Website Vulnerability Testing

Analyze and identify vulnerable attack vectors within web applications.

Part of the Penetration Testing for Small Businesses package.

*Revision 0.1*

Table of Contents

[1. Introduction 3](#_Toc506794594)

[2. Requirements 3](#_Toc506794595)

[3. Set up VirtualBox 3](#_Toc506794596)

[a. Download VirtualBox 3](#_Toc506794597)

[b. Install VirtualBox 3](#_Toc506794598)

[c. Add VirtualBox image from USB drive 3](#_Toc506794599)

[d. Launch VirtualBox image 3](#_Toc506794600)

[4. Run Vulnerability Scans 3](#_Toc506794601)

[a. Launch application 3](#_Toc506794602)

[b. Type URL 3](#_Toc506794603)

[c. Wait to complete. 3](#_Toc506794604)

[d. Verify results were transmitted. 3](#_Toc506794605)

[e. Shutdown VirtualBox image and exit VirtualBox. 3](#_Toc506794606)

# Introduction

This guide will take you through all the steps necessary to analyze your website for vulnerabilities. It will initially set up everything on your computer necessary to complete the tasks, then you will be guided through completing the scanning tasks. The vulnerabilities scanned for are SSL/TLS setup, and known WordPress installation issues. In the follow-up section in this document, more in-depth vulnerabilities will be discussed, as well as how you can do them yourself.

# Requirements

* Computer running Windows 7 or newer, with full Administrator access.
* Working internet connection.
* Beginner-intermediate computer skills.

# Set up VirtualBox

*If you already are familiar with how to install and use VirtualBox, skip to step C.*

### Download VirtualBox

Navigate your web browser to [https://www.virtualbox.org](https://www.virtualbox.org/).

Click the “Downloads” link in the left navigation bar of the webpage.

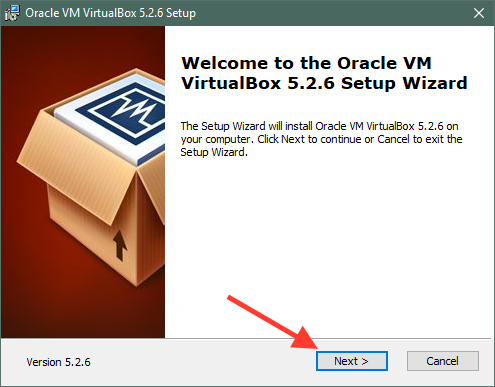


Under the “VirtualBox binaries” section, click on the “Windows hosts” link to download VirtualBox for your computer.

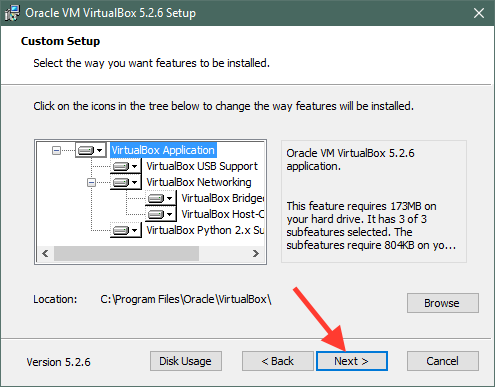


### Install VirtualBox

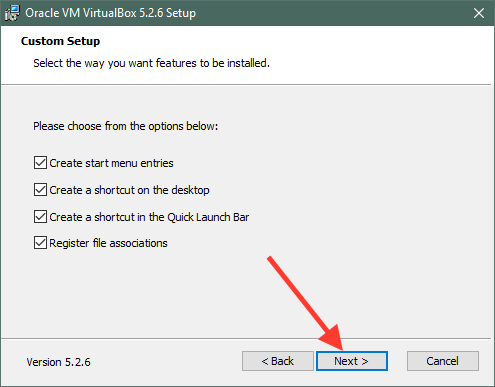
Once the download has completed, double-click the file to run it. You should see a screen similar to this (it’s acceptable if the version number is different). Click the “next” button.



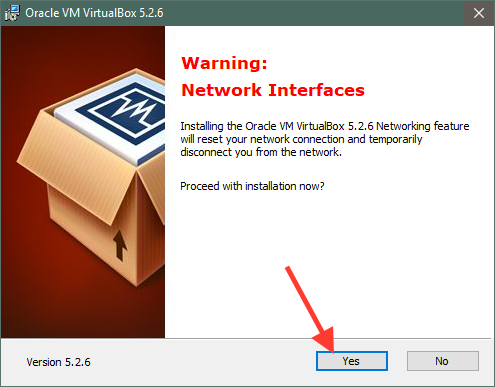
Leave the “Custom Setup” screen as-is, and click the “next” button.



