Department of Computer Science
FC College University

Department of Data Science
University of the Punjab

HO#1.2: 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:** 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 5:** 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 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

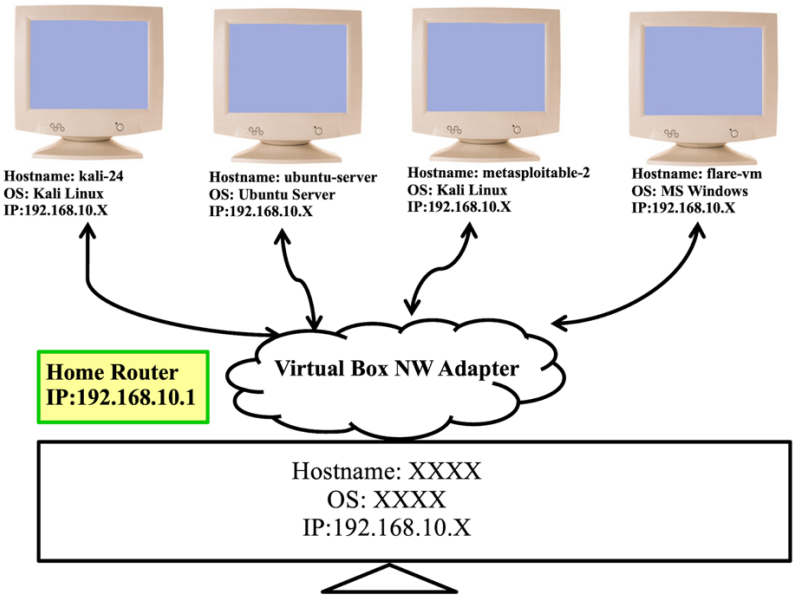
Installing Oracle VirtualBox on your Host Machine

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.

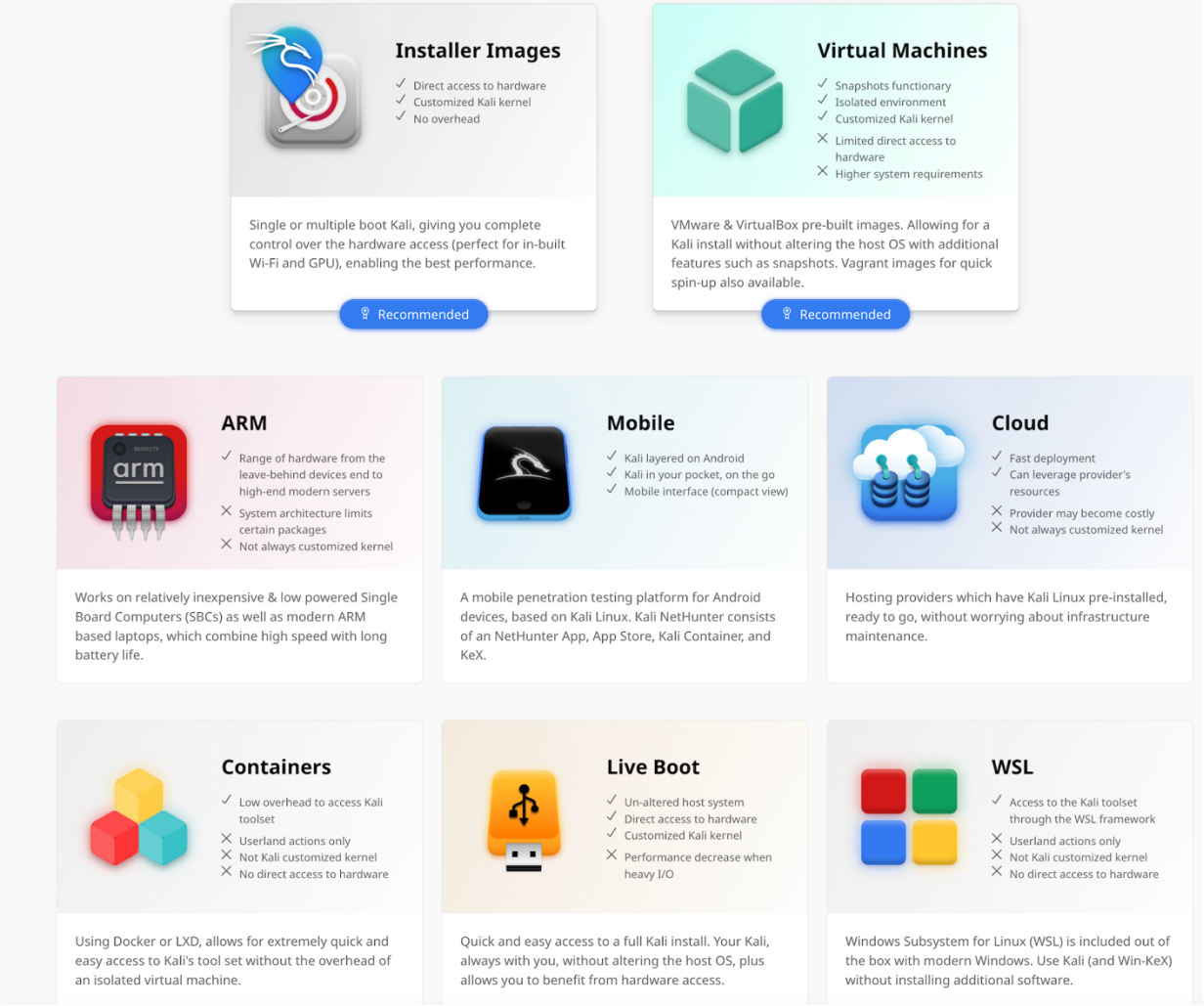
Overview of VMs and Guest Operating Systems



