General laboratory instructions

Laboratory for the class “Information Systems Security” (02TYMUV)
Politecnico di Torino – AA 2024/25
Prof. Antonio Lioy

prepared by:
Andrea Atzeni (shocked@polito.it)
Flavio Ciravegna (flavio.ciravegna@polito.it)

v. 1.0 (10/10/2024)

Contents

1 The laboratory work environment **1**

2 Setting up the laboratory environment at home **4**

2.1 Use of a virtualised environment 4

2.1.1 Suggested virtual configuration 4

2.1.2 Live VMs from an ISO 5

2.1.3 VM naming 6

A Additional packages **7**

1 The laboratory work environment

The laboratory exercises use the Linux distribution Kali, version 2024.3. We have created a “custom” ISO image of this Linux distribution, where we tested the exercises proposed throughout the laboratories. 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 unnecessarily overloading the network during laboratory time. We used XFCE as the unique Desktop Environment (now the standard one in the last Kali distribution) to minimize the system requirements.

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 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`.

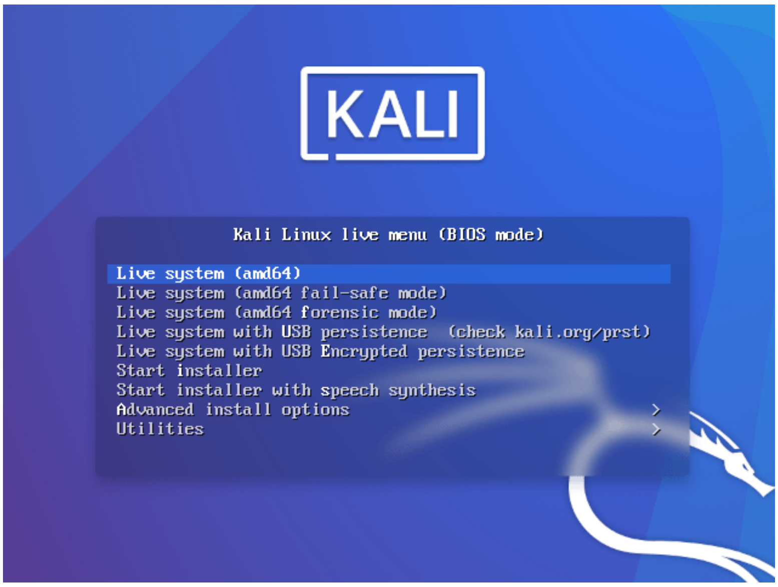

KALI
Kali Linux live menu (BIOS mode)
Live system (amd64)
Live system (amd64 fail-safe mode)
Live system (amd64 forensic mode)
Live system with USB persistence (check kali.org/prst)
Live system with USB Encrypted persistence
Start installer
Start installer with speech synthesis
Advanced install options
Utilities

Figure 1: Initial menu of Kali 2024.3.

At the end of the boot phase, Kali 2024.3 should have already configured the network correctly (since a DHCP server is available in the lab).

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

Figure 2: Kali Linux 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, 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):
We provide an ISO image for this lab (as described below), most of the exercises have been tested with this image. Alternatively, you could download a Kali VM from the Kali repository, but you might need to install additional packages. If this is your option you may 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. You might 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, 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 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 suggest not 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:
https://www.dropbox.com/scl/fi/p8w4kapazcmn1wccdns7q/kali-linux-2024.3-live-xfce-amd64.iso?rlkey=vt99d81gj0akec5q3fth8m04s&st=vdiaf9oc&dl=0
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 we suggest (the one we used to test the exercises with virtualisation on our PCs) includes three VMs, that shall run the customized Kali with reduced workload (e.g. RAM).

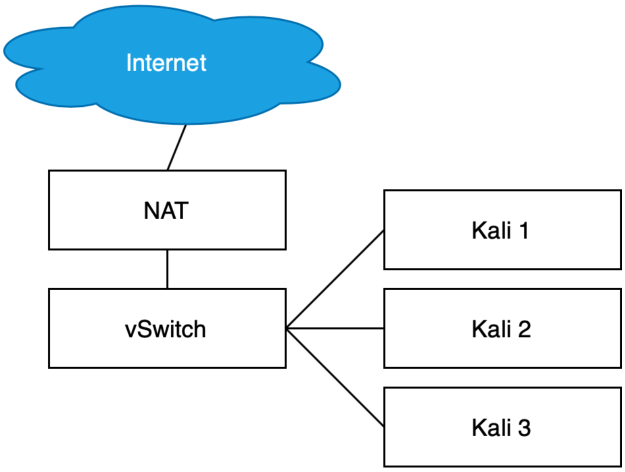


Figure 3: Network topology to recreate the laboratory environment with NAT Network and three VMs.

We provide 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.

The version we refer to in this document is 7.1.2 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`.