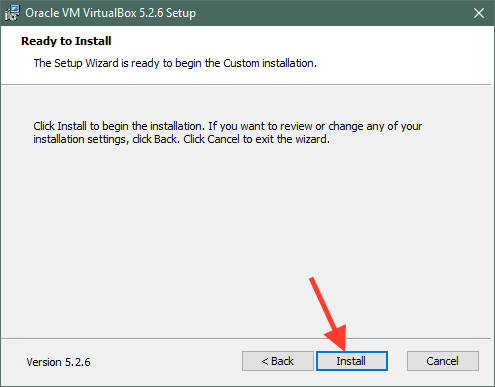
Continue to click “next” when this screen appears.



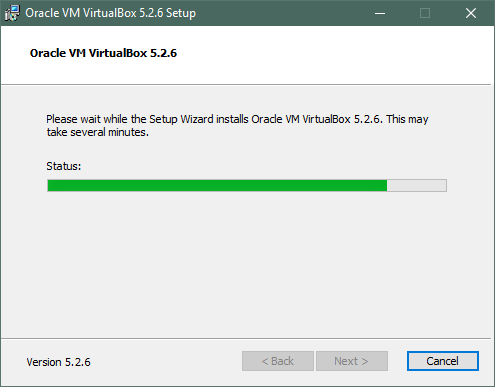
Click “Yes” on this warning screen.



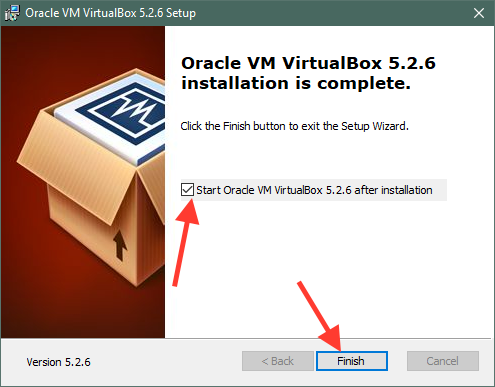
Click “Install” to begin the installation of VirtualBox on your computer.



Wait while VirtualBox completes its installation. Windows may ask you to approve the installation of a new network adapter for your computer, make sure to say “Yes” to that as well.



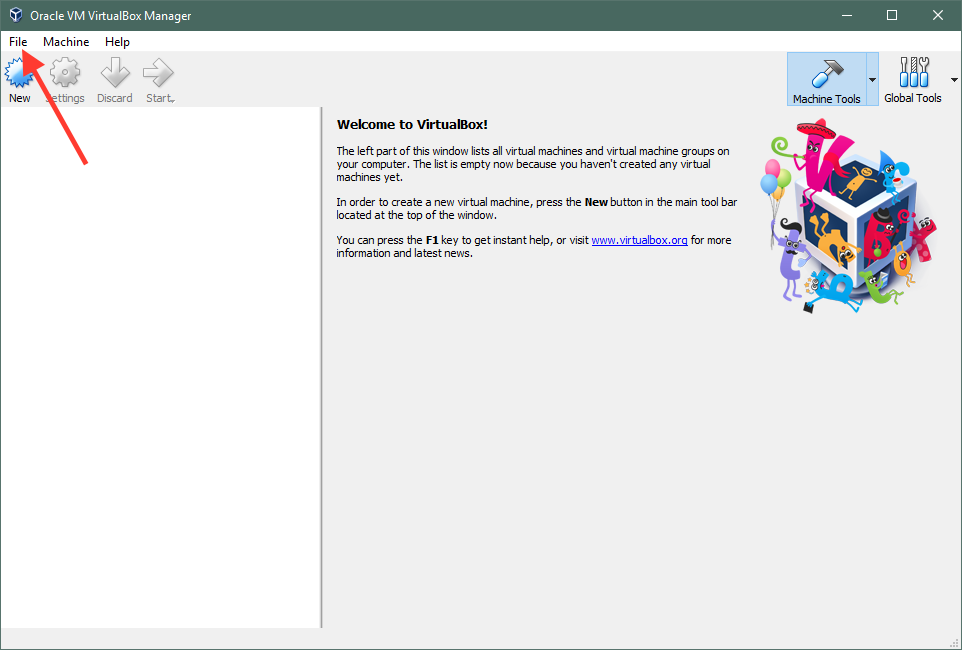
VirtualBox is now installed on your computer. Leave the checkbox checked, and process to part ‘c’ of these instructions.



