Department of Computer Science
FC College University

Department of Data Science
University of the Punjab

HO#1.1: Setting-up the Lab Environment

Overview and Options for setting-up a Virtual Hacking Lab

Dear Students, when it comes to setting up a test lab for learning Networking and Cybersecurity concepts, you need to have a network of multiple machines running different Operating Systems and services. This is required to have one or more attacking machine and some victim/target machines. From the attacking machines you can scan for vulnerabilities and later exploit them to gain access and later perform privilege escalation for installing back doors, keyloggers and rootkits on the target machines.

There exist different options using which you can have the flavor of working on different Operating Systems and connecting those machines in a network. Each of these options have their own merits and demerits. Some of the commonly used options are briefly described below:

- **Option 1:** Have a ***physical network*** of multiple machines, and install different Microsoft OSs, Linux distros on them. This is called bare metal installation and is costly.
- **Option 2:** To have the flavor of multiple Operating Systems, you can ***dual or triple boot*** on one machine. Limitation is you can boot either one of the OS at a time and require careful disk partitioning and boot loader configuration to ensure that all the OSs work without interference. The limitation is that only one OS will be running at a time and you cannot have a network of machines.
- **Option 3:** If you are using Windows 10/11, and want to get a flavor of some Linux distribution, you can use ***Windows Subsystem for Linux (WSL)***, which allows you to run Linux environment directly in Windows without the need for a dual boot setup. To check out details about WSL you get visit this link: https://learn.microsoft.com/en-us/windows/wsl/about or can watch this YouTube video: https://www.youtube.com/watch?v=AfVH54edAHU
- **Option 4:** You can run Linux distribution inside a ***Docker container*** on any system that supports Docker. This is also a light weight option that is particularly useful for those who need to run specific command line tools rather than the whole Linux environment. For details you can visit: https://docs.docker.com/desktop/install/windows-install/
- **Option 5:** Use a hypervisor, which is a ***virtualization software*** that is used to run many guest machines on one host machine. There are dozens of different ways to create and run virtual machines and the two main methodologies used are running VMs from your workstation, or running them from a dedicated server. For educational purposes the first option is better being free. The list of hypervisors is quite long, some famous are mentioned below:
    - Oracle VirtualBox: https://www.oracle.com/virtualization/virtualbox/
    - VMware Workstation/Fusion Pro: https://www.vmware.com/products/desktop-hypervisor.html
    - UTM: https://mac.getutm.app/
    - MS Hyper-V for Windows 10: https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/
    - Parallel Desktop for Mac: https://www.parallels.com/products/desktop/
- **Option 6:** You can create and deploy the operating system of your choice on a dedicated server on a cloud platform such as ***AWS, Azure or Google cloud***. This is beneficial for performing security tasks with scalable resources. For a kick start you can visit this link: https://www.linkedin.com/advice/3/how-can-you-use-linux-cloud-computing-skills-system-administration

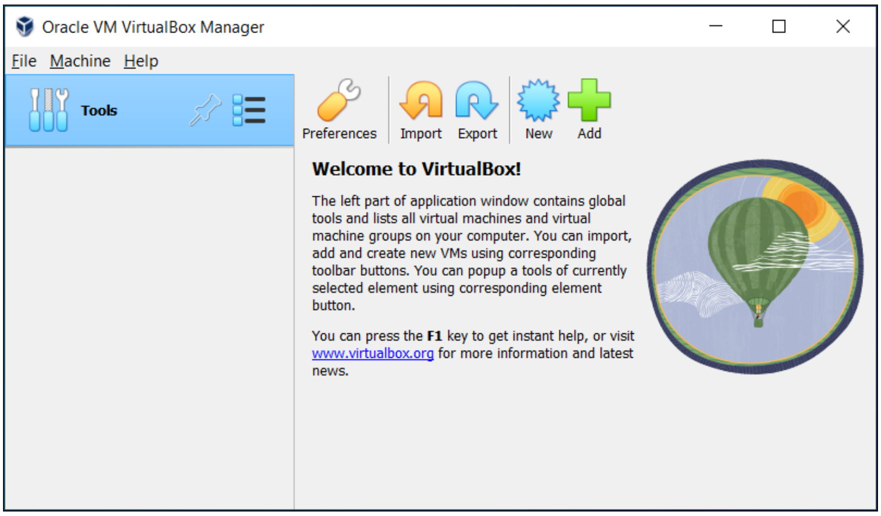
We will use Virtualization software Oracle Virtual Box for setting up of our lab ☺

