General laboratory instructions

Laboratory for the class "Security Verification and Testing" (01TYASM/01TYAOV)
Politecnico di Torino – AY 2023/24
Prof. Riccardo Sisto

prepared by:
Riccardo Sisto (riccardo.sisto@polito.it)

v. 1.0.4 (21/11/2023)

Contents

1 The laboratory work environment

Some of the laboratories use the Ubuntu distribution, version 20.04, available at Labinf, while others use the Kali Linux distribution, version 2022.3. 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. We have performed preliminary checks to verify that the required packages are installed so you would not have to download them during the laboratory. In this way, we avoid unnecessarily overloading the network during laboratory time. Moreover, we have reduced the ISO size and used XFCE as the unique Desktop Environment (now the standard one in the last Kali distributions) to minimize the system requirements, as not all the PCs in the lab are recent enough to guarantee good performance.

Figure 1: Initial menu of Kali 2022.3.

This material does not cover potential problems due to driver incompatibilities of your PC or network configuration at your place. However, they are rare.

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 will see a typical Grub menu like 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 2022.3 should have already configured the network correctly (since a DHCP server is available in the lab).

The X graphical server will start automatically, showing an XFCE Desktop Environment like in Figure 2.

Figure 2: Kali working environment.

Useful commands

We remind you of 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 curly brackets (i.e. { and }) report enumerates, and the words in *Italic* need to be replaced with the specific data required by the command.

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 the 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 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

NOTE

SETTING UP THE ENVIRONMENT (IN SHORT):
Download a VM from the Kali repository, unzip the downloaded file, move the obtained folder to your VMs folder, double-click on the ova file, and use it. You can always throw it away, download a fresh one, and start from scratch if you mess everything out. Clone it if you need more than one VM; you will save disk space. Read the instructions below if your personal PC has very limited resources or something fails.

The laboratory exercises proposed may require you to use more than one PC simultaneously. In the following sections, we describe how you can create a working environment similar to the one used in the laboratory with virtual machines at home.

2.1 Use of a virtualised environment

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

Kali provides, along with various ISO versions, Virtual Machines (VM) ready to run in the VMWare and VirtualBox virtual environments. Unfortunately, these VMs are rather big (Kali Full distribution is >2 GB for VMWare and 3 GB for VirtualBox) for the basic image. If you want to use the original Kali version or minimize the requirements, you must create a VM and install the selected distribution. If you only want to do the laboratories at home and you have a relatively recent PC, we don't suggest wasting time with installations.

Alternatively, we suggest you 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 DropBox of the course and then follow the instructions in Section 2.1.2. You could also use this ISO 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 PCs) includes three VMs, that shall run the Kali custom that we provided to perform the exercises with reduced workload (e.g. RAM).

We provide here the instructions to prepare the working environment for a virtual Security Lab Network composed of three Kali VMs. We propose to use Oracle VM VirtualBox, a free virtualisation product 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 it does not scale well when the number of VMs increases (compared to expensive commercial products). For this reason, managing more than two VMs on a single PC with only 2 GB RAM could be problematic because the system might be too slow. However, you should not have any usability problems if you have a recent PC with at least 8 GB RAM (or just with GVM).

The version we refer to in this document is 6.1.14 which 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.

> NOTE
>
> An alternative free product is VMware Player. According to the official documentation, VMware Player supports at most one VM at a 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. VMware vSphere Hypervisor is too big for the exercises proposed, while VMServer is not maintained anymore since 2010. Note that we have not tested any virtualisation environment for MacOS; however, students that used a virtualisation environment for MacOS during the last year have not reported any problems regarding the practical exercises in this environment (provided you run VMs for the new family of processors). If you already own a license, you can use VMware Workstation (note that we do not suggest that you should buy one, it's not needed).

In short, we suggest:

1. if you have enough computational resources (e.g., a recent PC), download a ready-to-use VM from the Kali website; you may have to install some packages (not a big issue, though),
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 (and look for some way to have persistence).

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 the DropBox of the course.

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, then select "Linux" as the operating system and "Debian (64 bit)" as the OS version (Kali is based on Debian).