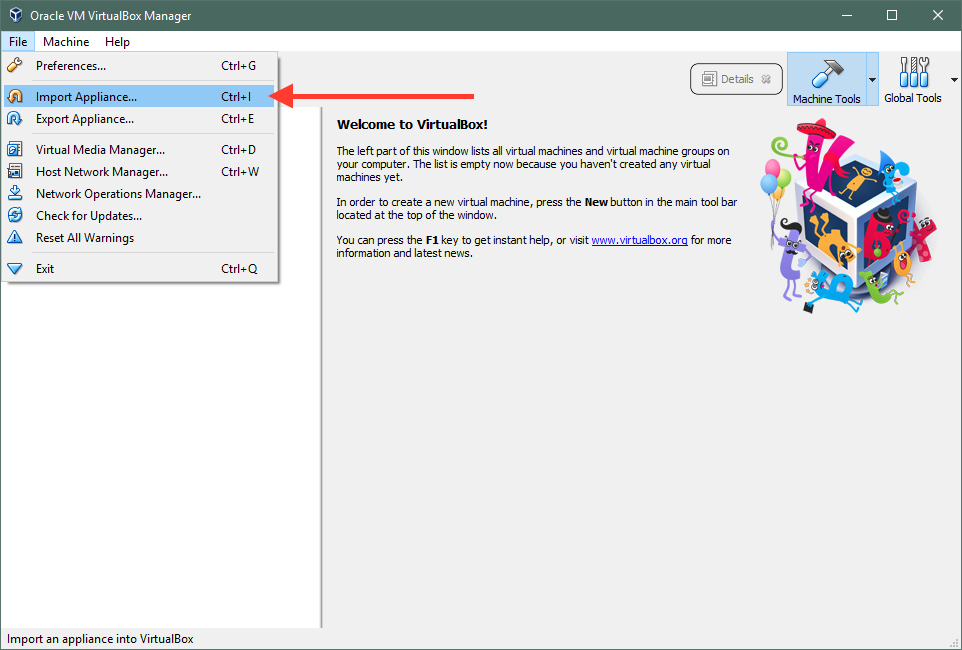
### Add VirtualBox image from USB drive

Upon opening VirtualBox, you should see a screen similar to this one.

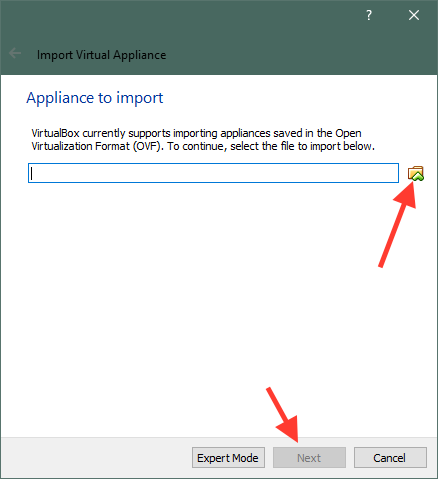
Open the “File” menu.



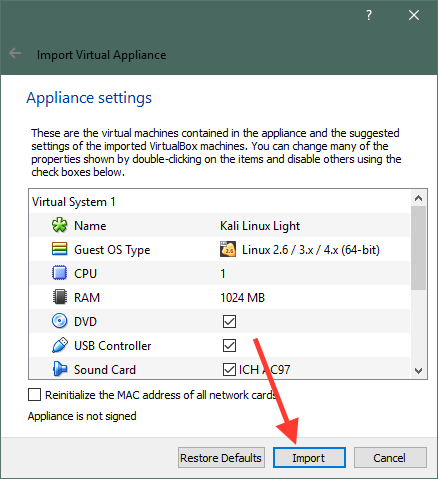
In that menu, click on the “Import Appliance…” item.



Verify the provided USB drive is plugged into a USB port on your computer. Click the Folder icon on the right of the text box, then in the pop-up window navigate to the USB drive. Select the file named “Kali Linux Light” (it may show an .ova extension on it). Upon selection, click “Next” as seen in the screenshot below.

