General laboratory instructions

Laboratory for the class "Cybersecurity" (01UDR)
Politecnico di Torino – AA 2021/22
Prof. Antonio Lioy

prepared by:
Diana Berbecaru (diana.berbecaru@polito.it)
Andrea Atzeni (andrea.atzeni@polito.it)

v. 1.0.0 (07/10/2021)

Contents

1 The laboratory work environment

The laboratory exercises use the Linux distribution Kali, version 2021.3. We have created a "custom" ISO image of this Linux distribution, where we tested the exercises proposed throughout the laboratories to ensure everything will work fine. Potential problems due to driver incompatibilities of your own PC or network configuration at your place are not covered in this material. We have performed preliminary checks to verify that the required packages are installed so that you would not have to download them during the laboratory. In this way we avoid to unnecessarily overload the network during laboratory time.

Moreover, we have reduced the ISO size and we adopted XFCE (as unique Desktop Environment) to minimize the system requirements, as not all the PCs in the lab are recent and/or guarantee high performance.

The ISO Live image of Kali can be selected directly from the Grub menu of the PCs in LabInf. The username and the password required to load the Live distribution are the following:

```
username:  security
password:  cybersec
```

At the boot of Kali you should see a menu similar to the one in Figure 1.

Choose "Live (forensic mode)" to start up the operating system.

When needed, authenticate yourself with username `kali` and password `kali`. The same password `kali` is valid also for the `root` user.

At the end of the boot phase, Kali 2021.3 should have already configured correctly the network (since a DHCP server is available in the lab).

The X graphical server should start up automatically and the working environment will look like in Figure 2.

Useful commands

We remind you some useful Linux commands required throughout the exercises. Note that the square brackets (i.e. [and]) indicate something optional, the angle brackets (i.e. < and >) indicate a choice, the words in *Italic* need to be replaced with the specific data required by the command. For example, the command

```
su [-] [ username ]
```

is used correctly if you type

```
su - Bea
```

assuming that *Bea* is a registered user in your system, but is also correct to use

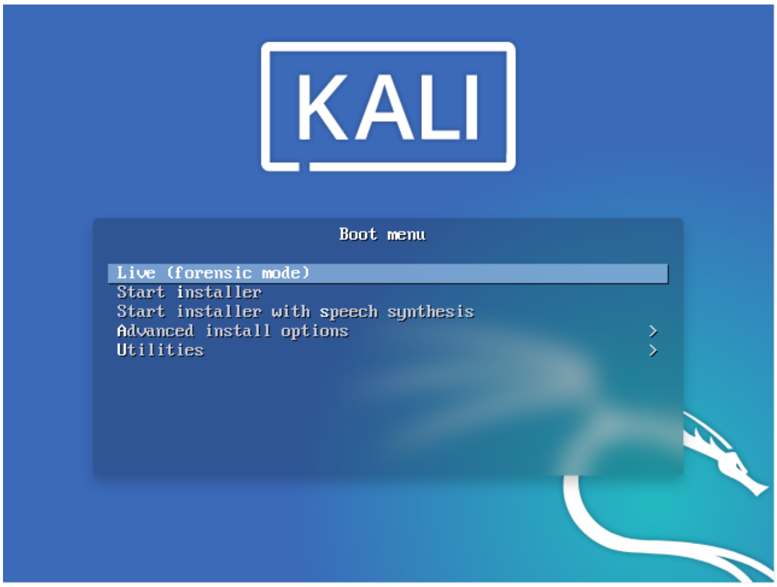


Figure 1: Initial menu of Kali 2021.3.

Trash
File System
Home
utility
Sicurezza dei sistemi informatici
KALI LINUX
"the quieter you become, the more you are able to hear"
Computer system security

Figure 2: Kali working environment.

```
su -
```

that is without the second optional parameter.

Some commands you would typically need to execute while running the proposed exercises are:

- To configure the keyboard in console mode, you can use the command:

  ```
  loadkeys language
  ```

  while in graphical mode you can use:

  ```
  setxkbmap language
  ```

  where *language* can be `it` for the Italian keyboard (which is the most frequent option in the lab) or `us` for the American keyboard (the default option).

- To create a new user:

  ```
  adduser username
  ```

- To change user, in particular to become `root` (if you do not specify a *username*, `root` is assumed):

  ```
  su [-] [ username ]
  ```

- To obtain more information on the use of a command/program:

  ```
  man program_name
  ```

- to start/stop/restart services:

  ```
  systemctl {status start | restart | stop | enable } servicename
  ```

  or

  ```
  service servicename { start | stop | restart }
  ```

  or

  ```
  /etc/init.d/servicename { start | stop | restart }
  ```

- To view the network configuration of your machine (IP address, netmask, . . .) with `net-tools`:

  ```
  ifconfig
  ```

  or by using the `ip` command:

  ```
  ip addr show
  ```

- To manually configure the network interface, e.g. to set the IP address with `net-tools`:

  ```
  ifconfig interface IP netmask network_netmask
  route add default gw IP_defaultGW
  ```

  or by using the `ip` command:

  ```
  ip addr add IP/netmask_CIDR dev interface
  ip route add default via IP_defaultGW
  ```

- to ask a new dynamic IP address to the DHCP server:

  ```
  dhclient
  ```

- if some script does not work and you cannot figure out the reason but you cut-and-pasted it from Windows or from the web, you can try with the following command

  ```
  dos2unix filename
  ```

  which will fix the frequent the newline issue (i.e. CR-LF in Windows, LF in Linux).

- To add a static route with net-tools:

  ```
  route add -net IP_destination_network netmask network_netmask gw IP_gateway
  ```

  or by using the ip command:

  ```
  ip route add IP_destination_route via IP_gateway dev interface
  ```

- To set a DNS server, add a line in the file resolv.conf with this syntax:

  ```
  nameserver IP_nameserver
  ```

  For read other options use the man resolv.conf command.

- To install a program contained in a specific package:

  ```
  apt-get install package_name
  ```

If the screen locks and you need to unlock it, use the “kali” user and the “kali” password.

2 Setting up the laboratory environment at home

The exercises proposed in the laboratories will require you to use two, at most three PCs at the same time. In the next sections, we describe how you can create at home a working environment, very similar to the one used in the laboratory, with either virtual or physical machines.

2.1 Use of a virtualised environment

You can use virtualisation to run in parallel one or more copies of Kali on a unique physical machine.

Kali provides, along with various ISO versions, also Virtual Machines (VM) ready to run in the VMWare and VirtualBox virtual environments. Unfortunately, these VMs are rather big (Kali Full distribution is 2.2 GB for VMWare and 3.4 GB for VirtualBox) for the basic image. If you want to use the original Kali version (either Full or Light), you have to create a VM and install the selected distribution.

Alternatively, we suggest you to create a VM with the customized Kali Live ISO that we provide as part of the course, as it has already been customized with all the packages needed. You can download this custom version from the following URLs and then follow the instructions in Section 2.1.2:

https://storage-sec.polito.it/external/kali/2021/kali-torsec-2021.iso

You could use the aforementioned ISO image to install persistent VMs on your host (e.g. using VirtualBox).

2.1.1 Suggested virtual configuration

The configuration that we suggest (as it’s the one that we used to test the exercises with virtualisation on our own PCs) includes three VMs, that shall run the Kali custom that we provided to perform the exercises with reduced workload (e.g. RAM).

Note: Once you create a VM, you may clone it (as described in Section 2.1.3) and then assign it an appropriate name (as described in Section 2.1.4).

We provide here the instructions to prepare the working environment for a virtual Security Lab Network, composed of three Kali custom VMs, as illustrated in Fig. 3. We propose to use Oracle VM VirtualBox, a free virtualisation product available for Linux and Windows platforms. From the computational point of view, VirtualBox is lighter than other tools if it is used to create a single VM, but is does not scale well when the number of VMs increases (compared to costly commercial products). For this reason, managing more than two VMs

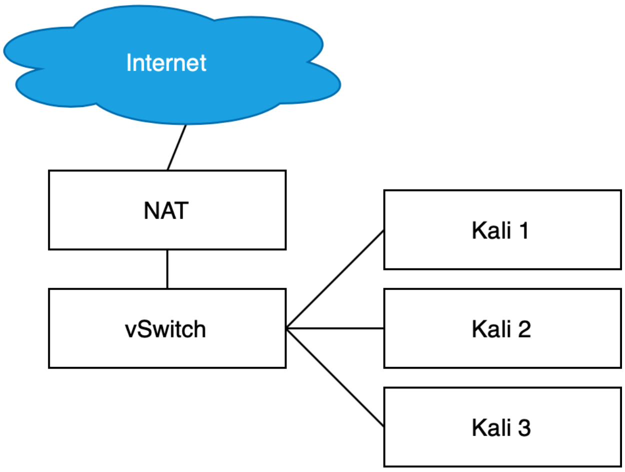


Figure 3: Network topology to recreate the laboratory environment with NAT Network and three VMs.

on a single PC with only 2 GB RAM could be difficult because the system might be too slow. However, you should not have any usability problem if you have a recent PC with at least 8 GB RAM.