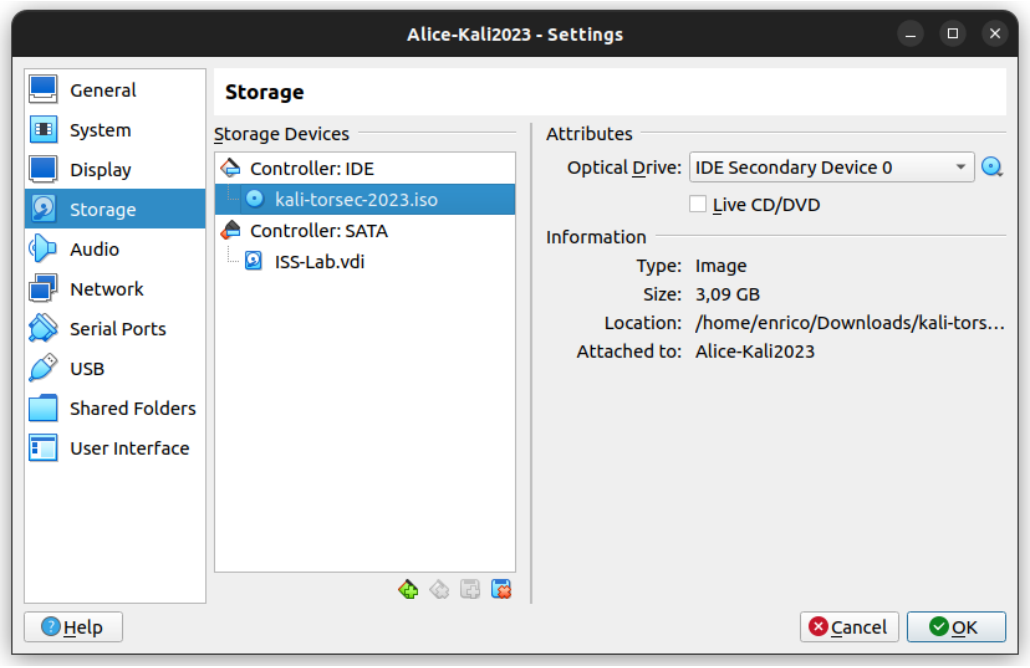

Figure 3: Selection of the Hard Disk with VirtualBox.

- *select the VM RAM size*. As already explained, we suggest you 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);
- 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-linux-2020.3-live-full-amd64.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.
- 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 VM naming

In the laboratories, the various VMs may perform different "roles" in the exercises. For example, besides Alice and Bob, which are used to indicate generic users instead of A and B, we will also use other names whose

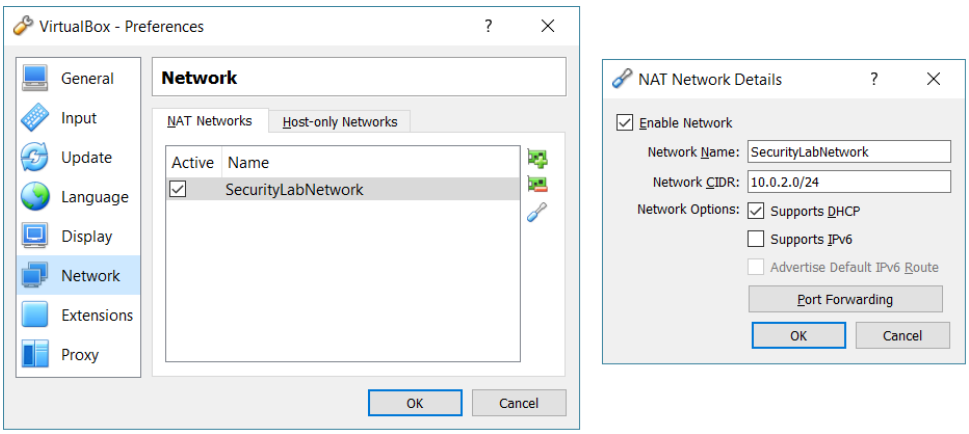

Figure 4: Configuration of a NAT Network with VirtualBox.

