HACKER HOUSE

Hands-On Hacking™

Getting Started

Table of Contents

Introduction

Welcome to the Hands-On Hacking™ training course! This course has been developed to teach ethical hacking in a classroom environment, using real-world situations and scenarios. Our course has been developed from several decades of experience in real-world hacking and unlike many courses, does not teach solely through academic examples. We prefer to simulate real scenarios and systems as closely as possible to give you a taste of real-world hacking in a sandbox environment. This document details the necessary student setup that is required to progress through our hands-on labs. You will need to follow these instructions to configure your system to meet the course expectations. Follow this guide to setup our sample lab and begin your ethical hacking adventure with Hacker House!

Setup Requirements

You will need a computer (laptop) with at least the following technical specifications to complete our course. Please note that these specifications represent the **minimum requirements**:

- 2 or more CPU cores (Intel i3 and above recommended)
- At least 4gb of RAM.
- Approximately 40gb free hard disk space (you *may* be ok with less).
- VirtualBox installed (https://www.virtualbox.org/).
- Hacker House sample lab "**hh-mailserver-v1-i386.hybrid.iso**" downloaded (available from https://hacker.house/training/).
- Pen-testing distro ISO downloaded (we recommend Kali Linux: https://www.kali.org/downloads/).

If your computer meets the above specifications and you have all the necessary files, then you should be able to progress and begin our step-by-step configuration guide below. If your computer does not meet the minimum requirements, then consider finding another computer before attempting to take this course.
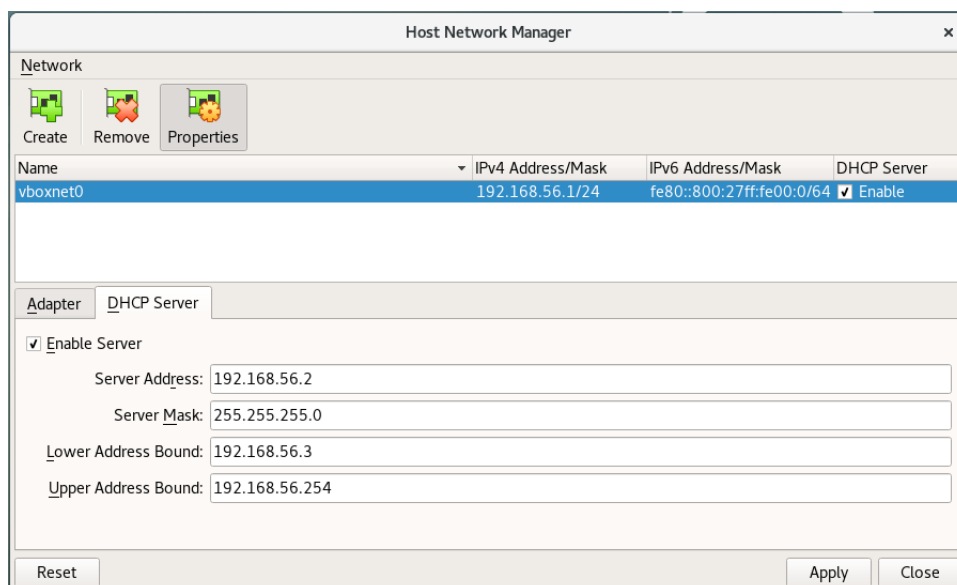
Virtual Machines

We will now show you how you can use your computer to run virtual machines. Your physical computer will *host* these machines (sometimes called guests). This approach allows you to run an entirely different operating system (OS) such as Linux, *within* your existing OS (e.g. Windows or MacOS). This means you can try new tools and techniques, without damaging your existing OS. The software we recommend for running virtual machines on our course, is called VirtualBox. Make sure you have downloaded and installed the correct version of VirtualBox (from https://www.virtualbox.org/) before proceeding.

