

# Introduction to Virtualisation

## Overview

Virtualisation enables multiple guest operating systems to simultaneously run on the same physical hardware. Modern processors have virtualisation extensions to support this and work better than older processors that run entirely software based virtualisation.

Hypervisors facilitate virtualisation, type 1 or bare metal hypervisors are operating system based and designed purely to run virtual machines.

Type 2 hypervisors are applications that are installed on existing operating systems (Windows, Linux) enabling guest operating systems to run in virtual machines on the host.

## Aims & Objectives

- Create a pair of virtual machines and virtual network, explain what virtualisation is and how it may be used in a business setting.
- Recognise the importance of network segregation to avoid breach of policy when operating penetration testing tools

## Acronyms

OS – Operating system

VM – Virtual Machine

Host – Machine running the hypervisor

Guest – VM running on the hypervisor/host

GUI – Graphical User Interface

ICMP – Internet Control Management Protocol

IP – Internet Protocol

TTL – Time to Live

## Important Note

Fully document each of the tasks you carry out, this will make the assessment easier as you will be able to refer to the notes you have made. **You must complete the disclaimer before undertaking this exercise. The University machines have VirtualBox installed, you may install and configure VirtualBox on your own computer. However, it is your responsibility to setup and maintain such a setup. The lab sessions and support sessions provide ample time for the collection of evidence for use in your assignment.**

## Tips

Virtualisation is a powerful tool employed by businesses and cloud computing providers. However, from experience type 2 hypervisors can be unstable. Therefore, it is best to document your work using the host OS and screen captures from the guest. It also helps to keep note of any commands you have issued in a text file, so that you can recreate a process quickly should your VM crash or become corrupt.

If your Virtual Machines become corrupt you can delete the them (and all the settings), by **closing VirtualBox** and deleting the following directories via the terminal:

```
rm -r ~/.config/VirtualBox/*
```

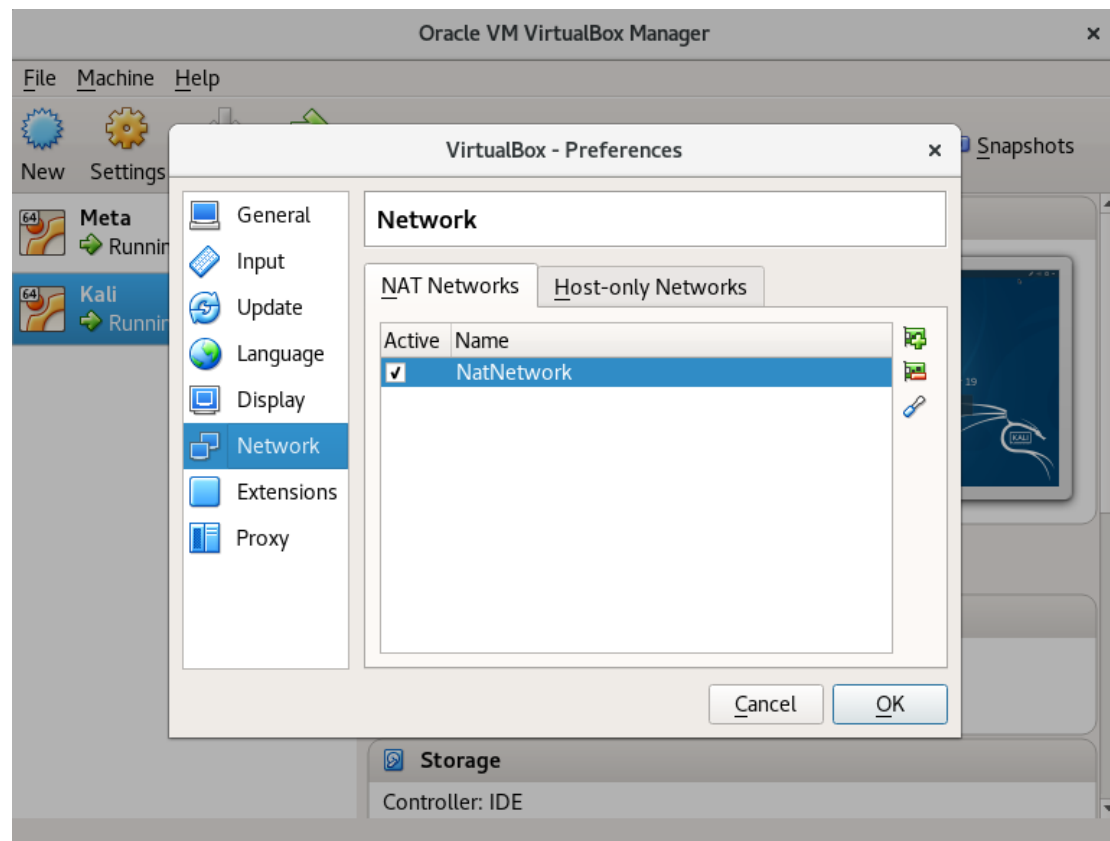
```
rm -r ~/VirtualBox\ VMs/
```

Be aware this will delete all virtual machines and VirtualBox settings.

## Task 1 – Setting Up a Virtual Machine

Virtualisation is widely used in business and teaching environments. It enables the creation of virtual machines and networks which can be connected to or separated from other networks. This is crucial when learning security techniques, which may damage or degrade networks and systems in a business environment. The coursework for this unit requires you to deploy a virtualised network. The guide below describes how to do this.

