



Source: Stable Diffusion AI

LABORATORY “oB”. SSI AUTOMATED INFRASTRUCTURES

DEPARTMENT OF COMPUTER SCIENCE. UNIVERSITY OF OVIEDO

Computer Security | 2022 – 2023 (V2.7 “S-81 Isaac Peral”)



CONTENT

Why Docker?	2
How do we work with the lab infrastructures?	2





Why Docker?

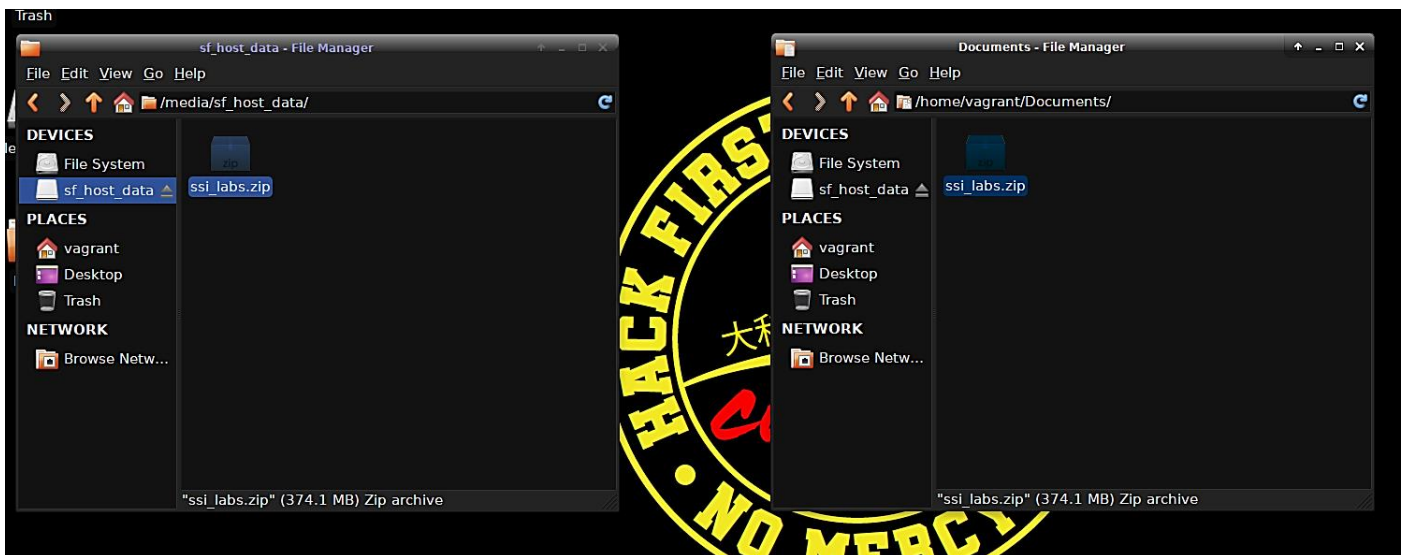
Docker is used in this course as a process isolation technique, and it is normally used to run executables that could get compromised. However, it is also especially useful also to emulate the machine infrastructures we are using in the labs, obtaining the following advantages:

- **You can deploy these infrastructures at home easily.** Just copy the files we provide you and run the appropriate scripts (`prepare_labX.sh` and `bulid_labX.sh`) to build each infrastructure.
- **Infrastructure building have only to be done once.** Attempting to build it again will detect that the infrastructure was already built and skip most (or all) steps.
- **These types of infrastructures use a lot less resources than equivalent VMs.** They are not VMs, but they are prepared to work as if they were, and most of our labs does not really require a real VM to be completed.
- *Docker* is available in *Windows*, *Linux*, and *MAC*. Tests have been performed in our *Ubuntu Server 18.04* VM, but nothing should prevent you to deploy the same infrastructure in different OS that supports *Docker* and *Docker Compose* (even natively). **Labs can be multiplatform! (NOTE: We could not test if this infrastructure works with a native installation of *Docker* and *Docker Compose* in *Windows* and *Mac*, so we do not recommend it).**
- The infrastructure you will build **is based on text files and official *Docker Hub* images**. This means that the building blocks are “official”, and the instructions are plain text files. If not because we also provide you with clones of real websites, your infrastructure **specification should only take a couple of Kb**.
- Yes, **all the infrastructures work efficiently inside our *Ubuntu* VM**. As we said, these are NOT virtual machines! 😊
- **You do not need to understand anything but this minimal instructions file about *Docker* and *Docker Compose* to work with them.** All is designed to work automatically via our scripts.
- **All *Docker* containers we supply with the ability to log in into them are configured as rich interactive terminals:** they come with `tmux`, mouse integration (`gpm` module), text-based graphical file browser (*Midnight Commander*, `mc`) and an advanced custom `nano` configuration to better edit files. This aims to increase your productivity when you work inside containers.