Installing Oracle VirtualBox on your Host Machine

Dear Students, you can install any virtualization software, but to keep this document simple and short we will be using Virtual Box. Visit the VirtualBox website and download the latest version for your operating system by visiting this link:

https://www.oracle.com/pk/virtualization/technologies/vm/downloads/virtualbox-downloads.html

They have versions for Windows, macOS, Linux, and Solaris systems. The standard installation options will be fine (we trust this isn't your first time installing a program, so we'll leave you to it). Once you are done with the installation, do not forget to install the VirtualBox Extension pack having the same version as of the VirtualBox that you have installed. This will unlock additional functionalities like full screen, shared folder access, disk encryption, USB device support and remote desktop access.

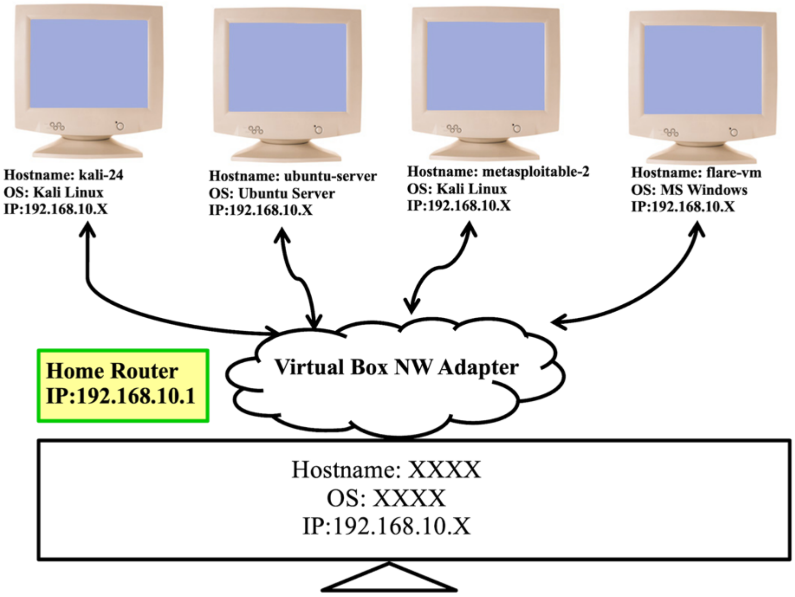


Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

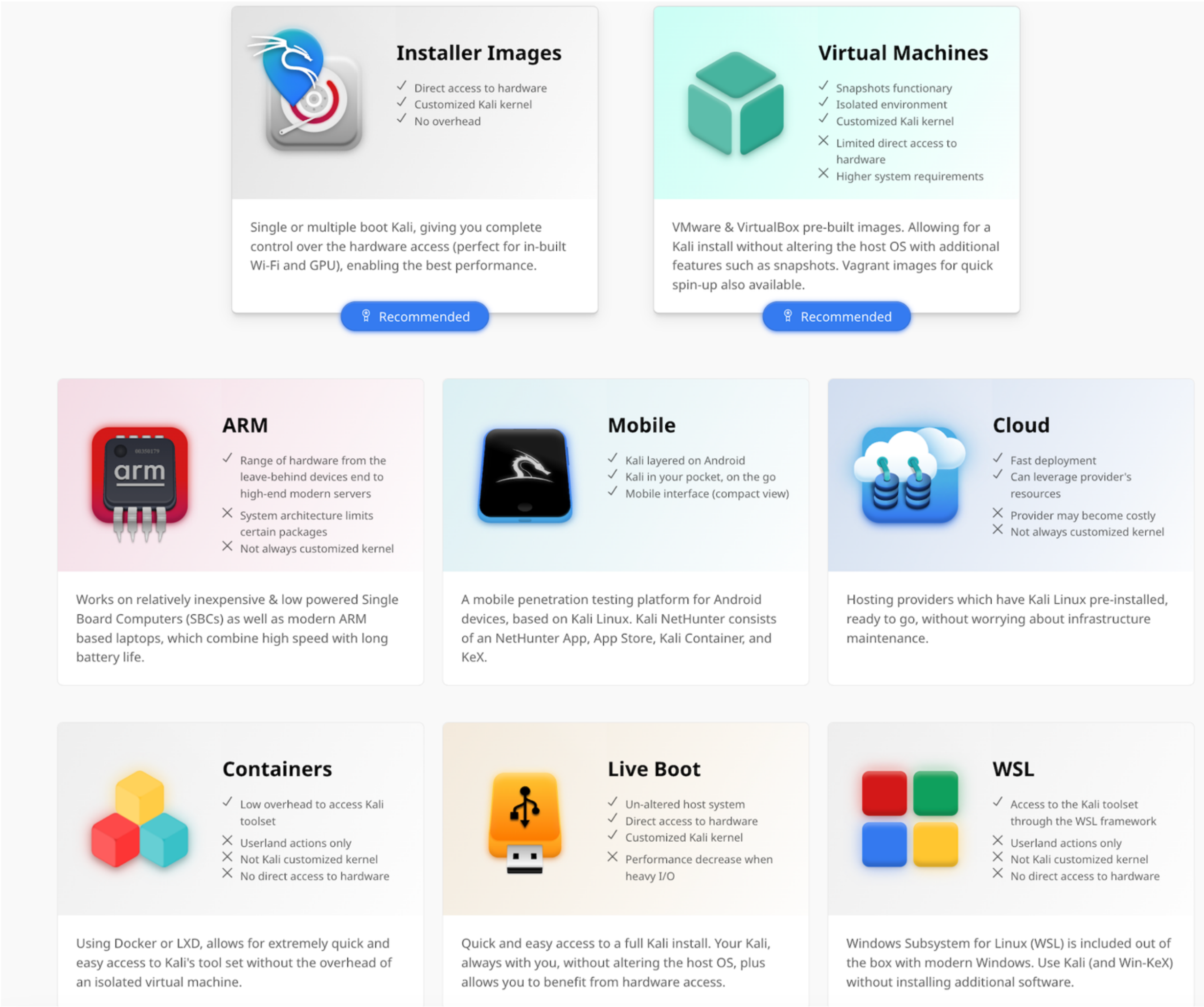
Overview of VMs and Guest Operating Systems



Installing Kali Linux inside VirtualBox

Kali Linux is a specialized Linux distribution designed for Security Researcher for Penetration Testing and Ethical Hacking. It provides security professionals, researchers, and enthusiasts with a comprehensive toolkit for assessing and securing computer systems. You can download its official ISO image installer images or pre-built Virtual Machines images by visiting the following link:

https://www.kali.org/get-kali/#kali-platforms



Installer Images

✓ Direct access to hardware
✓ Customized Kali kernel
✓ No overhead

Single or multiple boot Kali, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.

Recommended

Virtual Machines

✓ Snapshots functionary
✓ Isolated environment
✓ Customized Kali kernel
✗ Limited direct access to hardware
✗ Higher system requirements

VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.

Recommended

ARM

✓ Range of hardware from the leave-behind devices end to high-end modern servers
✗ System architecture limits certain packages
✗ Not always customized kernel

Works on relatively inexpensive & low powered Single Board Computers (SBCs) as well as modern ARM based laptops, which combine high speed with long battery life.