VirtualBox Host-Only Networking

You will need to configure a host-only network in VirtualBox, an option that is not enabled by default. To enable host-only networking click on the "Host Network Manager…" option under "File" after starting VirtualBox. You should then select "Create" in the Host Network Manager dialog, as shown in the image below:
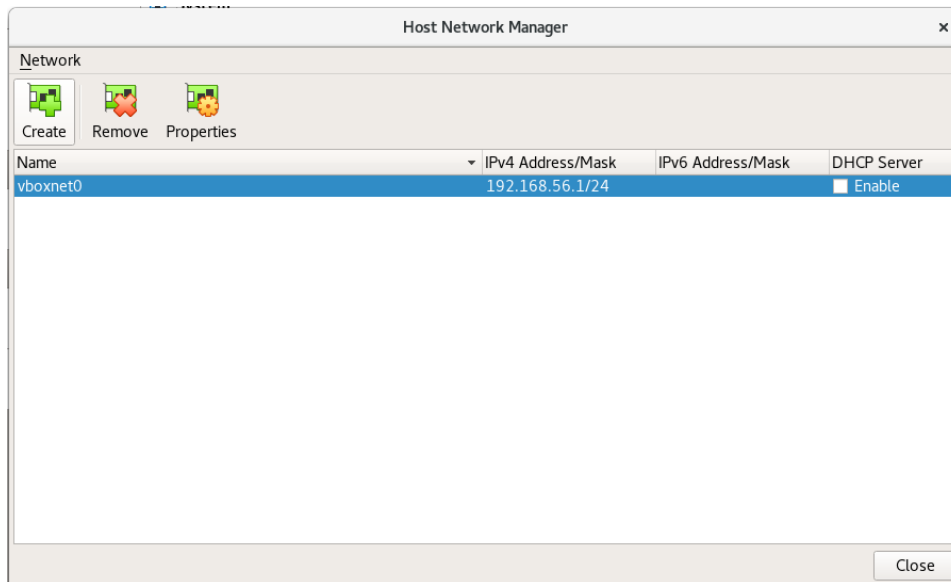

You should see a new network called "vboxnet0" appear. You will also need to make sure that the DHCP server for this network is enabled. With your new host-only network selected, click on "Properties". Select the "DHCP Server" tab, and then click the "Enable Server" check box. You can leave the other settings as they are. Click "Apply" and then "Close". You are now ready to begin the lab configuration.

Lab Configuration

You will need to create a new VirtualBox VM to make use of the provided mail server ISO image. Open VirtualBox and complete these steps to get the environment running:

