Virtual Cyber Lab Set-up

Introduction

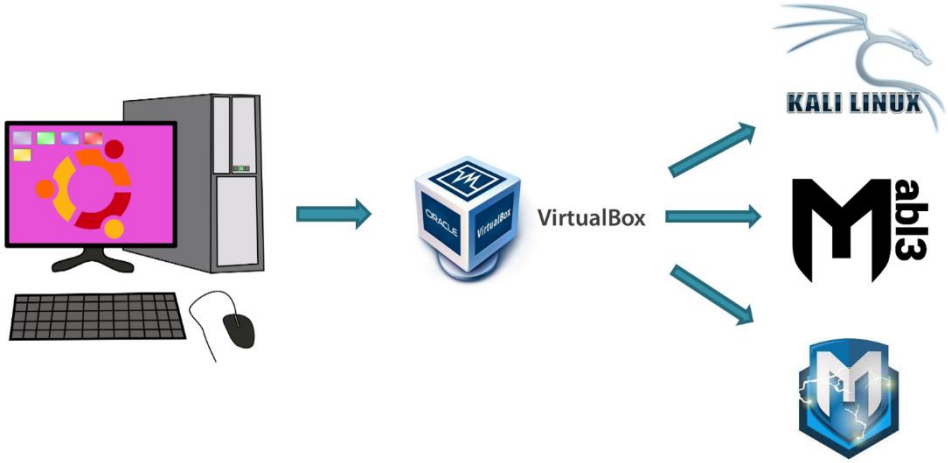
Practical training is necessary to learn hacking methods. We probably remember that hacking is only legal if we do it either on our own infrastructure or with the written permission of the owner. In order to stay within the law, a convenient solution is to prepare a virtual cyber security lab.

A cyber security lab can be set up entirely in a virtual environment while still accurately mirroring the physical environment. Therefore, all the experiments conducted in the virtual environment will be valid on the real infrastructure as well.

The virtual laboratory can be placed entirely on our computer. For this, install VirtualBox on the computer.

VirtualBox is a free and open-source virtualization software developed by Oracle. It allows you to run multiple virtual machines (VMs) on a single physical computer. Each virtual machine acts as an independent, self-contained computer with its own operating system and software.

We will create virtual computers and appropriate network infrastructure within the VirtualBox.



In Virtual Box, create a `KaliLinux` virtual computer, `Metasploitable 2` and `Metasploitable 3` computers and place them on a single network.

A Metasploitable computer is a computer intentionally saturated with vulnerabilities, which our KaliLinux will target for detecting these vulnerabilities and exploiting them for security breaches.

All the steps for creating the described environment are discussed in detail below.

Updating our computer OS

Before doing any important work, we always recommend updating your computer's operating system. In the case of Ubuntu, the update is done with the following two commands:

```
$ sudo apt update
```

```
$ sudo apt upgrade
```

Installing Virtual Box and Extension Pack

VirtualBox can be installed on almost all operating systems. There is official documentation at this address: `https://www.virtualbox.org/wiki/Downloads`

VirtualBox can be installed on Linux with the following command:

```
$ sudo apt install virtualbox
```

If the following error appears on the screen "Failed to start LSB: VirtualBox Linux kernel module", it means that you should disable secure boot on the computer. Restart the computer, enter the BIOS configuration and disable secure boot.

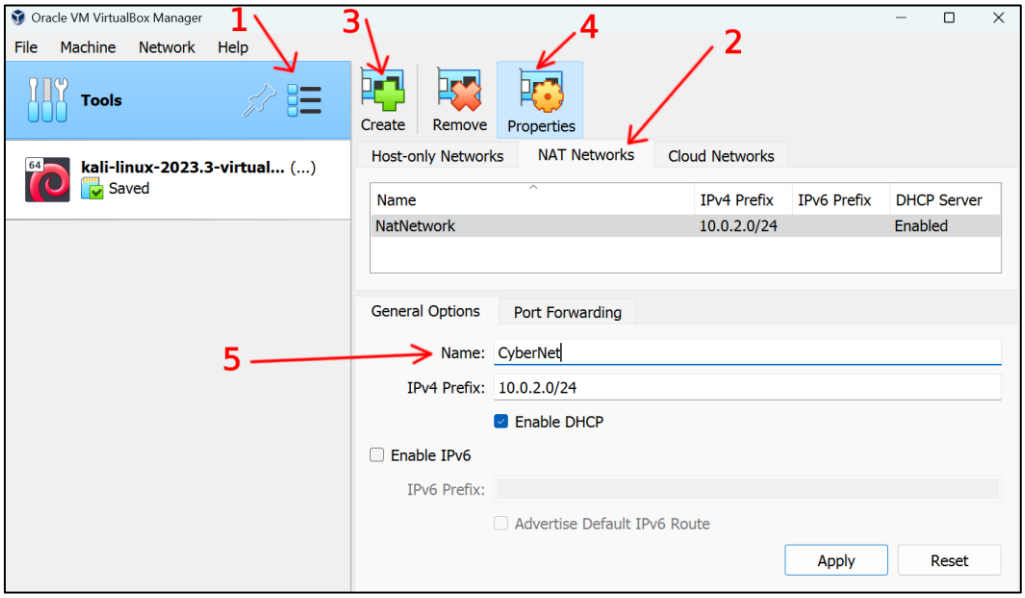
In order to fully use the functionality of VirtualBox, we need to install its extension pack.

