

Cybersecurity

Laboratory 01: Lab environment

First name:

Last name:

Index number:

Exercise date:

Used Lab equipment:

Group members:

Report submission

The document containing the exercise instructions includes active text fields where answers to the provided questions must be entered. As a result, once all answers are filled in (along with personal information of the individual completing the exercise), the document transforms into a report. It's recommended to open the file using Adobe Acrobat, or browsers such as Firefox or Chrome.

If you wish to maintain the functionality of the text fields after saving the file (allowing for future changes), avoid selecting the 'print to PDF' option when saving the file to your disk. For added safety against potential loss of entered data due to system crashes, save the file periodically.

Final report should be composed of the following files:

000000_PT_01.pdf (student ID: 000000, Lab number 01) - main report file (this file)

The report should be uploaded to Moodle no later than the fifth day after the end of the exercise.

Introduction

The objective of this lab task is to set up a virtual environment for penetration testing. Selecting appropriate tools, ensuring their user-friendliness, and maintaining up-to-date versions can ensure a smooth execution of testing as per the plan. Experienced penetration testers usually curate their own customized setups. Beginners in this field can opt for pre-made solutions like virtual machines running on the Kali Linux (KL) operating system [1].

Kali Linux is a Linux distribution based on Debian [2]. Debian follows the open-source and free software philosophy, allowing for unrestricted use and modification. KL, like Debian, is open-source, but it is specialized in addressing network security concerns such as penetration testing, digital forensics, and reverse engineering. Because it offers a comprehensive toolkit, it's particularly suitable for novice penetration testers. You can obtain KL as an .iso image, which can be installed on a PC. Alternatively, you can download a pre-configured virtual machine designed to work with popular virtualization platforms like VirtualBox [3] or VMware [4]). In this task, we will be setting up a virtual machine using VirtualBox. For practical testing, it's recommended to perform exercises on physical devices within a dedicated lab environment. However, if a dedicated lab is unavailable, a virtual environment suffices for initial experimentation. This environment will consist of three additional virtual machines: Metasploitable 3 [5], Metasploitable 2 [6], and Jangow [7]. All these virtual machines will be interconnected on an internal network within the VirtualBox environment.

Lab scenario

1 Installation of VirtualBox software

If VirtualBox (VB) is already installed on your computer, make sure it is the latest version. If not, update the software. If you do not have VB installed, download the latest version of the software (it is free) from the website: <https://www.virtualbox.org/wiki/Downloads>.

Once downloaded, run the installation programme and follow its suggestions. The installation is intuitive and does not require the user to have specific knowledge of operating systems. User interaction is reduced to going through the installation steps and clicking on the 'Next' button. Once the installation is complete, start VB. The main programme window shown in Figure 1 will appear.



Figure 1: VirtualBox main window

2 Import of a Kali Linux virtual machine

As already stated in the introduction, you can prepare the KL virtual machine yourself (i.e. install KL in a virtual environment) or you can use a ready-made machine, which can be downloaded from:

<https://www.kali.org/get-kali/kali-virtual-machines>.

In order to save time, we will use the ready-made machine. After downloading the version of your choice (64bit version suggested), the file `kali-linux-2023.2-virtualbox-amd64.7z` needs to be unpacked (e.g. with the free program 7zip). The archive contains two files: `kali-linux-2023.2-virtualbox-amd64.vbox` and `kali-linux-2023.2-virtualbox-amd64.vdi` (file names may differ - always download the latest version of KL).

To import a virtual machine from KL, double-click the `kali-linux-2023.2-virtualbox-amd64.vbox` file and the virtual machine will automatically be imported into VirtualBox (Figure 2).

