INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Tutorial 0

Introduction to the Forensic Environment

2024/2025

nuno.m.santos@tecnico.ulisboa.pt

Introduction

This guide will introduce you to the Kali forensic toolkit. Kali Linux is a live CD distro that has a large number of security tools already installed and configured. These tools can also be used for the purpose of collecting and examining digital forensic artifacts. Kali can be used throughout this course for all our lab assignments.

Figure 1: Kali Linux.

This tutorial is split into two parts. The first part will help you set up an environment in which you can run forensic tools and analyze digital artifacts. To this end, you must create a clean slate virtual machine and prepare it for storing artifacts using the Kali Live CD. The second part aims to provide an overview of the forensic tools you will find in the Kali distribution and to introduce you to how some of these tools are used for forensic activities. In particular, you have to perform several activities: explore unknown file artifacts, audit passwords using a password cracker, capture and examine network traffic, and audit existing public vulnerabilities of a given network.

Note that while some of the forensic tools contained in the Kali distribution can be used for post-mortem analysis, e.g., to examine file artifacts in the aftermath of a given incident, others can be used for live forensics, e.g., to collect evidence while a network penetration is taking place. For live forensics, in particular, an important step of every analysis process is to be prepared. There is often little time available to capture evidences before they disappear. For instance, open browse sessions, network sockets connections, executing processes, etc. Preparing your toolkit is important to enable you to act quickly.

1 Preparing the environment

For the purpose of this class, we will emulate a real forensic analysis process using a virtual environment. This virtual environment can be reproduced using your own laptops. However, it is possible that some of the steps explained here need minor adjustments given the specific characteristics of your installation.

Before we begin, you need to obtain Kali. If you are executing this tutorial from the Lab facilities, download Kali linux from: `https://turbina.gsd.inesc-id.pt/csf2324/resources/kali-linux-2023.2a-installer-amd64.iso`. Otherwise, download it from one of the official mirrors.

1.1 Configure the forensic (virtual) station

We will be using VirtualBox to virtualize Kali. You may download VirtualBox from `https://www.virtualbox.org/`. To configure the forensic virtual station, proceed as indicated in the following screenshots.

Start by clicking on the *New* button at the toolbar.

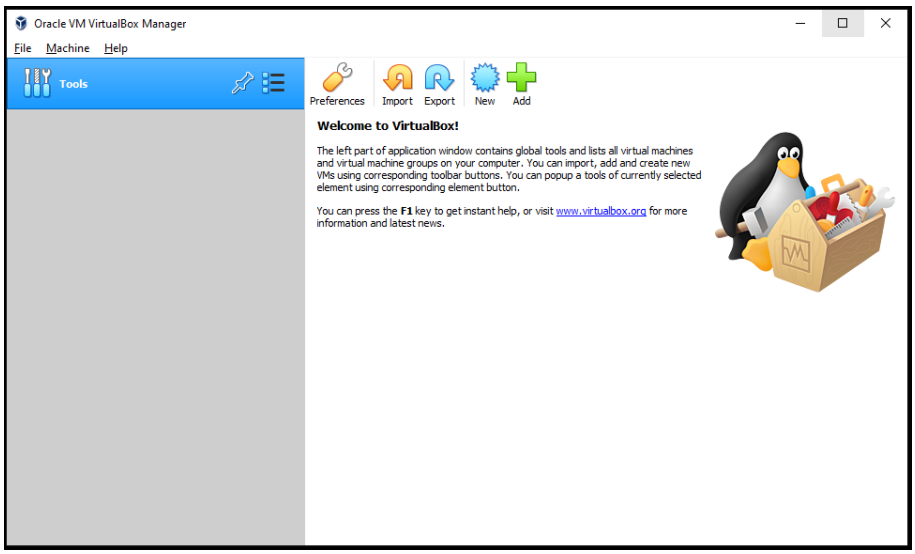

Figure 2: Create a new VM

As a first step, associate the downloaded image to the virtual machine.

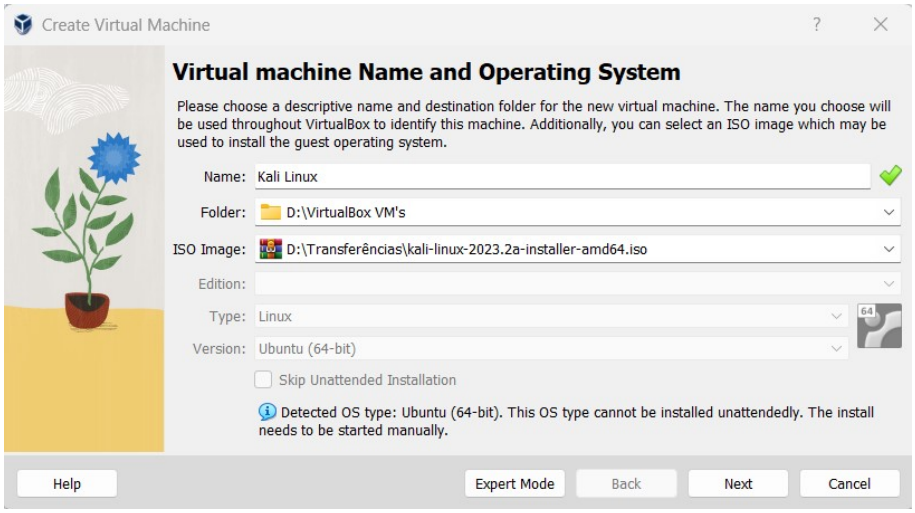

Figure 3: Customize the VM.