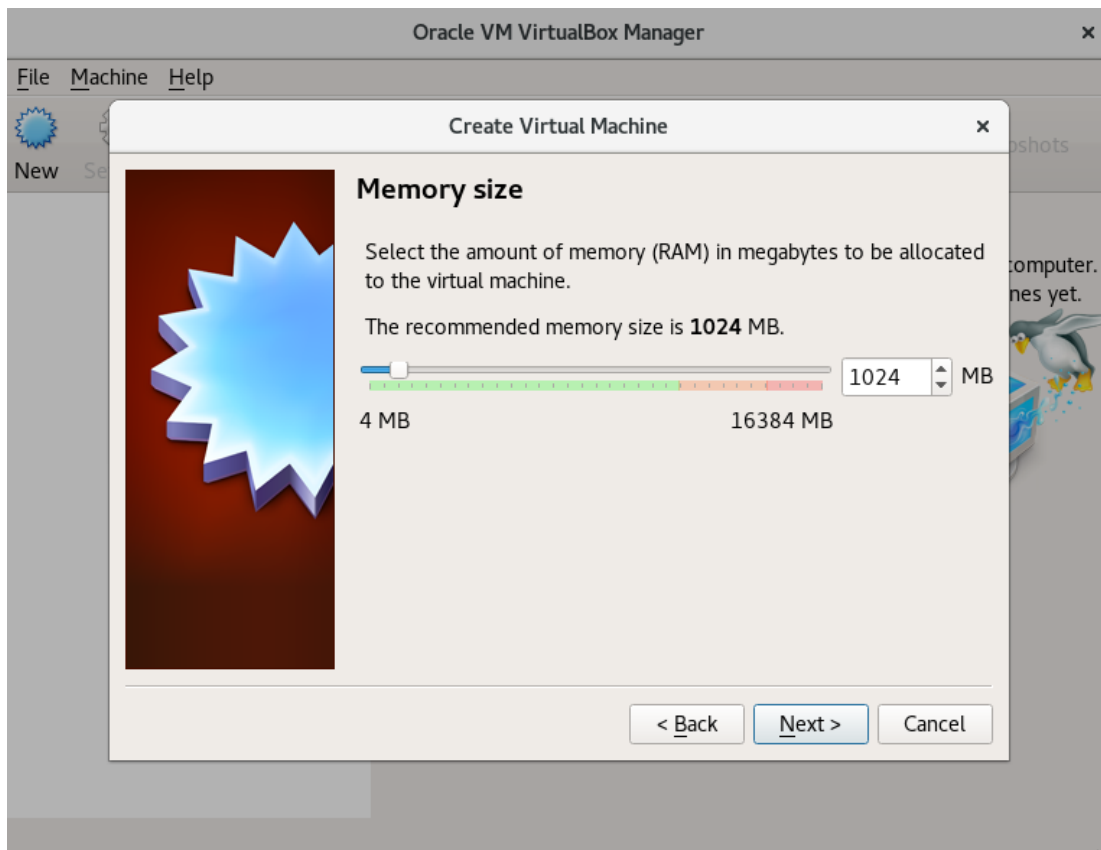
1. Open VirtualBox from the Ubuntu Activities menu (NB: you may need to search) and add the NAT network (“NatNetwork”) under the File > Preferences menu:



2. Create a New virtual machine named Meta, of type Linux, version Ubuntu (64-Bit):



3. Allocate 1GB memory to the virtual machine:

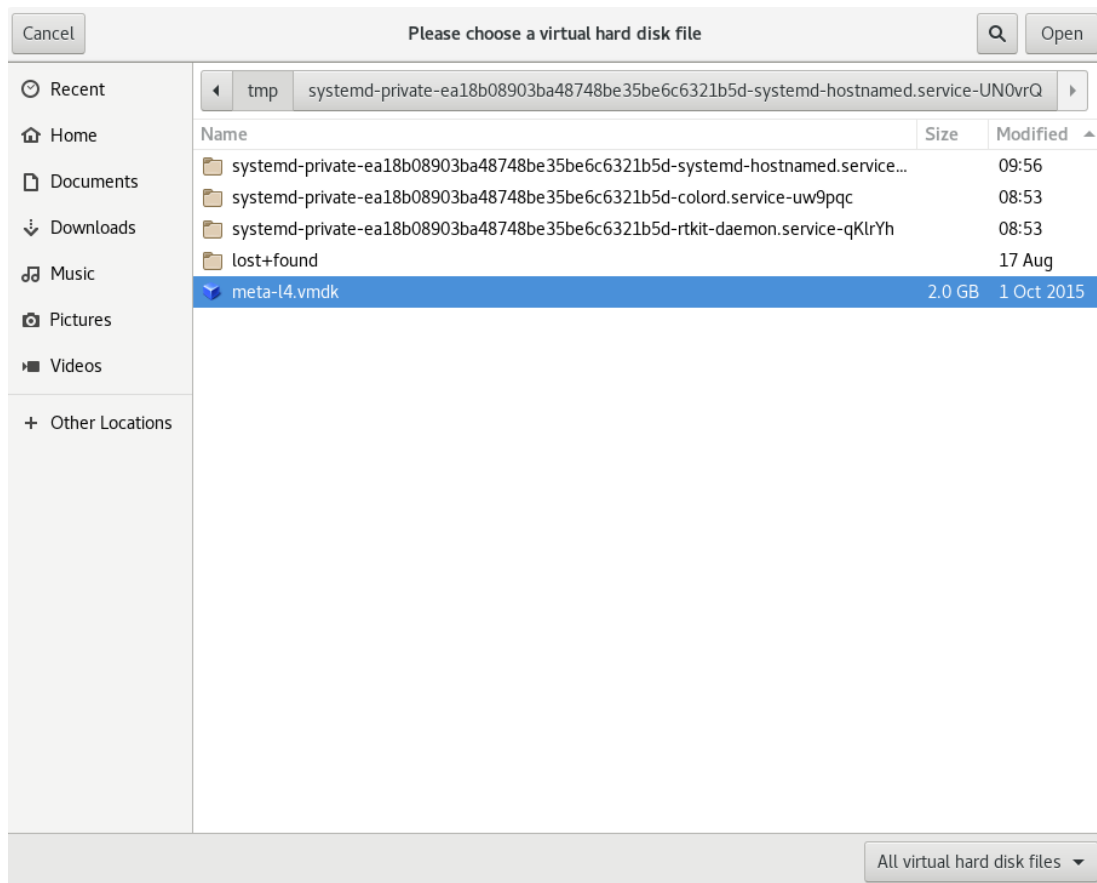


Click Next

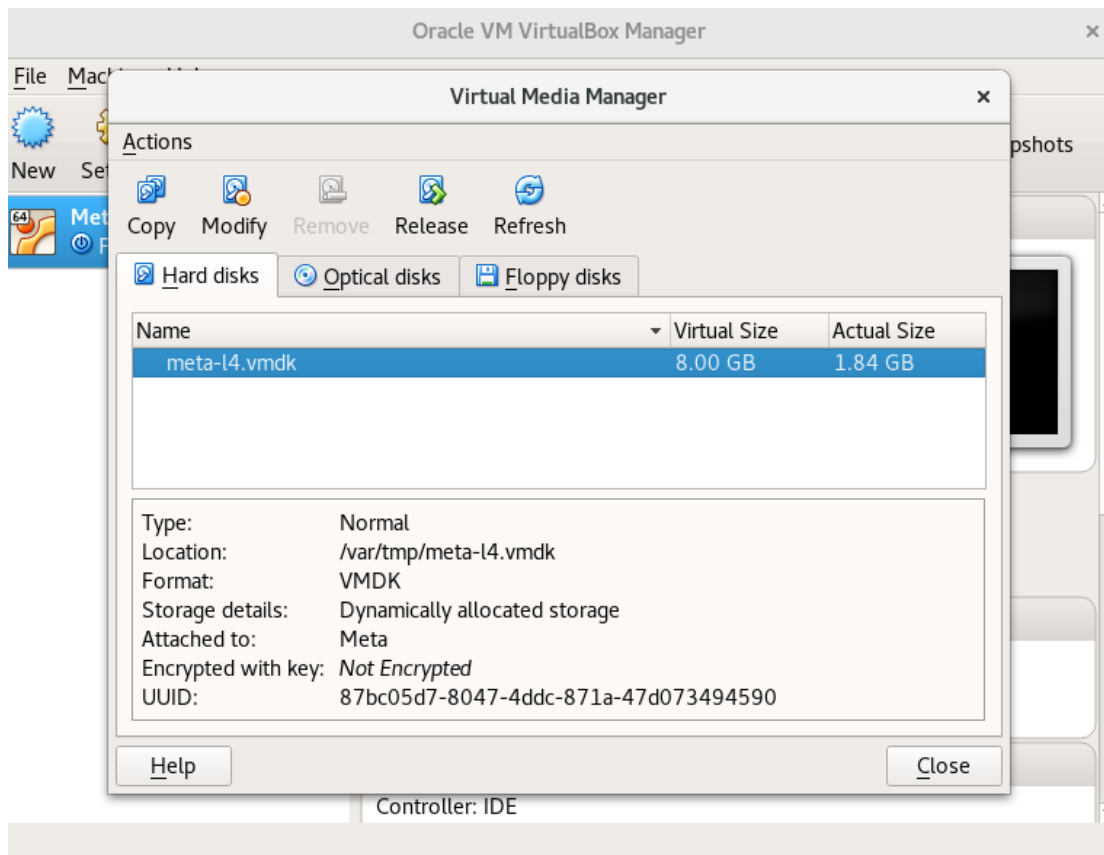
4. Select use an existing virtual hard disk file:



5. Navigate to Other Locations > Computer /var/tmp and select ('Open') the Meta-l4.vmdk file and create a new Virtual Machine instance:

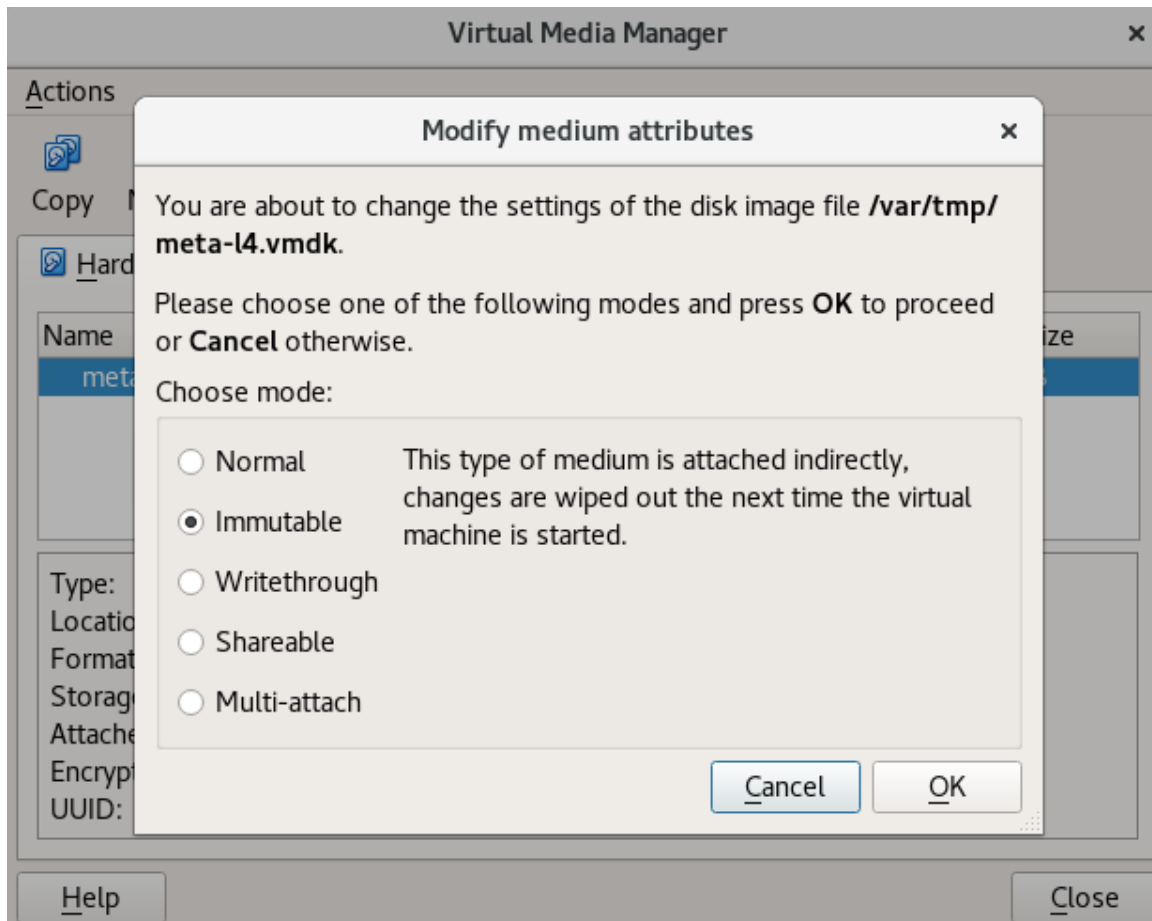


6. Select Virtual Media Manager from the File menu:

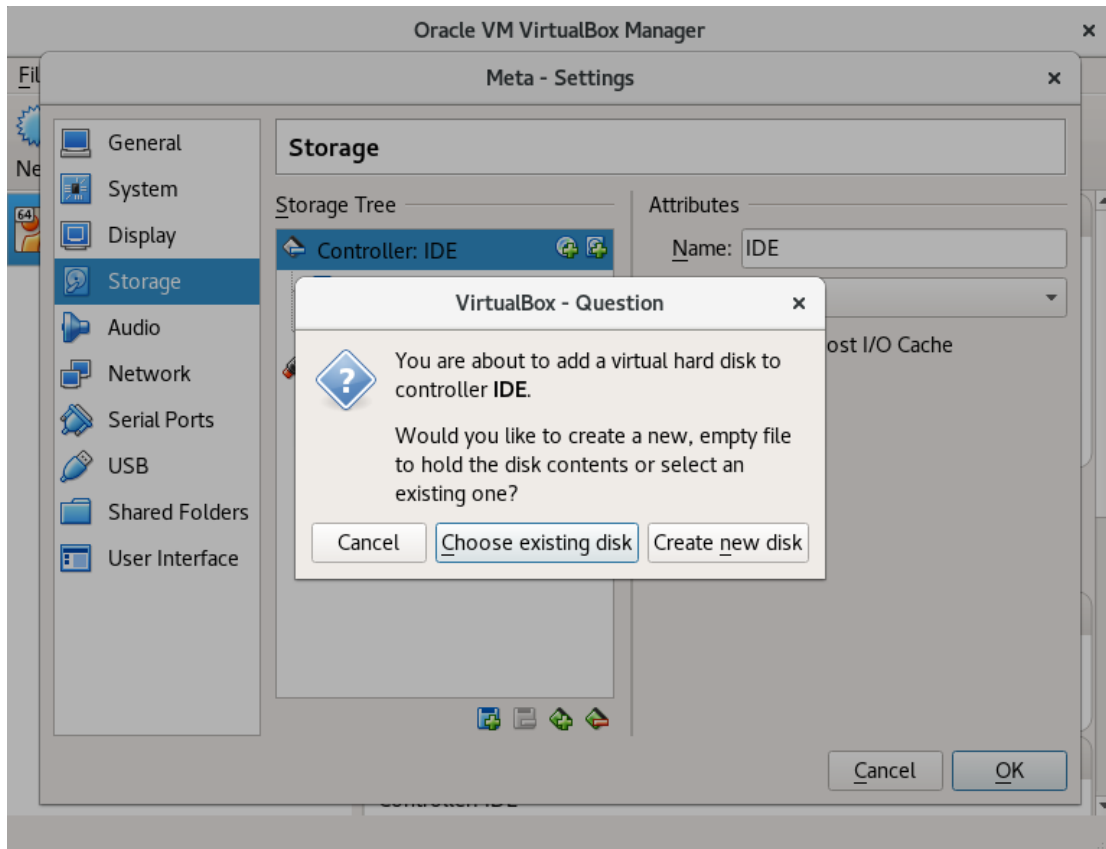




7. Release the disk, then Modify the disk to make it immutable:

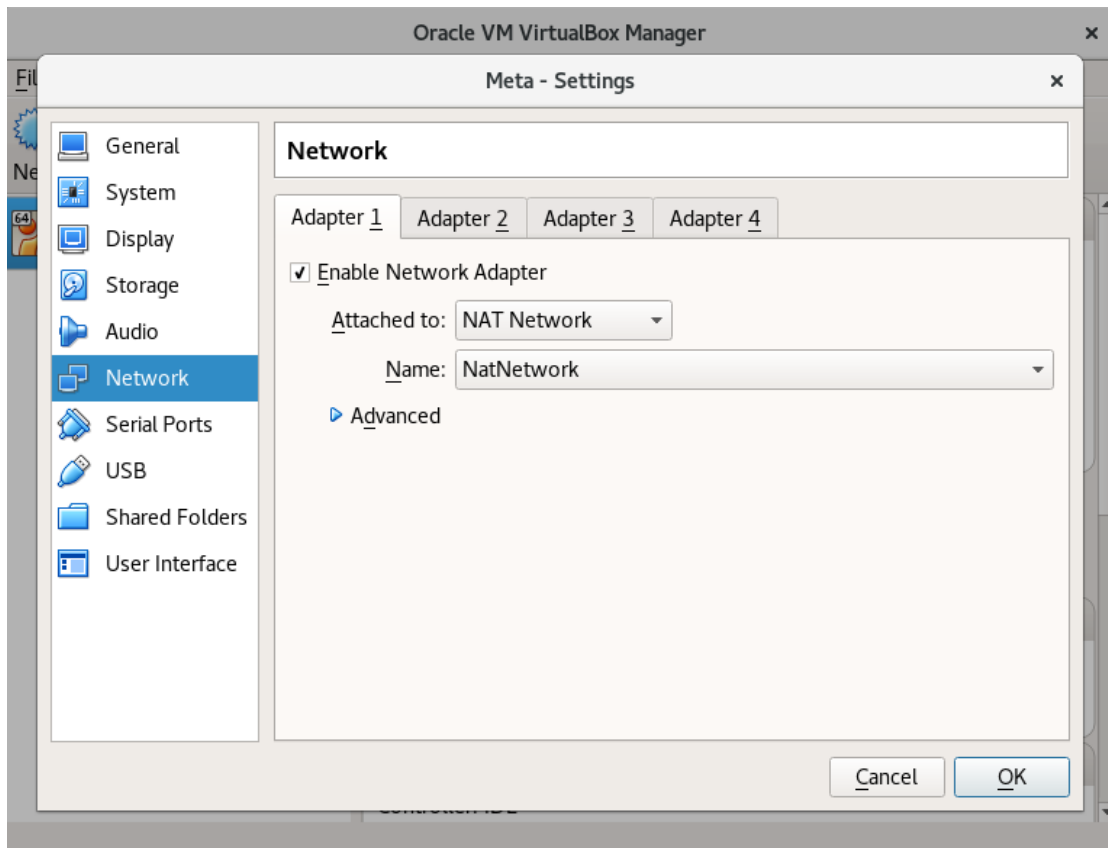


- Under the Settings menu for the Meta virtual