Extension pack is installed with the following command:

```
$ sudo apt install virtualbox-ext-pack
```

Creating the Nat Network in Virtual Box

Create a new `Nat Network` in VirtualBox. It is in this network that we will integrate the computers of our cyber laboratory. Connecting to a shared network is necessary for computers to be able to access each other and to enable one to hack another. To create a network we will have to press a few buttons, see the following image:



Let's call the network `CyberNet`, as shown in the picture.

Downloading and Installing Kali Linux

To download Kali Linux and install it in VirtualBox, use the official documentation: `https://www.kali.org/docs/virtualization/import-premade-virtualbox/`

In the official documentation, the Kali Linux virtual machine is allocated 2 gigabytes of RAM, but it will work with 1, and keep that in mind if your computer doesn't have a lot of memory.

Also note that 1 processor is quite enough for this machine. As you can see from the documentation, the user is `kali` and the password is `kali`.

Place the newly created virtual machine on the CyberNet network.

Downloading and Installing Metasploitable 2

Metasploitable 2 is a virtual machine that is pre-installed with many vulnerabilities. It is intended (mainly using Metasploit) to play attacks.

To download and install Metasploitable 2, use the official documentation: `https://docs.rapid7.com/metasploit/metasploitable-2/#powering-on-metasploitable-2`

This virtual machine should have 1GB of RAM and it should be placed in the same Nat Network.

As you can see from the documentation, the user is `msfadmin` and the password is `msfadmin`.

Installing Metasploitable 3

Metasploitable 3 is a virtual machine pre-installed with numerous vulnerabilities, primarily designed for practicing attacks using Metasploit. There are two versions of it, Linux PC and Windows PC.

prerequisites

Installing Metasploitable 3 is structurally different from Metasploitable 2. In the previous case, the computer was already equipped with programs, and we only needed to download and install it. In the case of Metasploitable 3, since it is based on `Windows Server 2008`, it cannot be distributed as a VirtualBox file due to Microsoft's requirements. Therefore, we will have to install some software tools to first download a clean version of this server and then install the appropriate security programs and add the necessary users.

The supporting software tools required to install Metasploitable 3 are:

- Packer: `https://www.packer.io/docs/install/index.html`
- Vagrant: `https://www.vagrantup.com/docs/installation/`
- Vagrant Reload Plugin: `https://github.com/aidanns/vagrant-reload#installation`

Follow the proper official documentation and install the above programs.

Installing Metasploitable 3

Note that you need to edit the `VagrantFile` if you want to install on a Linux-only or Windows-only machine.

For Linux users, the following commands are required:

```
$ mkdir metasploitable3-workspace
$ cd metasploitable3-workspace
$ curl -O https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile && vagrant up
```

For Windows users, the following commands are required:

```
mkdir metasploitable3-workspace
cd metasploitable3-workspace
Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -
OutFile "Vagrantfile"
vagrant up
```

Note that the installation time is quite long (2-3 hours).

Building Metasploitable 3

This step is not necessary if you have already downloaded and installed Metasploitable 3 according to the instructions in the previous chapter.

Download or clone Metasploitable 3 from its GitHub repository `https://github.com/rapid7/metasploitable3/`.

Note that if you have Hyper-V enabled, you must disable it for VirtualBox to fully function.

Run PowerShell with administrator rights and navigate to the Metasploitable 3 folder. Run the following command:

```
Set-ExecutionPolicy Unrestricted
```

Now we are ready to start the automated process. We need to run a script that will download a trial version of `Windows Server 2008` and install the necessary programs on it.

Run the following command to execute the script:

```
.\build.ps1 windows2008
```

The script will take about 1 hour to run. After that run the following command:

```
vargant up
```

After that, Metasploitable 3 will be installed in VirtualBox.

Configuring Metasploitable 3

The user of the virtual machine is `vagrant`, and the password is `vagrant`.

Give 1 or 2 gigabytes to the virtual machine. In some cases, 2 gigabytes and 2 CPUs create some problems.

Initially the screen size will be small. To increase the screen size, you need to insert the guest additions CD into the virtual machine (with the help of the following menu Device -> Insert guest additions CD image) and run the appropriate 64-bit program.

In some cases, this program hangs. In such cases, it is recommended to give only 1 processor and disable 3D acceleration for the virtual machine display.

Downloading and Installing Ubuntu machine

To download Ubuntu Linux and install it on Virtual Box, follow the official documentation: `https://ubuntu.com/tutorials/how-to-run-ubuntu-desktop-on-a-virtual-machine-using-virtualbox #1-overview`

Set at least 1GB of RAM to the virtual machine.

Initially the screen size will be small. To increase the screen size, the following actions are required:

1. Run the command: `sudo apt install linux-headers-$(uname -r) build-essential dkms`

2. Insert the guest additions CD into the virtual machine (with the help of the following menu Device -> Insert guest additions CD image) and run the appropriate script.

3. Restart the virtual machine.

The final set-up

Update Kali Linux and Ubuntu virtual machines using the `sudo apt update` and `sudo apt upgrade` commands.

Take a snapshot of all virtual machines. This will be useful for us to restore the machine in case of damage.