Mobile

✓ Kali layered on Android
✓ Kali in your pocket, on the go
✓ Mobile interface (compact view)

A mobile penetration testing platform for Android devices, based on Kali Linux. Kali NetHunter consists of an NetHunter App, App Store, Kali Container, and KeX.

Cloud

✓ Fast deployment
✓ Can leverage provider's resources
✗ Provider may become costly
✗ Not always customized kernel

Hosting providers which have Kali Linux pre-installed, ready to go, without worrying about infrastructure maintenance.

Containers

✓ Low overhead to access Kali toolset
✗ Userland actions only
✗ Not Kali customized kernel
✗ No direct access to hardware

Using Docker or LXD, allows for extremely quick and easy access to Kali's tool set without the overhead of an isolated virtual machine.

Live Boot

✓ Un-altered host system
✓ Direct access to hardware
✓ Customized Kali kernel
✗ Performance decrease when heavy I/O

Quick and easy access to a full Kali install. Your Kali, always with you, without altering the host OS, plus allows you to benefit from hardware access.

WSL

✓ Access to the Kali toolset through the WSL framework
✗ Userland actions only
✗ Not Kali customized kernel
✗ No direct access to hardware

Windows Subsystem for Linux (WSL) is included out of the box with modern Windows. Use Kali (and Win-KeX) without installing additional software.

Newbies in the field can read the following blog which describes in detail all the steps of installing Kali Linux in VirtualBox from ISO file as well as using VirtualBox image file.

https://www.stationx.net/how-to-install-kali-linux-on-virtualbox/

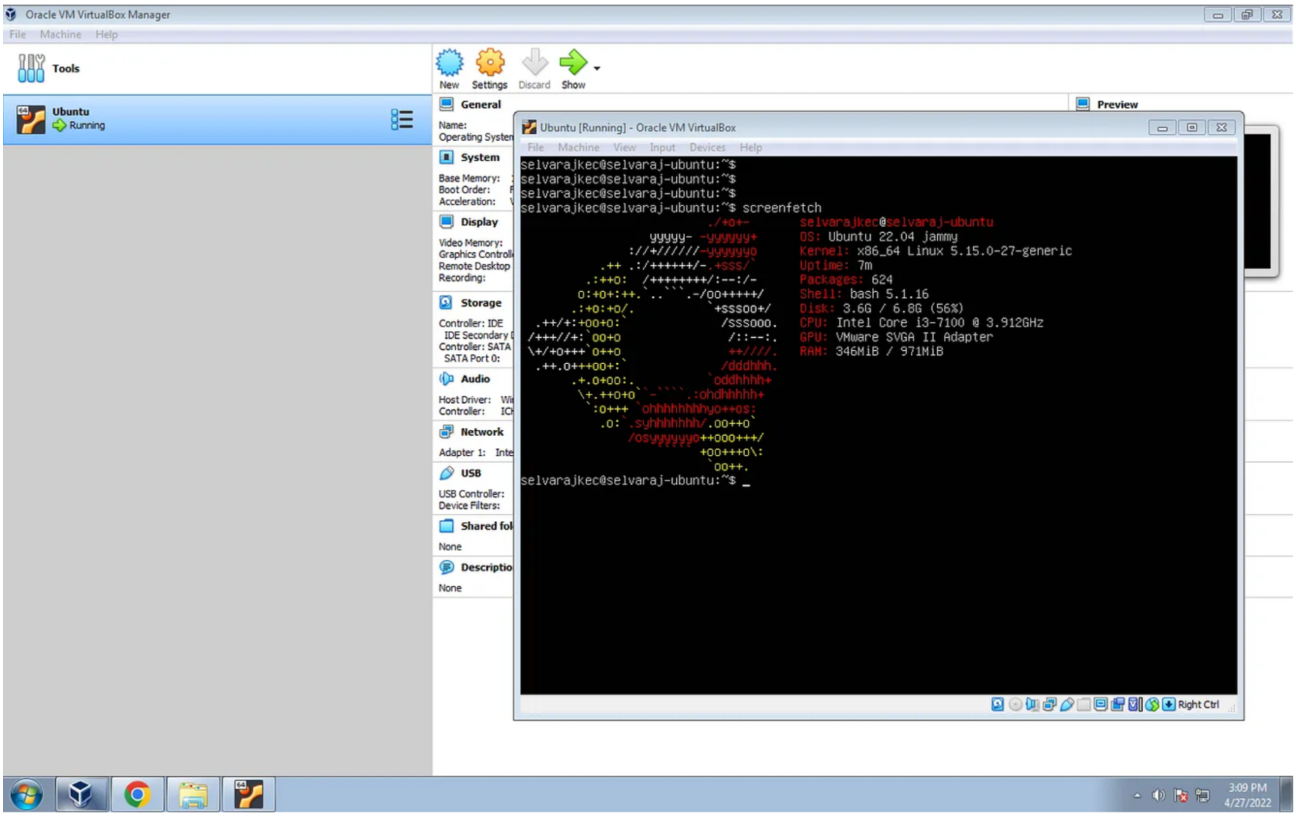
While creating your machine have a disk size of at least 50 GiB, and RAM size of 2 GiB. Once done installing Kali (or any other OS) in VirtualBox, do not forget to setup the network appropriately, so that you can ping all the machines within the network as well as machines on the Internet. If you have used the VirtualBox image of Kali, the username and passwords are both *kali*.

