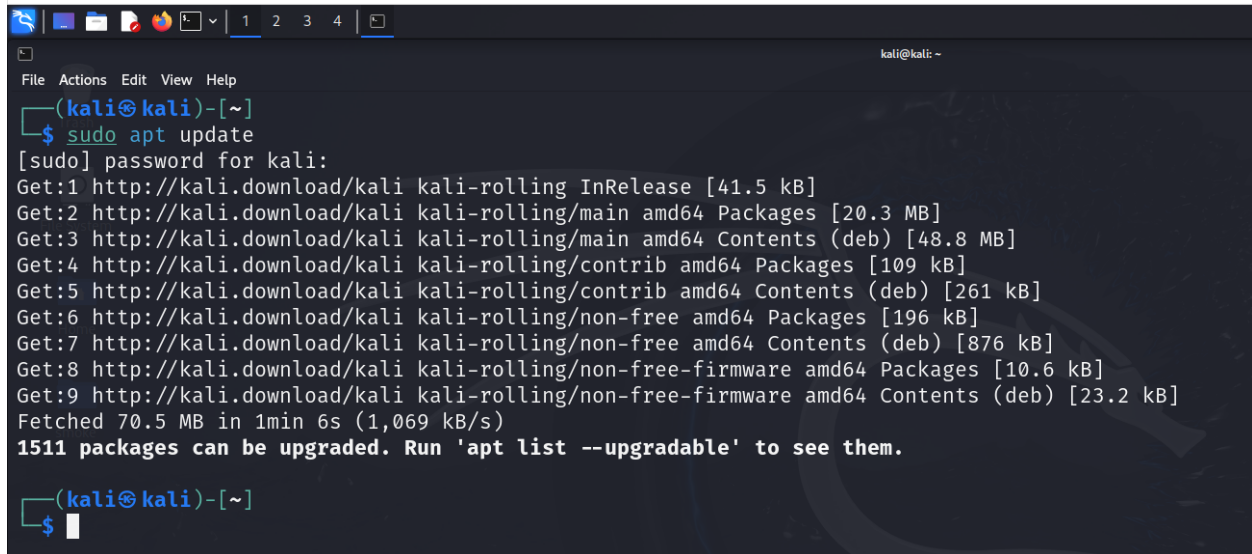


For operations that require root authorization, you will need to use “sudo” command on the terminal screen, in this case the password that must be entered is “kali”.

To ensure you are using the most up to date version of the machine, open a terminal screen, then enter the following commands:

```
sudo apt update
```

```
sudo apt full-upgrade -y
```



```
(kali㉿kali)-[~]
$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [48.8 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [109 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [261 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [196 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [876 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [23.2 kB]
Fetched 70.5 MB in 1min 6s (1,069 kB/s)
1511 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali㉿kali)-[~]
$
```

You will be prompted for the sudo password. Enter the default password “kali”. It is important to have these updates on a freshly installed Kali VM, otherwise both the OS and some hacking tools may not work properly. After all updates are finished, reboot the Kali VM to make sure all updates have been applied.

TASK 5

Done! Now we have a fully functioning Kali Linux Virtual Machine to begin hacking. It is useful to take a snapshot of the machine, from the virtualization software settings, once all the updates are done. This is useful if the VM image becomes damaged, in which case we can simply revert to the recently updated working version. Also, connecting the default network adaptor to the “Bridge Adapter” instead of NAT will benefit us in many subsequent hacking operations.

First, make sure that Kali is in shutdown state. In the Oracle VirtualBox Manager main window, click the Settings button, then follow the steps described in the figure.

Now, we can take a snapshot of the entire Kali VM.