3 Import of a Metasploitable 3 virtual machine

The Metasploitable 3 virtual machine was developed by the Rapid7 Metasploit team [5] with learning in the area of penetration testing in mind. It contains a number of vulnerabilities to be detected and exploited. It should be emphasised that the Metasploitable machine (and its ilk) should only be run in a virtual environment or with access to a dedicated laboratory network without direct access to the public network (public IP address). Running the machine with direct access to the public network can be used by hackers to take control of this machine and use it for further attacks. In the second part of the exercise, the skills learned will be applied to the laboratory network.

From <https://sourceforge.net/projects/metasploitable3-ub1404upgraded/files/>, download the Metasploitable 3 virtual machine image (file `Metasploitable3-ub1404.ova`) and import it into VirtualBox (VB). To import the machine into

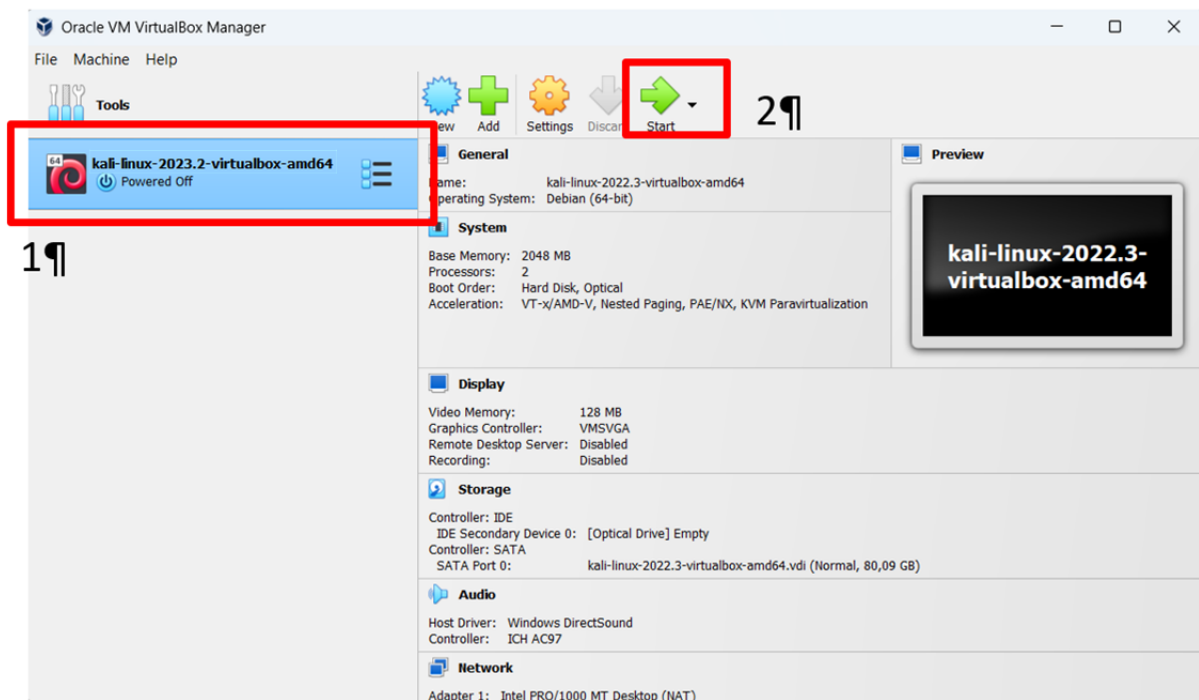


Figure 2: VirtualBox after importing the Kali Linux virtual machine (version: kali-linux-2023.2)

VB, go in the file explorer to the directory where the machine was saved after downloading and double-click on the Metasploitable3-ub1404.ova file. The VirtualBox import window will then appear (Figure 3):

