LAB 06A Metasploit

If you have KALI/ Parrot - on Vmware

Is your download speed great? (900 MB = very fast connection) #1 download and install
Metasploitable2: Vulnerable Linux Platform
http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

If you have KALI/ Parrot - on Virtualbox:

Do you have AWS account? #2
https://github.com/deanbushmiller/CEH-bootcamp/wiki/LABS#until-20210701-if-you-want-an-aws-victim-lab-based-upon-metasploitable-3

MY AWS AMI image is based upon Metasploitable 3 Windows platform https://github.com/rapid7/metasploitable3

If you have never used AMIs then watch:https://vimeo.com/566133957

Using my public AWS AMI image: it has different numbers in different regions
Owner : 613495877740

This image will be live until 20210701

Steps:

1. Login
2. Set the Region to one of these closest to you : us-west-1 / eu-west-2 / ap-southeast-1
3. From Services EC2
4. Images AMIs
5. Search: Public Images
6. Owner : 613495877740
7. If you are in the wrong region it will not show.

Assumption: you have one or the other

From here you can follow this simple lab below and/ or do the two best full fledge courses:
https://www.tutorialspoint.com/metasploit/index.htm
https://www.offensive-security.com/metasploit-unleashed/

Basic:
START Metasploit:

Metasploit Framework uses PostgreSQL as its database, so you need to launch it by running the following command in the terminal:

service postgresql start

You can verify that PostgreSQL is running by executing the following command:

service postgresql status

With PostgreSQL up and running, you need to create and initialize the msf database by executing the following command:

msfdb init

Launch the Metasploit Console

msfconsole

help

What is the IP address of your metasploitable victim? VICTIM:IP

For metasploitable 2

The list of flaws is here:
https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/

For metasploitable 3

The list of flaws is here:
https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities