General laboratory instructions

Laboratory for the class "Security Verification and Testing" (01TYASM/01TYAOV)
Politecnico di Torino – AA 2021/22
Prof. Riccardo Sisto

prepared by:
Cataldo Basile (cataldo.basile@polito.it)

v. 1.2.1 (27/10/2021)

Contents

1 The laboratory work environment

A different laboratory work environment will be used for Laboratories 1,3,6 and for 2,4,5.

Figure 1: Initial menu of Kali 2021.3.

1.1 Work environment for Laboratories 1,3,6

For Laboratories 1,3,6 you will 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 enough to guarantee reasonable 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.

At login, authenticate yourself with username `kali` and password `kali`.

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
```

Figure 2: Kali working environment.

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

```
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.

1.2 Work environment for Laboratories 2,4,5

For the Laboratories 2,4,5 you will use the Ubuntu Linux available in the Labinf physical machines or the Labinf VMs, that are identical to them.

The Labinf VMs are always available. Here are the instructions to access them:

1. Install the virt-viewer client (available for all platforms at https://virt-manager.org/download/)
2. Go to the portal https://vlabinf.polito.it/ovirt-engine/web-ui/ and login with the same credentials you use for didattica.polito.it (check that the Profile is set to polito.it).
3. After login you should see the pool of VMs called ”vlabinf-ubuntu-2021-22-??”. You can start a VM by clicking on ”Run”. Then, when the VM status is shown as ”Running”, you can have access to the started VM by choosing the ”SPICE Console” from the drop-down menu.

2 Setting up the laboratory environment at home

For Laboratories 2,4,5, the necessary software can be installed on Ubuntu Linux 18.04 (the OS available at Labinf) as explained in the Appendixes at the end of this document (Appendix A ”Additional packages” and

Appendic C "Install additional tools"). The exercises proposed in the laboratories 1,3,6 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 virtual machines. In fact, you can use virtualisation to run in parallel one or more copies of Kali on a unique physical machine.

2.1 Suggested virtualization software

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 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 VM. 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 us any problem regarding the practical exercises in this environment). If you already own a license, you can use VMware Workstation (note that we do not suggest you to buy one).

2.2 Prepare the virtual machines

Kali provides, along with various ISO versions, also Virtual Machines (VM) ready to run in the VMWare and VirtualBox virtual environments. Therefore, you have three possibilities to have a Kali VM to be used for this laboratory:

1. *create a Live VM that loads the custom ISO provided with the course material* (see Section **??**).

   It is the scenario we tested the most (and the one closer to one you will experience in the physical laboratory) is the one that uses Live VMs . It uses less resources but you have to find ways to save you data, as Live VMs do not have persistence and you will lose you information when the VM is shutdown.

2. *download a ready-to-use VM from the Kali website* (see Section 2.3).

   The ready-to-use VMs are the most convenient way to have your environment ready in minutes. Unfortunately, they re rather big (Kali Full distribution is 2.2 GB for VMWare and 3.4 GB for VirtualBox) as they include a large number of packages (but not all the ones needed for these laboratories, that are listed in Appendix A). They also use a very demanding graphical environment that uses a lot of RAM and CPU. Moreover, you don't have full control on the installation options (which is OK if you just want to use these VM for the laboratories).

3. *manually create a new VM and install a fresh copy of Kali from an ISO.*

   If you want to create a new VM and install a fresh (and persistent) copy of Kali, you have to create a new VM and install the selected distribution using one of the official Kali ISO installation:

   https://cdimage.kali.org/kali-2021.3/kali-linux-2021.3-installer-amd64.iso

   Alternatively, you could use the custom Kali Live ISO that we provided as part of the course, as it has already includes all the packages needed but, at the same time, tries to minimize resource consumption. You can download this custom version from the following URLs and then follow the instructions in Section 2.2.1:

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

   Refer to the official Kali documentation if you want to follow this approach.

In short, we suggest:

1. if you have enough computational resources (e.g., a recent PC), download and use a ready-to-use VM from the Kali website
2. if you don't have enough computation resources, install the custom Kali Live we provided as part of the course,
3. if you don't have enough disk space but at least 8GB RAM, use the Live VM using the ISO we provided you.