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



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

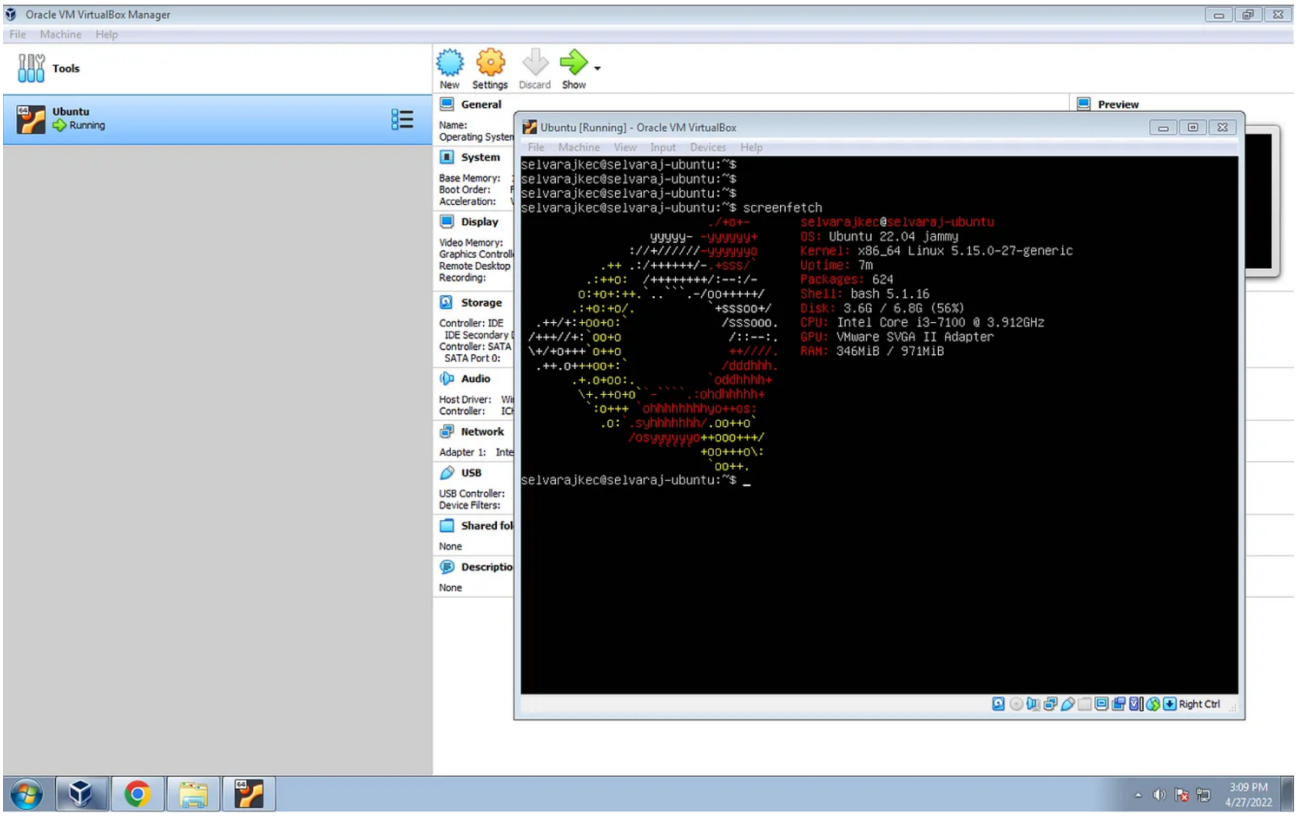
Ubuntu server is an operating system that is exactly the same as the Ubuntu Desktop variant, but it doesn't include a GUI or a lot of the pre-packaged junk that Ubuntu Desktop does. As a result, there are major increases in performance since the operating system doesn't have to process having a GUI open 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



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 and also runs a customized ***Ubuntu 8.04 server***. 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.

