# Lab – Anonymize Kali Using Whonix

Overview

In this lab, you will learn how to remain fully anonymous using the Whonix Gateway while Kali Linux on the Internet. Running Kali Linux as a virtual machine can be an ideal hacking platform for launching attacks, but Kali is only as anonymous as the connection it uses.

Tor is an effective traffic obfuscation network, and while the Tor Browser alone cannot support a hacker's behavior, when combined with Whonix, Kali traffic is wholly anonymized and safe from a Man-In-The-Middle Attack.
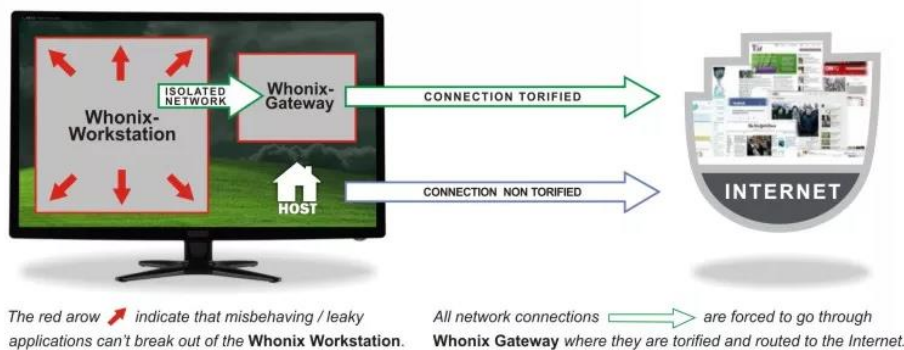

Begin the Lab!

We first need to download the OVA file for Whoinx. The download for the Whonix can be downloaded using the following link Download Whonix or by pointing your browser to https://www.whonix.org/
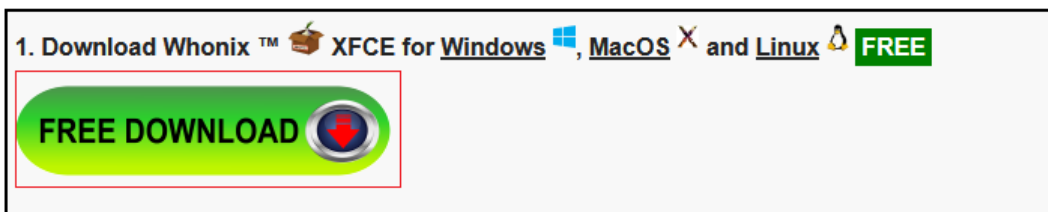

Whonix downloads as an OVA file. Once the importation of the OVA into VirtualBox is complete, you will have two virtual machines.

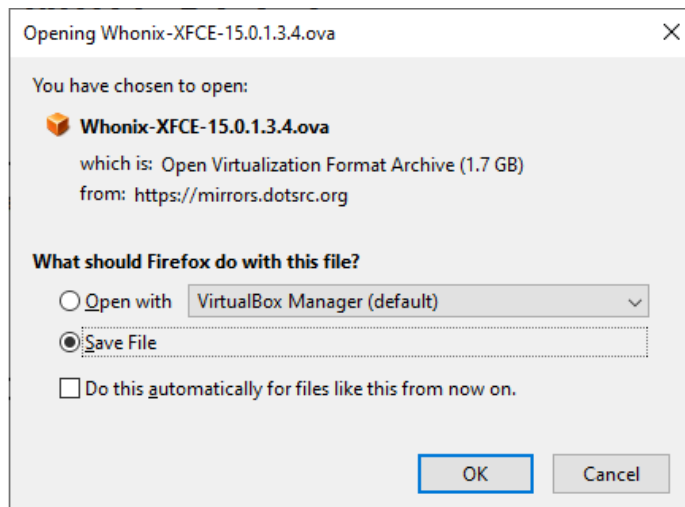| Whonix with XFCE *(with a graphical interface)*	Whonix with CLI *(text terminal only)*
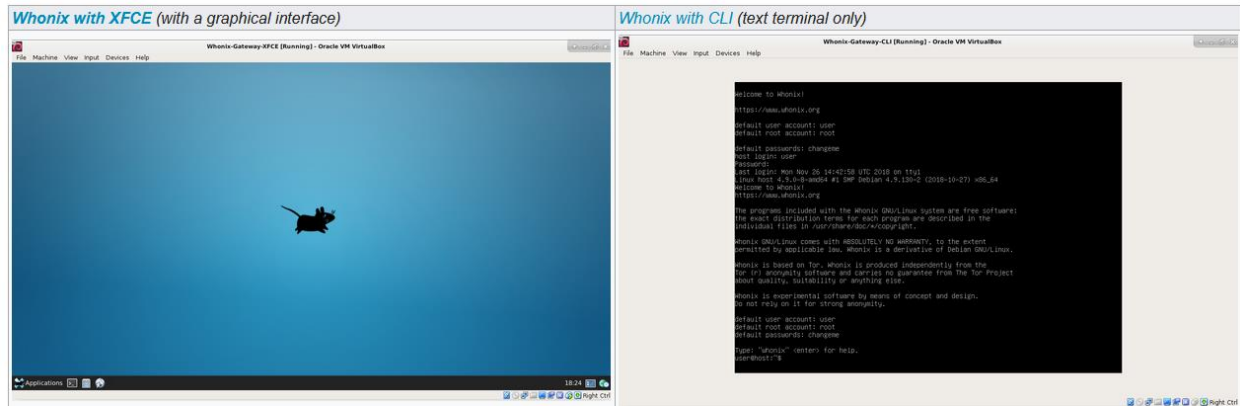
Please choose:

- A) **Whonix with XFCE** (recommended for beginners); <u>or</u>
- B) Whonix with CLI.

Whonix ™ for VirtualBox with XFCE

1. Download Whonix ™ 📦 XFCE for <u>Windows</u> ⊞, <u>MacOS</u> ✕ and <u>Linux</u> 🐧 **FREE**

FREE DOWNLOAD 🔴

Save the OVA to a location on your local machine. Remember where you saved it.

Opening Whonix-XFCE-15.0.1.3.4.ova   ✕

You have chosen to open:

📦 **Whonix-XFCE-15.0.1.3.4.ova**

    which is: Open Virtualization Format Archive (1.7 GB)
    from: https://mirrors.dotsrc.org

What should Firefox do with this file?

○ <u>O</u>pen with   VirtualBox Manager (default)   ⌄

⦿ <u>S</u>ave File

☐ Do this <u>a</u>utomatically for files like this from now on.
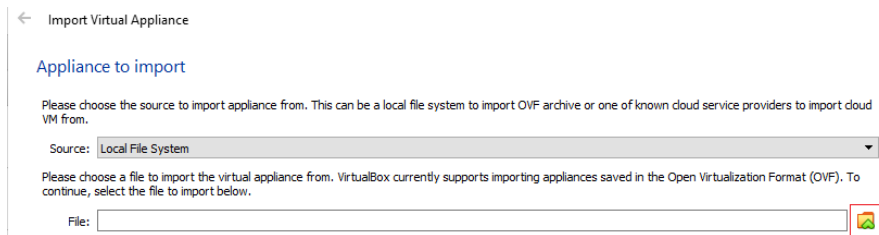
OK   Cancel

For this lab, we will use the VirtualBox Management console to import and create our two virtual machines.

Inside of VirtualBox, click on File, and from the context menu, select Import appliance.
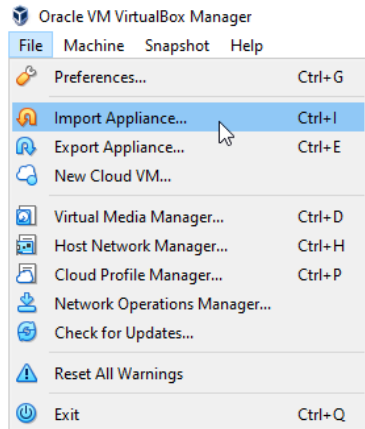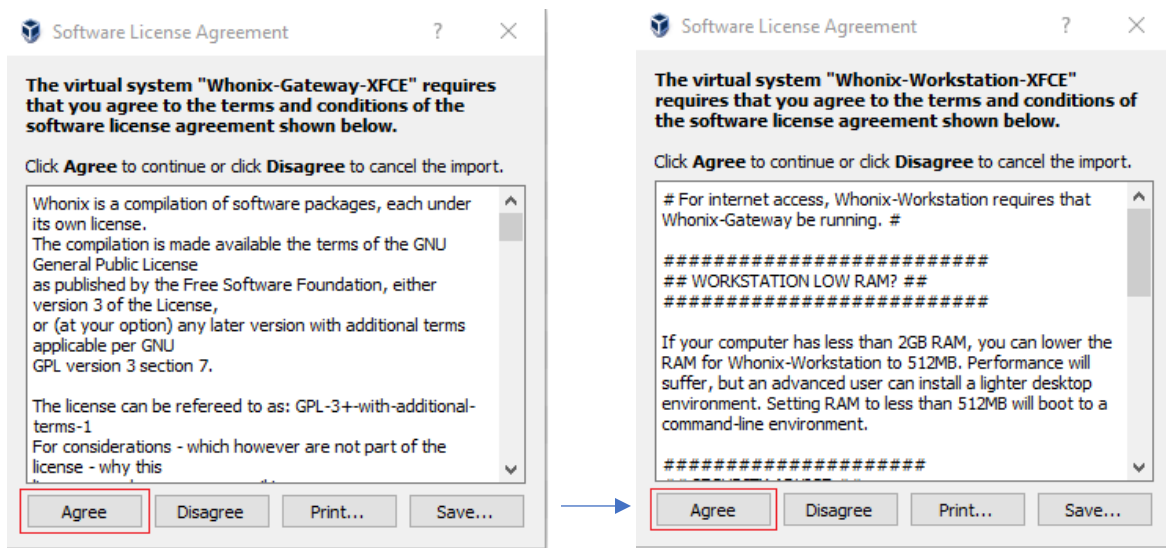
On the first page of the import wizard, use the browse option to find your OVA file and x2 click to import the appliance. Click next.
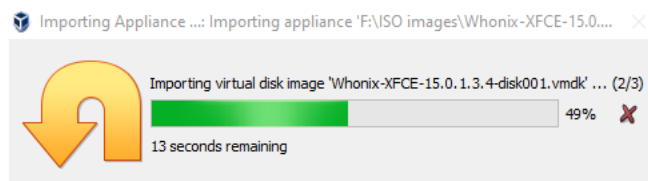

On the next page, accept the defaults and click install.
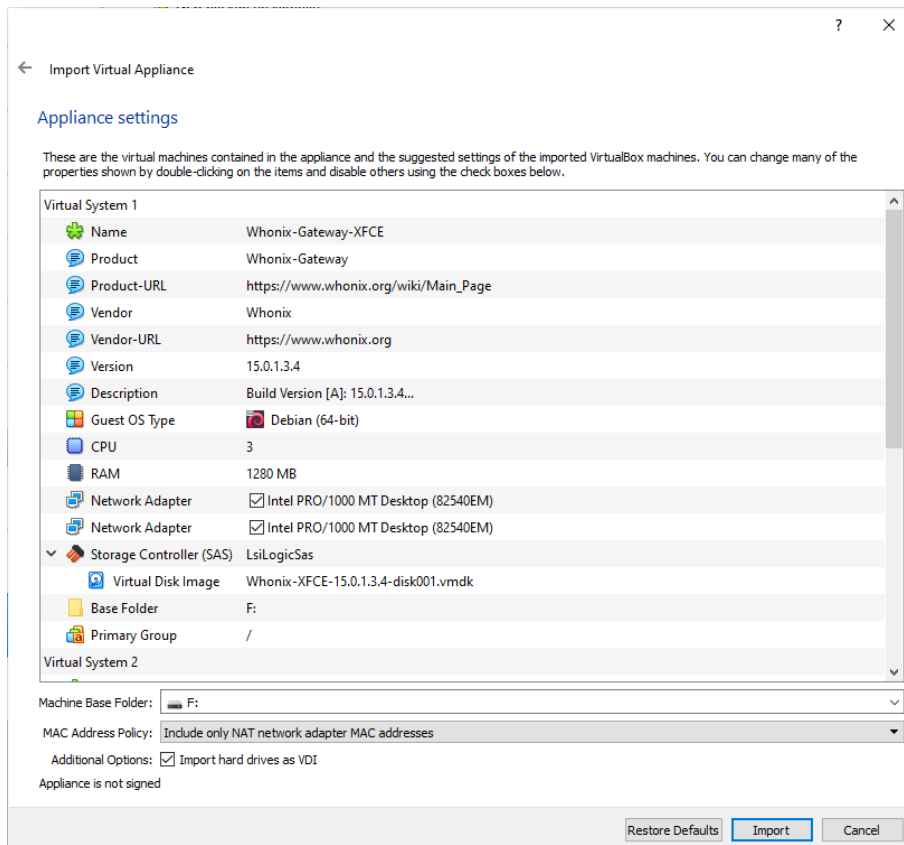
Agree to the license agreement.