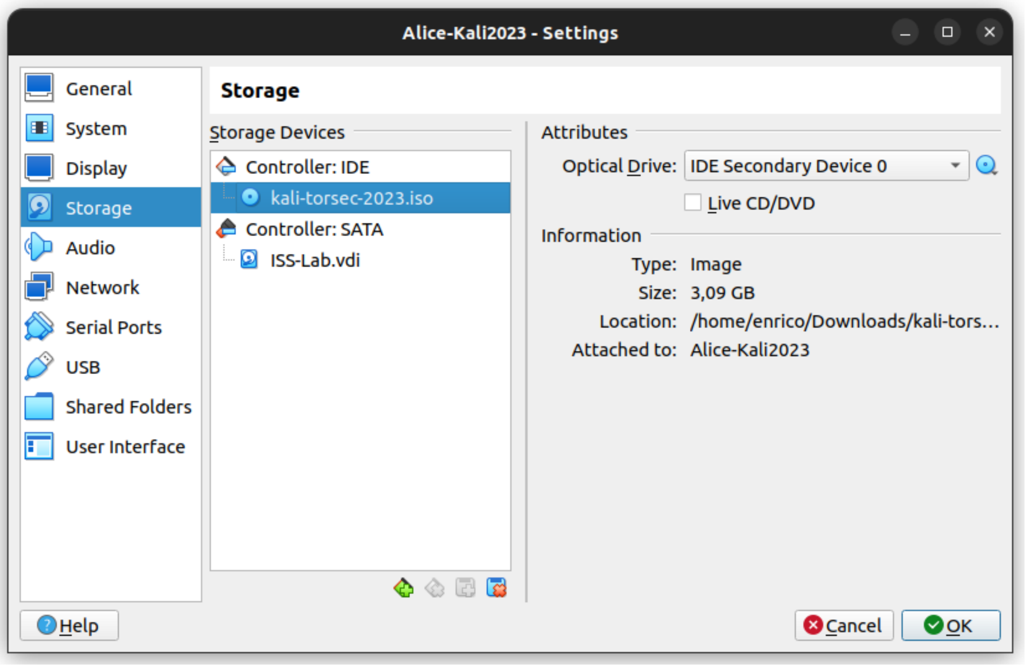
> NOTE
>
> An alternative free product is VMware Player. According to the official documentation, VMware Player supports at most one VM at a time. In practice, this limitation is not applied, and you should be able to execute more than one VM. We have not tested the practical exercises with this product, 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. 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).

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.

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).



Alice-Kali2023 - Settings

Storage

Storage Devices

- Controller: IDE
  - kali-torsec-2023.iso
- Controller: SATA
  - ISS-Lab.vdi

Attributes

Optical Drive: IDE Secondary Device 0

□ Live CD/DVD

Information

Type: Image
Size: 3,09 GB
Location: /home/enrico/Downloads/kali-tors...
Attached to: Alice-Kali2023

Figure 4: Selection of the Hard Disk with VirtualBox.

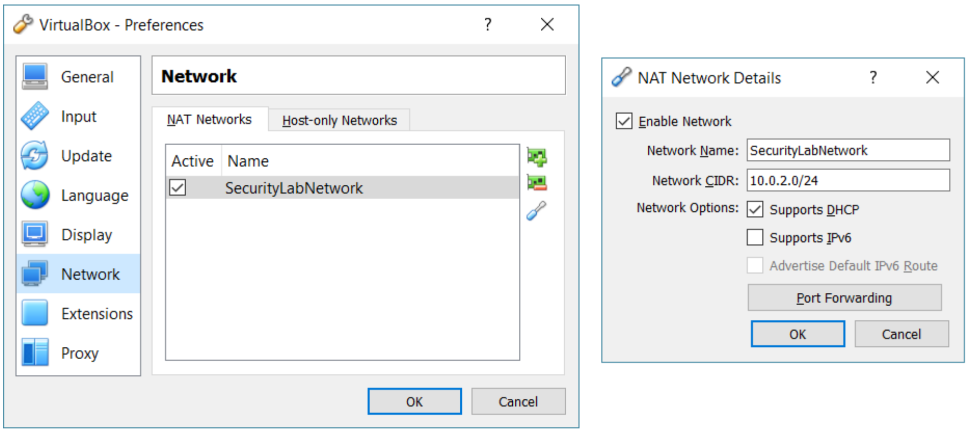
- *select the VM RAM size*. As already explained, we suggest you allocate at least 1 GB for the VMs with Kali
- *configure Hard Disks*. Unpin the “Do not add a Virtual Drive” option and continue (we will configure a DVD later).

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. 4);
- 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-2024.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 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 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).



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.

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* if you want to see details about a specific installed package, and `apt-get` *package-name* to verify and install a missing package):

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