1. From the drop-down "Machine" menu, select "New…".
2. Enter "Hacker House mailserver01" in the *Name* field.
3. The *Machine Folder* can be left as-is. This is where your VM's settings will be stored.
4. Select "Linux" from the *Type* drop-down menu.
5. *Version* should be set to "Linux 2.6 / 3.x / 4.x (32-bit)"
6. *Memory size* should be set to **at least 1024MB**
7. **Do not add a virtual hard disk**
8. Click "Create".
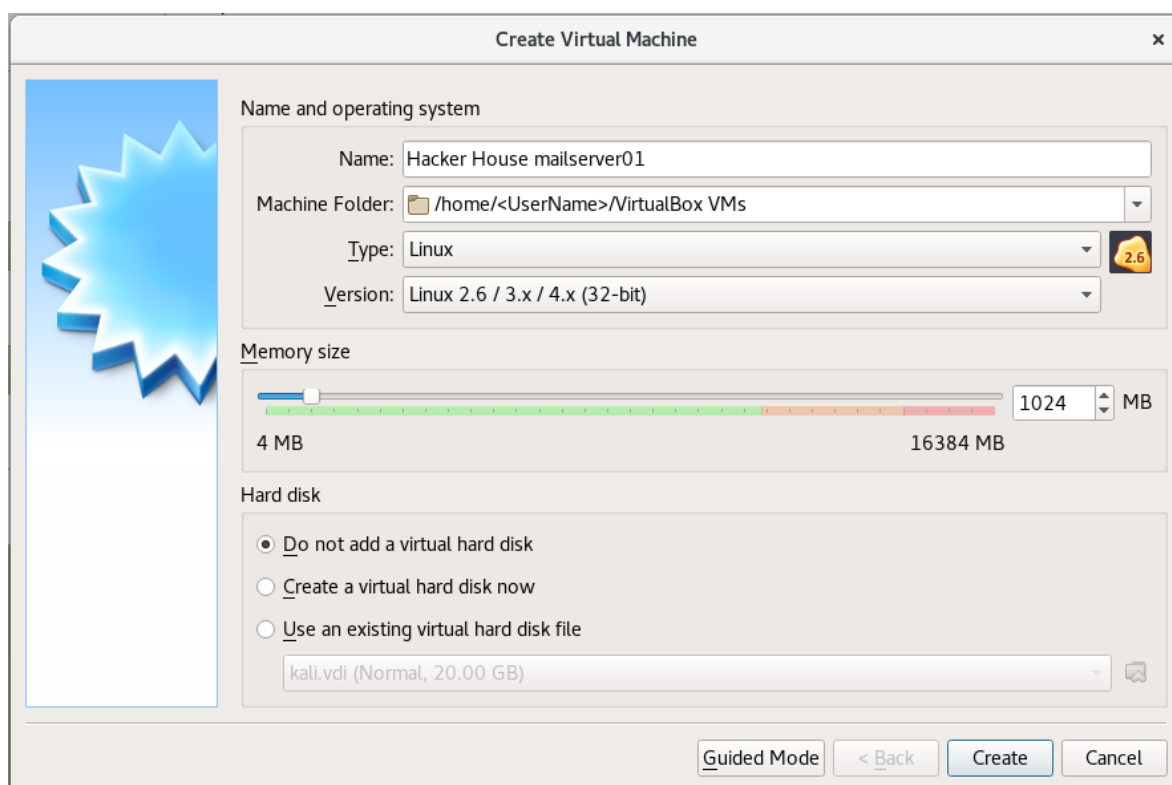
Right-click on your new "Hacker House mailserver01" VM from VirtualBox's main screen and then click "Settings…". Click on "Storage" on the left, and then click on the CD icon next to the "Optical Drive:" menu. You will then be able to add the mail server ISO (**hh-mailserver-v1-i386.hybrid.iso**) by selecting "Choose Virtual Optical Disk File…" from the drop-down menu. The image below shows what the Settings dialog should look like, once the ISO has been added. Do not click OK, as we still need to configure networking.
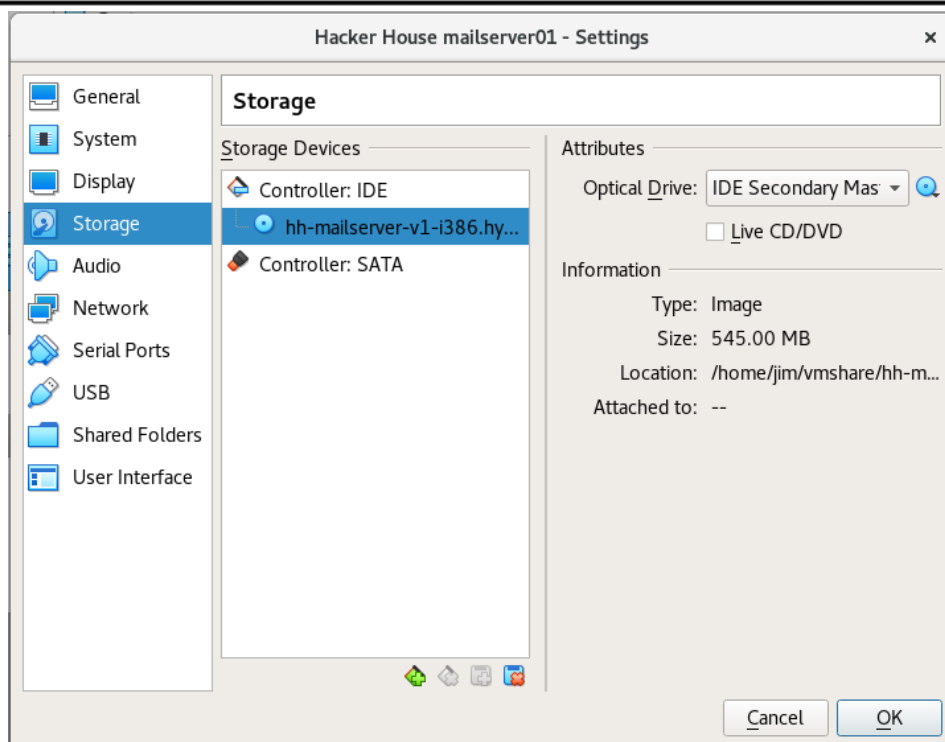
Use the menu on the left to select "Network". Set "Adapter 1" to be *attached to* "Host-only Adapter", this ensures the VirtualBox host can only talk to your computer and not the Internet or your local network. Click "OK" to save changes.
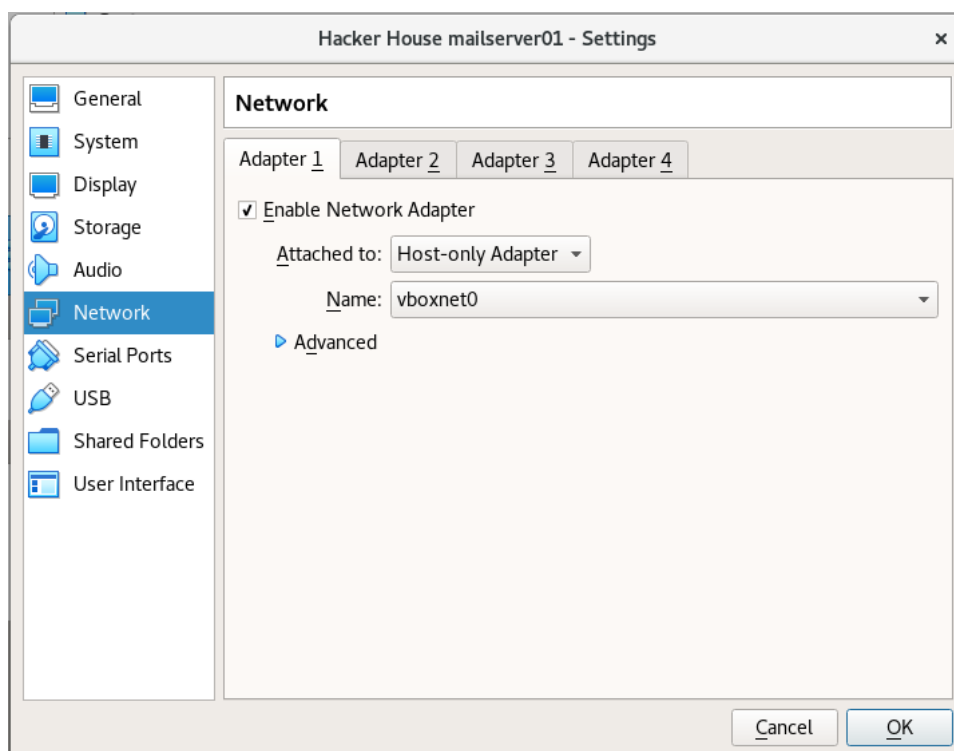
WARNING: Hacker House labs are intentionally designed to be insecure and vulnerable to hacking. It is strongly advised they are never connected to a live network unless you are completely sure of your actions.

