CYBR545- Kali Linux Exercise #3

(Team-based, 100 points)

### Due on Sunday 3/5/2023 @11:49PM Group No.:

### Group members names:

# Grading Rubric:

Questions 1,3,4: 20 points each  
Question 2: 50 points  
Question 5: 10 points

# Introduction and submission:

One of the benefits of using virtualization is the capability to snapshot/restore your environment. At this point your Kali Linux install is fairly vanilla unless you have installed other tools on the VM.

In this Kali Linux Lab, step one will be to take a snapshot of your VM, so you have a good restore point in the future in the event you ever corrupt your installation. This can be accomplished using Machine > Take Snapshot on the VirtualBox menu while your VM is running. You can refer to the Oracle docs for more information[1].

Once you create you snapshot, the next part of this lab is to get docker installed and running on your VM. Docker is a set of platforms as a service (PaaS) product that use OS-level virtualization to deliver software in packages called containers. Containers are isolated from one another and bundle their own software, libraries, and configuration files; they can communicate with each other through well-defined channels. Because all the containers share the services of a single operating system kernel, they use fewer resources than virtual machines.

To run docker on a VM, you may need to enable nested virtualization if you are using an AMD processor. Enable the Nested VT-x/AMD-V checkbox under the processor tab of your VM. See Figure 1.

Graphical user interface, text, application, email

Description automatically generated

Figure : Screenshot of System settings in VM

If assistance is needed to setup docker on your VM, see the tutorial video [2] that shows an easy method to stand up docker and running a container.

Upon success of installing docker, please proceed to install docker-compose as well your VM by using the command in Figure 2:

**

Figure : Command to install docker on Kali Linux

Create a docker-compose.yml file for a hello-world test. (If you’re unsure how to create this, please refer to the documentation [3].) The file should be named docker-compose.yml and the contents are given in Figure 3 : (note the tabs in the formatting)

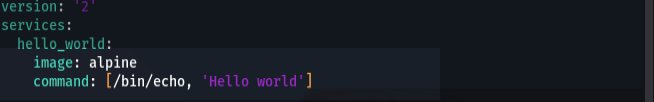


Figure : Code content of the docker-compose.yml file

The above docker file will pull the default Alpine Linux container and then echo Hello World

Run the yml file and provide a screenshot of docker container hello-world running by issuing command in Figure 4:



Figure : Command to run the yml file

Create a vulnerable network for lab purposes by running the command shown in Figure 5 on your Kali VM



Figure : Command to create a vulnerable network

Now start a vulnerable container called metasploitable2using the command provided in Figure 6.



Figure : Command to start Vul. Container

Once the container is running type (services.sh)within the metasploitable container terminal window. This will start a bunch of vulnerable services on the container. Now that you have a vulnerable target running under docker, this is the penetration testing component of this exercise.