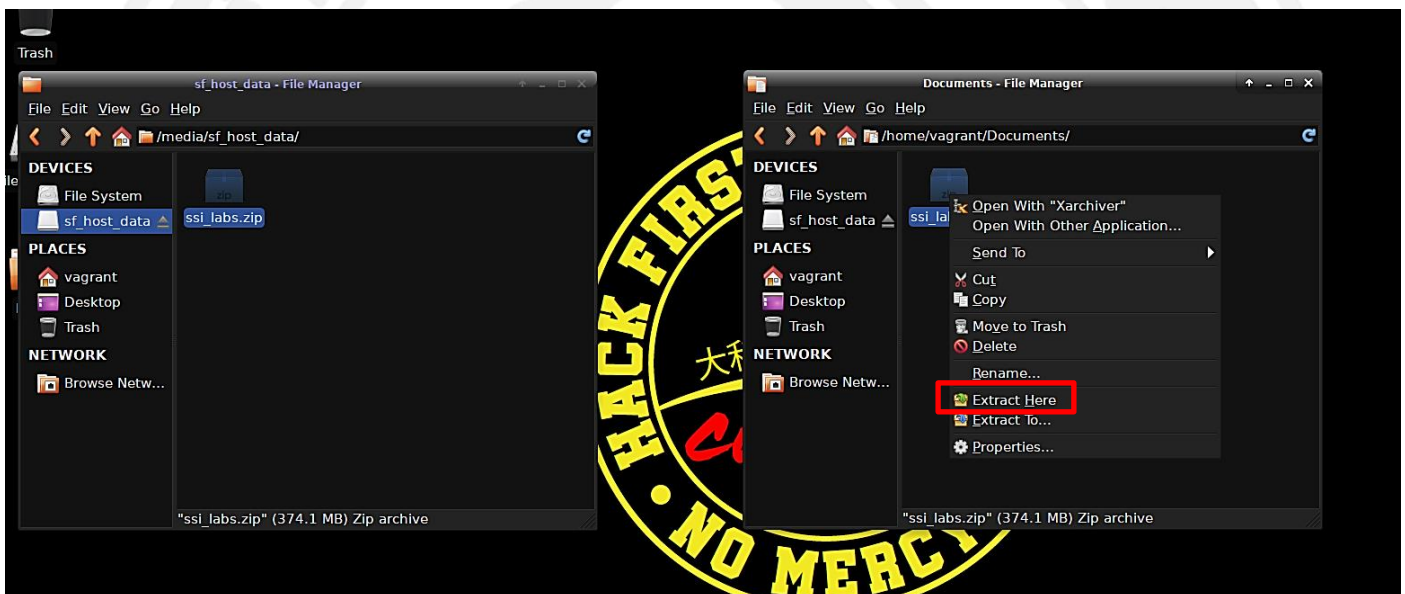
NOTE: *Docker* containers are **expendable environments**. This means that they are not prepared to install more software that the one we provided you with inside each one of them. However, in case you need additional software for some reason, you can do it as in a normal *Ubuntu* installation. Bear in mind though that, **once you quit the laboratories, your changes to their containers will be lost**.

How do we work with the lab infrastructures?