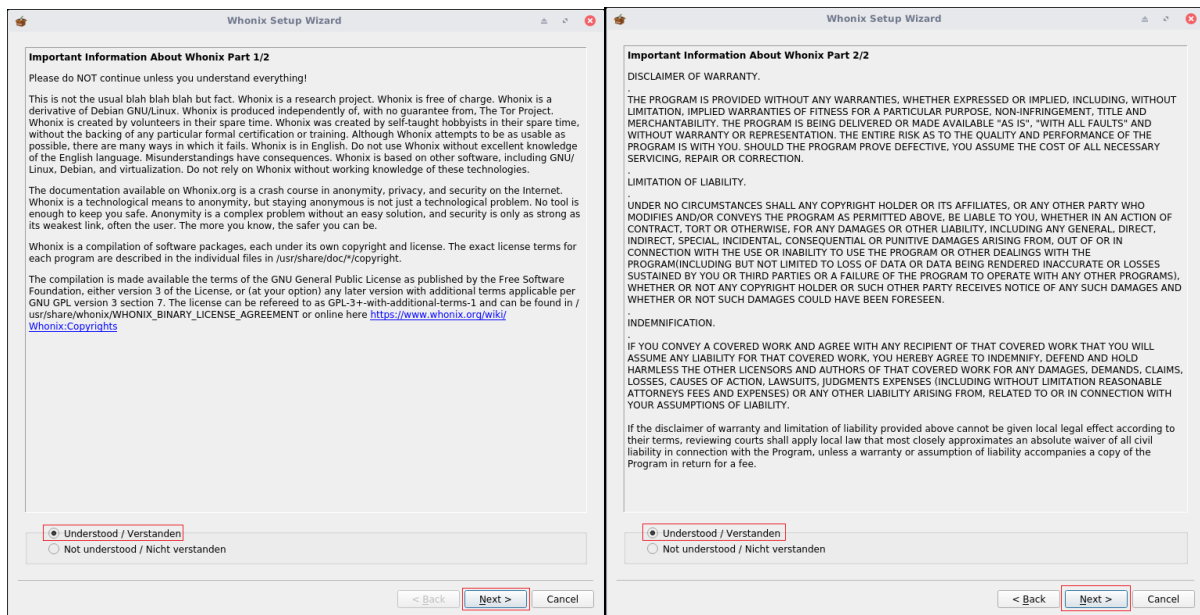The OVA file begins with the import process.

Once the install is complete, you will have two virtual machines installed. One is the Whonix Gateway, and the other is the Whonix workstation.
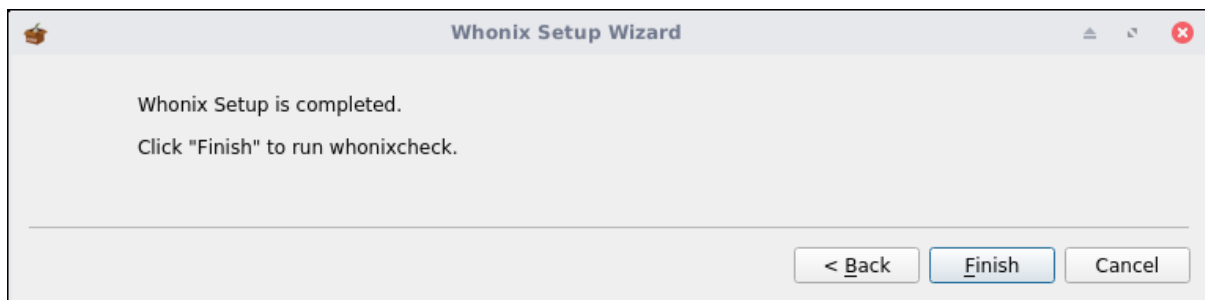