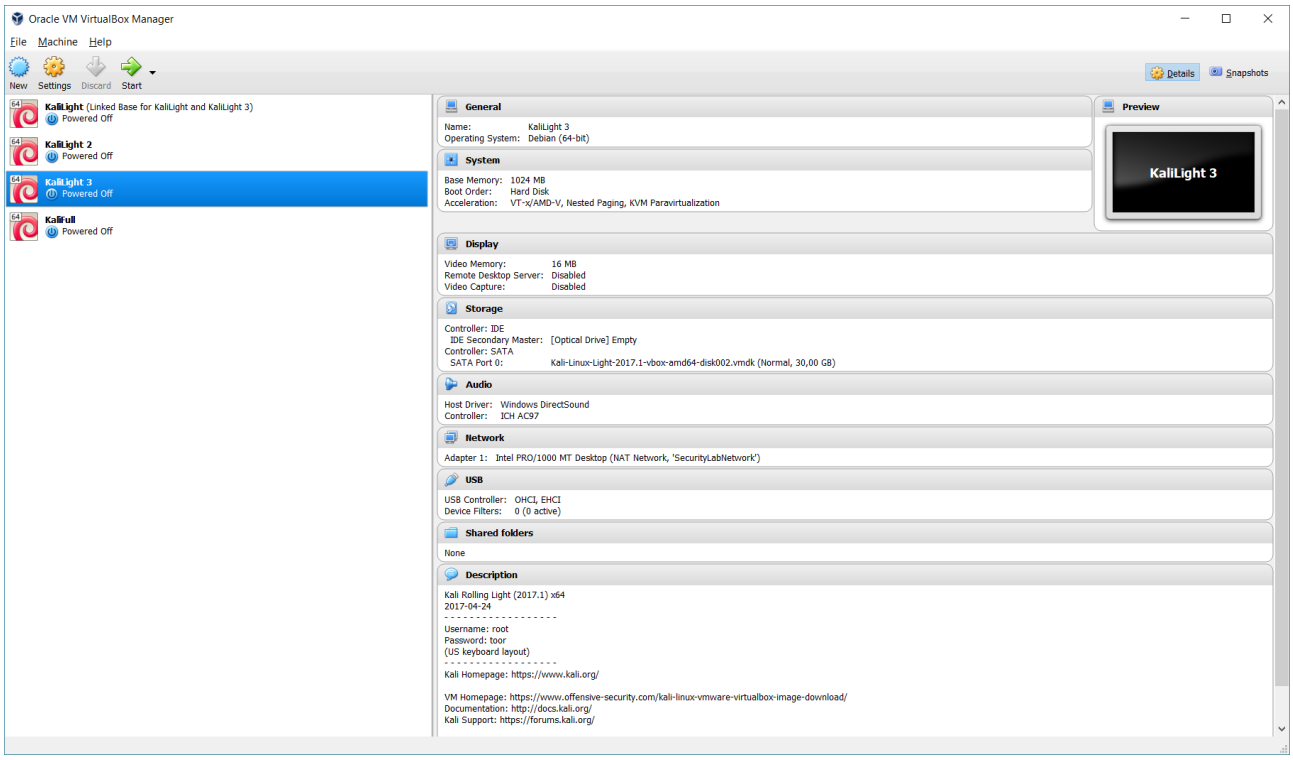

Figure 5: VirtualBox window after the preparation of the virtual laboratory.

initials recall their role in the practical exercise. 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 want to check that the following packages have been installed (use `apt show` *package-name*. For instance, you may want to see details about a specific installed package, and `apt-get` *package-name* to verify and install a missing package):

- 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 designed to be used with VMWare. Luckily, even if the VMs cannot be directly imported, the `.vdi` disks are compatible with VirtualBox.

For instance, you can download the Metasploitable2 VM from the link below

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

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 your 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 in the list of 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 the 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.

As explained in Section 2.1.2, you will have to set up the network.

Appendix C Install additional tools

C.1 Install proverif

This installation procedure has been tested on Ubuntu 20.04 (the same OS available in the lab).

Install the dependencies

```
sudo apt update
sudo apt install build-essential
sudo apt install ocaml
sudo apt install ocaml-findlib
sudo apt install graphviz
```

```
sudo apt-get install gtk2.0
```

Download and install lablgtk

```
wget https://github.com/garrigue/lablgtk/archive/refs/tags/2.18.12.tar.gz
```

Decompress and install it with the following commands:

```
tar xvf 2.18.12.tar.gz
cd lablgtk-2.18.12
./configure && make world
sudo make install
```

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

```
wget https://bblanche.gitlabpages.inria.fr/proverif/proverif2.05.tar.gz
tar xvf proverif2.05.tar.gz
cd proverif2.05
./build
./test
```

Copy the executables

```
proverif
proverif_interact
proveriftotex
```

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

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

We have manually installed the `gvm` packages with

```
sudo apt-get install gvm
```

then we used the following command

```
sudo gvm-setup
```

> **NOTE**
>
> You can also find a Kali VM in the Dropbox of the course with GVM installed, configured, and all the packages downloaded.

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

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

However, this is not how we installed it on the course VM, so you may notice differences, e.g. in the admin user's password).

In both cases, be prepared. It will be a lengthy task also with fast internet access.

> **ATTENTION**
>
> This year GVM moved from Postgres 15 to Postgres 16, you may experience even more problem than usual, as one Postgres extension developed for v15 seldom fails with v16.

C.3 Install flawfinder

This installation procedure has been tested on Ubuntu 20.04 (the same OS available in the lab).

Flawfinder can be installed simply by

```
sudo apt install flawfinder
```

C.4 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
```

C.5 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 if it is not already installed. The FindSecBugs jar file can be downloaded from

https://find-sec-bugs.github.io/download.htm

You can check whether the plugin is already installed by going to the Preferences item in the Window menu. Then, choose Java - SpotBugs and select the Plugins and misc settings tab. If the plugin is not yet installed, it can be installed by clicking Add and selecting the plugin jar file that was downloaded.