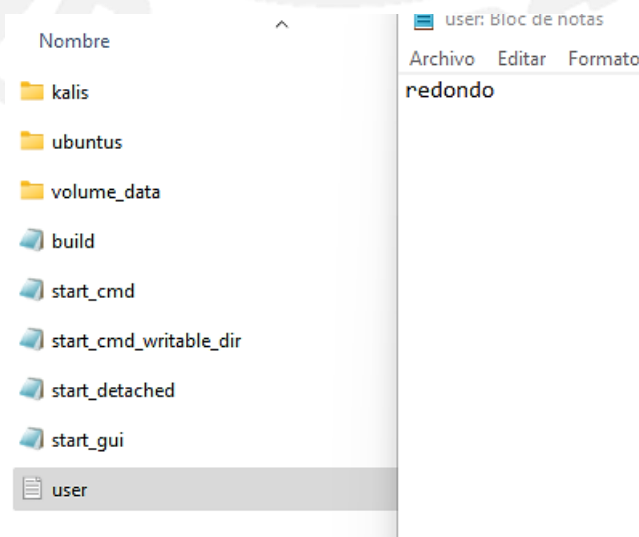
The first thing you must do is to download the file with the infrastructures of all the labs. To do that, copy the `ssi_labs.zip` file to a folder in the VM. If you use Option 1 to build the VM, this file is already present in its `sf_host_data` folder (the one used to share contents with your PC). The option 2 has the file placed in `/ssi_files/`. If you made your own VM, you need to download the file from the Virtual Campus.



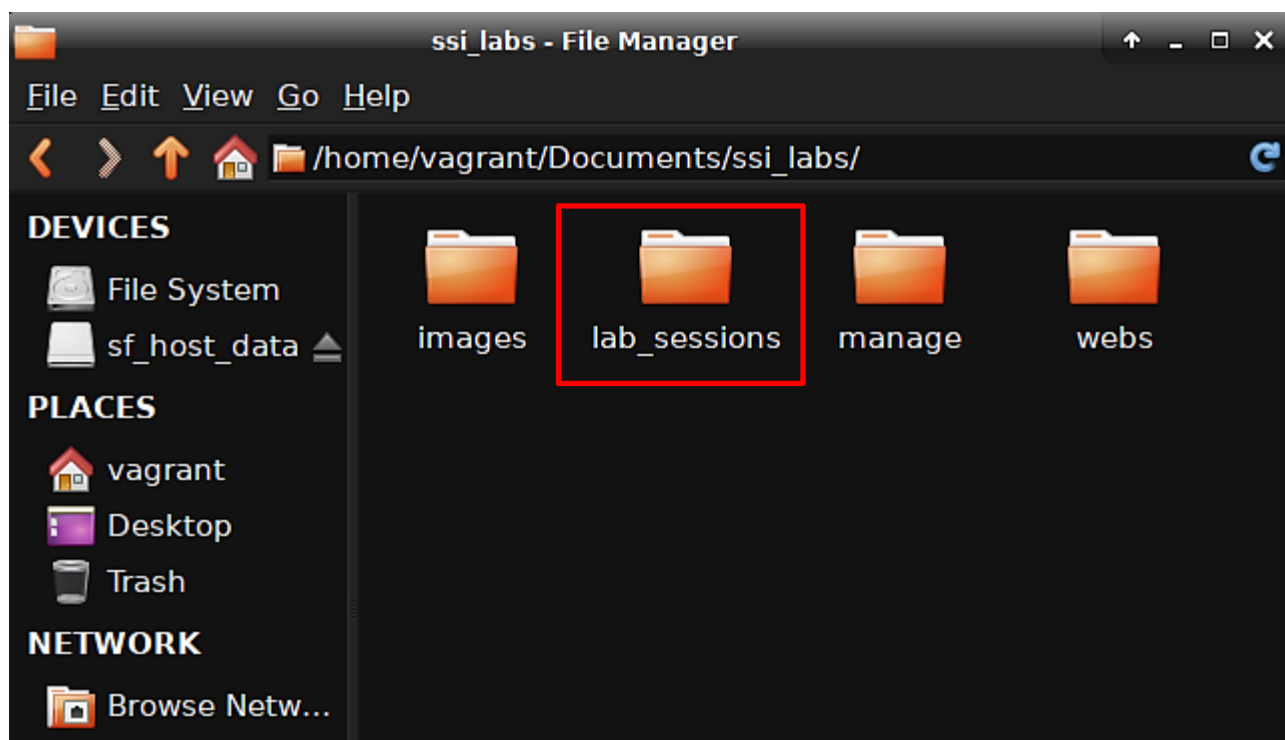
Once you copy the file, unzip it. The GUI has an embedded option to do that. You can also use the **unzip** command line tool.