machine, select Storage, and click on the icon "IDE" and select "Choose existing disk" and select `/var/tmp/Meta-l4.vmdk`:

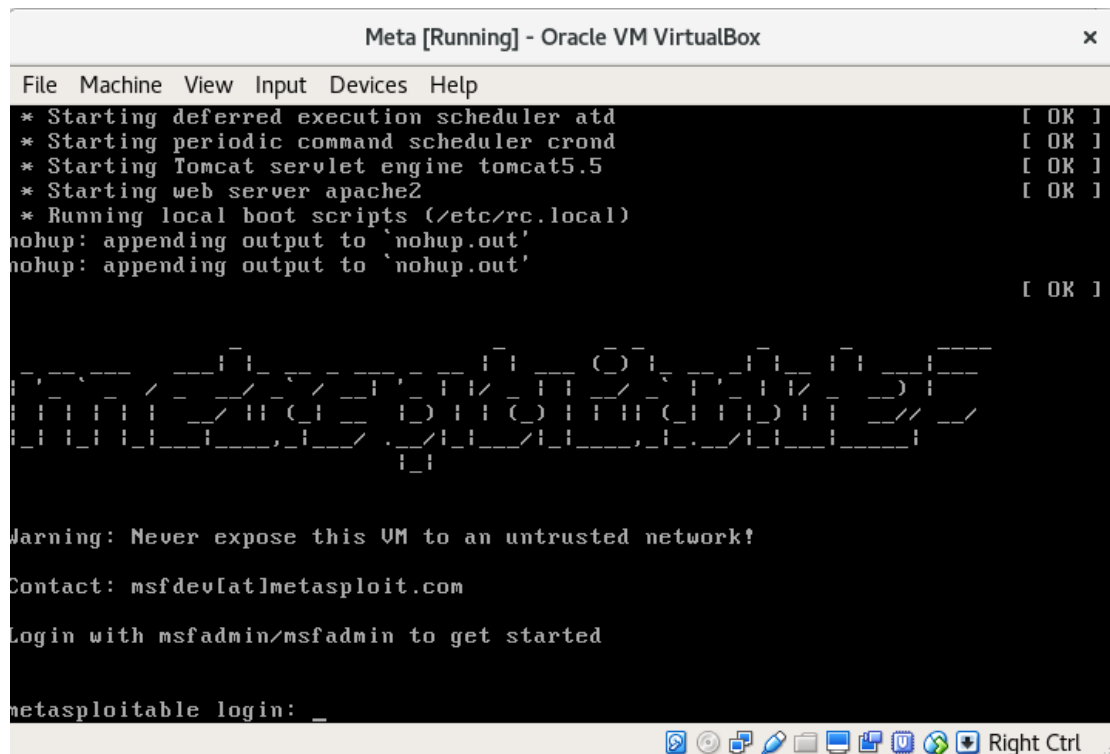


Note this step may seem to be a repeat of an earlier step, however it is necessary as the virtual machine images used at MMU are immutable.