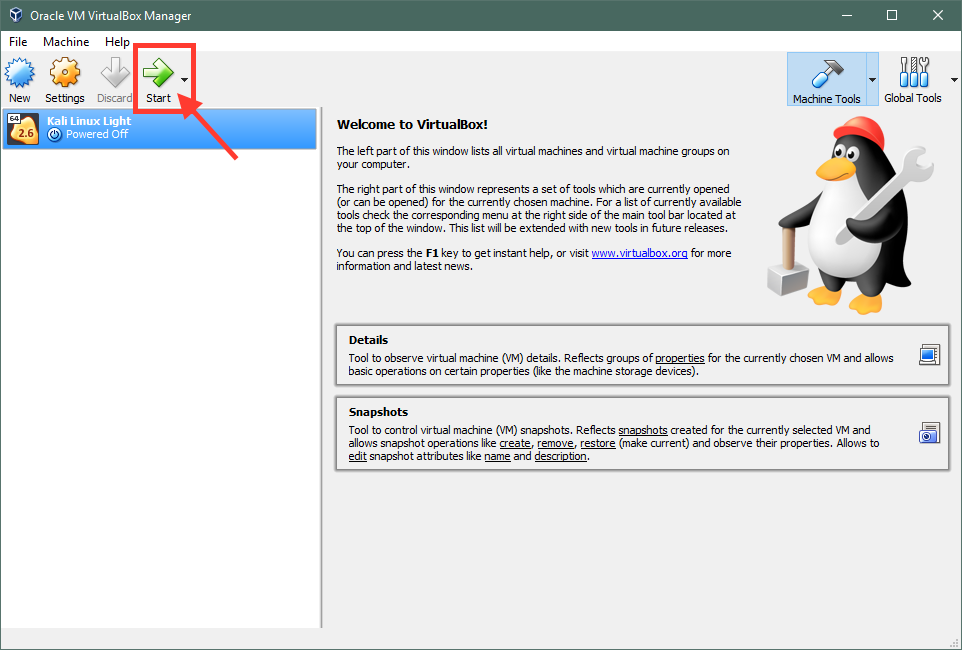


Verify the Name field is the same as below, then click “Import” to load the virtual machine onto your computer. This may take several minutes.



### Launch VirtualBox image

Now that the VirtualBox Image (or virtual machine) is setup in VirtualBox, select it in the left sidebar and click the big “Start” button with the right-facing green arrow.

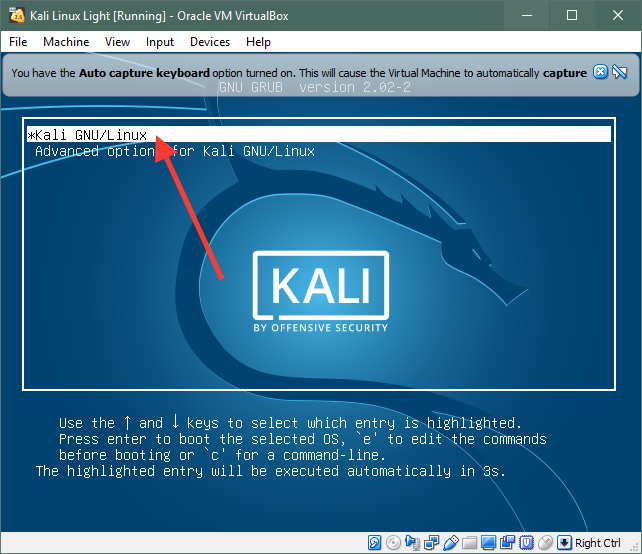


This will start the virtual machine on your computer.