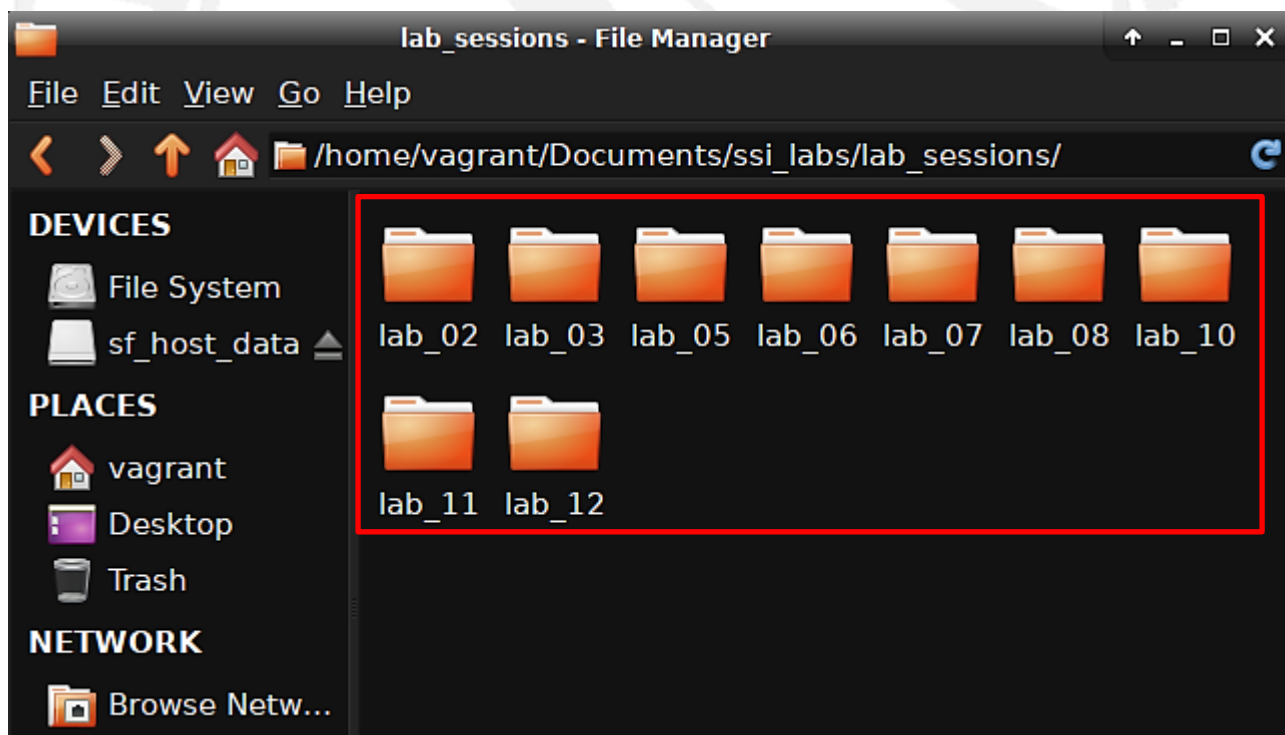
Once all is unzipped, go to the **ssi_labs/images** folder and locate the **user.txt** file. **Change the username present there** for the one you want to use in the lab infrastructures. It is recommended to use the same you put when you created the virtual machine, but any valid *Linux* username can be used.