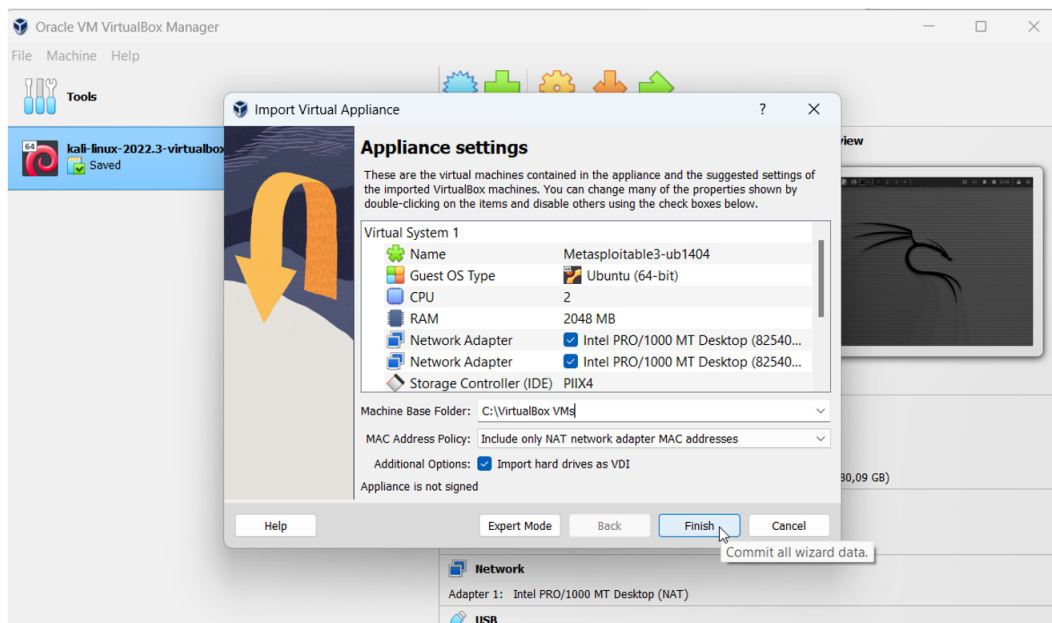


Figure 3: Import window (Metasploitable3)

When the 'Finish' button (Figure 3) is clicked, the import will start and, once completed, the Metasploitable machine will appear in the list of available machines (Figure 4).

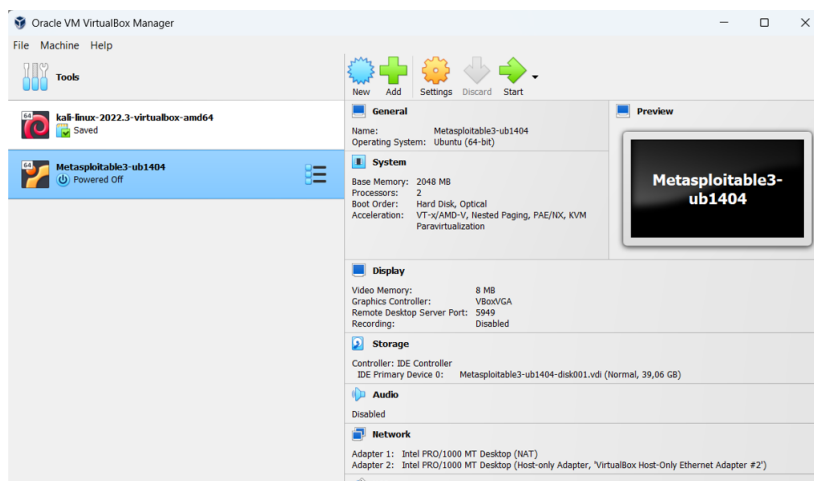


Figure 4: VirtualBox after importing the Metasploitable 3

4 Import of Metasploitable 2 virtual machine

Metasploitable 2 is an older version of the machine described in the previous chapter. It contains a number of vulnerabilities, the detection of which will serve to gain knowledge about penetration testing.

Download the virtual machine from <https://sourceforge.net/projects/metasploitable/> and then import it into your VirtualBox environment.