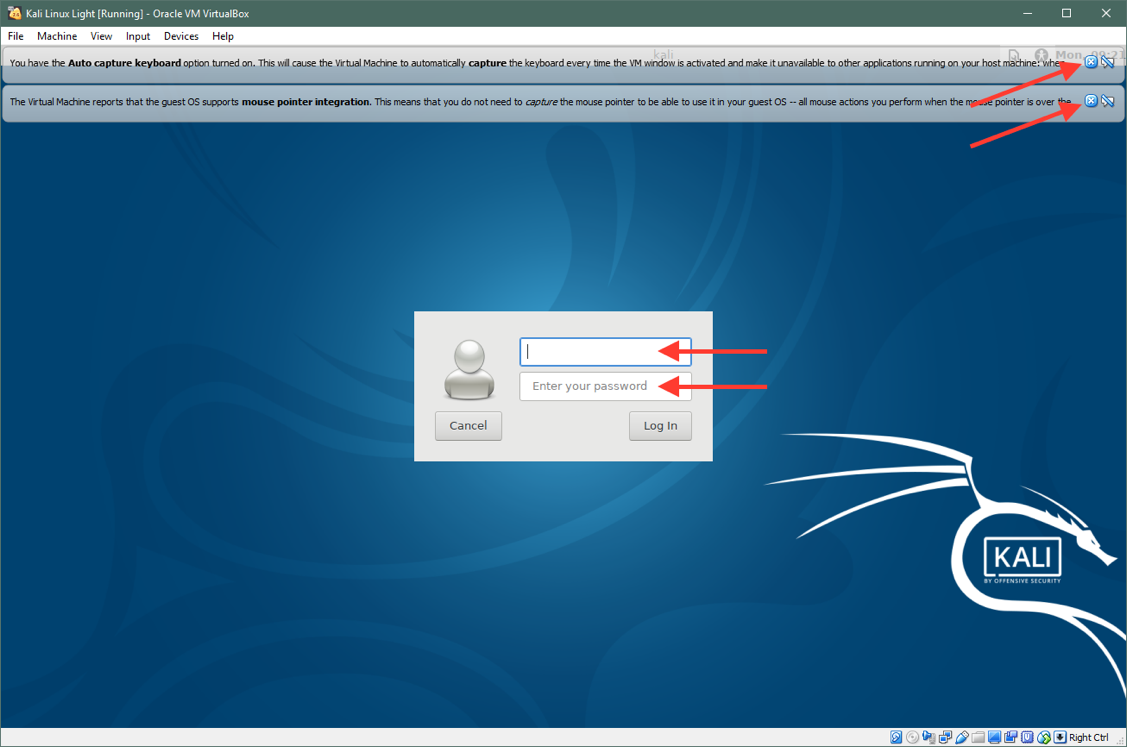
Essentially, this simulates a whole second working computer, but without the need for you to purchase one. Instead, this new computer runs *inside* your computer.

The tools used for this set of tests require a Linux-based operating system, whereas your computer is running Microsoft Windows.

This screen is part of the booting process for the virtualized operating system. Make sure the first option in the list is selected by using your arrow keys. If it is, wait 3 seconds or hit enter.



Once the login screen appears, login with the username “root” and password “toor”. The notification boxes at the top of the screen may be dismissed as well.



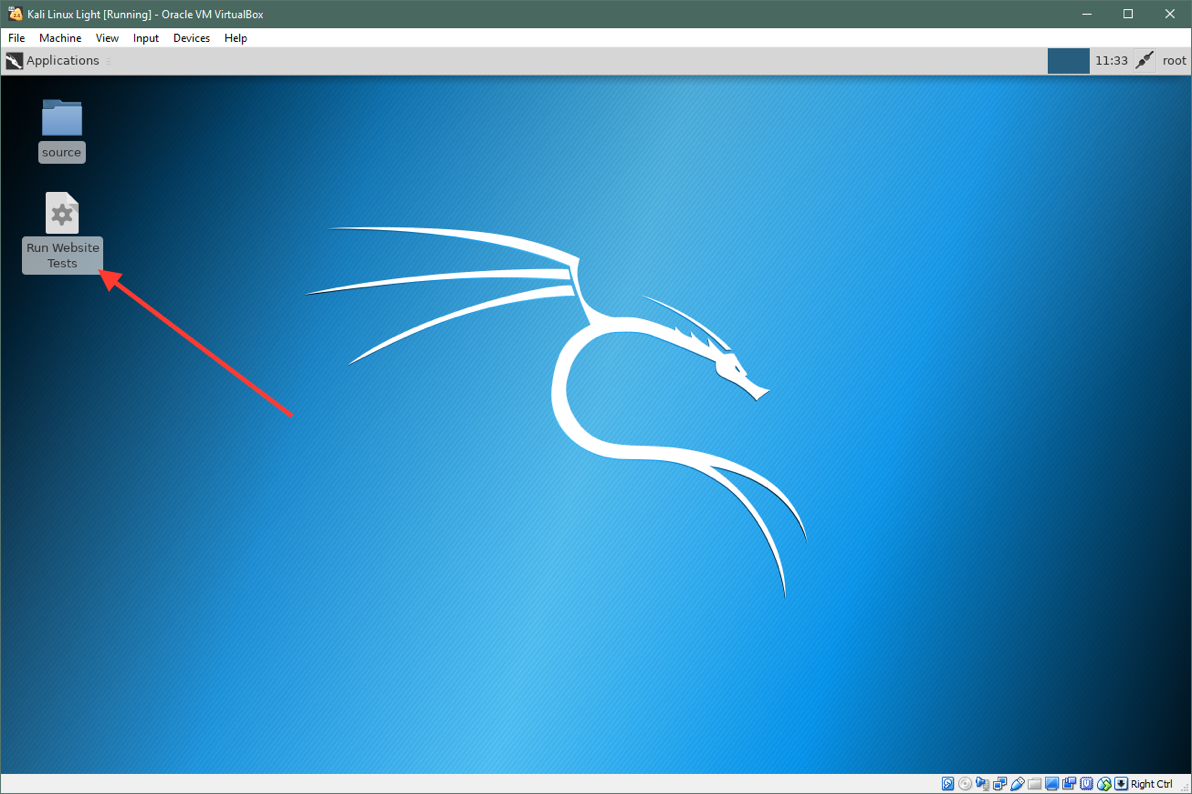
You should then end at a screen looking similar to this:

### 

# Run Vulnerability Scans

### Launch application

Double click on the desktop item labeled “Run Website Tests” with the gear icon.



### Type URL

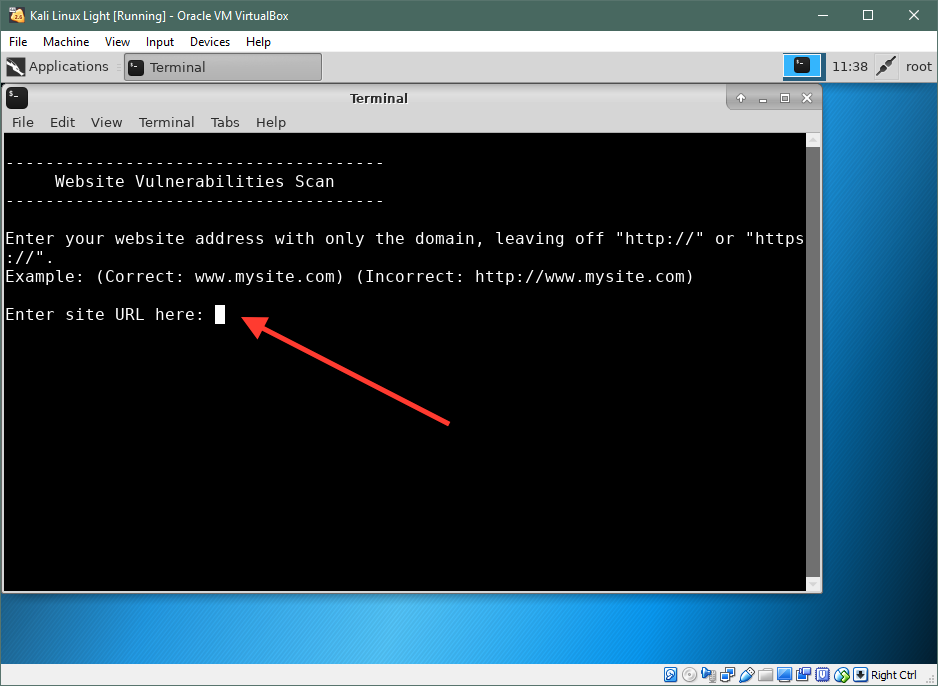
Enter the URL of your website that you would like to test, then press “Enter”.

Use the URL you would normally use to access your website’s front page,

leaving off the beginning “http://” or “https://”.

