Introduction: Preparation of our Lab Environment

Notes up front:

- approximately 40GB of space are needed
- this includes software from untrusted sources, keep it contained
- here, I will assume VirtualBox as virtualisation solution, not due to its technical superiority, but just because it is available for all relevant platforms, this is not to prevent you from using your solution of choice
- for the networking configuration, you have the option to go with your paranoia or to just get it working. So why make a fuzz? Because from the security tester's perspective, it is an essential practical issue.
- All metasploitable virtual machines can be found at [REDACTED], accessible with password *[REDACTED]*

The idea is to have at least two virtual machines set up at any time. A target, i.e., victim machine with metasploitable, which we will target in our exercises. And our attacker host, the Kali VM, from which we will perform most of our exercises.

Notes concerning the Windows Subsystem for Linux (WSL)

- WSL is an option for installing Kali. WSL 2 is a full virtualisation solution running a Linuxy Kernel, still, by default the system is integrated with your local System, this convenience is one of the key features. You might therefore consider a separate virtualisation environment, which provides a stronger separation of the attacking host from your actual work environment, and if just because the integration sucks.
- Also note that in the past, there have been issues with WSL interacting with Virtual Box. These are solvable.
- When using WSL, having graphical user interfaces is possible. But the means were included only with Windows 11. For earlier versions of Windows, you will need to manually install an *X11 server*.

Installing Virtual Machines for our Labs

Installing VirtualBox

For Linux users, please take your operating system packages, as installed by your package manager.

Windows and MacOS people, you have to go the long way.

1. Install VirtualBox that is appropriate for your machine under "... platform packages" from virtualbox.org.
2. Install VirtualBox extensions. Download from here.
3. Install VirtualBox Oracle VM VirtualBox Extension Pack: On the same webpage, locate the heading VirtualBox ... Oracle VM VirtualBox Extension Pack. Click on "All supported platforms". This should download the extension .vbox-extpack . Double click on the file that is downloaded and this will automatically install the extension to VirtualBox.

Installing Kali Linux

1. Download the VM Image
    1. Preferably the updated image from the nextcloud share above.
    2. Otherwise, the original VM image. In this case, make sure to select the appropriate virtualisation solution, i.e., "VirtualBox Image", and the version of Kali that's compatible with your system.
2. In case of the original image, please use the documentation.
3. When using the cloud image, select "import" from the menu, or double-click on the file. You will see a window that will allow you to import the virtual machine.
4. RAM: click on the Kali-Linux tab, which can be seen on the left side of the window. Then, click on the Settings. Modify the amount of RAM. 1 GB is fine but you can change it to 2 depending on how much you have on your host machine.
5. CPU: Click on Settings then Click in the Processor tab. By default, we have two processors assigned to it. 1 CPU is enough but you can make it 2 depending on your host machine.
6. Network settings: to allow VM-Interconnect, please read the section on Setting up Inter-VM Communcations for a more detailed set of options. You can use "Nat Network"ing to just get the machine online and interconnected with other VMs. For this, click on Settings then on Network. On "Attached to" select "Nat Network". More details below.
7. Your virtual machine is ready. Click OK.
8. Double click your Kali VM to start.

The default username as well as the password is kali.

When you log into Kali for the first time make sure to update it the following commands in the terminal: "sudo apt update" and then "sudo apt upgrade"

If you want to use a different distribution, please make sure to install the following tools: nmap, whois, host, etherape pnscan, legion, nessus, netcat, mysql, johntheripper, metasploit, gvm/the greenbone security assistant.
This list might get updated while the course runs.

Installing Metasploitable3

This is software on the completely not trustworthy side. Keep it well contained.

The easiest method to get metasploitable running, and the fastes, is to download the ova for use with VirtualBox for the Linux version of metasploitable3 from vagrantup.com or the nextcloud share given above. They also provide images for other virtualisation solutions. After downloading, unzip it and rename the resulting file to end in ".ova". Technically, it is a tar archive, changing the extension will allow Windows to understand the contents better. Also, VirtualBox itself will directly list it in the import dialog, which filters by name. Alternatively, you can also just empty the "filter" combo box at the bottom of the import dialog and select the unzipped file. Renaming the file to end in ".ova.gz" will also list it in the import dialog, but VirtualBox will not let you proceed with the import.

