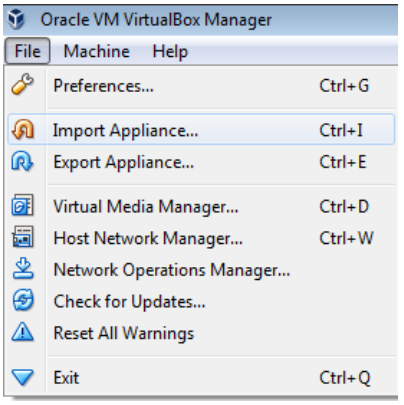
Virtual Network Configuration

We will be setting up a **Windows XP SP3** virtual machine and a **Linux virtual machine** as an isolated network within VirtualBox. Both VMs will be created from existing Virtual appliances. Afterwards, network traffic between the two VMs will be captured and observed using **Wireshark**. After the network is set up, verify connectivity from both ends.

Steps:

Download the Windows XP 32-bit OVF (Open Virtualization Format) appliance named '**Malware analysis 2.ova**" from the link below:
https://drive.google.com/open?id=18qXSx4Po9AMBB4TopZxuM-ZCU3ffJpuw
Create a new virtual machine from the appliance by using the '*Import Appliance*' tab from the '*File*' menu.



Next, download the REMnux ® appliance named '**remnux-6.0-ova-public.ova**" from the link:
https://drive.google.com/u/0/uc?id=1pdcfoDq5hLQBBelLP3KE64d7duWOk7D
Create a new virtual machine from the appliance by using the '*Import Appliance*' tab from the '*File*' menu.

REMnux ® is a lightweight Ubuntu based Linux distribution for malware analysts (https://remnux.org/).

After importing the appliance into VirtualBox, power up the REMnux machine and install VirtualBox guest additions. Install VirtualBox guest additions on the machine using the following commands:

Note: For Your convenience, both of these machines have been placed on Xeon at the following link: \\cactus1\Xeon\Fall 2022\information Security\Lab Setup

```
$ sudo apt-get update

$ sudo apt-get install virtualbox-guest-dkms
```

Restart the REMnux VM.

On the XP machine, configure the network interface with IP address **192.168.10.1**. Both VMs now need to be placed in an **isolated network**. Use the settings on the Virtual Box manager to change their network configurations from '*NAT*' to *'internal network'*. Make sure that the network has the same name for both machines.

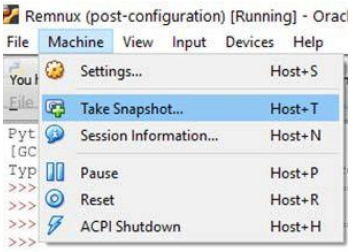
On the XP machine, configure the network interface with address **192.168.10.1**: Control Panel > Network Connections > Local Area Connection >right click > properties Select Internet Protocol (TCP/IP) and click on the 'Properties' tab

On the Linux machine, u se the following command to configure the interface with IP address **192.168.10.2**.

sudo ifconfig **eth0** 192.168.10.2 netmask 255.255.255.0 broadcast 192.168.10.255

eth0 is the name of the network interface which can be found by using the command: *'ifconfig' or 'sudo ifconfig'*

After configuring both machines, create **a snapshot** of the current state of both of them. Go to 'Machine' menu on the VM:



Start up **Wireshark on the REMnux machine**, open a command line terminal on the Windows VM and send ICMP packets to the machine (ping the remnux machine from the windows machine).

Verify the communications between the VMs from Wireshark's packet capture.

Open up a command line terminal on the REMnux machine and send ICMP packets to the XP machine. Verify the communications from Wireshark.

Finally, clear up all operations performed since the last snapshot, which is a typical thing you should do during malware analysis to restore your analysis machine to a clean state (i.e. before the malware was executed). To return to the previous snapshot (which you took before sending packets between them), close the VM from the 'X' close button on the top right corner. A dialog box will come up that will allow you to check '*Restore current snapshot …..*'. When the VM restarts, it will return to the previous snapshot.