You can start your new VM by right-clicking on it, and then selecting "Start" from the drop-down menu. After the machine boots up, you will be welcomed with a screen similar to the one shown below. Make a note of the IP address underneath "This host can be found on:" - You will need it later. In this case, the IP address is 192.168.56.4.
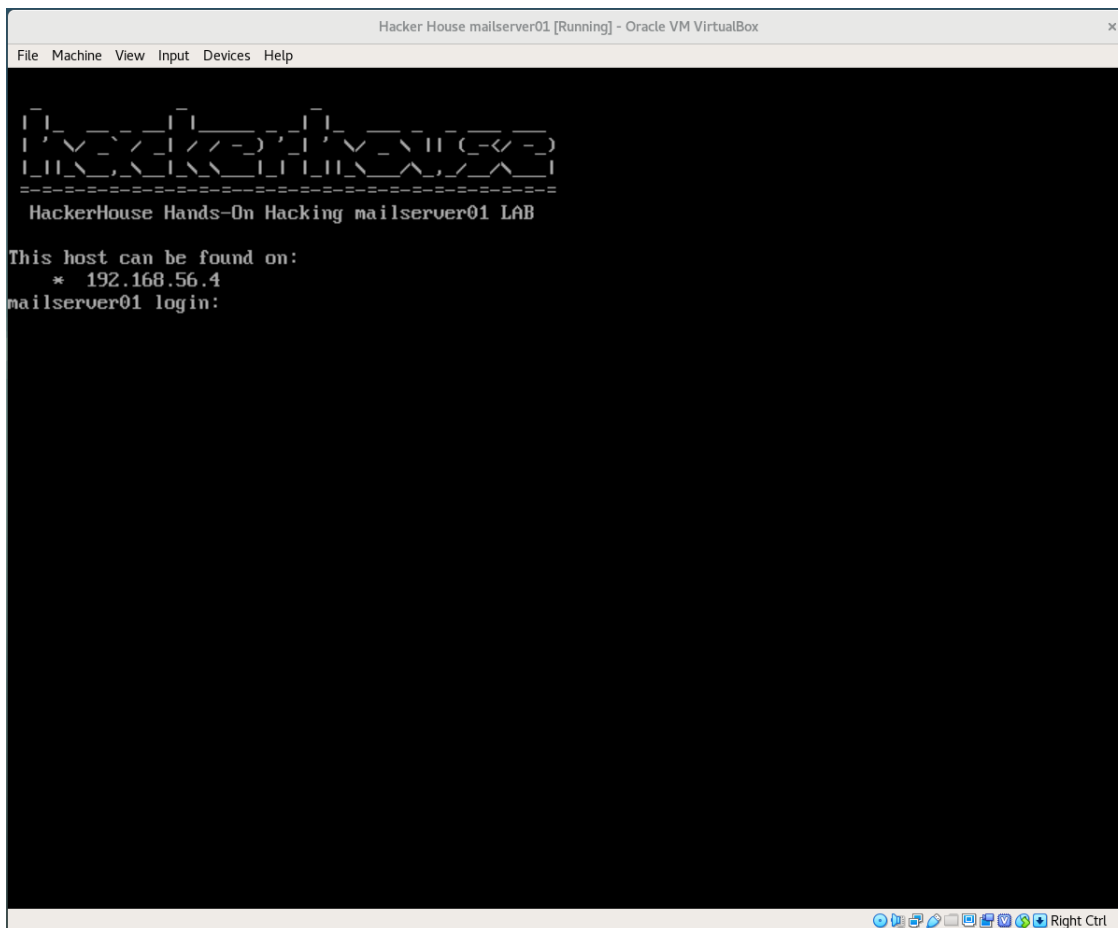