- **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/

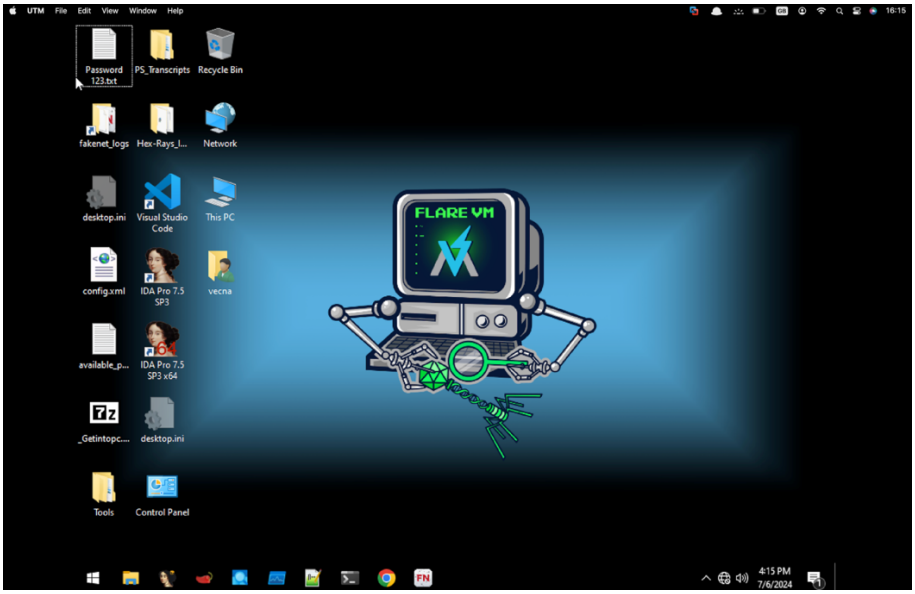
Installing FLARE-VM inside VirtualBox

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.

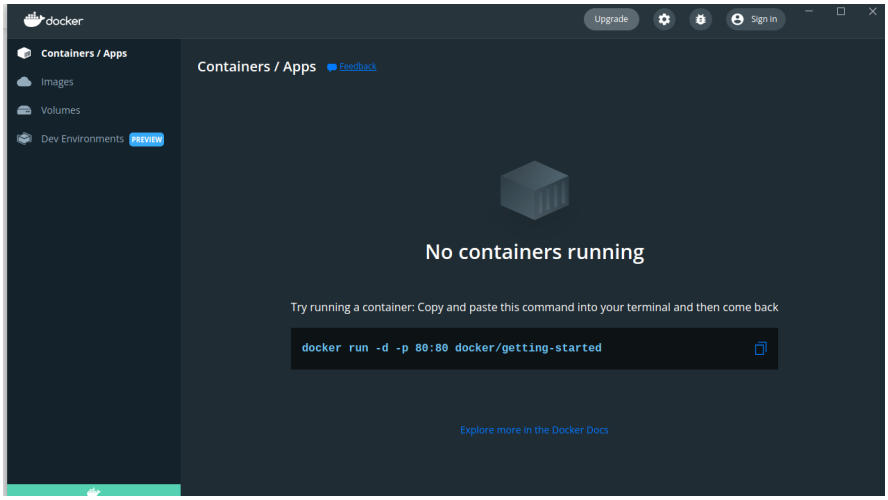


Installing Docker on our Host Machine

Dear Students, if you are interested, you can use Docker instead of VirtualBox to set up the lab environment. For this, first visit the Docker website and download the latest version of Docker Desktop for your operating system (Windows in my case) by visiting this link:

https://docs.docker.com/desktop/setup/install/windows-install/

They have versions for Windows, Debian, Ubuntu, and Fedora. After downloading you have to install it. Once installation is completed you have to launch it and it will look like this:



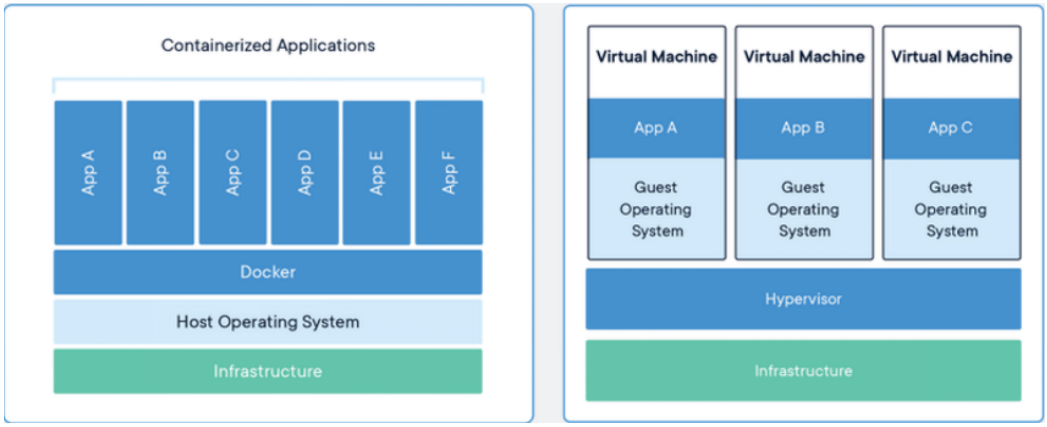
Docker Image:

A Docker image is like a blueprint or recipe for creating containers. It contains everything needed to run an app, including the code, tools, and settings. Containers are built from images, making them reusable and consistent.

Docker Container:

A Docker container is like a lightweight, portable mini-computer that runs only the apps and tools you need. It uses shared resources from your actual computer but stays isolated, so it doesn't interfere with other programs. Think of it as a neat, self-contained box for running software consistently anywhere!

Docker's Container vs VMs

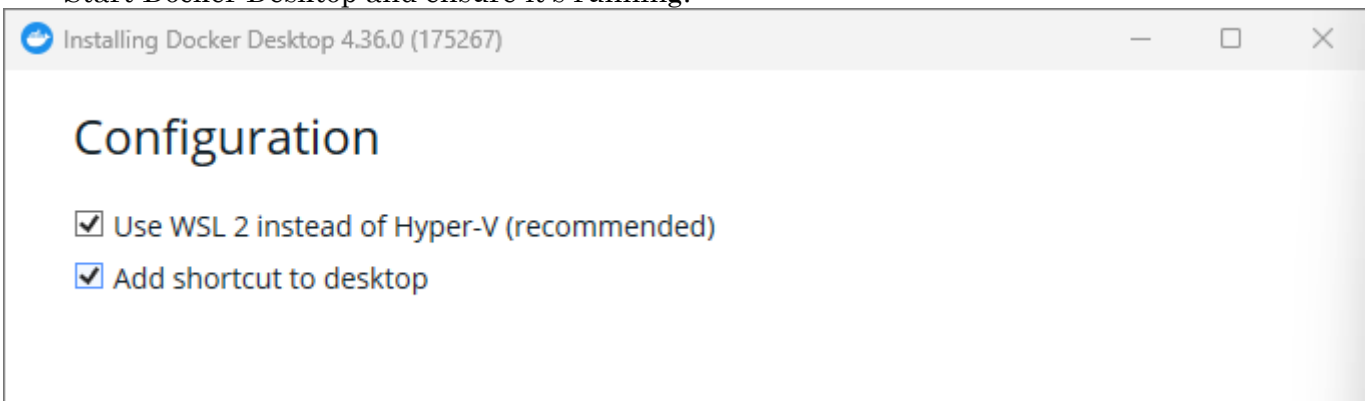


Pull Kali Linux Image from Docker Hub

You can download Kali Linux image from Docker Hub (an app store for Docker). It's an online repository where you can find, share, and download Docker images. It hosts both official images and user-created ones, making it easy to set up containers quickly. Another way to download Kali Linux image is via CLI. Let's pull it via Docker Hub:

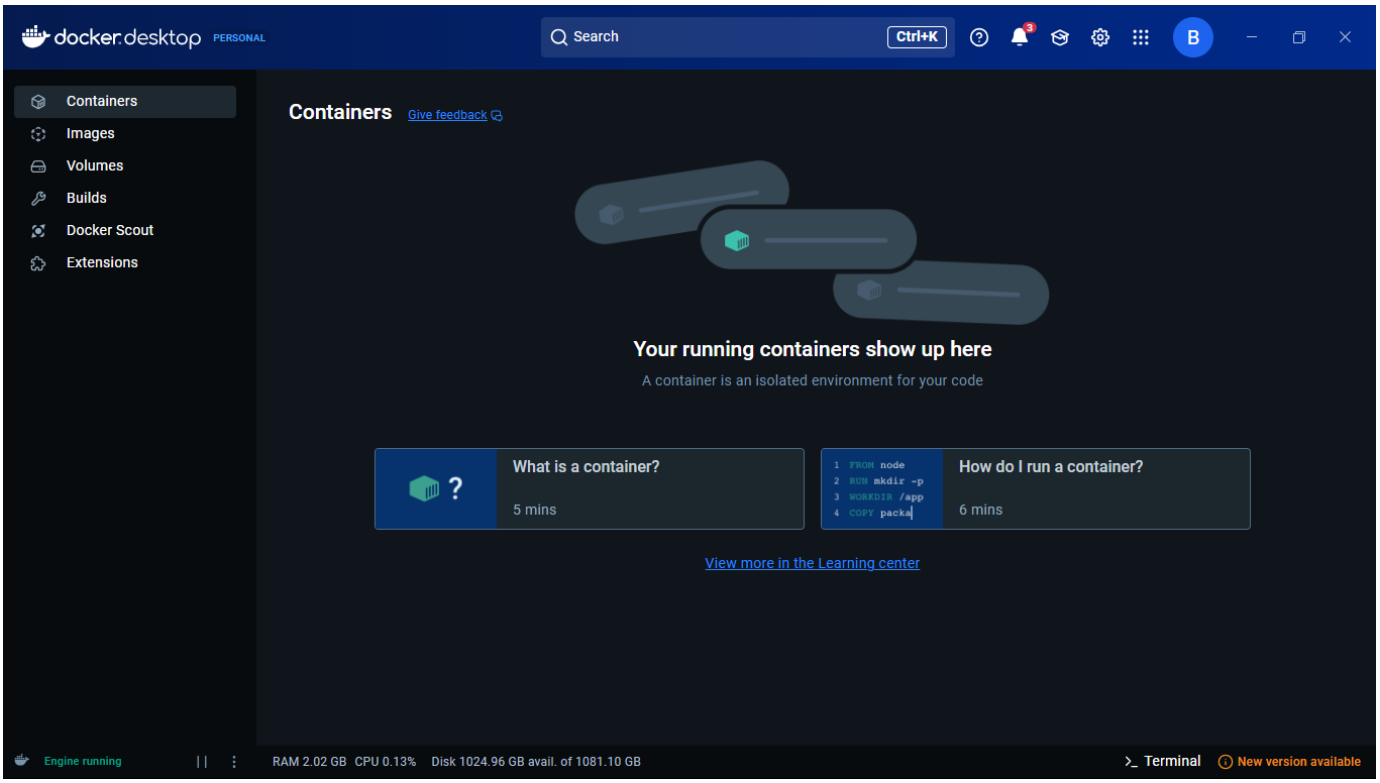
1. Install Docker Desktop

- Download and install Docker Desktop from Docker's website. https://hub.docker.com/
- Ensure WSL2 is enabled on Windows if prompted during installation.
- Start Docker Desktop and ensure it's running.