**Launch the Whonix Gateway**

Launch the Whonix Gateway. When you first access the Gateway, you will be greeted with some information you will need to acknowledge.
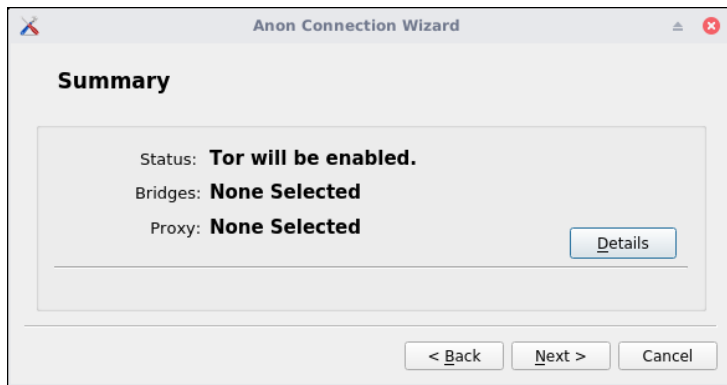
You will have to agree that you understand one more time, and finally, on the last page, you can click finish.
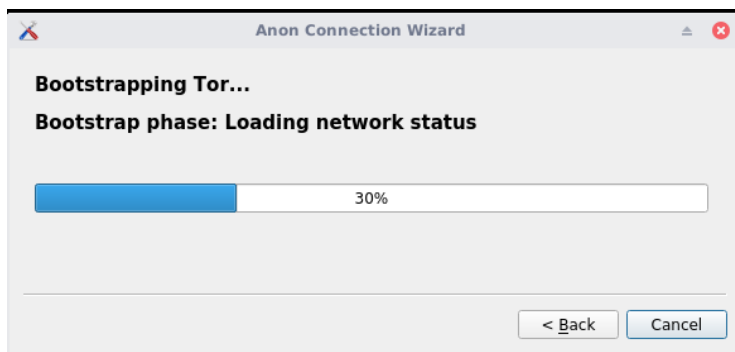