If you did not see the message above on successful boot, go back and review your configuration to ensure you have met the minimum requirements and that you followed the instructions correctly. If you do not have an IP address in the console, try pressing return a couple of times as DHCP can sometimes be delayed. If you still do not see an IP address, make sure that the DHCP server for your host-only network is enabled. Congratulations if you made it this far, the lab is ready for use!

Pen-Test VM Configuration

We now need to create a pen-test VM using a downloaded ISO (Kali Linux or equivalent). This machine will be used to work through the example attacks. There are plenty of guides online for installing a virtual machine for persistent use and we advise you create such a setup using as many CPU cores and memory as possible. For now, we will keep things simple and show you how to setup a minimal environment for training use. Complete these steps to get the environment running:

1. Open VirtualBox and from the drop-down "Machine" menu select "New…".
2. Enter "Kali Linux" in the *Name* field.
3. Leave the *Machine Folder* as it is.
4. Select "Linux" from the *Type* drop down menu.
5. *Version* should be set to "Linux 2.6 / 3.x / 4.x (64-bit)".
6. *Memory size* should be set to at least 1024MB, the more the better.
7. **Do not add a virtual hard disk.**
8. Click "Create".
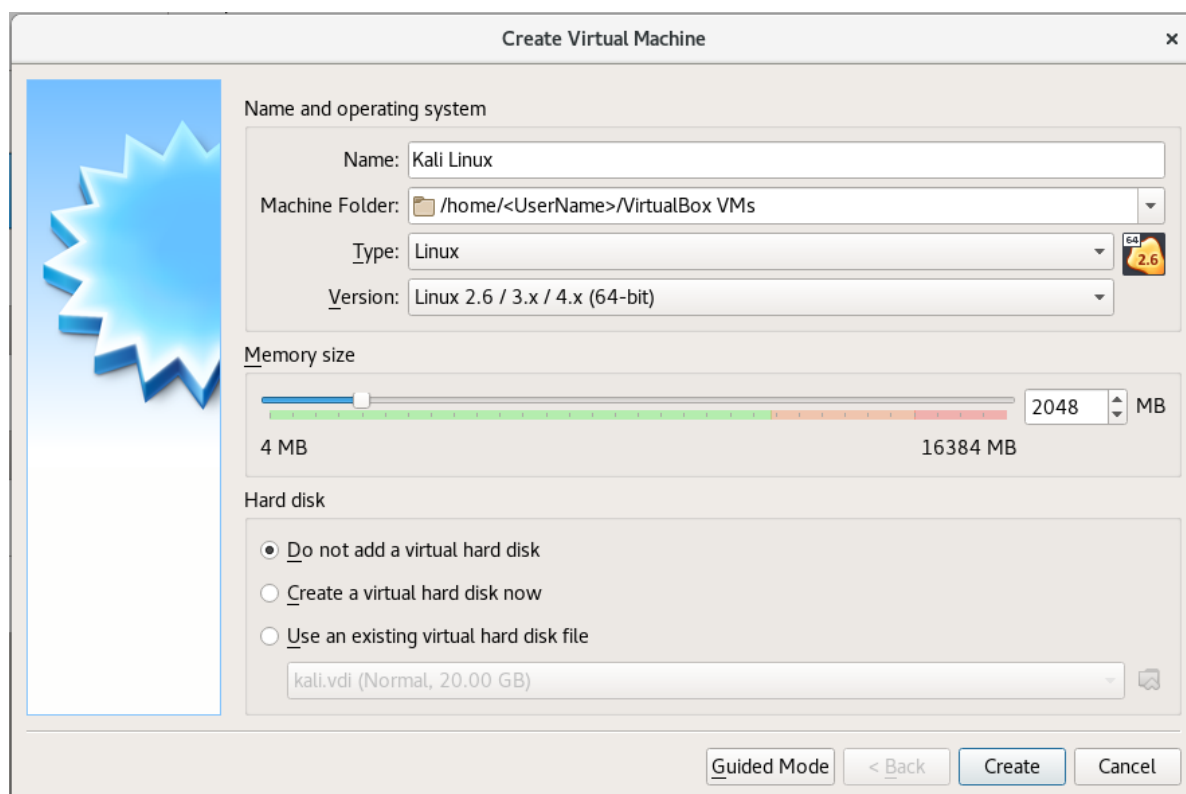
Right-click on your newly created "Kali Linux" VM from the VirtualBox main screen, and then click "Settings…". You now need to add the "**kali-linux-2019.1a-amd64.iso**" file (or a more up-to-date ISO) to the machine's virtual CD drive. Click on "Storage", on the left of the Settings dialog, and then click on the CD icon next to the "Optical Drive:" menu. You will then be able to add the ISO by selecting

