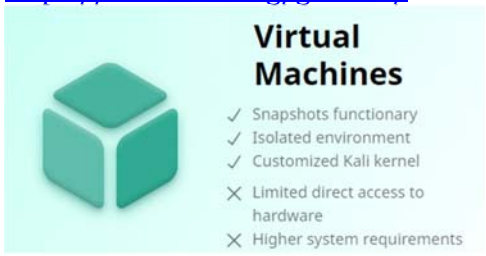
Lab 1

VMs Setup, Running Basic Information Gathering Tools

1. Install Virtual Box (VB) in your personal PC
   - Download and install VirtualBox
   https://www.virtualbox.org/wiki/Downloads

   - Download and install VirtualBox Extension Pack
   https://www.virtualbox.org/wiki/Downloads

2. Install Kali Linux in your personal PC
   - Download Kali Linux (select Virtual Machines > VirtualBox64: download kali-linux-2022.2-virtualbox-amd64.ova)
   https://www.kali.org/get-kali/



   - Import Kali Linux
   - In VirtualBox, Select File > Import Appliance > Select the ova file > Agree with the Software Licence Agreement
   (You may want to change folder to where you want to store your virtual machine)

3. Running VMs on Virtual Box/Configuring your VirtualBox setting

   - [Important] The trickiest part of setting up VB is configuring network. There are a few options to manage network on VB but in this subject, we will mainly use the **NAT Network** setting. The following setting MUST be set while Kali is not operating.

      1. Click “File” (on the left corner of the VB Manager window) → Select “Preferences” → Click “Network” on the left panel → Click + icon on the right side of the window; “NatNetwork” will be created

→ Click OK (In the NatNetwork, your VB is going to be a gateway router and a DHCP server. All the VMs attached to the NatNetwork will be assigned IP addresses allocated by your VB.)

2. Now select <Your Kali Machine> (On the list in you main VB window)→ Right click → Select "Settings" → On the pop-up window → select "Network".
3. Now, in the "Adapter 1" tab, check "Enable Adapter Network" if this is not selected. → Select "NAT Network" from the drop-down list for "Attached to"; NatNetwork will be selected as "Name" → Click OK. This will enable your Internet connection in the Kali.
4. Now, turn on your Kali VM and login with username `kali` and password `kali`.
5. The last important step is to boot Kali to make the network setting change take effect; Check the network setting by run `ifconfig.` Your System must have 2 network interfaces which are "eth0" and "lo".
6. Check "eth0" is assigned with IP address (indicated as inet).

4. Installing (loading) Metasploitable VM

- Metasploitable(2) will be used as a target machine, which is purposely set up as vulnerable.

- Download Metasploitable from https://sourceforge.net/projects/metasploitable/

- Unzip "metasploitable-linux-2.0.0"
- Open VB, go to Machine → New
- Give a name "Metasploitable2", select "Linux" in Type, and "Ubuntu (32-bit)" in Version
- Choose the memory size (512MB or 1GB)

- Select "Use an existing hard disk file", browse to the folder where you have extracted the zip files and select the 'vmdk' file available (click "Add" to browse the file if necessary)

- Click "Create"

- Configure the network of Metasploitable2 in the same way as you do for the Kali linux.

- Login to Metasploitable2 with username `msfadmin` and password `msfadmin`.
- After login again, run `ifconfig` to find the IP. Now, go back to your Kali machine and `ping <IP of Metasploitable2>` to check if it's live. You can also run the ping command from Metasploitable2 VM.

5. Run the following information gathering tools such as **nslookup** and **whois** to answer the following questions.

    a. What is the IP address of your local DNS server (resolver)?
    b. What is the IP address(es) of our university website, `www.uow.edu.au`?
    c. What is the name of the primary authoritative DNS server of our uow domain (uow.edu.au)?
    d. What is the name of the mail server of our uow domain (uow.edu.au)?
    e. What is "Registrar Name" of our uow domain?

6. Run `traceroute` from your host machine (Windows or Mac) to answer the following questions.
    a. Issue the following command in the terminal: `sudo traceroute -I howtogeek.com` (or `tracert howtogeek.com` on Windows) and see how many hops exist between your network and the destination. (Note that `sudo` means you run the following command as a root. - The traceroute command needs root privilege. Note also that -I indicates the ICMP probing. In Unix-based systems including Mac OS, the UDP probing for traceroute is default, which is often blocked by firewall.)
    b. Can you determine the boundary of your home network?
    c. What is the destination IP address (in this task, `howtogeek.com`)?
    d. Can you determine the boundary of the Singapore network (the last hop the packet is still in Singapore)?

7. Try to get email addresses of UOW students. You may need to use `theHarvester`.
    (Try to issue `theHarvester –d uowmail.edu.au -b google`)

8. Perform "ego-search"- Googling your name, id etc. Are you comfortable with the result?

9. Discuss what kind of information can be obtained mainly by using the following web-based information gathering tools:

    a. https://whois.domaintools.com
    b. https://sitereport.netcraft.com/
    c. https://searchdns.netcraft.com/
    d. https://www.yougetsignal.com/tools/web-sites-on-web-server/

10. Try to use the above web-based tools to get various information about wikipedia.org.

Homework: Install Ubuntu 22.04 on your VirtualBox. Configure the network setting so that your Ubuntu VM will belong to the same NAT Network.