The version we refer to in this document is 6.1.26 that you can download from the URL:
`https://www.virtualbox.org/wiki/Downloads`

Its documentation is available at the URL:
`https://www.virtualbox.org/wiki/Documentation`

For the installation, look at chapter 2 of the guide Oracle VM VirtualBox User manual:
`http://download.virtualbox.org/virtualbox/UserManual.pdf`.

For the network configuration, look at chapter 6 of the same guide.

> NOTE
>
> An alternative free product is VMware Player. According to the official documentation, VMware Player supports at most one VM at the time, in practice, this limitation is not applied and you should be able to execute more than one. We have not tested the practical exercises with this product, so we cannot provide support for its use. Other free products have not been deemed adequate for this course. VMware vSphere Hypervisor is too big for the exercises proposed, while VMServer is not maintained any more since 2010. Note that we have not tested any virtualisation environment for MacOS; however, students that used in the past virtualisation environment for MacOS have not reported any problem regarding the practical exercises in this environment). If you already own a licence, you can use VMware Workstation (note that we do not suggest that you should buy one).

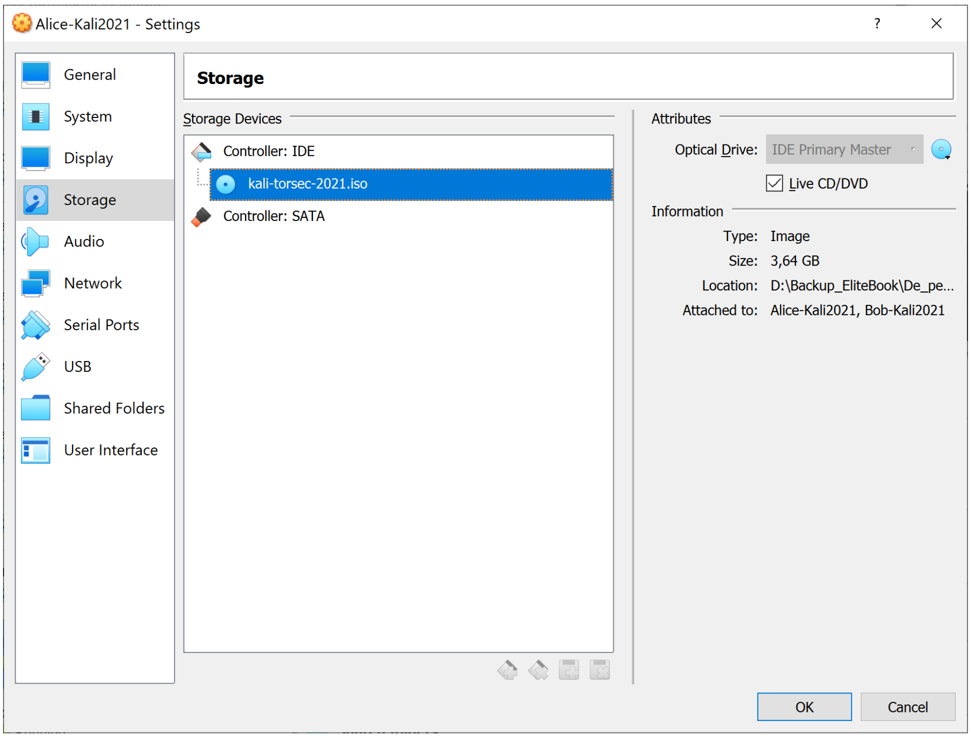
2.1.2 Live VMs from an ISO

In this case, you will run Live Kali from an ISO file by mounting it on the virtual DVD of an ad hoc VM. Therefore, you need a local copy of the ISO we built for this class. You can download the official ISO image from here:

`https://storage-sec.polito.it/external/kali/2021/kali-torsec-2021.iso`

To create a Live VM from an ISO with Oracle VM VirtualBox, you can press the “New” button, which starts the wizard that allows you to create a new VM by performing the following steps:

- *define VM name and operating system.* You have first to assign a name (you can follow our suggestions in Section 2.1.4), then select “Linux” as operating system and “Debian (64 bit)” as OS version (Kali is based on Debian).