Installing Ubuntu Server inside VirtualBox

Ubuntu server is an operating system that is exactly the same as the Ubuntu Desktop variant, but it doesn't include a GUI or a lot of the pre-packaged junk that Ubuntu Desktop does. As a result, there are major increases in performance since the operating system doesn't have to process having a GUI open at the same time as running servers. Ubuntu Server is basically like having the terminal window of Ubuntu in full screen mode, but you cannot close the terminal window and it is the interface used to interact with the operating system.

For this course, we will be using it to learn all the Internetworking stuff and using servers like `time`, `daytime`, `echo`, `telnet`, `ssh`, `ftp`, `apache`, `PostgreSQL` and so on. At times we may use it as a target/victim machine as well. You can download it's official ISO image by visiting the following link:
https://ubuntu.com/download/server

Newbies in the field can read the following blog which describes in detail all the steps of installing Ubuntu Server inside VirtualBox:
https://medium.com/@selvarajk/install-ubuntu-server-on-virtualbox-57d9b9d490a5



~~~
selvarajkec@selvaraj-ubuntu:~$
selvarajkec@selvaraj-ubuntu:~$
selvarajkec@selvaraj-ubuntu:~$
selvarajkec@selvaraj-ubuntu:~$ screenfetch
                          ./+o+-       selvarajkec@selvaraj-ubuntu
                  yyyyy- -yyyyyy+      OS: Ubuntu 22.04 jammy
               ://+//////-yyyyyyo      Kernel: x86_64 Linux 5.15.0-27-generic
           .++ .:/++++++/-.+sss/`      Uptime: 7m
         .:++o:  /++++++++/:--:/-      Packages: 624
        o:+o+:++.`..```.-/oo+++++/     Shell: bash 5.1.16
       .:+o:+o/.          `+sssoo+/    Disk: 3.6G / 6.8G (56%)
  .++/+:+oo+o:`             /sssooo.   CPU: Intel Core i3-7100 @ 3.912GHz
 /+++//+:`oo+o               /::--:.   GPU: VMware SVGA II Adapter
 \+/+o+++`o++o               ++////.   RAM: 346MiB / 971MiB
  .++.o+++oo+:`             /dddhhh.
       .+.o+oo:.          `oddhhhh+
        \+.++o+o``-````.:ohdhhhhh+
         `:o+++ `ohhhhhhhhyo++os:
           .o:`.syhhhhhhh/.oo++o`
               /osyyyyyyo++ooo+++/
                   ````` +oo+++o\:
                          `oo++.
selvarajkec@selvaraj-ubuntu:~$ _
~~~

