In this unit, hands-on labs and assignments will be conducted on a dedicated virtual machine image. You are strongly suggested to follow the guidelines to setup your own hands-on environment before doing your assignments and labs. The environment includes the virtual machine software, e.g., VirtualBox and Linux (Ubuntu), with which you can work on the assignments and labs using your own personal computers. Getting familiar with them is critical.

If you have a MacBook with an Apple Silicon chip, a separate document is available in Moodle for **Task 1 - VM Setup.** To check whether your MacBook has a Apple Silicon chip follow **these steps.**

1 VM Setup

Host Operating System: Lab setup will work on Windows, macOS (Intel) or Linux host operating systems.

Guest Operating System:
A pre-built Ubuntu VM appliance (OVA) (FIT-NetworkSecurity 5.5GB) can be downloaded from **this link.**

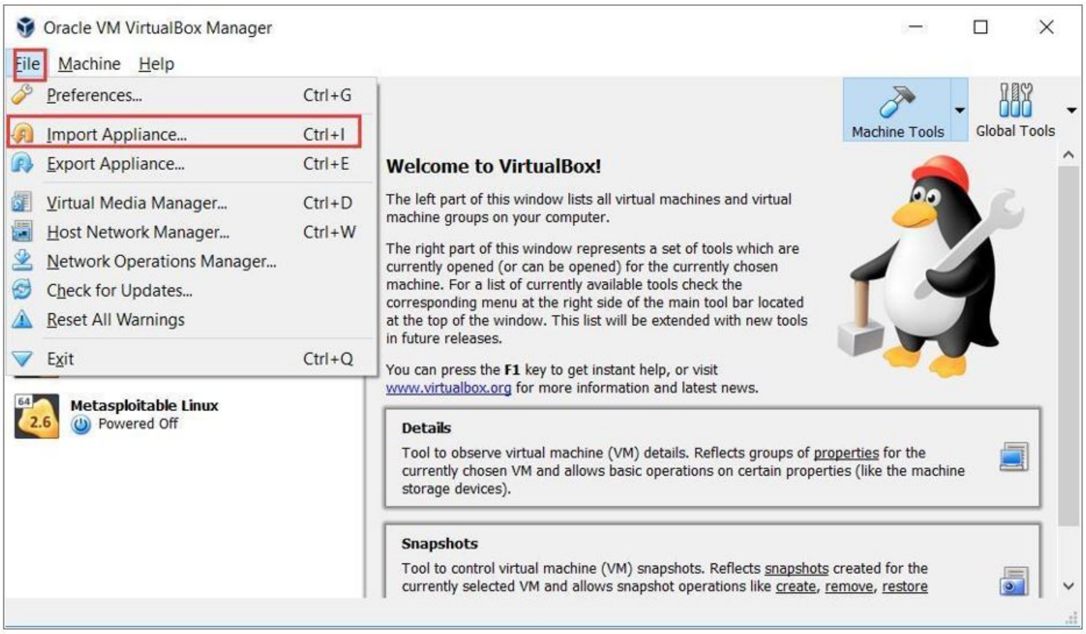
Virtual Machine Software:
VirtualBox is recommended for the labs and the assignment in this unit. VirtualBox is open-source and completely free. It can be downloaded at `https://www.virtualbox.org/wiki/Downloads`. Go to the download page shown as below and choose the appropriate installation package according to your host operating system.

Although other virtualization products like VMware Player and Parallels Desktop are also compatible to use, the teaching staff may not be able to support issues with those software.

VM Specifications: It's recommended to allocate 2 vCPUs and 4GB or more memory to smoothly run the VM.

User Manual of the Pre-built Ubuntu 20.04 VM:
We use a Windows 10 machine as the setup example. You can host the Ubuntu image using VirtualBox by performing the following steps:

1. Install VirtualBox player using the downloaded installer.
2. Launch VirtualBox player.


Oracle VM VirtualBox Manager
File
Machine
Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
Virtual Media Manager... Ctrl+D
Host Network Manager... Ctrl+W
Network Operations Manager...
Check for Updates...
Reset All Warnings
Exit Ctrl+Q
Metasploitable Linux
Powered Off
Machine Tools
Global Tools