5 Jangow virtual machine

As a third test virtual machine, a Jangow machine. It is a machine available at www.vulnhub.com which is a kind of collection of virtual machines that can be freely used for learning about cyber security. Download the Jangow machine from <https://www.vulnhub.com/entry/jangow-101,754/> and import it into the VirtualBox environment.

6 KaliLinux update

As the Kali Linux virtual machine will be used as a pentester toolkit, it is good practice to update it before using it for testing. To do this go into the properties of the machine and change its network properties so that it can communicate with the Internet. This can be NAT or Bridged Adapter (see figure 5) Now start the machine. Once the machine is

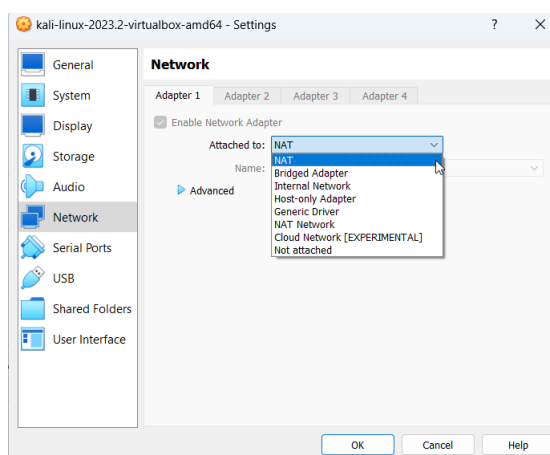
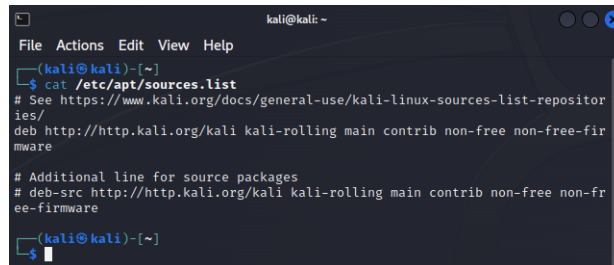


Figure 5: Kali Linux network options

up and running, switch on the terminal and check that the machine has been automatically assigned an IP address (terminal -> command: ifconfig). Now enable the Kali update:

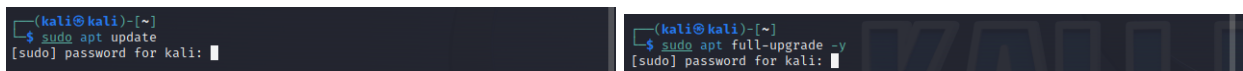
1. check that the package sources are up to date (cat /etc/apt/sources.list)



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ cat /etc/apt/sources.list  
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-repositor  
ies/  
deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-fir  
mware  
  
# Additional line for source packages  
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free non-fr  
ee-firmware  
(kali@kali)-[~]  
$
```

Figure 6: Kali Linux packets sources

2. update system (sudo apt update, sudo apt full-upgrade -y)



```
(kali@kali)-[~]  
$ sudo apt update  
[sudo] password for kali:   
  