The only folder you need to worry about from now on is **lab_sessions**



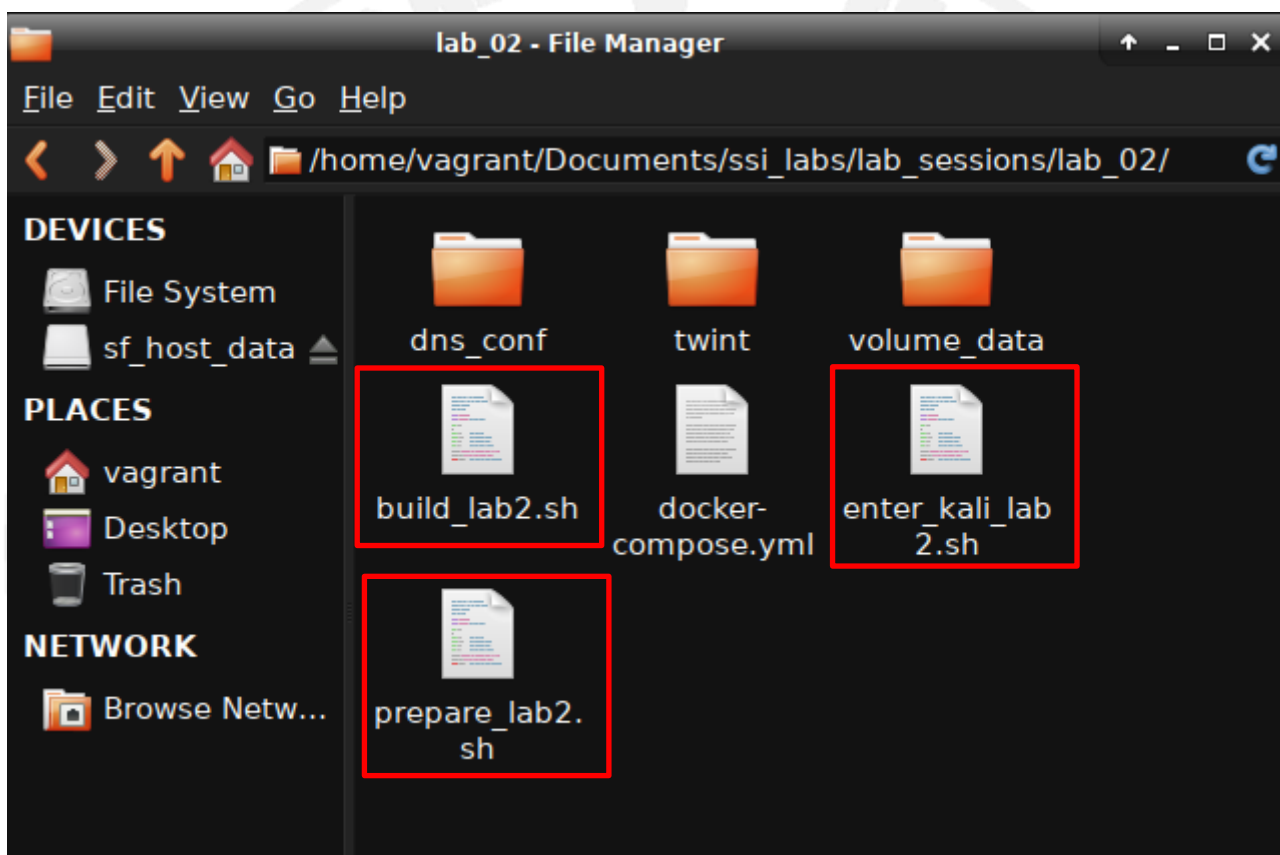
Go inside this folder and enter the lab session you are going to work with. Missing session numbers mean that these sessions use the infrastructure of a previous lab, or they do not require one:



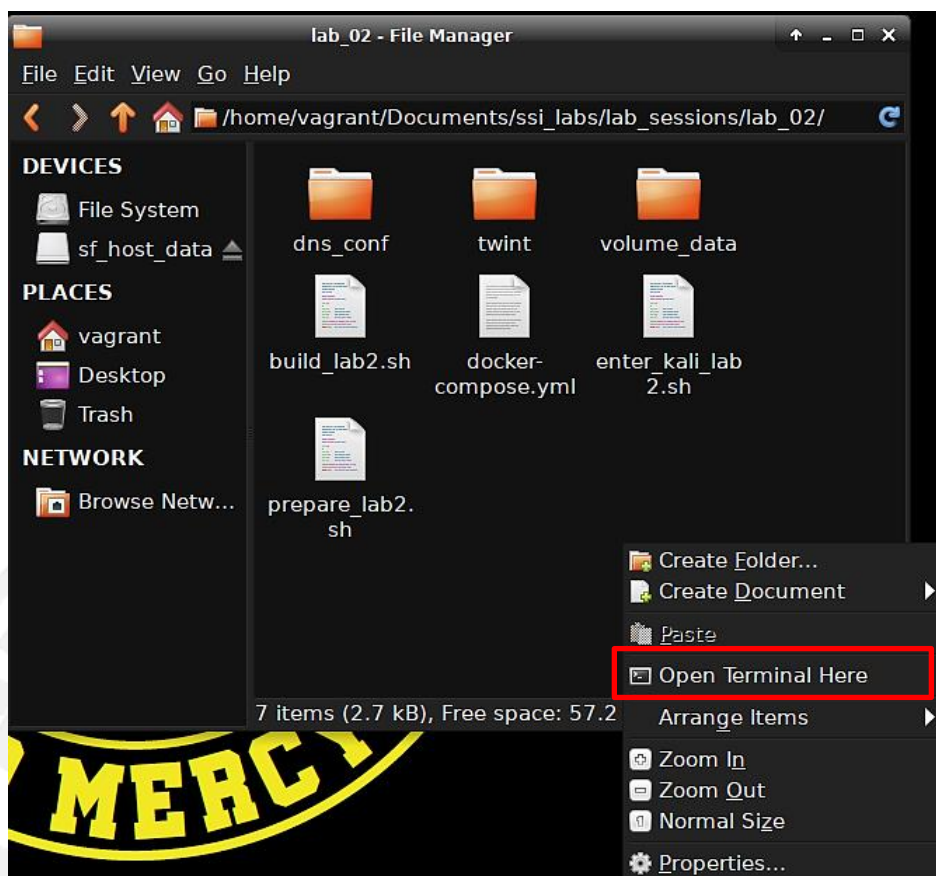
Inside lab folders you will find these elements, which will be detailed later. Rest of the elements not present in this list are not important for this course. **NOTE: all laboratories will work the same as explained here!**

- **prepare_labX.sh**: This is the file you must run first to prepare all the laboratory prerequisites and infrastructures.
- **build_labX.sh**: This file must run after the **prepare_labX.sh** one and builds all the laboratory components.

- **enter_XXXX.sh**: Scripts to log in in different components of the laboratory, as specified in each laboratory instructions. Not all elements of the laboratory are meant to be logged in, so do not worry if the number of **enter_XXX.sh** scripts is less than the elements in the lab. **Login will use the same username you previously specified in the `user.txt` file**, which is also a *sudoer* user. Every component in the infrastructure has a different hostname matching the corresponding lab diagram to enable you to better understand where you are. Also, *Kali* and *Ubuntu* containers have different “flavors” (color palette and bash prompt).
- **volume_data** folder: Everything you write in the **/shared** folder of any container you can log in will be placed in the corresponding subfolder on this one (one per machine hostname). **Consequently, you can write something here in the VM and immediately obtain it in the corresponding container.** This is meant to be an **easy mechanism to share files between the containers and the VM/host**.



The recommended way of working with every lab is to open two terminals in the corresponding lab folder like this:



In the first terminal, run the **prepare_labX.sh** script and wait for it to finish. You only need to do this once, but please **ensure** that you **have network connection** during the process. If lost, run **prepare_labX.sh** again:

```
vagrant@vagrant: ~/Documents/ssi_labs/lab_sessions/lab_02
File Edit View Search Terminal Help

Uniovi: Computer Science School (EII)
Computer System Security (SSI)

: Ubuntu 18.04 XFCE4 VM (Cores: 2, RAM: 1992.91Mb)
: Tuesday, 28/12/2021, 09:29:28 AM
: HACK FIRST, HACK HARD, NO MERCY!

Current dir: /home/vagrant/Documents/ssi_labs/lab_session
s/lab_02
Internet?: Yes

Need a GUI? Type startx. Need instructions about a command in the GUI? run gman
and search it
No GUI? need more terminals? Do Alt+F2, F3, etc. or run tmux. Need a file browse
r? Run mc
Absolutely no clue about the command you should use for something? Run apropos <
what you want to do> and see your options
vagrant@vagrant:~/Documents/ssi_labs/lab_sessions/lab_02$ ./prepare_lab2.sh
Building the ssi/ubuntu_base image...
Sending build context to Docker daemon 4.54kB
Step 1/10 : FROM ubuntu:focal
focal: Pulling from library/ubuntu
```