On the next screen, you can tell Whonix how you want the Gateway configured. Accept the default setting.
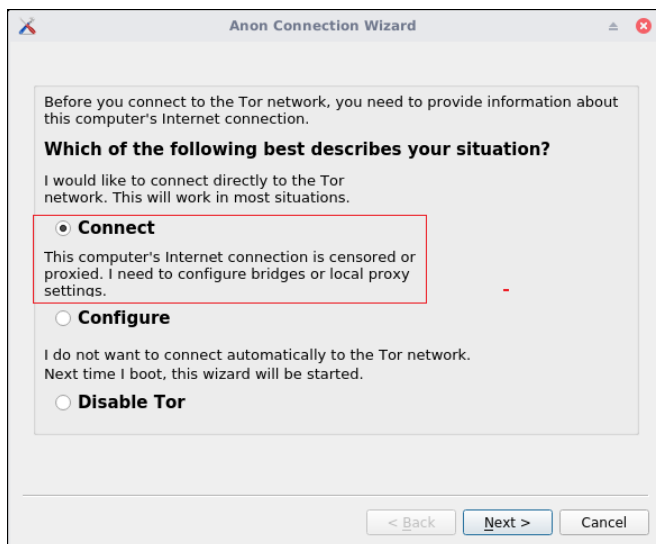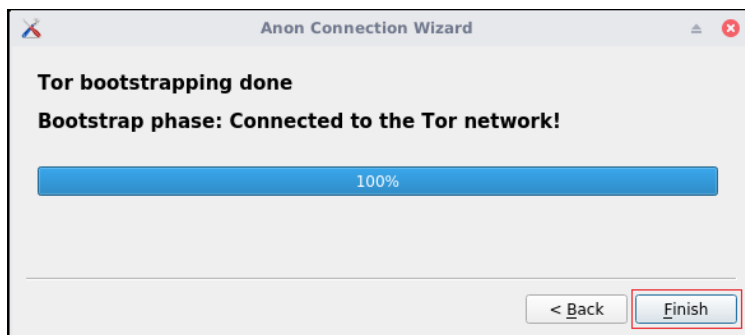
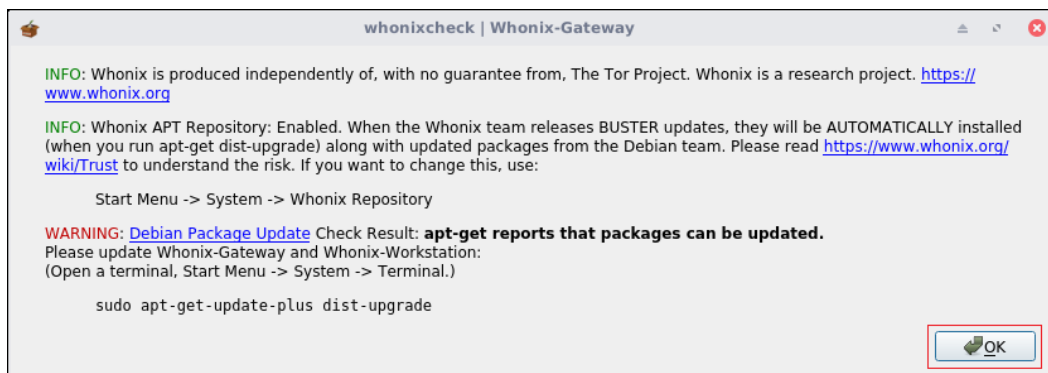The next screen is a summary of your selection. Click next.

The next screen starts the connection to the Tor network.

On the last screen, you can click finish.

Once the Tor network starts, a check will be run and to see if any updates are available.
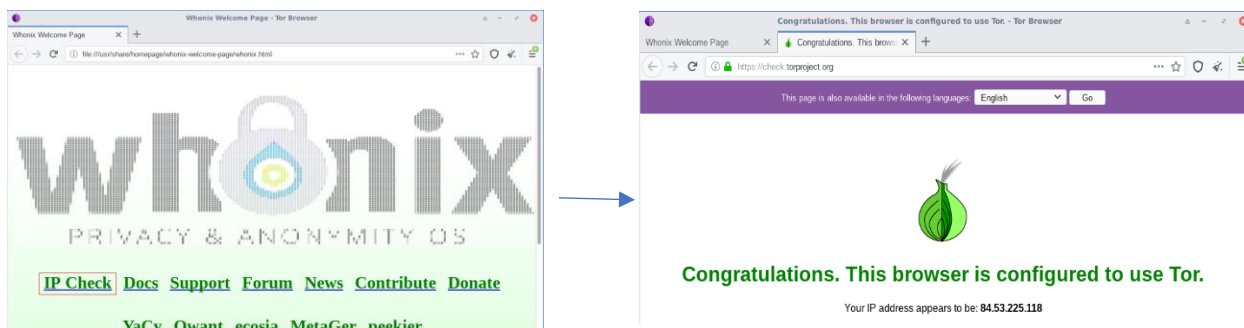
Launch the Whonix Workstation

You can now launch your Whonix Workstation. You will have to agree to the same three-part understanding. The Whonix Workstation is preconfigured to work with the Whonix Gateway, so there will be nothing to configure. The Workstation has loaded, it will conduct a connection check. Once the connection check completes, you will see the same info messages you had to acknowledge with the Gateway.

Once the connection check has been completed, you can check your Tor connection by launching the Tor browser and conducting an IP check.


When the TOR browser opens, click on the IP Check option to see if you are on the Tor network.