9. Under the Meta virtual machine Settings window, change the Network settings so your virtual machine is attached on Adapter 1 to Nat Network: NatNetwork:



10. Once all these tasks are completed, select OK, then Start your newly created Meta virtual machine:



11. Login using `msfadmin` as the username and password. If your mouse pointer gets trapped in the Virtual Machine, hold the right control key on the keyboard.
12. Configure the system to use the UK keyboard using the following command:

```
sudo loadkeys gb
```
13. Check the IP address of the Virtual Machine using the `ifconfig` command.

## Task 2 – Deploying Kali

To assess the Metasploitable virtual machine for vulnerabilities we will be using Kali Linux in the coming weeks. This task explains how to deploy Kali Linux, a security testing Linux distribution.

1. Create a Virtual Machine named Kali, type Linux, version Ubuntu (64-bit)



**Create Virtual Machine** [X]

**Name and operating system**

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.


Name:

Type:  

Version:

2. Allocate 4GB memory to the Virtual Machine:

Create Virtual Machine



### Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **1024 MB**.

4096

MB

4 MB16384 MB

< Back

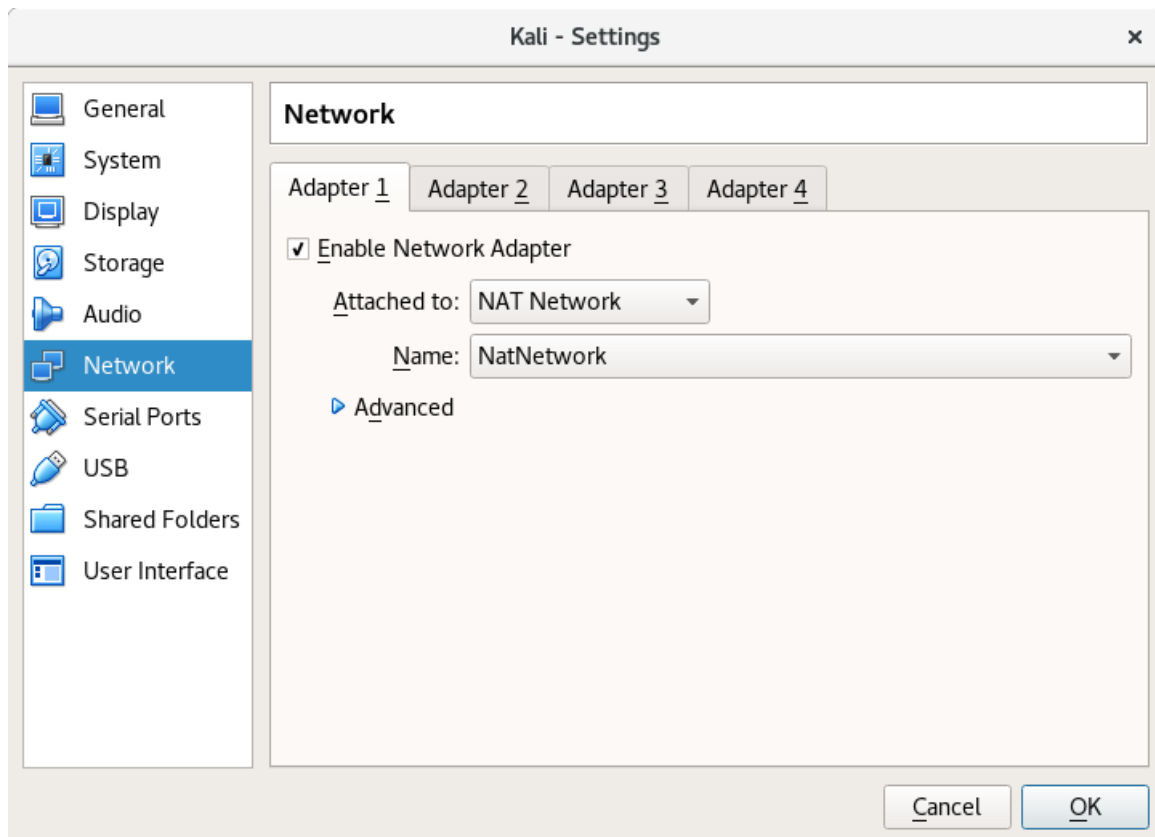
Next >

Cancel

3. Do not add a virtual hard disk, select Continue at the warning pop up:

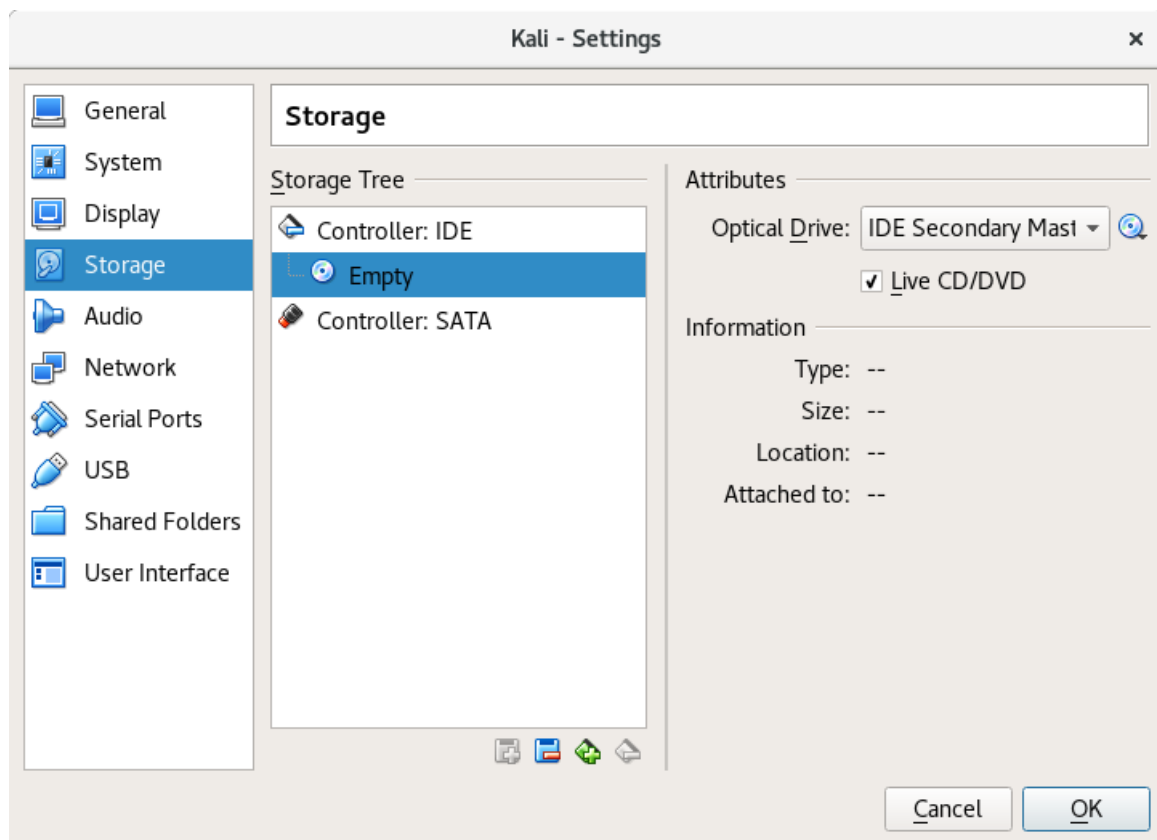


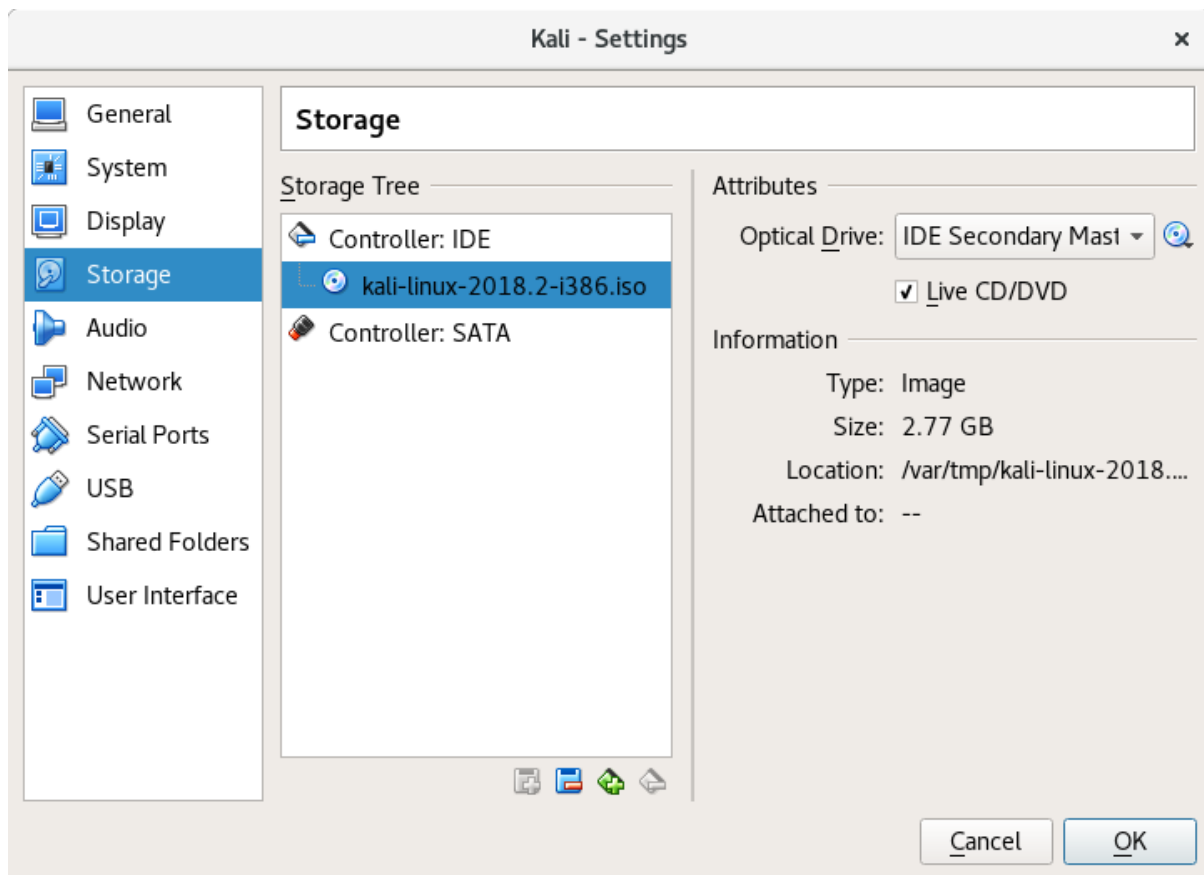
4. Under the settings for the new Kali virtual machine configure the network as before:



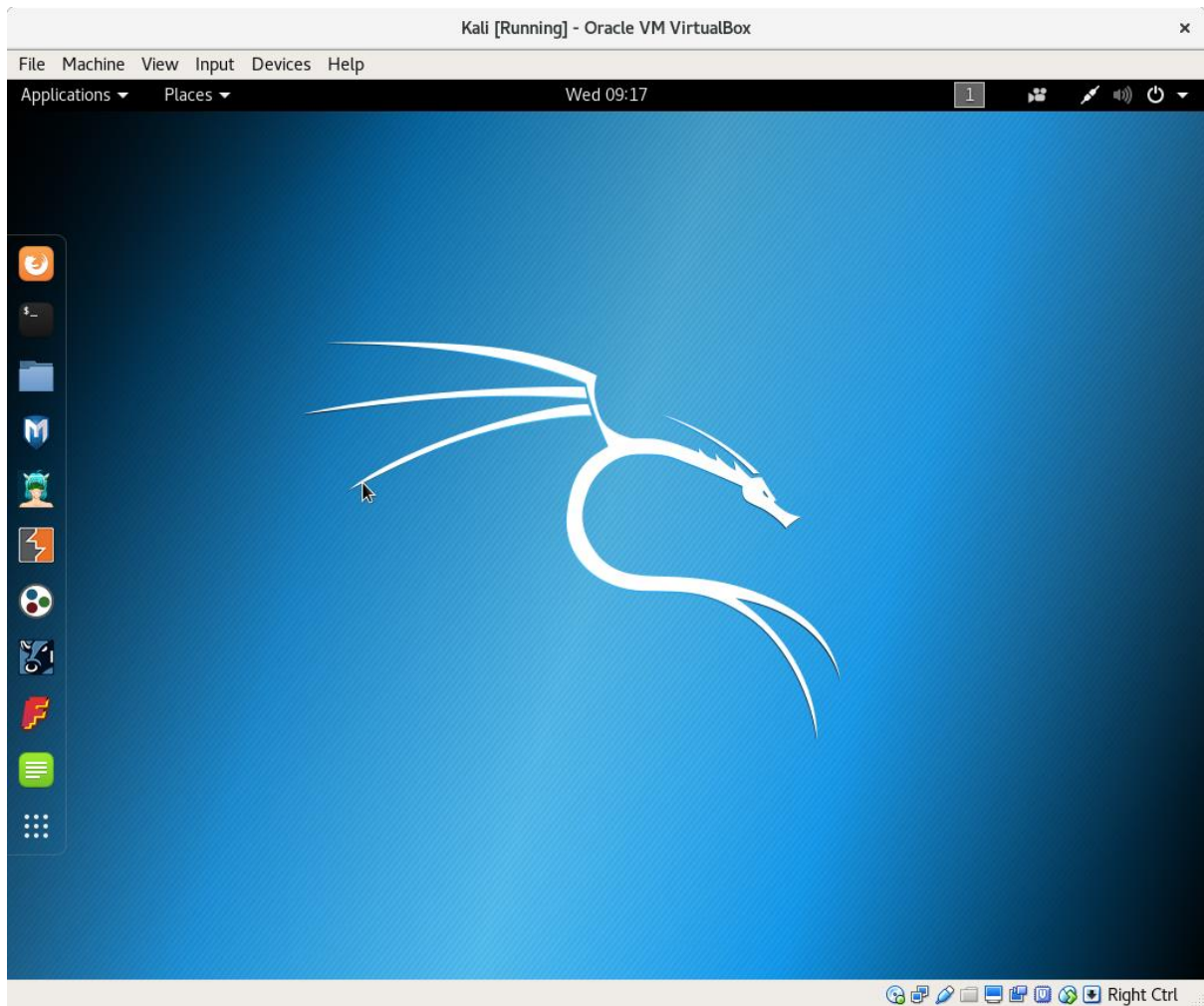


5. In the Storage settings, select Empty, select the Live CD/DVD checkbox, and then click on the righthand CD icon and the Choose Virtual Optical Disk File at `/var/tmp/kali-linux-2018.2-i386.iso`:





6. Start the Kali virtual machine, and select the first item on the bootloader menu by pressing enter. Select to Capture your mouse. If your Kali session times out, the password to login is **toor**.



7. Configure the keyboard mapping for Kali by opening the terminal and using the following command:

```
setxkbmap gb
```

### Task 3 – Check Network Reachability

Check both the virtual machines can reach each other;

From Kali ping the IP address of the Metasploitable virtual machine.

From Metasploitable ping the IP address of the Kali virtual machine.

### Task 4 – Virtualisation and the Cloud

Explore the virtual machines you have deployed and consider how virtualisation may be used in a business environment. Research the link between virtualisation and cloud computing, consider the advantages virtualisation/cloud computing bring to a business and document your findings.

## Task 5 – Computer Misuse Act 1990

Review the computer misuse from the link below, paying attention to the Computer Misuse Offenses.

<http://www.legislation.gov.uk/ukpga/1990/18/contents>

Consider how the use of virtualisation will prevent accidental contravention of the Computer Misuse Act while using penetration testing tools. Document your answer as it is relevant to the coursework.

## Extended Task / Homework

Deploy VirtualBox on your home computer or laptop (See download on moodle), download the OVA file from Moodle and deploy the Metasploitable virtual machine. The OVA will automatically unpack itself if you double click on the file. You should adjust the settings to those used in the lab with the exception of the networks setting, which should be set to **host-only networking**.