Once this finishes, run the **build_labX.sh** script and wait for it to stop its output. **Do not close this terminal!**



```
vagrant@vagrant: ~/Documents/ssi_labs/lab_sessions/lab_02
File Edit View Search Terminal Help
Processing triggers for ca-certificates (20210119) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Removing intermediate container ee5ef3c28580
---> 8be7abe998fd
Step 4/6 : USER $USER_NAME
---> Running in ffeba72eafdb
Removing intermediate container ffeba72eafdb
---> a90174f73975
Step 5/6 : WORKDIR /home/$USER_NAME
---> Running in 4d23fa89de57
Removing intermediate container 4d23fa89de57
---> b8f46a94a9c9
Step 6/6 : LABEL          maintainer="Jose Manuel Redondo Lopez" version="1.2" d
description="Kali image for SSI enumeration laboratories (2021-2022)"
---> Running in d73926ea700b
Removing intermediate container d73926ea700b
---> d40fa9944f35
[Warning] One or more build-args [USER_NAME] were not consumed
Successfully built d40fa9944f35
Successfully tagged ssi/kali_for_enumeration:latest
vagrant@vagrant:~/Documents/ssi_labs/lab_sessions/lab_02$ ./build_lab2.sh
```

When the lab finishes building, you can now use the available `enter_XXX.sh` scripts to login into the appropriate containers for the current lab, using the second terminal you opened:

```
vagrant@vagrant: ~/Documents/ssi_labs/lab_sessions/lab_02
File Edit View Search Terminal Help
lab2_web_epl | * Starting Apache httpd web server apache2
lab2_kali | You can also have a file browser with the 'mc' command (Midnight C
ommander)
lab2_web_asturias | * Starting OpenBSD Secure Shell server sshd
lab2_web_epl | AH00558: apache2: Could not reliably determine the server's fully
qualified domain name, using 172.2.0.4. Set the 'ServerName' directive globally
to suppress this message
lab2_web_asturias | ...done.
lab2_web_epl | *
lab2_web_asturias | * Starting Apache httpd web server apache2
lab2_web_epl | * Starting OpenBSD Secure Shell server sshd
lab2_web_asturias | AH00558: apache2: Could not reliably determine the server's fully
qualified domain name, using 172.2.0.6. Set the 'ServerName' directive globally
to suppress this message
lab2_web_asturias | *
lab2_dns_server | * Starting domain name service... named
lab2_dns_server | ...done.
lab2_web_epl | ...done.
lab2_web_epl | * Starting Apache httpd web server apache2
lab2_web_epl | AH00558: apache2: Could not reliably determine the server's fully
qualified domain name, using 172.2.0.3. Set the 'ServerName' directive globally
to suppress this message
lab2_web_epl | *

vagrant@vagrant: ~/Documents/ssi_labs/lab_sessions/lab_02
File Edit View Search Terminal Help
Uniovi: Computer Science School (EII)
Computer System Security (SSI)
: Ubuntu 18.04 XFCE4 VM (Cores: 2, RAM: 1992.91Mb)
Tuesday, 28/12/2021, 09:29:33 AM
: HACK FIRST, HACK HARD, NO MERCY!
Current dir: /home/vagrant/Documents/ssi_labs/lab_session
s/lab_02
Internet?: Yes

Need a GUI? Type startx. Need instructions about a command in the GUI? run gman
and search it
No GUI? need more terminals? Do Alt+F2, F3, etc. or run tmux. Need a file browse
r? Run mc
Absolutely no clue about the command you should use for something? Run apropos <
what you want to do> and see your options
vagrant@vagrant:~/Documents/ssi_labs/lab_sessions/lab_02$ ./enter_kali_lab2.sh
```