For example, a correct URL looks like: *www.example.com*

An incorrect would be: *https://www.example.com*



### Wait to complete.

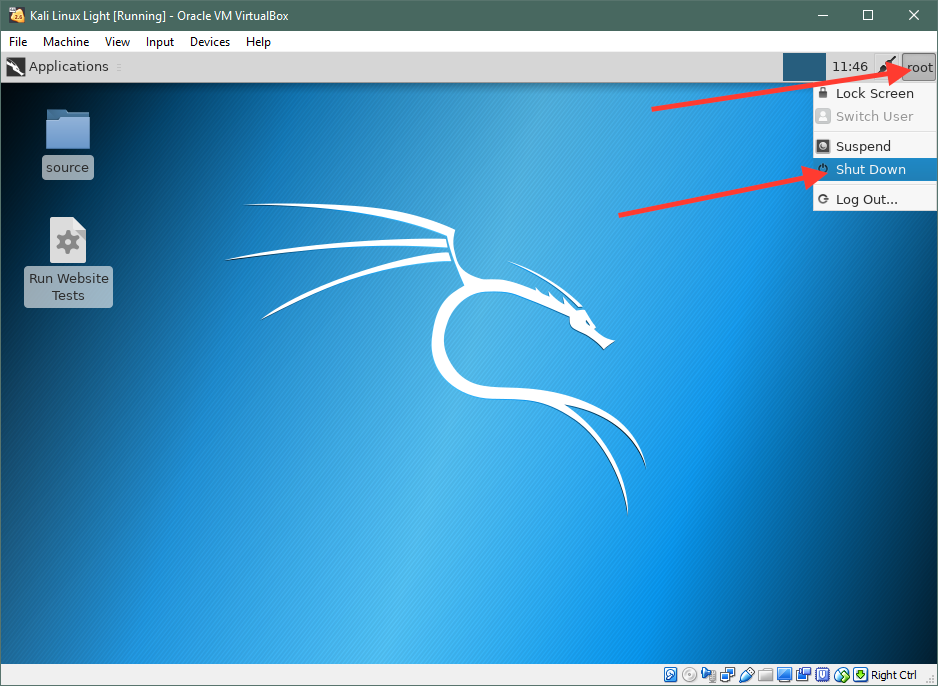
The set of scans will be dispatched and may take up to 20 minutes to complete. There should not be any interaction needed from you on this step. Watch the process to make sure no error messages appear. Such messages do appear, notify your representative from the group you purchased this package.

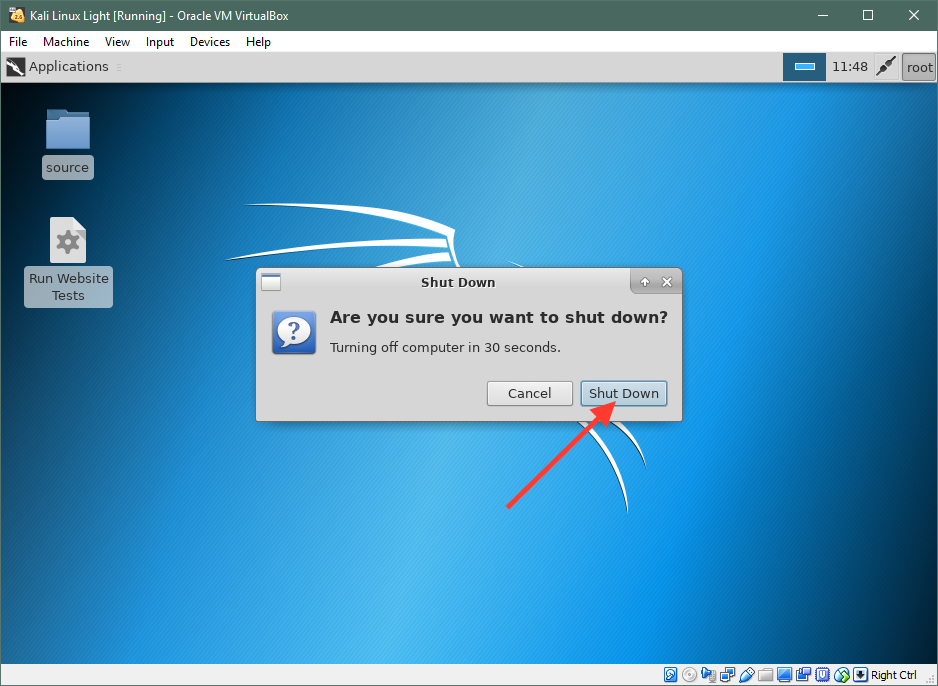
### Verify results were transmitted.

// TODO: Show and transmit packges.

### Shutdown VirtualBox image and exit VirtualBox.

Once all the above steps are complete, close the terminal application by clicking the “X” in the top right corner. Click the “root” button at the top right of the virtual machine’s window, and click “Shut Down”.



In the resulting popup window, click the button labelled “Shut Down”.

Upon clicking that button the virtual machine will exit. You may exit VirtualBox now as well.

All web application testing steps are complete. Expect to hear back soon about how your website performed in our tests.

Thank you for using this toolkit!