> NOTE
>
> Once you have prepared one VM, you may clone it (as described in Section 2.4) and then assign it an appropriate name (as described in Section 2.5).

2.2.1 Create a Live VM 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 2.5), then select "Linux" as operating system and "Debian (64 bit)" as OS version (Kali is based on Debian).
- *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. 3);

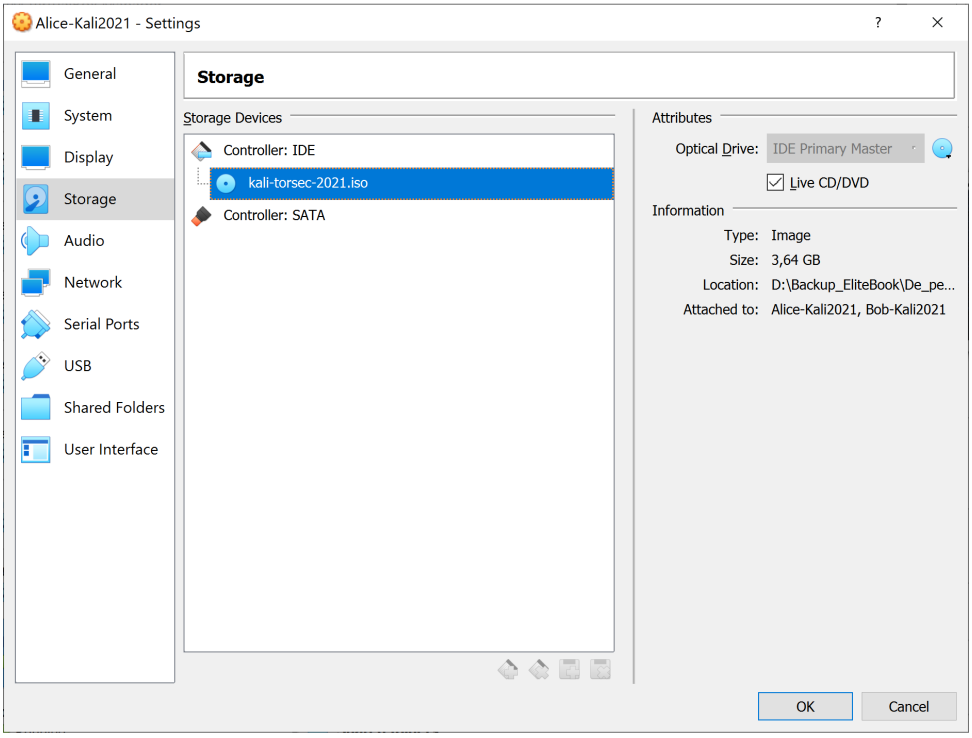

Figure 3: Selection of the Hard Disk with VirtualBox.

.

- click on the "device CD/DVD" button below the "Controller IDE", from the "Attributes" Tab change it to "IDE Primary Master". Click on the disk icon (just right of the IDE Primary Master 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. 4.

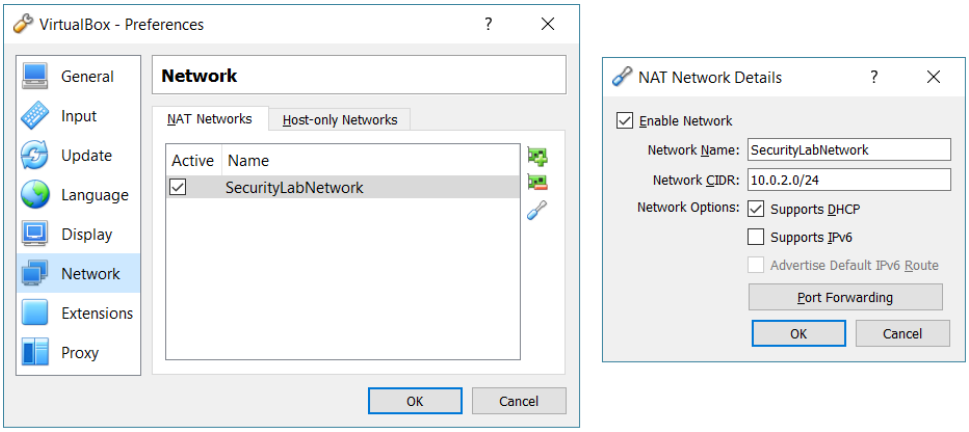

Figure 4: Configuration of a NAT Network with VirtualBox.