(kali@kali)-[~]  
$ sudo apt full-upgrade -y  
[sudo] password for kali:   

```

Figure 7: Kali Linux update

Important: once the update process is complete, switch off the machine

7 Virtual network

To ensure that the tasks carried out as part of the exercises do not adversely affect the operation of the university's network, all machines used should be connected to an internal network named PT_lab_net. To connect a given virtual machine to this network, create a network properties window for this machine, select this Internal Network and choose a name from the drop-down list. If PT_lab_net is not in this list, enter it there (which is equivalent to creating it). For subsequent virtual machines this network will already be available.

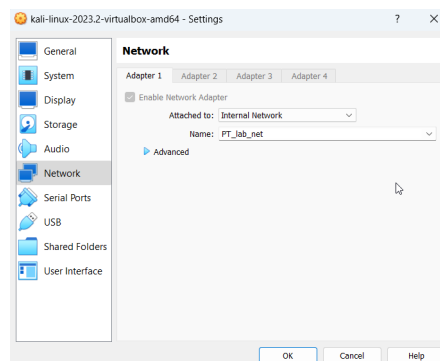


Figure 8: Kali Linux network settings

With this configuration, the test network shown in Figure 7 will be built.

8 DHCP server

To enhance the virtual environment, a DHCP server will be run on the PT_lab_net test network. The functions of the server will be performed by VirtualBox. To start the DHCP server for the internal network, go to the directory (command line) where VirtualBox is installed and then run the following command:

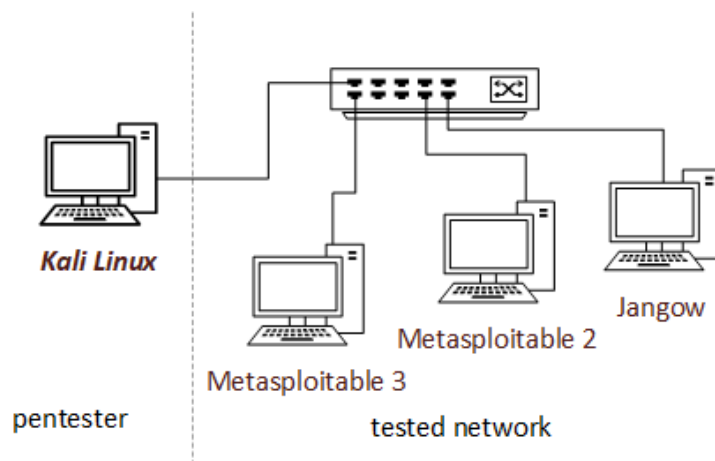


Figure 9: Virtual test environment topology