Notice the logo change when you logged in? You are now `<your username>` (sudoer user) inside a *Kali Linux* container created to emulate a VM. Follow the corresponding lab instructions to start doing your tasks. **EVERY LAB HAS THE SAME WAY OF SETTING UP THEIR INFRASTRUCTURE! Happy hacking! 😊**

```

redondo@lab2_kali: ~
File Edit View Search Terminal Help
what you want to do> and see your options
vagrant@vagrant:~/Documents/ssi_labs/lab_sessions/lab_02$ ./enter_kali_lab2.sh
.....;;ccc,.
.....';lx0.
..'''.:ld;
..';:;,x,
..'''.
...      0Xxoc:,. ... Escuela de Ingenieria Informatica (EII)
...      ,ONkc;;cok0dc',,. Seguridad de Sistemas Informaticos (SSI)
      OMo      ':odo.
dMc      :00;      Kali Rolling (Docker Container)
0M.      :.o.      Tuesday, 28/12/2021, 09:38:56 AM
;Wd      HACK FIRST, HACK HARD, NO MERCY!
;X0,
,d00dlc;...      Internal IPs: 172.18.0.2,172.2.0.7
..',;:cd00d:,.      Internet?: Yes
      :d;.';:
      'd, .'
      ;l ..
      .o
      c

Remember that 'tmux' opens a multi-pane terminal
You can also have a file browser with the 'mc' command (Midnight Commander)
redondo@lab2 kali:~$

```

To stop a lab, go to the build terminal and **press Ctrl+C**. Please wait for the cleanup to be completed (you return to the bash prompt, as in the image) before exiting the terminal. You will be automatically logged out of every container of the lab you are currently logged on:

```
vagrant@vagrant: ~/Documents/ssi_labs/lab_sessions/lab_02
File Edit View Search Terminal Help
lab2_dns_server * Starting domain name service... named
lab2_dns_server ...done.
lab2_web_eii ...done.
lab2_web_eii * Starting Apache httpd web server apache2
lab2_web_eii AH00558: apache2: Could not reliably determine the server's fully
lab2_web_eii qualified domain name, using 172.2.0.3. Set the 'ServerName' directive globally
lab2_web_eii to suppress this message
lab2_web_eii *
^CGracefully stopping... (press Ctrl+C again to force)
Stopping lab2_web_eii ... done
Stopping lab2_dns_server ... done
Stopping lab2_web_eii ... done
Stopping lab2_web_uniovi ... done
Stopping lab2_kali ... done
Stopping lab2_web_asturias ... done
Going to remove lab2_web_eii, lab2_dns_server, lab2_web_eii, lab2_web_uniovi, lab
b2_kali, lab2_web_asturias
Removing lab2_web_eii ... done
Removing lab2_dns_server ... done
Removing lab2_web_eii ... done
Removing lab2_web_uniovi ... done
Removing lab2_kali ... done
Removing lab2_web_asturias ... done
vagrant@vagrant:~/Documents/ssi_labs/lab_sessions/lab_02$

vagrant@vagrant:~/Documents/ssi_labs/lab_sessions/lab_02
File Edit View Search Terminal Help
what you want to do> and see your options
vagrant@vagrant:~/Documents/ssi_labs/lab_sessions/lab_02$ ./enter_kali_lab2.sh
.....;ccc,
.....;lx0;
.....;ld;
.....;X;
.....0Xxoc;.. ... Escuela de Ingenieria Informatica (EII)
.....,ONKc;,,cok0dc',.. Seguridad de Sistemas Informaticos (SSI)
.....OMo :odo.
.....dMc :00; Kali Rolling (Docker Container)
.....OM. :.o. Tuesday, 28/12/2021, 09:38:56 AM
.....;Wd HACK FIRST, HACK HARD, NO MERCY!
.....;X0;
.....,d00dlc;... Internal IPs: 172.18.0.2,172.2.0.7
.....'.,',cd00d;.. Internet?: Yes
.....:d;';'
.....'d;..'
......o
.....c

Remember that 'tmux' opens a multi-pane terminal
You can also have a file browser with the 'mc' command (Midnight Commander)
redondo@lab2 kali:~$ vagrant@vagrant:~/Documents/ssi_labs/lab_sessions/lab_02$
```