Storage

Storage Devices

- Controller: IDE
  - kali-torsec-2021.iso
- Controller: SATA

Attributes

Optical Drive: IDE Primary Master

☑ Live CD/DVD

Information

Type:	Image
Size:	3,64 GB
Location:	D:\Backup_EliteBook\De_pe...
Attached to:	Alice-Kali2021, Bob-Kali2021

Figure 4: Selection of the Hard Disk with VirtualBox.

.

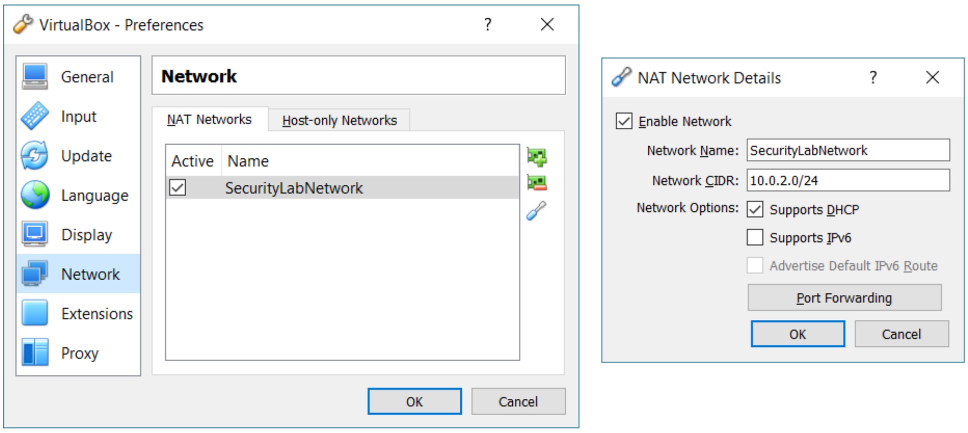
- *select the VM RAM size*. As already explained, we suggest you to allocate at least 1 GB for the VMs with Kali
- *configure Hard Disks*. Unpin the “Do not add a Virtual Drive” option and continue (we will configure a DVD later).

Now select the VM you have just created and click on “Settings” to add a virtual CD/DVD device:

- select “Storage” (a window will appear as in Fig. 4);
- click on the “device CD/DVD” button below the “Controller IDE”, from the “Attributes” Tab change it to “IDE Primary Device”. Click on the disk icon (just right of the IDE Primary Device label) to mount a drive, then click on “choose a virtual CD/DVD file” and select the Kali ISO you want to execute (e.g. `kali-torsec-2021.iso`). Finally, check the “Live CD/DVD” box.
- create a new “NAT Network”. To do so, click on “File” then on “Preferences...”. From the Tab “Network” create a new “NAT Network” by clicking on the icon “Add New NAT Network”. A new line “NATNetwork” will appear in the list. Subsequently, right click on “Edit NAT Network”, rename it to “SecurityLabNetwork”, check whether DHCP support is enabled and choose a range of IP addresses (if this is the first one you create, the range 10.0.2.0/24 should be fine). You should get two windows similar to those in Fig. 5.
- connect the VMs imported in the “SecurityLabNetwork”. Right click on the name of the VM, choose “Preferences...” then click on Tab “Network”. In the Tab “Adapter 1”, change the option “Attached to:” from NAT to NAT Network, verify that in the field “Name” (that have just appeared) it is also present “SecurityLabNetwork”.

2.1.3 Cloning VMs

For the execution of the exercises, in some laboratories you may need two VMs, in others up to three VMs.