"Choose Virtual Optical Disk File…" from the drop-down menu. Do not click "OK" yet; we still need to configure networking.
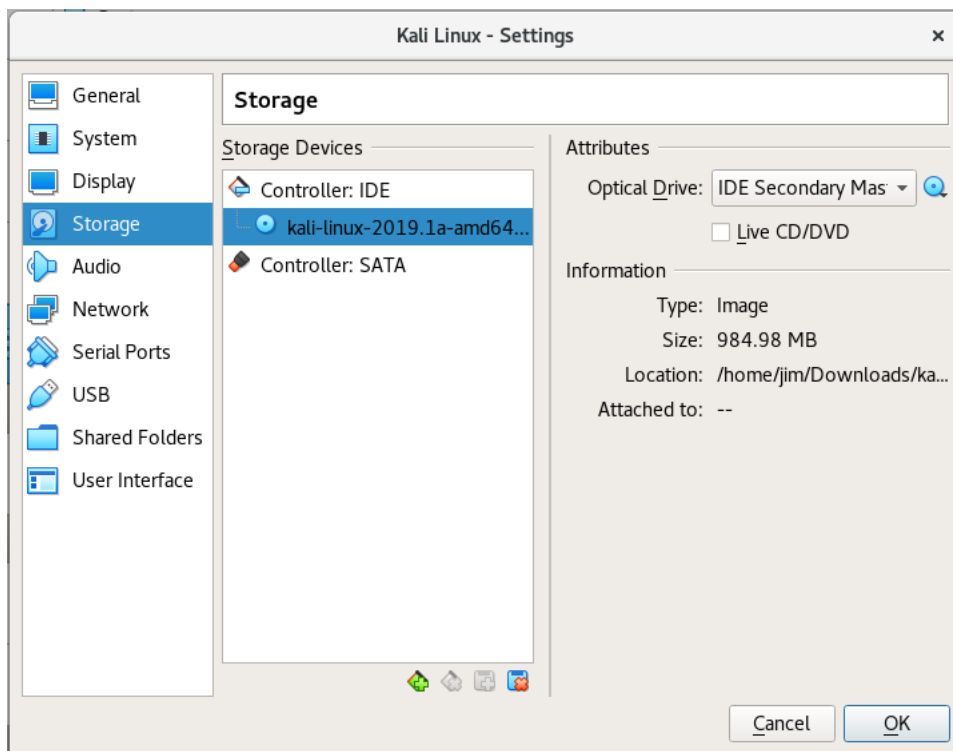
Use the menu on the left to select "Network". Set "Adapter 1" to either "NAT" (the default) or "Bridged Adapter".
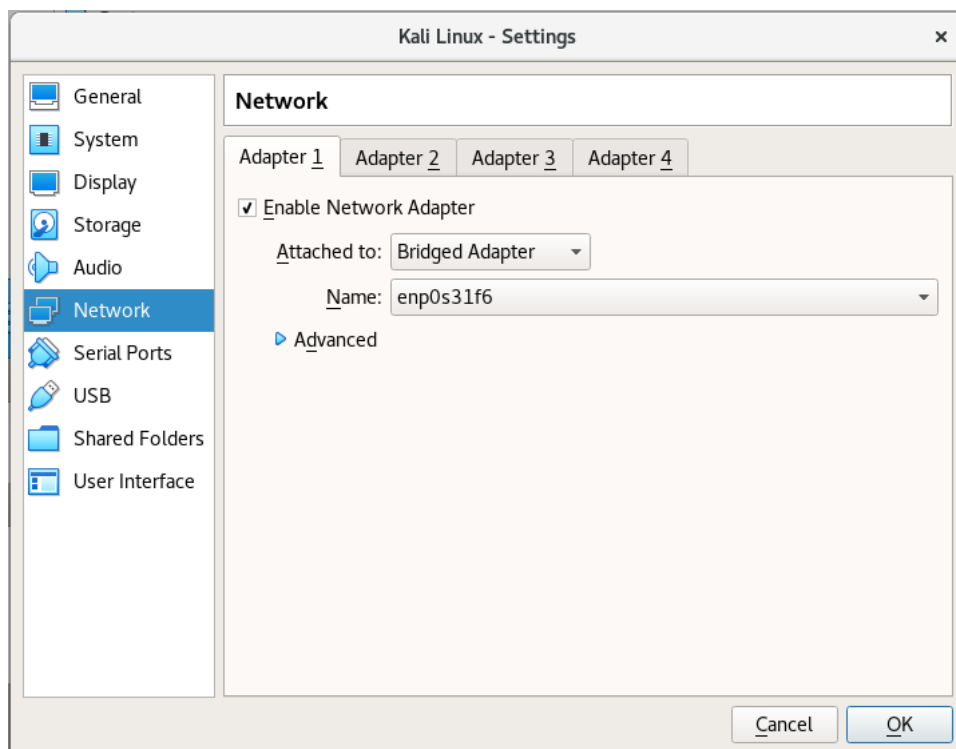
If using "Bridged Adapter" you are able to set which host network interface the VM will use, e.g. your Wi-Fi adapter. Set "Adapter 2" to be enabled and select "Host-only Adapter". This allows your pen test VM to be dual-homed, giving it Internet access if required, as well as a connection to the host-only network you