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

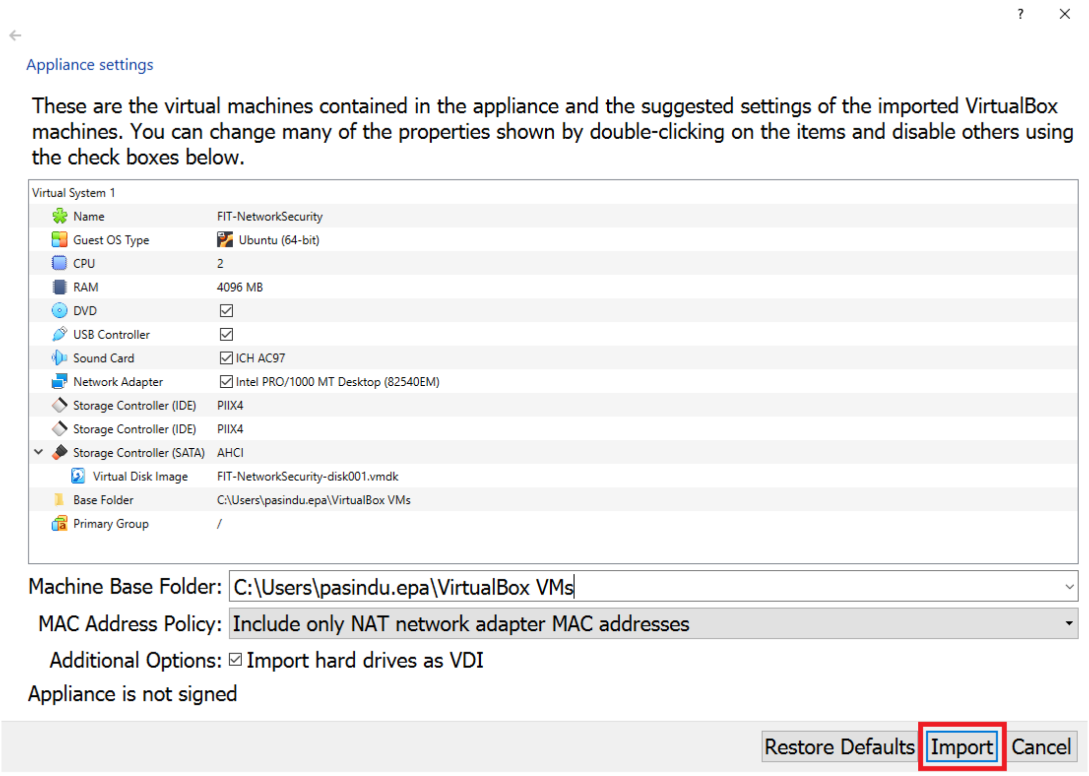
The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. For a list of currently available tools check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be extended with new tools in future releases.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

Details
Tool to observe virtual machine (VM) details. Reflects groups of properties for the currently chosen VM and allows basic operations on certain properties (like the machine storage devices).

Snapshots
Tool to control virtual machine (VM) snapshots. Reflects snapshots created for the currently selected VM and allows snapshot operations like create, remove, restore

3. Select File and Import Appliance.



Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1	
Name	FIT-NetworkSecurity
Guest OS Type	Ubuntu (64-bit)
CPU	2
RAM	4096 MB
DVD	☑
USB Controller	☑
Sound Card	☑ ICH AC97
Network Adapter	☑ Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (IDE)	PIIX4
Storage Controller (IDE)	PIIX4
Storage Controller (SATA)	AHCI
Virtual Disk Image	FIT-NetworkSecurity-disk001.vmdk
Base Folder	C:\Users\pasindu.epa\VirtualBox VMs
Primary Group	/