```
C:\Program Files\Oracle\VirtualBox>vboxmanage dhcpserver add --network=PT_lab_net --server-ip=192.168.100.1
--lower-ip=192.168.100.10 --upper-ip=192.168.100.50 --netmask=255.255.255.0 --enable
```

The result of this command will set the parameters for PT_lab_net:

- IP address of dhcp server: 192.168.100.1
- The first IP address of DHCP server: 192.168.100.10
- The last IP address of DHCP server: 192.168.100.50
- Mask: 255.255.255.0

Thanks to the DHCP server, it will be possible to expand the virtual test environment with additional machines without much difficulty without having to manually assign addresses.

9 Initial start-up

Double-click on the name of the virtual machine (box 1, Figure 2) or click on the start button (box 2, Figure 2) and then wait for the virtual machine to start (Figure 3).

To log in use the following login credentials: username: kali, password: kali After logging in run the terminal (command line) and check the ip address of the machine (ifconfig command) and then check if the machine has the possibility of communicating with the Internet e.g. using the ping command check the availability of the web server serving the wp.pl service (ping wp.pl command). If KL receives replies from the wp.pl server it means that communication with an external network is possible. If communication with the external network is possible, check the network settings of the machine again.

What is the IP configuration of the Kali Linux machine (IP address, mask, default gateway)?

All the tools available in KL are grouped thematically (Figure 9). To display this menu, click on box 1 (Figure 9).

You can find more details about Kali by selecting option 42 - Kali&OffSec Links. Nevertheless, the penetration testing tool is ready to go.

You can now proceed to start the remaining virtual machines. Once they are up and running, check the IP addresses. This can be done from within the KL machine by running the netdiscover program in a terminal. What and how many IP addresses have been detected using netdiscover?

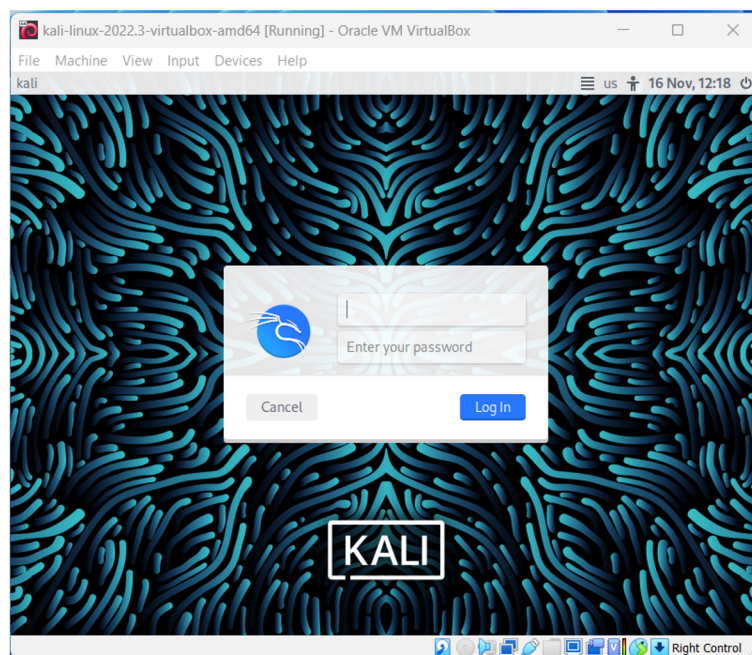


Figure 10: Virtual machine (Kali Linux) running

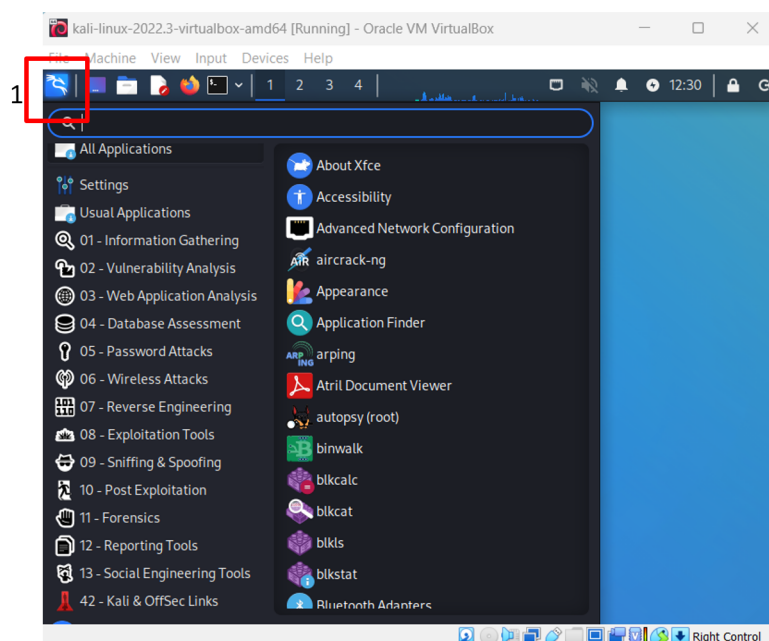


Figure 11: Tools available in Kali Linux

References

- [1] "Kali Linux, project website," <https://www.kali.org/>, accessed: 2023-06-15.
- [2] "Debian, project website," <https://www.debian.org/>, accessed: 2023-06-15.
- [3] "Virtual box, project website," <https://www.virtualbox.org/>, accessed: 2023-06-15.
- [4] "Wmware, software website," <https://www.vmware.com/>, accessed: 2023-06-15.
- [5] "Metasploitable 3, project website," <https://www.rapid7.com/blog/post/2016/11/15/test-your-might-with-the-shiny-new-metasploitable3/>, accessed: 2023-06-15.
- [6] "Metasploitable 2, project website," <https://docs.rapid7.com/metasploit/metasploitable-2/>.
- [7] "Jangow, project website," <https://www.vulnhub.com/entry/jangow-101,754/>, accessed: 2023-06-15.

Additional notes

If provided space for an answer is insufficient, use this additional space.

