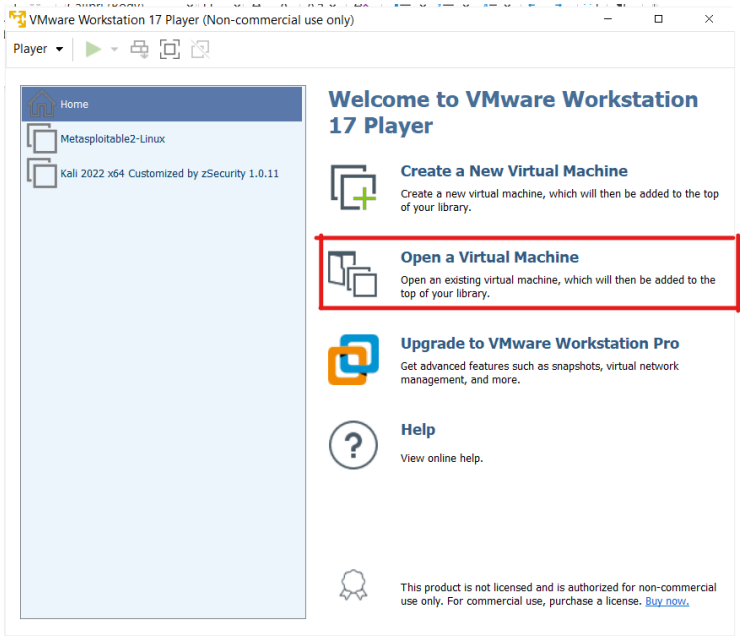
Downloading the resources.

- First install python if it is not previously installed.
- Python can be installed from here.
- Once python is installed, please open terminal if you are using Linux machine or command prompt if you are using a windows machine.
- After opening terminal/command prompt type the following 2 commands.
  1) pip install requests
  2) pip install bs4
- Now install VMware Workstation Player, it can be downloaded from here.
- While VMware is being installed, download Metasploitable machine from here.
- Once the Metasploitable machine is downloaded, extract the files.
- Now open VMware Workstation Player on our machine and select the "open a virtual machine" option as shown below.



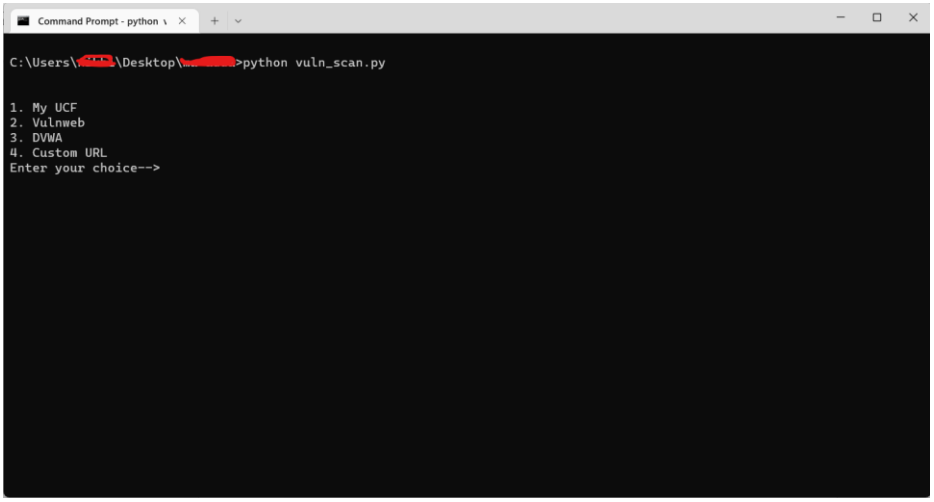
- Once the option is selected, go to the folder where the Metasploitable machine was extracted.
- Select the VMware virtual machine configuration file and select open.
- Once the option is selected it will be placed in the left side panel of the VMware workstation player as shown above
- Now right click on the metasploitable2-Linux machine and click on settings.
- In settings select network adapter and select NAT and click on okay.
- Now select the machine and click on play virtual machine. This should turn the device on.
- Once the device is switched on login into the machine with the following credentials.

Username: msfadmin
Password : msfadmin

- Now type if config in the machine to know the IP address.
- Now run the vulnerability scanner on your host machine.
- To run the scanner, open terminal or command prompt on your machine and navigate to the location where you saved the scanner.

Now type “python VulnScanner.py” to run the scanner

It should provide you with the below options.



- Select the required option and follow the instructions provided by the tool.
- After providing all the details the tool will scan the required website and return any vulnerabilities that are found.

The below image is an example of the output.