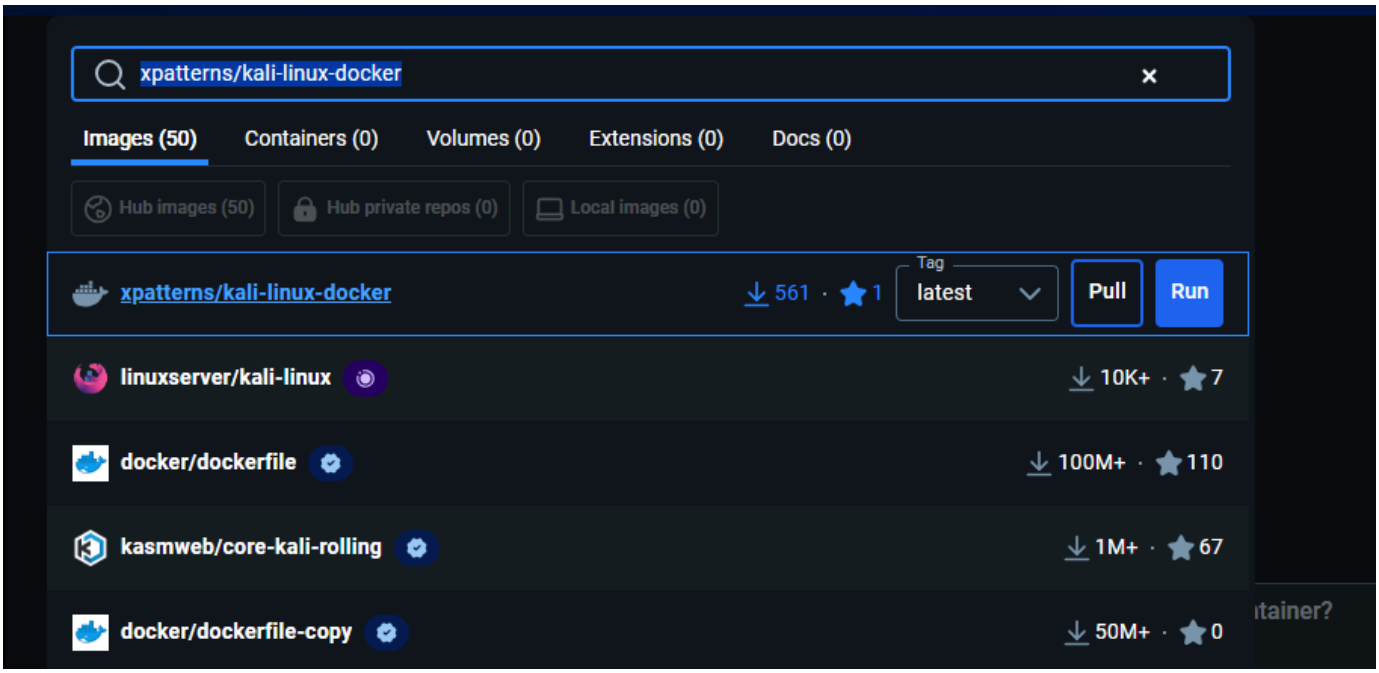
2. Log in to Docker Hub

- Open Docker Desktop.
- Log in with your Docker Hub credentials or create an account at Docker Hub.



3. Search for Kali Linux on Docker Hub

- Go to the Docker Hub website
- Search for `xpatterns/kali-linux-docker`
- Click it and copy the pull command



4. Pull the Kali Linux Image

- Open a terminal (Command Prompt, PowerShell, or Docker Desktop terminal).
- Pull the image directly from Docker Hub: ***`docker pull xpatterns/kali-linux-docker`***

```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\User> docker pull xpatterns/kali-linux-docker
Using default tag: latest
latest: Pulling from xpatterns/kali-linux-docker
1eb522968923: Download complete
1eb522968923: Downloading  569.4MB/4.258GB
e5b4b7133863: Already exists
d4ecedcfaa73: Already exists
b2860afd831e: Download complete
340395ad18db: Already exists
Digest: sha256:3596940d661b972b1309a439c17a93e33e83073cc83cf27f2e9e61c07cd7478f
Status: Downloaded newer image for xpatterns/kali-linux-docker:latest
docker.io/xpatterns/kali-linux-docker:latest
PS C:\Users\User> docker images
REPOSITORY                    TAG       IMAGE ID       CREATED       SIZE
tleemcjr/metasploitable2      latest    e559450b37dc   7 years ago   2.3GB
peakkk/metasploitable         latest    74836b448d57   7 years ago   1.94GB
xpatterns/kali-linux-docker   latest    3596940d661b   8 years ago   13.4GB
PS C:\Users\User>
```

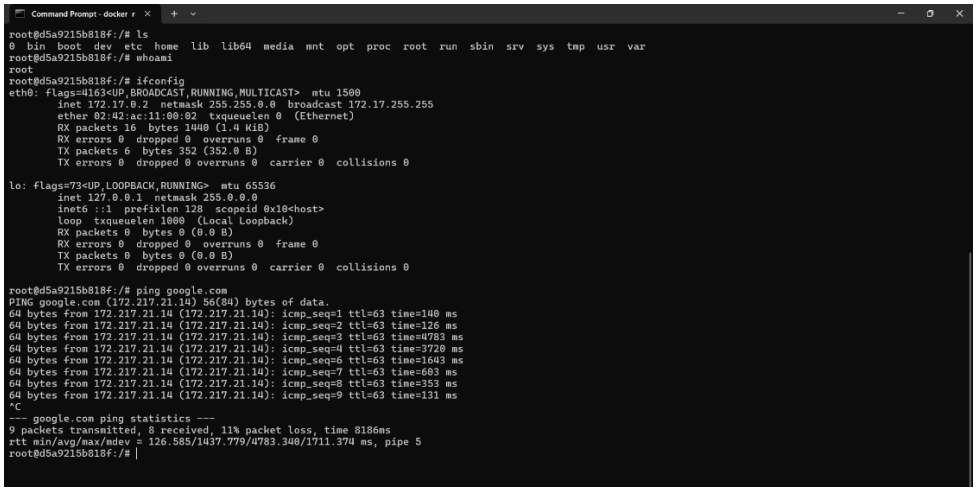
5. Run the Kali Linux Container

- Start the container using the pulled image:

docker run -it xpatterns/kali-linux-docker

```
Windows PowerShell
PS C:\Users\User> docker run -it xpatterns/kali-linux-docker
root@5549b1120c65:/# whoami
root
root@5549b1120c65:/# ls
0    boot  etc   lib    media  opt   root  sbin  sys  usr
bin  dev   home  lib64  mnt    proc  run   srv   tmp  var
root@5549b1120c65:/# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
mysql:x:105:109:MySQL Server,,,:/nonexistent:/bin/false
```

- This will give you access to Kali Linux's command-line interface (CLI).
- Congratulations! Now you're running Kali Linux from Docker Hub on Docker Desktop!