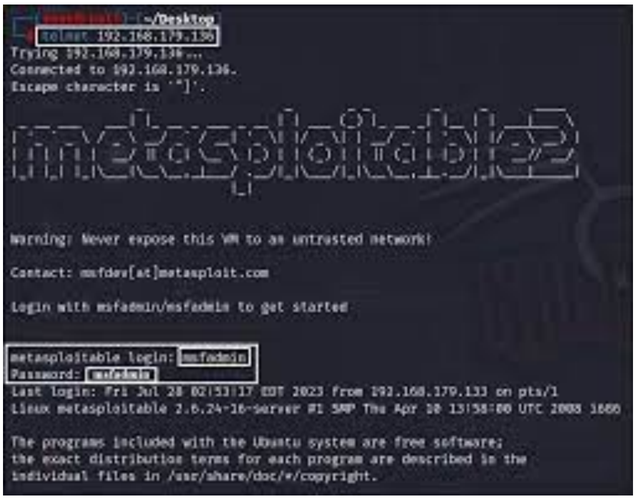
Many a times we need to copy files from one machine to the other. One way of doing that is to use the Shared Folder. For that you must install Virtual Box Guest Additions. If you have not done this in your OS course visit this link:
https://carleton.ca/scs/tech-support/virtual-machines/transferring-files-to-and-from-virtual-machines/

Installing Metasploitable 1-3 inside VirtualBox

Dear students, Metasploit is a framework that is (and should be) present in every hacker's arsenal. You can understand its importance as it comes installed with most of the famous security-based Linux distributions, Kali Linux and BlackArch.

Metasploitable is an intentionally vulnerable virtual machine designed for training, exploit testing, and general target practice. Unlike other vulnerable virtual machines, Metasploitable focuses on vulnerabilities at the OS and NW services layer instead of custom, vulnerable applications. To date, it has three versions that are publicly available:

- **Metaasploitable-1** was released on May 19, 2010, the time when most of the servers were running Linux. It was a customized ***Ubuntu 8.04 server*** to be installed on VMware 6.5 image. A number of vulnerable packages were included, including an install of tomcat 5.5 (with weak credentials), distcc, tikiwiki, twiki, and an older mysql. But when compared to the scanners and exploits available in MSF, the first version was very minimal. Moreover, it was created to run on VMware, although VirtualBox was present at that time. So Metasploitable-1 was not tested on VirtualBaox.
- **Metasploitable-2** was released on June 13, 2012. It was beefed up with vulnerabilities. It had backdoors (vsftpd), unintentional backdoors (distccd), weak passwords and much more. Nearly 30 exposed ports could be seen in a complete Nmap scan. It also had vulnerable web applications: DVWA and Mutillidae, which allowed hackers to practice webapp pentesting which includes getting shells, remote code execution, and also privilege escalation attacks. It works fine on both VirtualBox and VMware. But the hackers' thirst to have a vulnerable Windows machine to test against is not quenched.



```
~/Desktop
telnet 192.168.179.136
Trying 192.168.179.136...
Connected to 192.168.179.136.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password: msfadmin
Last login: Fri Jul 28 02:53:17 EDT 2023 from 192.168.179.133 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

- **Metasploitable-3**, was released on the latter half of 2016. As both of its predecessors were vulnerable Linux variants and with the increase in Windows products (both desktops and servers), it was time to have some vulnerable Windows version as well. So Metasploitable-3 has its Linux variant that uses a customized ***Ubuntu 14.04 server*** OS. Similarly, there exist a Windows variant of Metasploitable-3 that uses a customized ***Windows 2008R2 server***.

We will mostly be using Metasploitable 2 in this course, however, you can download and install them all from the following links:

- **Metasploitable 1:** https://www.vulnhub.com/entry/metasploitable-1,28/
- **Metasploitable 2:** https://www.vulnhub.com/entry/metasploitable-2,29/ ,
- **Metasploitable 3:** https://github.com/rapid7/metasploitable3

Newbies in the field can read the following blog to download and install

- Metasploitable-2:https://mwaseemaw.medium.com/virtual-box-setup-metasploitable-2-2af9c157f364
- Metasploitable-3: https://www.stationx.net/how-to-use-metasploit-in-kali-linux/

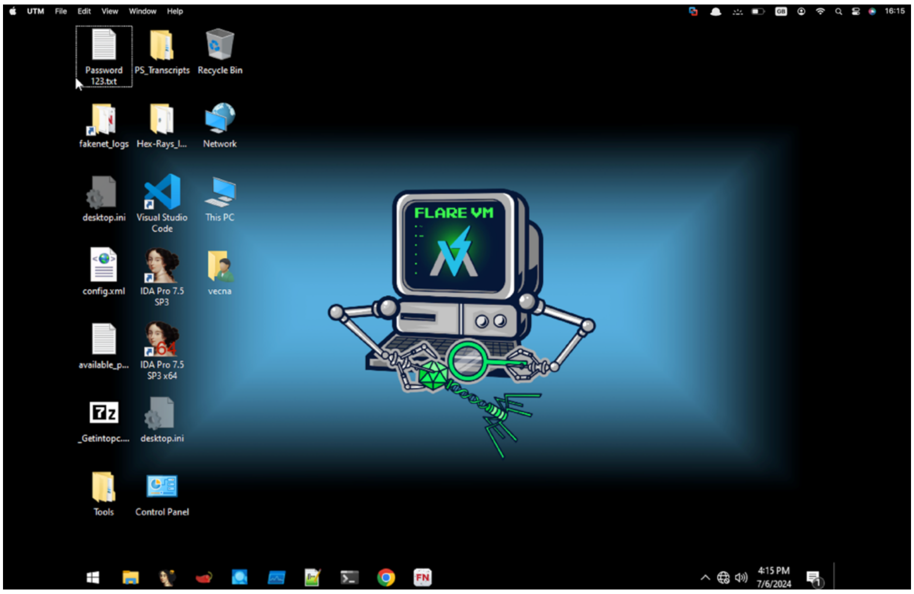
Installing FLARE-VM inside VirtualBox

My dear students, while performing the static and dynamic analysis of malware samples, we MUST ensure to prevent accidental infection of production systems or networks. For instance, use virtual machines or sandbox environments to analyze malware samples safely. FlareVM is a freely available and open-sourced Windows-based security distribution designed for reverse engineers, malware analysts, incident responders, forensicators, and penetration testers. FLARE VM delivers a fully configured platform with a comprehensive collection of Windows security tools such as debuggers, disassemblers, decompilers, static and dynamic analysis utilities, network analysis and manipulation, web assessment, exploitation, vulnerability assessment applications, and many others.

Steps to create FLARE-VM:

- Create a Windows (Win10) virtual machine
- Disable updates and Microsoft Windows Defender
- To install the necessary tools run the installation script available at this link: https://github.com/mandiant/flare-vm

For your ease, we have already prepared a VirtualBox .ova file FLARE-VM that you can download from the link by your instructor with ***username:password*** of ***`vecna:dartsec`*** respectively.



Disclaimer

The series of handouts distributed with this course are only for educational purposes. Any actions and or activities related to the material contained within this handout is solely your responsibility. The misuse of the information in this handout can result in criminal charges brought against the persons in question. The authors will not be held responsible in the event any criminal charges be brought against any individuals misusing the information in this handout to break the law.