created. The mail server will be accessible to your Kali Linux VM using this host-only network. Make sure you click "OK" to save the changes you've made.
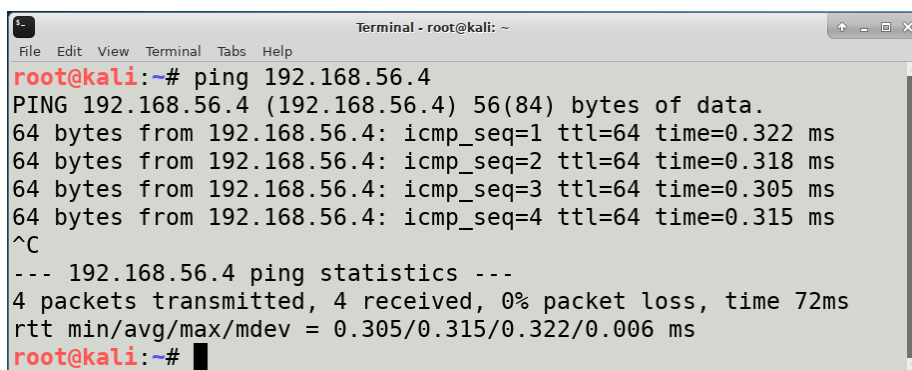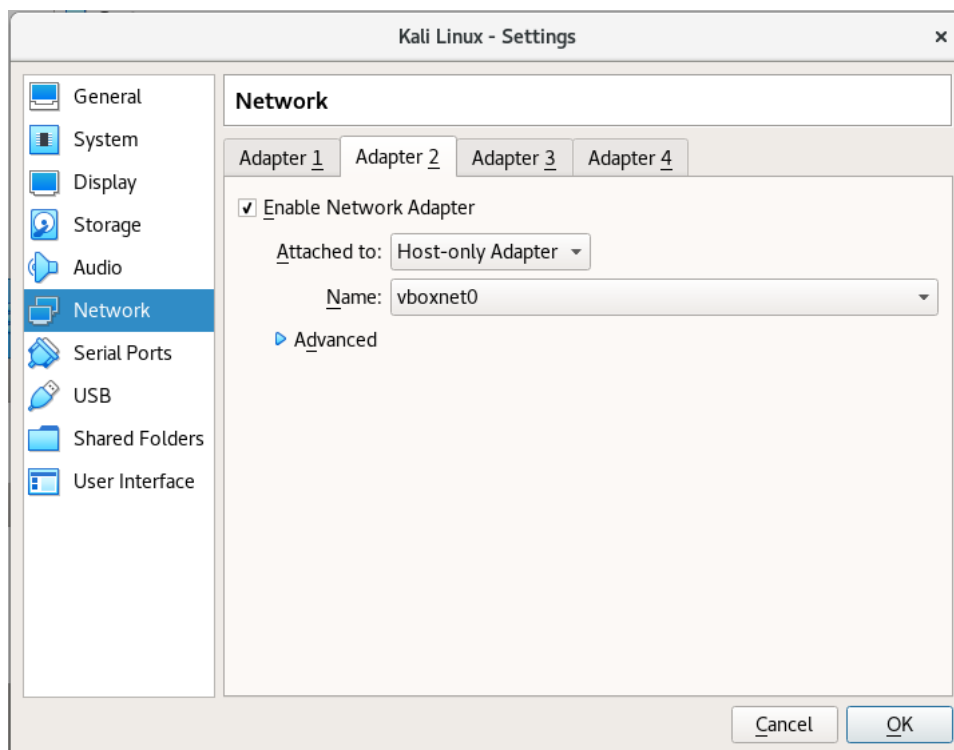
From VirtualBox's main screen you, you can right-click on your "Kali Linux" VM and choose "Start" from the menu. From the Kali Linux boot menu, select the "Live" option (highlighted by default). After the machine boots up you will be presented with a login screen. You can login in with "root" as the username, and "toor" as the password. After logging in, you will see the Kali Linux default desktop.