Next, customize the VM. Set at least 2GB of memory. For the workstations in the lab, choose 4GB (4096 MB). Then adjust the number of CPUs according to your physical machine.

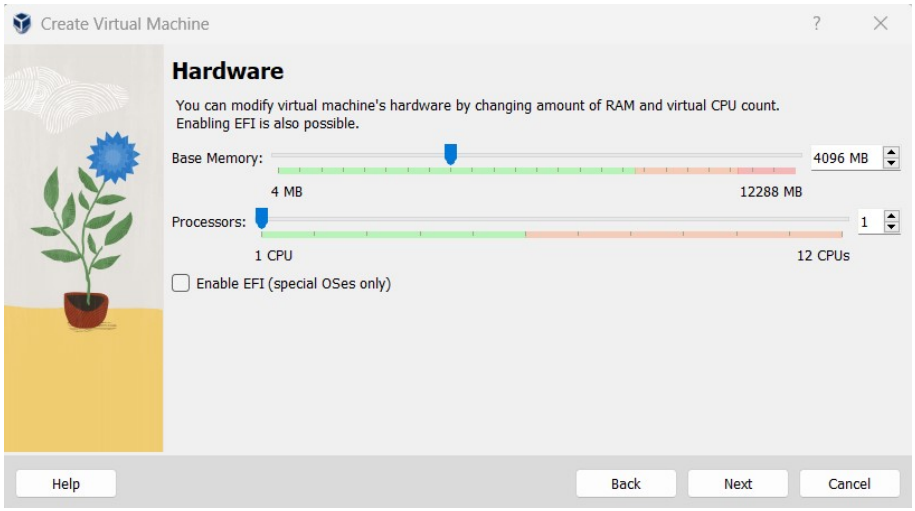

Figure 4: Define the Storage size

Finally, adjust the storage size to at least 20GB. In real-world scenarios, we often require 100s of GB, due to the need of saving disk images and analysis/extractions of evidence in these disks.

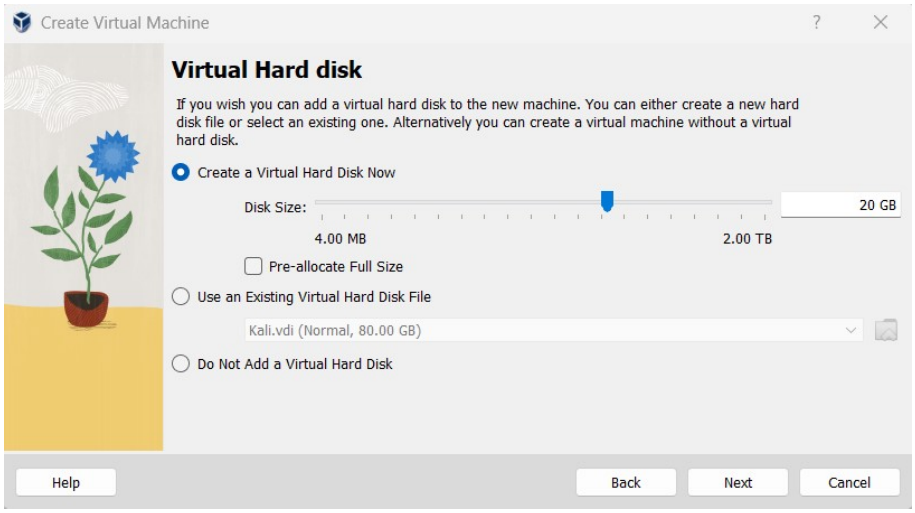

Figure 5: Associate the Kali image.

1.2 Starting Kali linux

Start the virtual machine selecting the VM at the Virtualbox side pane and then choose *start*. Once the VM boots up, select "**Graphical Install**" and then press *enter*.

Figure 6: Kali Linux - Boot screen

Choose your desired settings or follow the predefined options to complete the installation process.

> Note: When prompted to enter a root password enter "**kali**" so that we can demonstrate the usage of a password cracker later on. This password can always be updated later.

Finally, make sure to install the **GRUB boot loader** on your main partition as shown in Figure 7

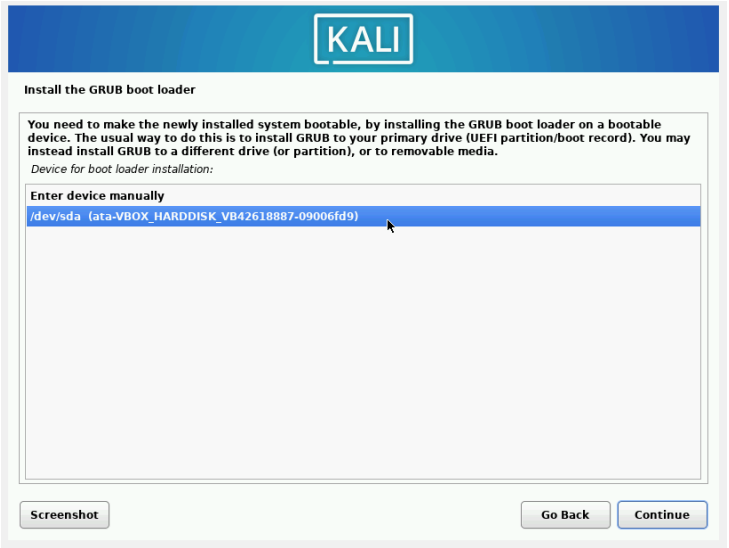

Figure 7: Installing the GRUB boot loafer

1.3 Explore the tools available in Kali

The Kali website has a description of all the tools installed in the distro. Tools are organized in several sections according to the kind of analysis they are designed to do. Navigate the menus as shown in Figure 8 and check the website `https://www.kali.org/tools/` for more details.

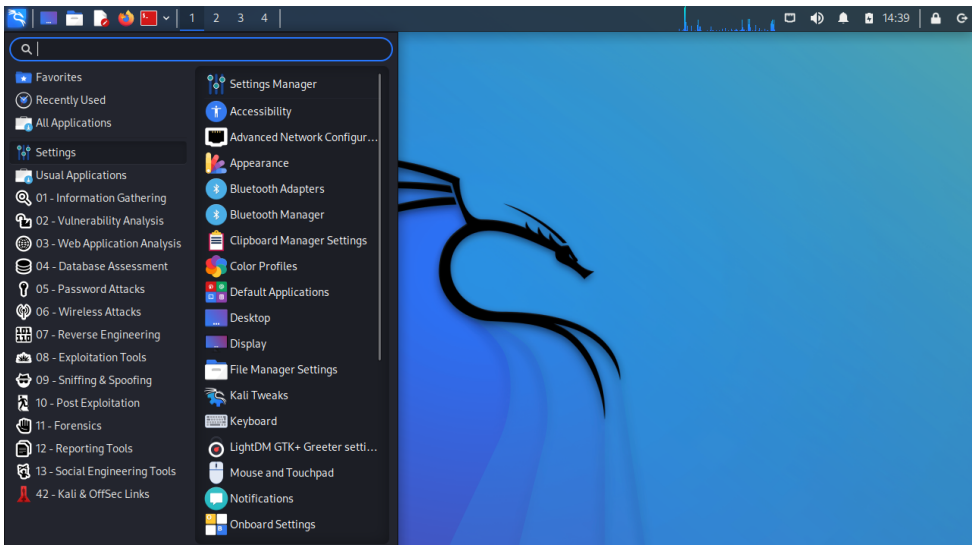

Figure 8: Kali's forensic tools

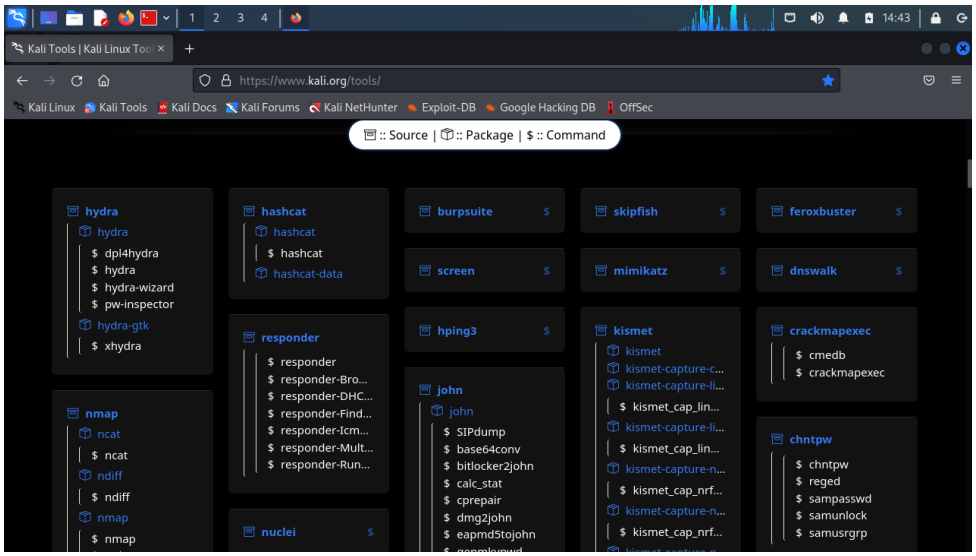

Figure 9: Kali packages list