- 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”.

2.3 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 2.2.1. This section is for them, so if you have already performed the installation described in Section 2.2.1 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 5. 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).

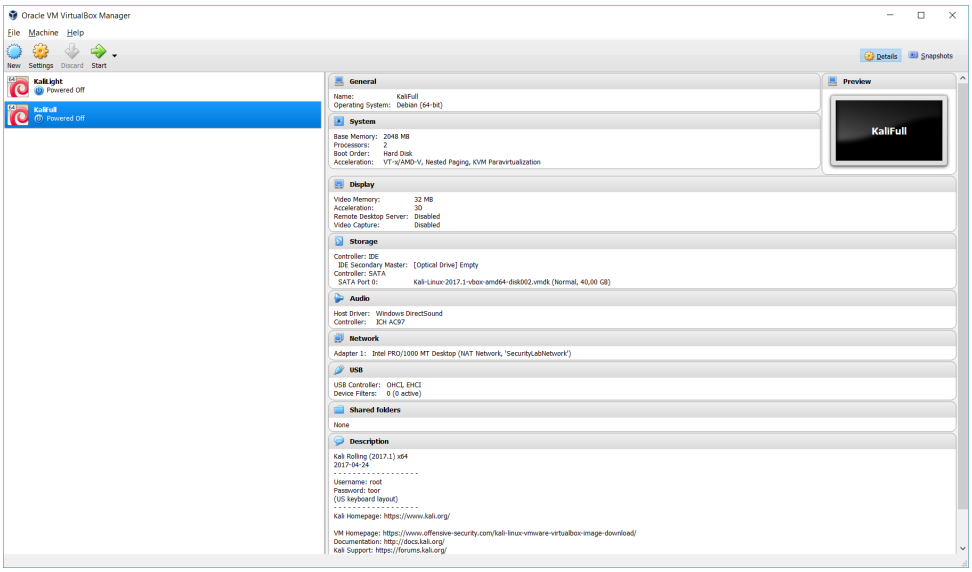

Figure 5: VirtualBox after you have imported the two VMs.

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).

2.4 Cloning VMs

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

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.

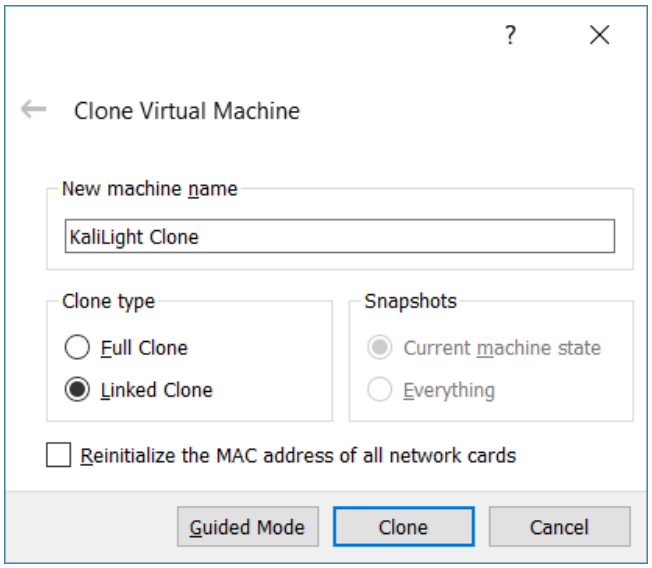

Figure 6: Window used to clone the VMs in VirtualBox.

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).

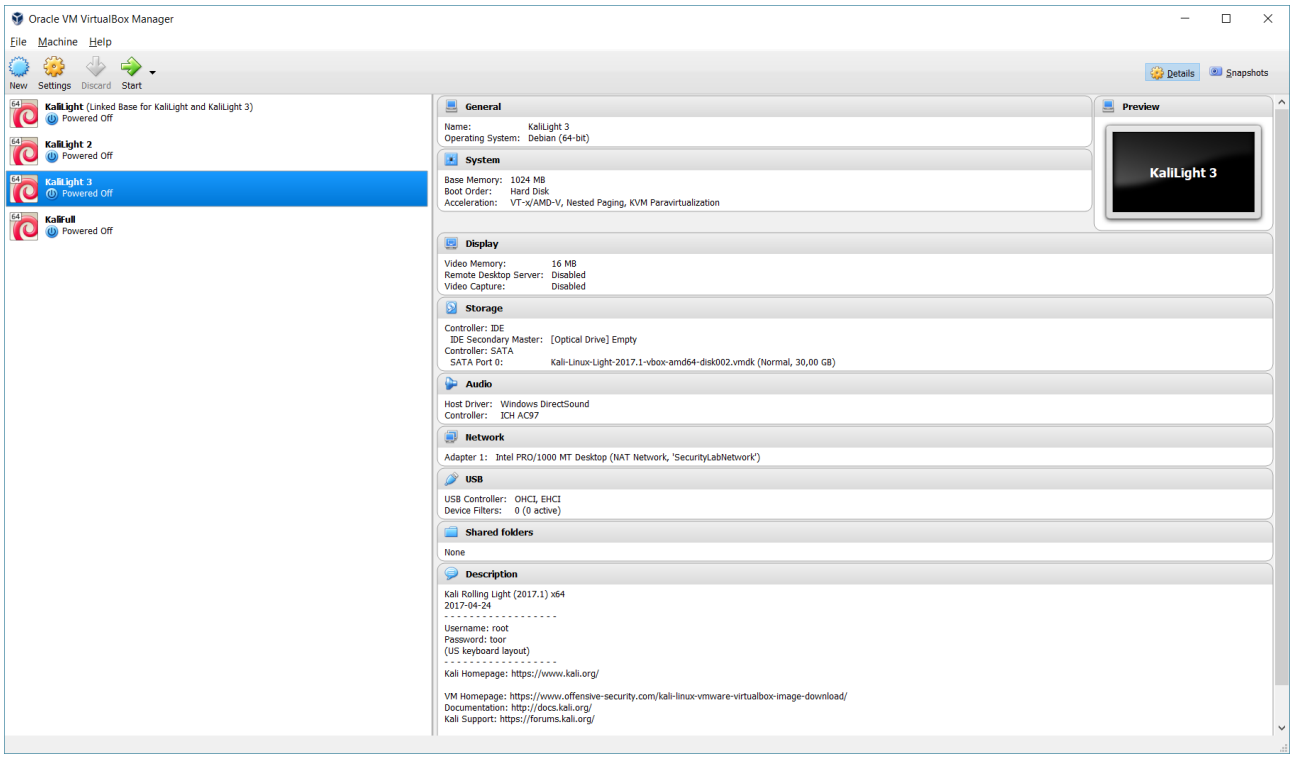

Figure 7: VirtualBox window after the preparation of the virtual laboratory.

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

Appendix A 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):

- `build-essential`
- `ocaml`
- `graphviz`
- `gtk2.0`
- `gvm`
- `gvmd`
- `gvm-tools`
- `gvm-common`

Appendix B Import a VMWare appliance into VirtualBox

In one of the labs you will have to download a virtual machine that has been designed to be used with VMWare. Luckily, even if the the VMs cannot be directly imported, the `.vdi` disks are compatible with VirtualBox.

For instance, you can download the Metasploitable2VM from the link below

https://sourceforge.net/projects/metasploitable/

Open the `metasploitable-linux-2.0.0.zip` file and copy the `Metasploitable.vmdk` file in a folder of your choice, e.g. a subfolder of the `VirtualBoxVms` folder.

In you VirtualBox application

1. run the Virtual Media Manager (available from the `File` Menu item or by pressing CRTL+D);
2. press the "Add a Disk Image" button;
3. select the `Metasploitable.vmdk` from the location where you have just extracted.

The `Metasploitable.vmdk` disk will appear the list of the available resources.