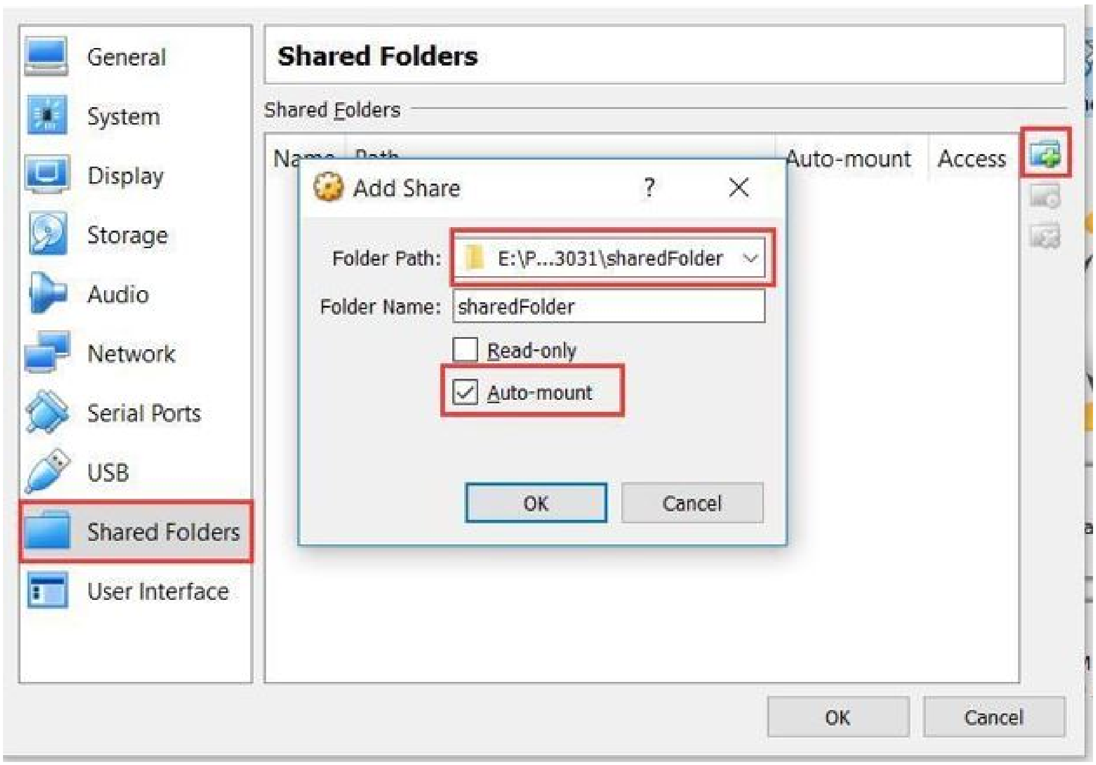
Machine Base Folder: C:\Users\pasindu.epa\VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ☑ Import hard drives as VDI

Appliance is not signed

4. Create Shared folder between the VM and your host machine. Right click on the VM and go to `settings` -> `Shared Folders`.



Add Share

Folder Path: E:\P...3031\sharedFolder

Folder Name: sharedFolder

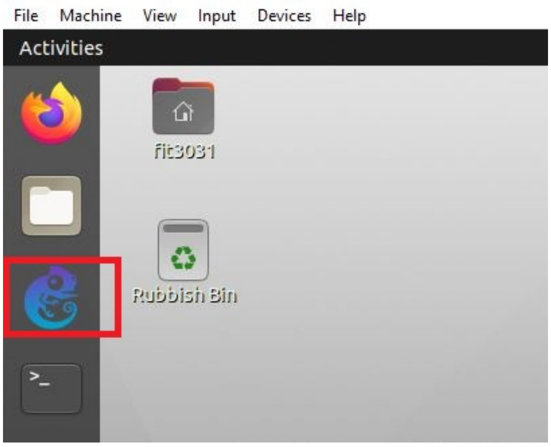
☐ Read-only

☑ Auto-mount

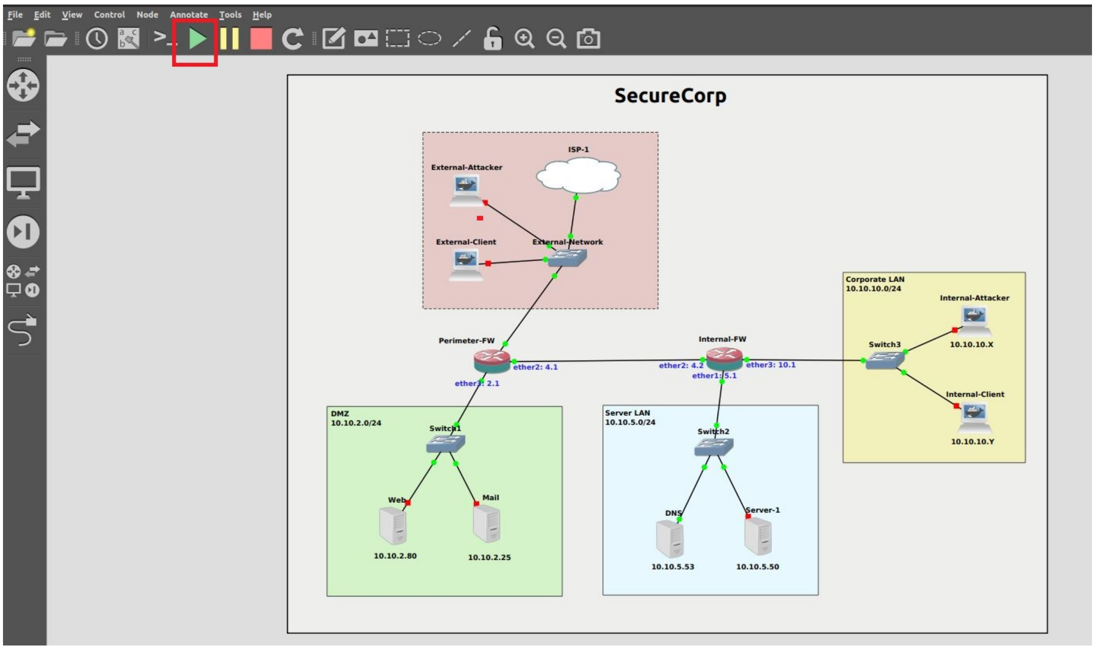
5. Start the VM by double clicking on it. The username and password for the VM is same: `netadmin`.