Login information for the vagrant hosted ova:
username: vagrant
password: vagrant

Make sure to change the Network settings according to Setting up Inter-VM Communcations or to just set them to "NAT Network". Whatever your choice, make sure you have implemented the same option for both, the Kali and the metasploitable3, VMs.

When the installation is done, you will have a Linux instance of metasploitable3 installed.

Note that it is also possible to create Windows instances, the vagrant link for example provides two image downloads, one for Linux and one for Windows. Also, when building your own metasploitable3 image, the procedure should create both flavours.

Setting up Inter-VM Communcations

To be able to perform actual penetration testing between the two virtual machines---Kali and metasploitable---we have to enable them to communicate, i.e., we have to put them onto the same (virtual) network.

I am sorry for adding this information post-hoc, I overlooked this issue when adapting the previous years' course information. Actually, you can continue to use the setup as presented, but I will also present a rather more sophisticated setup, which you might want to prefer when working with other peoples VMs instead of just giving them access to the internet.

Descriptions here are for VirtualBox. For other virtualisation solutions, similar options exist.

The following table from [1] nicely shows the options for having two VMs communicate with each other in VirtualBox:

	VM <-> Host	**VM1 <-> VM2**	**VM -> Internet**	**VM <- Internet**
HostOnly	Yes	Yes	No	No
Internal	No	Yes	No	No
Bridged	Yes	Yes	Yes	Yes
NAT	No	No	Yes	Port forwarding
NAT Network	No	Yes	Yes	Port forwarding

I will present the simple "NAT Network" (NATNet) option, which doesn't allow to enforce who communicates with whom easily, and the combination of "Internal Networking" with "NAT" access to achieve a more sophisticated virtual network topology.

Note to users of other virtualisation solutions: you will need to figure out how to establish networking between the VMs. In VMWare, the virtual network facility seems to be the way to go, but I do not know how to configure a dhcp server to have ip addresses of the VMs being configured automatically. For WSL2, be aware that you need HostOnly-Networking to be able to contact the metasploitable VM. The latter, I would never want to have outside of a dedicated virtualisation solution. Especially not in WSL.

NAT Network---The easy option

The easiest way will be using the "NAT Network" (NATNet) option, which will allow all VMs to connect to the internet connection of the host OS. For another, slightly more complicated solution, check the next section.

In VirtualBox, choose "File" -> "Properties" and select "Network". Then click on add, to create an entry "NatNetwork". Please check the options to make sure that the check box in front of "DHCP" is selected.

Then, you can select the Kali VM, "Settings" from the menu bar at the top and in the following window "Network" on the left. Note that the machine has to be shut down to be able to perform changes here. Now select "NAT Network" and make sure the name is set to the NatNetwork entry you created above.

Then, perform the same steps for the metasploitable3 VM.

You can also check this video at youtube for details on how to create a NAT Network.

Internal Network---The more complex network

A more sophisticated way will be using the "Internal Network" option, which will prohibit internet access from the VMs using it, which should be fine. Especially for the metasploitable3 VM, where we might want to call this a desired feature.

In case you want to have internet access from, e.g., for updating the Kali VM and having access to online documentation, you create a second network adapter and choose "NAT" for that one. Be careful that you might need to add a second "wired connection" for Kali Linux's NetworkManager due to the tool's internals, i.e., for each network interface card, there has to be one connection configured, because one connection can only be used by one interface card at a time.

This way, you can interact with the metasploitable VM from the Kali VM in a controlled manner without setting up a firewall.

To setup "Internal" networking in a simple way, you will need to either (1) configure static ip addresses on both hosts (2) enable a dhcp server on the kali machine (3) enable a dhcpserver in Virtual Box. Which I will shortly cover here.

Unfortunately, you will need to do this on the command line. Windows users might for maximum convenience need to change to the directory containing the VBoxManage binary, to avoid inputting endless paths.

```
> VBoxManage list intnets

> VBoxManage list dhcpservers

> VBoxManage dhcpserver add --network=intnet --lowerip 10.0.0.2 \
        --netmask 255.255.255.0 --upperip 10.0.0.254 \
        --ip 10.0.0.1 --enable
```

This will create a dhcpserver which distributes ip addresses to the VMs on "intnet" using the ip range 10.0.0.0/24. Note that the backslash \ at the end of the line indicates that the command continues on the next line.

For being able to check your configuration, you can log in to metasploitable3. When downloaded from vagrant, use
username: vagrant
password: vagrant .

References

[1] Virtual Box forum entry discussing networking options