You can power off the Whonix Workstation as we will not need it for the remainder of this lab.

The big take away about the Whonix Workstation is that you can use it for anonymous browsing in conjunction with the Whonix Gateway much the same way you would use any workstation. The Workstations VirtualBox connection is set to communicate through the Gateway using the VirtualBox Internal Network adapter.
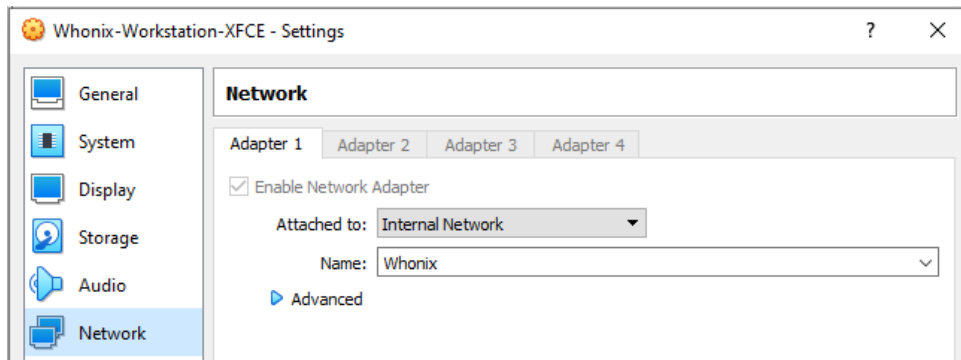
Configure your Kali Linux

The configuring of Kali to route its connection through the Whonix Gateway is quite simple.

Currently, Kali is configured to use DHCP, but we will need to set the wired network connection with a static IPv4 address required to find and communicate with the Whonix Gateway.

Ensure that your VirtualBox network adapter for Kali is set to Internal Network >Whonix.
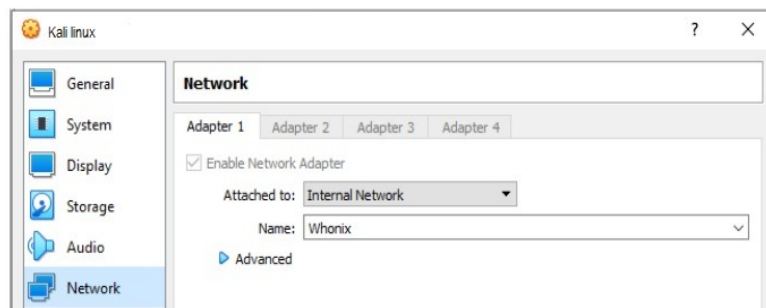
To begin, click on the Kali application icon and in the search window type networking, and from the results, click on Advanced Network Configuration.
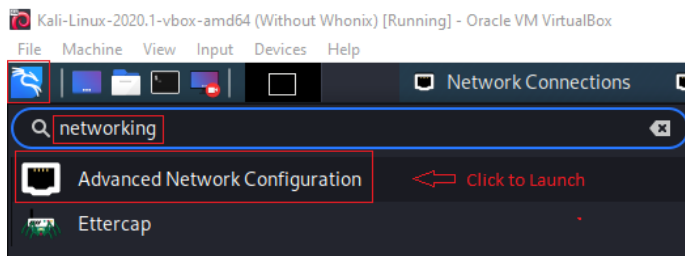
When the configuration wizard loads, click on IPv4 Settings. Under addresses, click the Add button.