Example Test

Providing you configured both VirtualBox instances correctly, you should now have a simulated mail server running, with a network connection to your penetration testing platform (Kali Linux). You can now perform a simple test to ensure that both hosts can communicate with each other correctly. From your "Kali Linux" VM, perform the following steps:

1. Open up a terminal
2. Type "ping" at the prompt, followed by the IP address of your "Hacker House mailserver01" VM and hit enter on your keyboard.
   a. Using the example IP from earlier, this command would be: "ping 192.168.56.4"
3. You should see output from the ping command, similar to that shown in the image below.
4. Use Ctrl+C on your keyboard to cancel the ping command after a few seconds.

If you do not see responses from the mail server VM, then go back and validate that both VMs' network settings are correctly configured. Make sure that the mail server is running, and that you have used the correct IP address too.

If you did see replies from the mail server VM (note the "4 packets transmitted, 4 received" text in the output shown above) then you are ready to begin hacking! Try running Nmap from the terminal, with the same IP address you've just used, for example "nmap 192.168.56.4". If after waiting a little while, you see a list of open ports like those shown in the image below, then you have successfully port scanned your virtual mail server!

```
                          Terminal - root@kali: ~                        ⬦ ‒ ☐ ☓
File  Edit  View  Terminal  Tabs  Help
root@kali:~# nmap 192.168.56.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-11 12:02 BST
Nmap scan report for 192.168.56.4
Host is up (0.000082s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
9/tcp    open  discard
21/tcp   open  ftp
25/tcp   open  smtp
37/tcp   open  time
79/tcp   open  finger
80/tcp   open  http
110/tcp  open  pop3
113/tcp  open  ident
143/tcp  open  imap
443/tcp  open  https
993/tcp  open  imaps
995/tcp  open  pop3s
MAC Address: 08:00:27:A6:8F:BF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
root@kali:~# ▮
```

If you do not see a list of open ports or you're experiencing other difficulties, ensure that you do not have any security software running (such as a firewall or anti-virus product) that is interfering with the connection between your Kali Linux VM and your mail server VM. Make sure that the ping command worked, before attempting this Nmap scan.

Ready

If you followed all the steps in this guide correctly, and successfully completed the "Example Test" section, you are ready to begin! Watch and work through the sample video on the Hacker House website. You will find a link to this video at: https://hacker.house/training. The video will show you how we teach this course - through practical demonstrations that you can repeat yourself with the provided virtual machines. Most modules have their very own VM, so there is plenty to explore beyond the mail server!

Before attending our training, whether that's in a real classroom, or our virtual classroom, ensure that you were able to complete the steps in this "Getting Started" guide. You should have successfully set up the mail server VM, and a Kali Linux VM. Your computer's hardware should be comfortable running these machines at the same time. If you have any concerns, or want more information about the steps in this guide, or any aspect of our training, please do not hesitate to contact us (see our web site, https://hacker.house for the most up-to-date contact information).

Thank you for expressing an interest in our Hands-On Hacking™ training course. We hope to see you in one of our classes, or in our online student forum soon. Hack the planet!