Get Metasploitable(s) in Docker

Dear students, to install **Metasploitable2** and **Metasploitable3** using Docker, you can pull the images from the following links. These pre-built images allow you to set up vulnerable environments quickly for ethical hacking and penetration testing.

Metasploitable 1: ***docker pull peakkk/metasploitable:latest***
Metasploitable 2: ***docker pull tleemcjr/metasploitable2***
Metasploitable 3: ***docker pull edurange2/metasploitable3***

Verifying and Accessing Metasploitable in Docker

Once you have successfully pulled and run the Metasploitable image, follow these steps to verify that it is running and interact with it.

1. Check Available Docker Images

To confirm that the Metasploitable image has been downloaded, use: ***docker images***

This command lists all available images on your system. In the output, you will see **REPOSITORY**, **TAG**, **IMAGE ID**, **CREATED**, and **SIZE** of the images.

```
PS C:\Users\User> docker pull peakkk/metasploitable:latest
latest: Pulling from peakkk/metasploitable
3521837e2af8: Download complete
e4140977a7a0: Download complete
Digest: sha256:74836b448d5704e91096a8af344bbab028a8fb9f2c3b111122f16d1824afa2f8
Status: Downloaded newer image for peakkk/metasploitable:latest
docker.io/peakkk/metasploitable:latest
PS C:\Users\User> docker images
REPOSITORY              TAG       IMAGE ID       CREATED       SIZE
peakkk/metasploitable   latest    74836b448d57   7 years ago   1.94GB
PS C:\Users\User>
```

2. Run the Metasploitable Container in the Background

To start the Metasploitable container in **detached mode** (running in the background), use:

docker run -it -d peakkk/metasploitable:latest

- `-it` → Runs an interactive session
- `-d` → Runs the container in the background
- `peakkk/metasploitable:latest` → Specifies the Metasploitable 1 image

Upon execution, this command returns a **container ID**, which represents the running instance of Metasploitable.

```
Windows PowerShell   Windows PowerShell
PS C:\Users\User> docker run -it -d peakkk/metasploitable:latest
ed327b2e0e28a04ac6bb36a79cf7f34c0c9c97174e173e3eeda9d8e578ec8629
PS C:\Users\User> docker ps
CONTAINER ID   IMAGE                          COMMAND             CREATED
STATUS          PORTS

                                                                   NAMES
ed327b2e0e28   peakkk/metasploitable:latest   "/sbin/init.real"   16 seconds ago
Up 15 seconds   21-23/tcp, 25/tcp, 80/tcp, 111/tcp, 139/tcp, 445/tcp, 512-514/tcp,
1099/tcp, 1524/tcp, 3306/tcp, 3632/tcp, 5432/tcp, 5900/tcp, 6000/tcp, 6667/tcp, 669
7/tcp, 8009/tcp, 8180/tcp, 32963/tcp, 37537/tcp, 45458/tcp   amazing_chatelet
4d1d59983a1b   peakkk/metasploitable:latest   "/sbin/init.real"   11 minutes ago
Up 11 minutes   21-23/tcp, 25/tcp, 80/tcp, 111/tcp, 139/tcp, 445/tcp, 512-514/tcp,
1099/tcp, 1524/tcp, 3306/tcp, 3632/tcp, 5432/tcp, 5900/tcp, 6000/tcp, 6667/tcp, 669
7/tcp, 8009/tcp, 8180/tcp, 32963/tcp, 37537/tcp, 45458/tcp   gallant_shannon
PS C:\Users\User>
```