2 Using GNS3

In this unit, we are utilising GNS3 to emulate, configure, test and troubleshoot networks. GNS3 allows us to run a small topology consisting of only a few devices on our VM.
GNS3 is already installed in the VM and configuration file is also provided. Open GNS3 by clicking on its icon:



Select `open project from disk` and open `/home/netadmin/GNS3/projects/SecureCorp/SecureCorp.gns3` file. Click on the green button to start the configuration, it will take few minutes to load all devices.



Using GNS3 we can virtualize real hardware devices, all the devices in `SecureCorp` network have real operating systems loaded in them. You can right click on any of the device and to go `console` and execute commands. The workstations/servers are Ubuntu docker containers, the routers are Mikrotik routers and switches are normal Cisco switches.

Currently the containers do not have any software installed, we will install relevant applications as we progress in the labs. Familiarise yourself with GNS3 and the `SecureCorp` network, the topology is self explanatory, however if you have any questions, please ask your tutors or post on the the Ed forum.

3 Docker

Docker is an open source containerization platform. Containers simplify delivery of distributed applications and are made possible by process isolation and virtualization capabilities built into the Linux kernel. We use Docker containers as light-weight virtual machines in GNS3 networks.

4 Lab Tasks

1. Open SecureCorp project in GNS3 and start all nodes.

2. Add a new Ubuntu 20.04 container to the Corporate LAN and name the node as Internal-Client-2

3. Connect Internal-Client-2 to Switch3

4. Configure Internal-Client-2 network adapter with DHCP IP configuration.

5. Start the node and run the below command on the console to install the packages which include the essential tools such as nslookup, ip addr, ping, arp, netstat, nano text editor etc. Before you start working on any new Ubuntu 20.04 node you need to install these basic packages. These Docker containers are extremely light-weight and do not include any extra tools in them.

   ```
   apt update; apt install -y iputils-ping iproute2 dnsutils nano
   ```

6. Check connectivity to Internet and DNS. Check connectivity with other nodes in the SecureCorp network.

7. Stop the node and re-configure network adapter with static IP configuration to match the LAN.

8. Start the node and check connectivity to Internet and DNS. Check connectivity with other nodes in the SecureCorp network.

5 GNS3 Tips

1. Please note that not all folders in GNS3 nodes are persistent, files which are not in persistent folder gets deleted when you close GNS3. You can find the persistent folder list by right-clicking on the node and going to "Configure->Advanced" section. We recommend to always work in your home folder (/home).

2. If you decide to modify GNS3 configuration (you may actually need to do it for some labs/assignment), make a snapshot of your VM first, this way if you want to go back to the original configuration, you can just restore the last snapshot instead of importing the whole VM.

3. When you start SecureCorp configuration in GNS3, it may take sometime to load all nodes, keep an eye on CPU usage on the right pane of GNS3, wait until CPU usage is normal i.e. it's not 100%, and wait until all nodes are green.

4. If you have any issue with a node, instead of restarting the whole configuration, right click on the node and stop it and start it again.

5. Every time you add a new container, you will have to install the essential networking tools using the below command.

   ```
   apt update; apt install -y iputils-ping iproute2 dnsutils nano
   ```

6. If you want to add a fresh copy of the SecureCorp project, follow the below instructions and a new project will appear in the Project Library in GNS3:

   For Intel VM, run the following command on your VM's terminal:

   ```
   gdown 1txs3a3XHXsuA8-Qy2iXaM9rqWQai_hDA ; sudo bash ./install_SecureCorp.sh
   ```

   Or for Apple Silicon VM, run the following command in GNS3 VM Shell. Instrcutions on how to access the shell is given in the appendix section of the Apple Silicon lab setup document:

   ```
   gdown 1naJ3OgxuirbdwcWjgnQ4FwE3hmPOyTfS ; sudo bash ./install_SecureCorp_arm.sh
   ```