Active	Name
☑	SecurityLabNetwork

☑ Enable Network

Network Name: SecurityLabNetwork

Network CIDR: 10.0.2.0/24

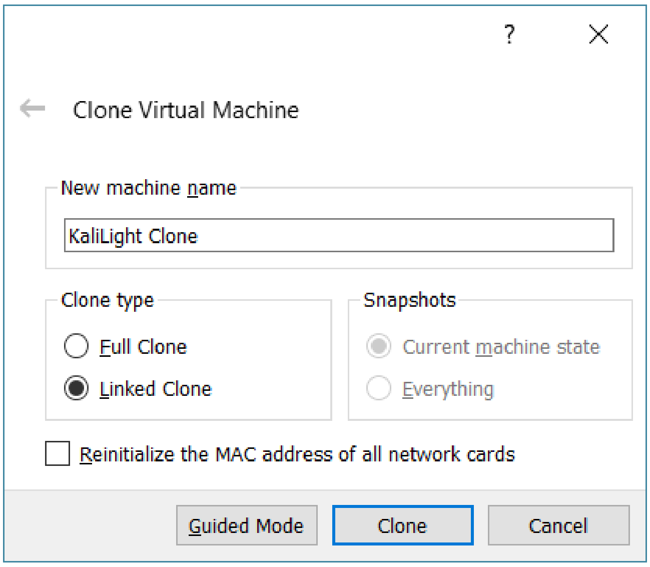
Network Options: ☑ Supports DHCP

□ Supports IPv6

□ Advertise Default IPv6 Route

Figure 5: Configuration of a NAT Network with VirtualBox.

To this purpose, you may clone the VMs you have just created (e.g. the Kali VM with the correct network configuration based on the custom ISO). To do so, right click on the name of the VM to clone, which should be switched off. Then choose "Clone...", select the name to be given to the new clone (e.g. KaliLight Clone) and select the option "Linked Clone" (that will allow you to save space on disk, reduce RAM usage and will allow you to increment the performance by using the advanced options of VirtualBox), as illustrated in Fig. 6.



New machine name: KaliLight Clone

Clone type:
○ Full Clone
● Linked Clone

Snapshots:
● Current machine state
○ Everything

□ Reinitialize the MAC address of all network cards

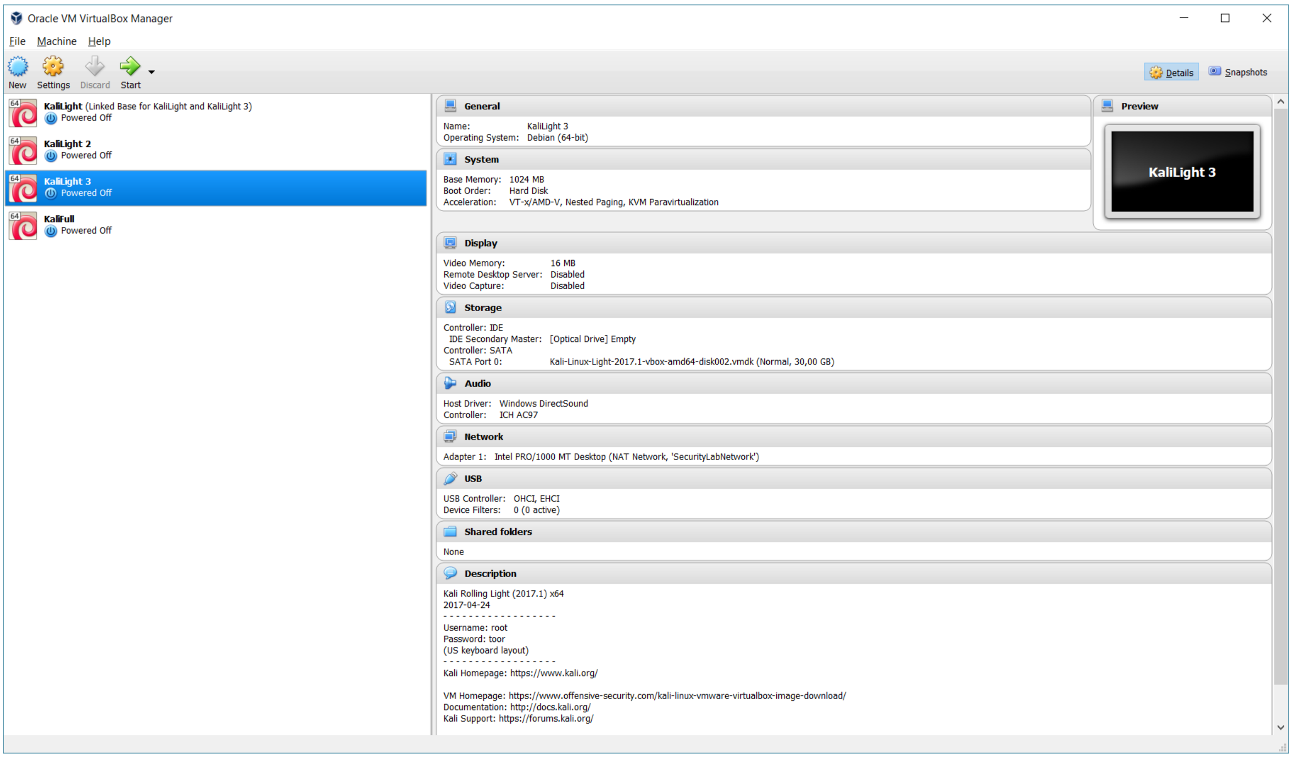
Figure 6: Window used to clone the VMs in VirtualBox.