3. Access the Running Metasploitable Container

To interact with the Metasploitable system, use:

docker exec -it <container_id> bash

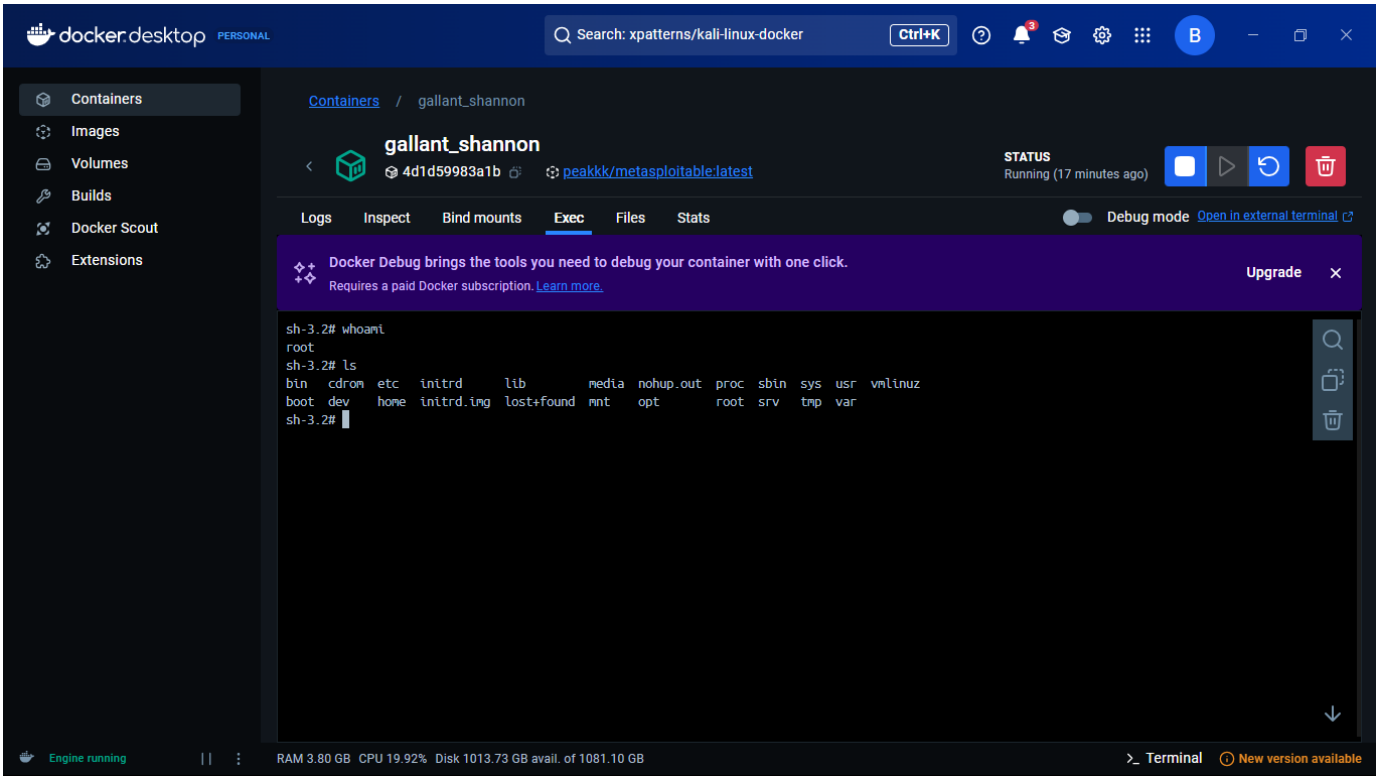
Replace `<container_id>` with the actual **container ID** obtained from the `docker run` command.

```
@4d1d59983a1b: /   Windows PowerShell
PS C:\Users\User> docker images
REPOSITORY                  TAG       IMAGE ID       CREATED       SIZE
tleemcjr/metasploitable2    latest    e559450b37dc   7 years ago   2.3GB
peakkk/metasploitable       latest    74836b448d57   7 years ago   1.94GB
PS C:\Users\User> docker exec -it 4d1d bash
root@4d1d59983a1b:/# whoami
root
root@4d1d59983a1b:/# ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@4d1d59983a1b:/#
```

This command opens a **Bash shell** inside the running container.

Running Commands via Docker Desktop Interface (Exec Tab)

In addition to running commands through the terminal, you can also execute commands directly within the Docker Desktop interface using the **Exec** tab. Once the container is running, navigate to the Docker Desktop application, locate your Metasploitable container in the list of running containers, and click on it. Inside the container details, you'll find an **Exec** button that allows you to open a terminal session directly within the container. This provides an easy-to-use, graphical way to interact with the container without needing to use the command line interface. From here, you can run Linux commands, verify services, and explore the system just as you would in the terminal.



Newbies in the field can watch the following video which describes in detail all the steps to run Kali Linux and Metasploitable2 in Docker Desktop from Docker Hub:

https://www.youtube.com/watch?v=QinRdVCDg-k

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.