Now create a fresh new virtual Machine:

1. press the "New" button, then give a name (e.g. Metasploitable2), select Linux/Other Linux as operating system (one single core and 512 MB RAM are more than enough for this VM);
2. select the "Use an existing virtual hard disk file", then pick the `Metasploitable.vmdk` disk you have added before.

You will have to setup the network as explained in Section 2.2.1.

Appendix C Install additional tools

C.1 Install proverif

Install the dependencies

```
sudo apt install build-essential
sudo apt install ocaml
sudo apt install graphviz
sudo apt install gtk2.0
```

Download and install lablgtk

```
wget https://github.com/garrigue/lablgtk/releases/download/lablgtk2188/lablgtk-2.18.8.tar.gz
```

Decompress and install it with the following commands:

```
tar xvf lablgtk-2.18.8
cd lablgtk-2.18.8
./configure && make world
sudo make install
```

Decompress, install, and verify the installation with the following commands:

```
wgethttps://prosecco.gforge.inria.fr/personal/bblanche/proverif/proverif2.02pl1.tar.gz
tar xvf proverif2.02pl1.tar.gz
cd proverif2.02pl1
./build
./test
```

Copy the executables

```
proverif
proverif_interact
proveriftotex
```

in a directory in the user path (the user local bin or `/usr/local/bin`)

C.2 Install OpenVAS / Greenbone Vulnerability Manager (GVM)

A very quick and effective way to install OpenVAS (which has been renamed into Greenbone Vulnerability Manager (GVM) from the version 9 (GVM 11) is by executing the following scripts on this GitHub repository:

https://github.com/anubisthejackle/kali-openvas-install

However, this is not the way we installed it for testing the lab. We have manually installed the `gvm` packages

```
apt-get install gvm
```

then we used the following command

```
gvm-setup
```

In both cases, be prepared, it will be a long task also with a fast internet access.

C.3 Install flawfinder

Flawfinder can be installed simply by

```
sudo apt install flawfinder
```

C.4 Install SpotBugs and FindSecBugs as Eclipse plugins

SpotBugs is an Eclipse plugin, while FindSecBugs is a SpotBugs plugin specialized for security-related analyses.

Before installing SpotBugs and FindSecBugs, make sure you have already installed

1. Java jdk 1.8.0 or higher
2. Eclipse for Java EE Developers 4.6 or higher

If you miss item 1, you can install it as

```
sudo apt install openjdk-11-jdk
sudo apt install openjdk-11-source
```

If you miss item 2, you can install "Eclipse IDE for Enterprise Java Developers" by downloading it from https://www.eclipse.org/downloads/packages/ and extracting the archive in any location.

As an alternative, you can download the eclipse archive eclipse_vt.tar.gz from the course dropbox folder and extract it in any location. This copy already contains the SpotBugs plugin installed, so you can omit its installation.

In order to install the SpotBugs plugin, you need to select the command "Install new software" from the Help menu. Then, you enter the SpotBugs update site: https://spotbugs.github.io/eclipse/ and you install SpotBugs.

Once you have installed SpotBugs, you need to install FindSecBugs. In order to do so, you need to download the FindSecBugs jar file from

https://search.maven.org/remotecontent?filepath=com/h3xstream/findsecbugs/findsecbugs-plugin/1.11.0/findsecbugs-plugin-1.11.0.jar

and save it where you prefer. If you downloaded the eclipse archive, this jar file is already inside the archive (eclipse/findsecbugs folder).

Finally, you need to configure the FindSecBugs plugin: select the Preferences item in the Window menu. Then, choose Java - SpotBugs. Select the Plugins and misc settings tab and click Add. Here, select the FindSecBugs jar file and confirm the addition.

C.5 Install PVS-Studio (for C/C++)

The installation on Linux can be done according to the steps illustrated in

https://habr.com/en/company/pvs-studio/blog/462659/

```
wget -q -O - https://files.viva64.com/etc/pubkey.txt | sudo apt-key add - sudo wget -O
/etc/apt/sources.list.d/viva64.list https://files.viva64.com/etc/viva64.list sudo apt-get
update sudo apt-get install pvs-studio
```

The free educational license can be installed by giving the command

```
pvs-studio-analyzer credentials PVS-Studio Free FREE-FREE-FREE-FREE
```