After you have clicked on the button "Clone", a new VM will appear and the text "Linked Base for KaliLight 3" will be appended to the original VM (see an example in Fig. 7).

2.1.4 VM naming

In the laboratories, the various VMs perform different "roles" in the exercises. For example, besides Alice and Bob, that are used to indicate the generic users A and B, we will also use other names whose initials recall the role they have in the practical exercise (e.g. Carol to indicate the VM of the Certification Authority, Frank for the Firewall). To avoid confusion, we advise you to rename each VM before running the exercises (rename for example Kali1 as Alice, Kali2 as Bob, and so on).

Right click on the name of the VM to rename (e.g. KaliCustom) and then click on "Settings...". A window will appear, open at the Tab "General > Basic", where you can change the name by modifying the text in the field



KaliLight (Linked Base for KaliLight and KaliLight 3)
Powered Off
KaliLight 2
Powered Off
KaliLight 3
Powered Off
KaliFull
Powered Off

General
Name: KaliLight 3
Operating System: Debian (64-bit)

System
Base Memory: 1024 MB
Boot Order: Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali-Linux-Light-2017.1-vbox-amd64-disk002.vmdk (Normal, 30,00 GB)

Audio
Host Driver: Windows DirectSound
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'SecurityLabNetwork')

USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders
None

Description
Kali Rolling Light (2017.1) x64
2017-04-24
- - - - - - - - - - - - - - - - - -
Username: root
Password: toor
(US keyboard layout)
- - - - - - - - - - - - - - - - - -
Kali Homepage: https://www.kali.org/

VM Homepage: https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/
Documentation: http://docs.kali.org/
Kali Support: https://forums.kali.org/

Figure 7: VirtualBox window after the preparation of the virtual laboratory.

"Name" (e.g. in Alice (KaliCustom)).

Appendix A Import a Kali VM

IMPORTANT NOTE: Someone may prefer to use the Kali VMs instead of downloading and running the custom Live Kali distribution described in Section 2.1.2. This section is for them, so if you have already performed the installation described in Section 2.1.2 then you can skip this section.

Let us assume you have a running VirtualBox, you can proceed with the creation of the VMs necessary for the execution of the proposed lab exercises in the following way:

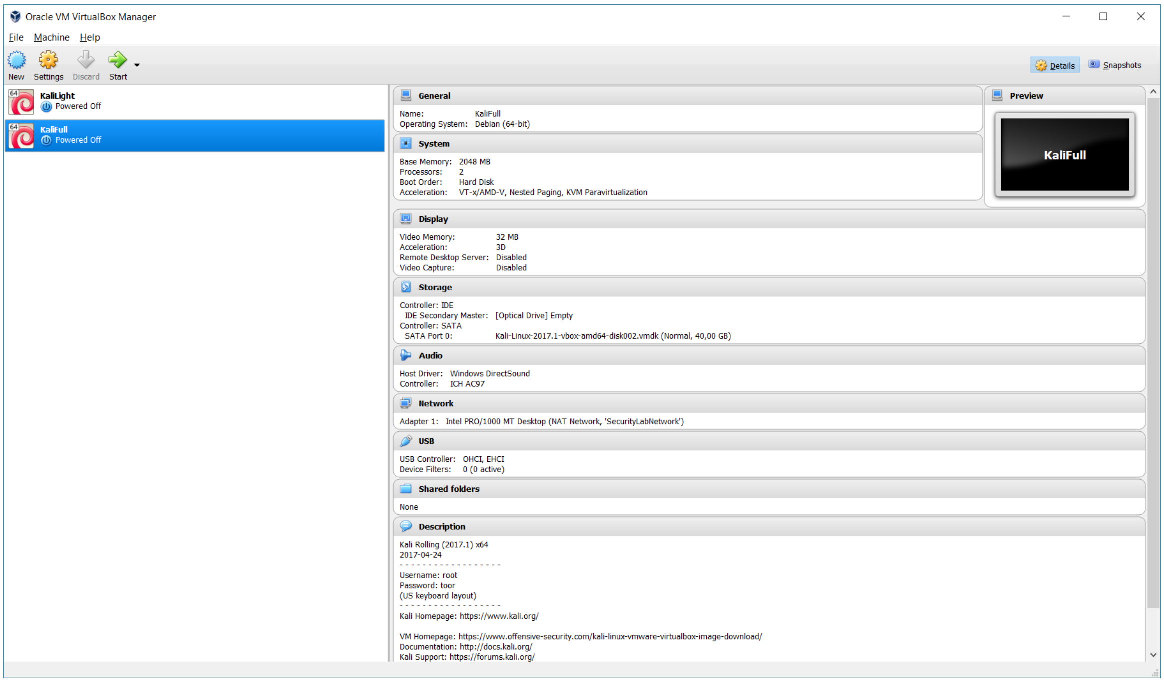
1. download the VMs from the following link from the Tab "Kali Linux VirtualBox Images" (pay attention to choose the correct versions on 32 or 64 bits):

   `https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/`

2. import the downloaded VMs in your system. To do so, click on "File" then on "Import appliance". It will appear a window that will allow you to choose the file corresponding to the downloaded VM. After you have chosen the downloaded file, a window that illustrates the main characteristics of the imported VMs will appear. At the left of the VirtualBox window there will appear one new VMs as illustrated in Figure 8. By pressing right click on the name of the VMs and then on "Settings" you can change the resources associated to the VMs that you have just created. We advise you to allocate at least at least 1 GB for the VMs with Kali (the default is 2 GB).

3. delete the images downloaded from the Kali Linux website, if you don't need them anymore.

4. configure the network as described previously (NAT Network on SecurityLabNetwork).



```
General
Name:              KaliFull
Operating System:  Debian (64-bit)

System
Base Memory:   2048 MB
Processors:    2
Boot Order:    Hard Disk
Acceleration:  VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display
Video Memory:           32 MB
Acceleration:           3D
Remote Desktop Server:  Disabled
Video Capture:          Disabled

Storage
Controller: IDE
  IDE Secondary Master:  [Optical Drive] Empty
Controller: SATA
  SATA Port 0:           Kali-Linux-2017.1-vbox-amd64-disk002.vmdk (Normal, 40,00 GB)

Audio
Host Driver:  Windows DirectSound
Controller:   ICH AC97

Network
Adapter 1:  Intel PRO/1000 MT Desktop (NAT Network, 'SecurityLabNetwork')

USB
USB Controller:  OHCI, EHCI
Device Filters:  0 (0 active)

Shared folders
None

Description
Kali Rolling (2017.1) x64
2017-04-24
- - - - - - - - - - - - - - - - - -
Username: root
Password: toor
(US keyboard layout)
- - - - - - - - - - - - - - - - - -
Kali Homepage: https://www.kali.org/

VM Homepage: https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/
Documentation: http://docs.kali.org/
Kali Support: https://forums.kali.org/
```

Figure 8: VirtualBox after you have imported the two VMs.

A.1 Additional packages

Regardless of the chosen option, you may check that the following packages have been installed (use `apt show` *package-name* to see details on the installed package, `apt-get` *package-name* to verify and install the missing packages):

- `vsftpd`
- `hexedit`
- `strongswan`
- `libstrongswan-extra-plugins`
- `dkms`
- `lynx`
- `s-nail`
- `alien`
- `nsis`
- `httptunnel`
- `net-tools`
- `ettercap`
- `ptunnel`
- `nmap`
- `openssl`
- `hashdeep`
- `p7zip-full`
- `apache2`