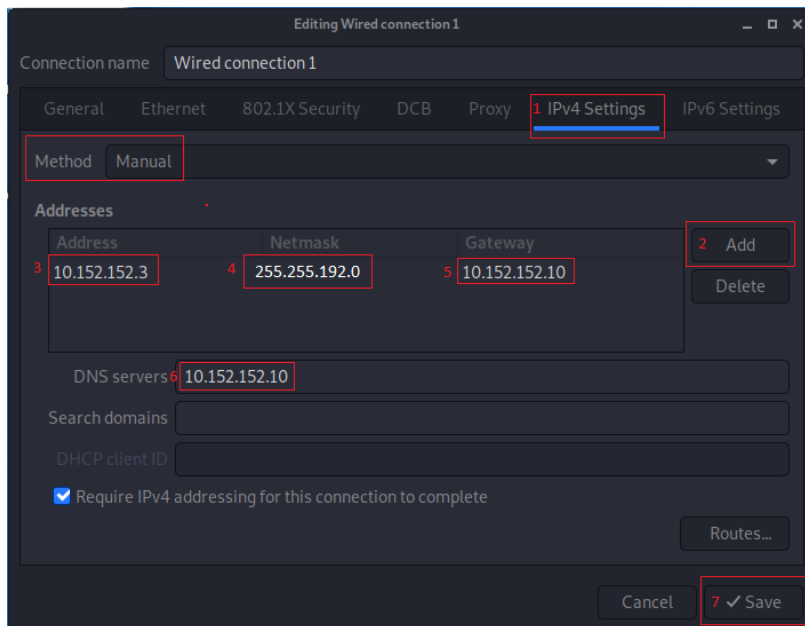In the Addresses window type the following IP address information.

Address: 10.152.152.3

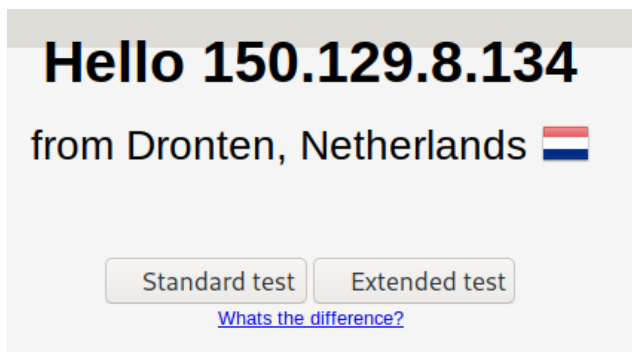Netmask: 255.255.192.0

Gateway: 10.152.152.10
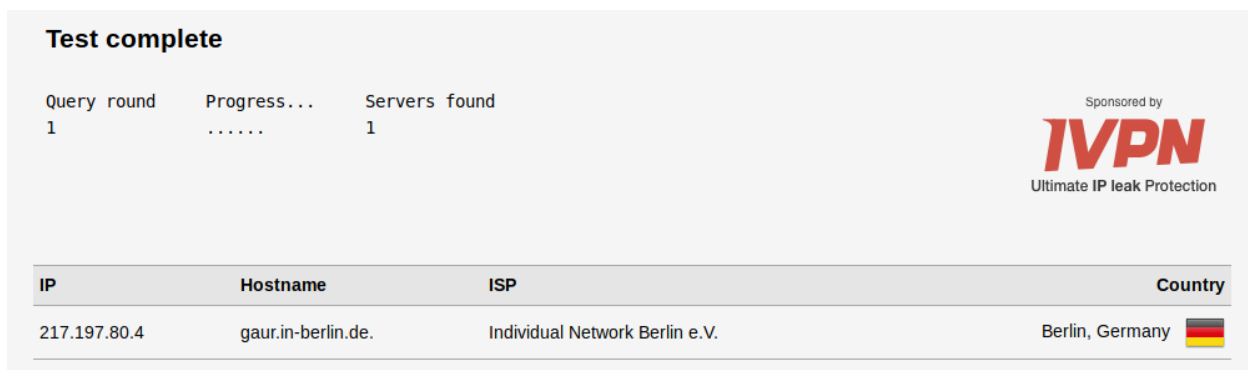
DNS servers: 10.152.152.10

You can now open your Kali browser and attempt to access the Internet. To see your assigned Tor IP address and your location, you can go to www.dnsleaktest.com to confirm you are using the Whonix Gateway.

My IP address and location are shown as being in the Netherlands.

My DNS server is in Berlin, Germany.

Looking good!

Summary –

In this lab, you learned how to work anonymously with Kali using the Whonix Gateway. Whonix uses the Tor network to ensure your data stays encapsulated. Though there is no 100% sure way to ensure complete anonymous browsing, the Whonix Gateway is about as close as we can get. When we add in a commercial VPN, we add in still another layer of anonymity.

End of the lab!