Lab 1

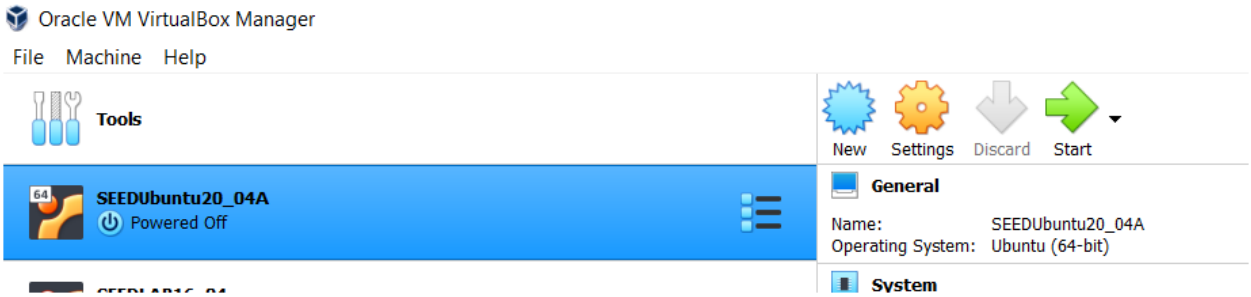
Due Sept 18/19/20/14 (on your class day)

In this lab, you need to complete the following tasks. In your solution, whenever applicable, you need to provide screenshots to prove your work.

SEEDLAB Setup on your computer: SEEDUbuntu 20.04 at https://seedsecuritylabs.org/labsetup.html

Warning: Do not use Ubuntu 16.04; **Cloud setup** follows https://seedsecuritylabs.org/labsetup.html or my file.

1. Complete the SEEDLAB setup. You can set up on your computer or cloud (if your computer is not possible). Provide a screen shot as a proof of completing your task. Here is an example of setup on my own computer.



Warning: In this lab, the screen shots certainly can not serve as sound evidence for your task completion. You need to be honest. Successful completion of this lab is essential for your study in this course.

2. This question considers sniffing http packet.

- Start your Wireshark capture.
- On your browser, access website of your choice. I recommend http://www.example.com (as it is simple and it is easy to find out on the Wireshark packet list).
- Stop Wireshark

Answer the following questions. In your solution, the screen shot needs to mark the ip addresses required in the questions. If you can not find the answer, try: (1) clear your browser history and (2) clear your ubuntu DNS cache **$ sudo systemd-resolve - - flush-caches**

a. In order to access the selected website, your browser will first issue DNS query to find out the ip address of this website. Find this query packet and the response packet. What is the ip address of the website? You can apply filter **dns** in your Wireshark to restrict the packet list to DNS packets only.

b. The source IP address of the DNS query packet will be your IP address and the destination IP address of the DNS query packet will be the DNS server's IP address. What is the ip address of this DNS server? What is the ip address of your machine?