Lab 1: Introduction to Lab Environment and Kali Linux

Preliminaries

Our lab environment is provided by our school cloud, which is powered by VMware vSphere. In this lab environment, each student owns the following three VMs:

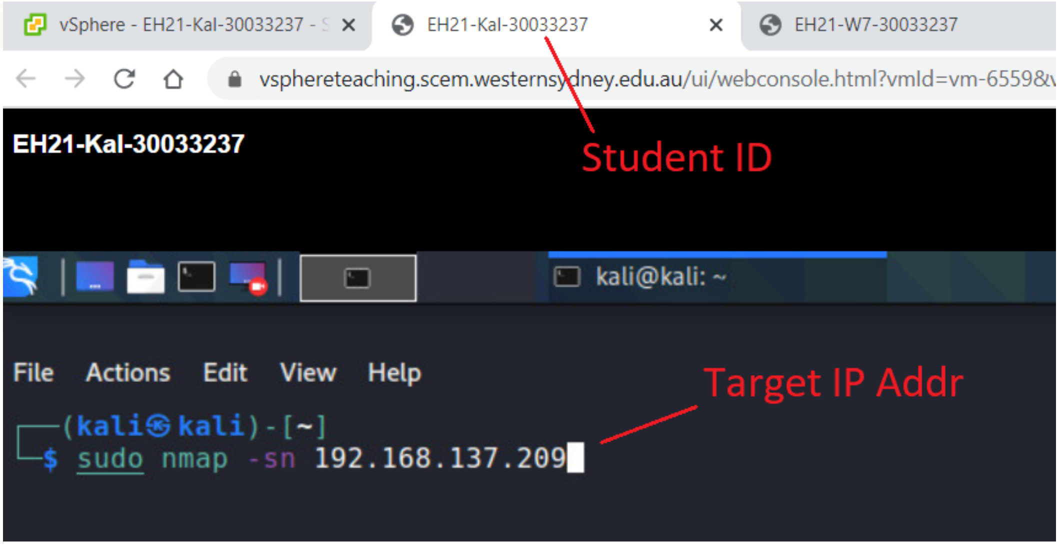
- Kali Linux (the attacking VM)
- Windows 7 (a deliberately vulnerable Windows VM to be attacked)
- Metasploitable 2 (a deliberately vulnerable Ubuntu Linux VM to be attacked)

All the three VMs are connected to a virtual LAN via a virtual switch. The virtual LAN is, in turn, connected to external network via NAT. To use these VMs, you need to connect to the School's VMWare vCenter Server using a web browser as detailed in our Lecture 1B.

Note that the performance of VMs may become slow. You should deem this as normal, especially when many students are using the school cloud at the same time. Also, **you should not perform any updates of the OSes and programs on the VMs,** otherwise your experiments results may not be the same as what we teach in lectures.

Lab Report Requirements

1. **Your report must include the hierarchical label for each question before your answer.** As for the question body, it is optional.
2. When you are asked to include a screenshot into your report**, the screenshot must include the top tab of the VM window that shows your Student ID.** If you are using VMs created on your own laptop, then the screenshot must show the IP address of the target somewhere. For instance, the target IP can appear in your command line, or if the command line does not include the target IP, you can use 'ip a' command to display the IP address intentionally. An exemplar screenshot is included as follows.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.137.209
```

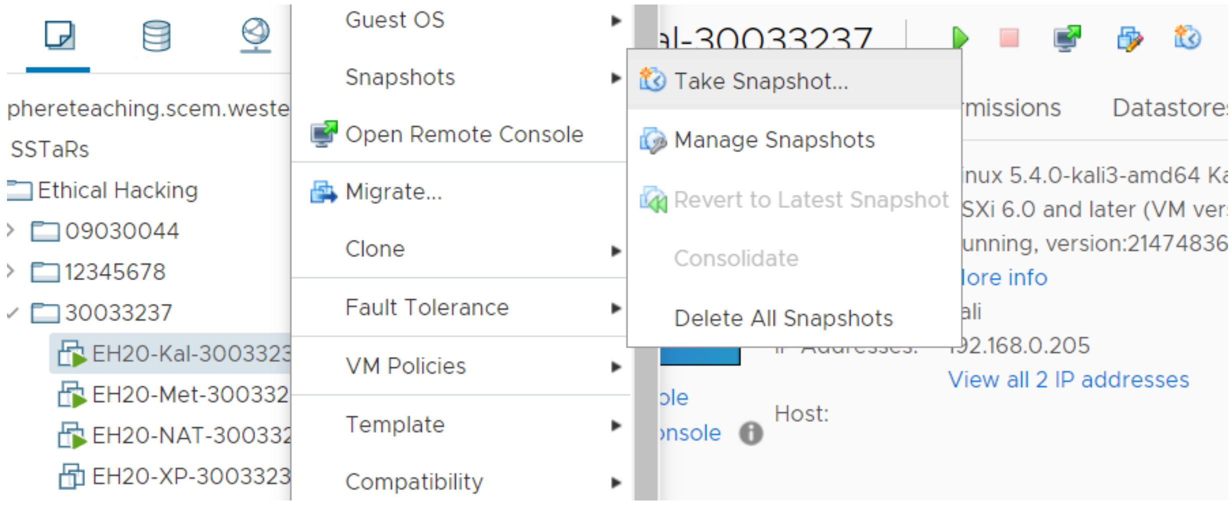
NB: Failing to satisfy above requirements will cause you lose marks for relevant questions. These requirements apply to future lab reports as well.

Tasks

Complete the following tasks and write your answers for all questions into your lab report.

1. Before you start using these three VMs, create the snapshots of them first. A snapshot is a copy of the VM's disk file (VMDK) at a given time. Snapshots can be used to restore VM to a previous state when system errors occur.

   In this task, you should create a snapshot named 'Initial' for each of your VMs by right-clicking the VM name and then clicking 'Snapshots' → 'Take Snapshot' (an exemplar screenshot is provided below).



   Later in this semester, if you destroy a VM, you can revert to its initial state using the snapshot created in this lab.

   In your lab report, you should include a screenshot of the opened 'Manage Snapshot' for each of your VMs, showing that the 'Initial' snapshot has been created.

   1.1 Include the screenshot for Kali VM.
   1.2 Include the screenshot for Metasploitable2 VM.
   1.3 Include the screenshot for Win7 VM.

   Note: A screenshot can be obtained by using tools such as 'Snipping Tool', which is available in Windows Start menu → Windows Accessories.

2. Power on the Win7 VM, and login to the admin account (password: admin123). Start a command window.

   2.1 Use the command 'ipconfig' to determine the IP address of this VM. Write the result to your lab report.
   2.2 If you need the MAC address of the VM as well, what option you should add to the 'ipconfig' command?
   2.3 Use the command 'netstat -an -p tcp' to determine which TCP ports are in a listening state. Write the result to your lab report.
   2.4 In your report, also explain the meanings of the options '-a' and '-n'. You can use the command 'netstat /?' to find out the answer. (Note: although 'netstat' is deprecated in Linux, it is not in Windows)

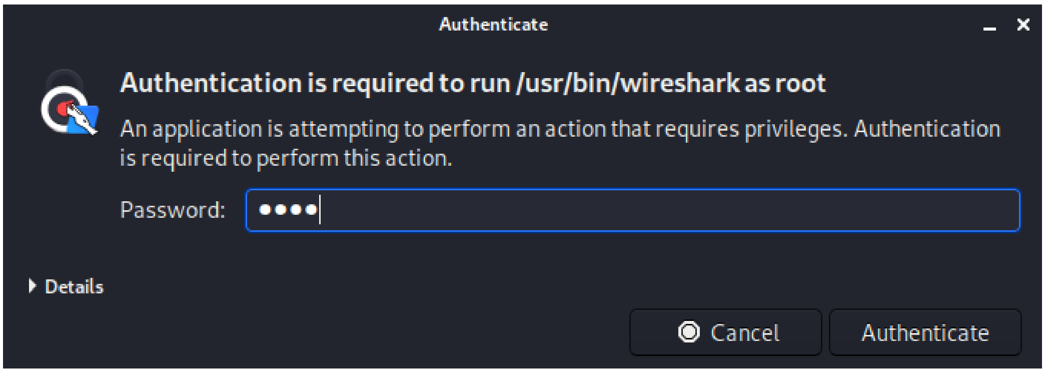
3. Power on the Metasploitable2 VM, and login with username 'msfadmin' and password 'msfadmin'. Note that when you enter a password to a Linux system, oftentimes no wildcard letter will be displayed for each letter you type. What you should do is to finish typing the entire password and then hit ‘Enter’.
   - 3.1 Use the 'ip a' command to show the IP address and MAC address of this VM. Write the result to your lab report. (Hint: look for the result from the output for Ethernet interface ‘eth0’)
   - 3.2 Use the command 'ss -ant | more' to determine which TCP ports are listening. Write the result to your lab report.
   - 3.3 In your report, also explain the meanings of the options '-a', '-n', and the operator ‘|’.

   Finally, press the 'Ctrl + Alt' to leave this VM.

4. Power on the Kali Linux VM. Login with username 'kali' and password 'kali'. Please refer to Appendix A for how to use its desktop environment. Start a terminal.
   - 4.1 Use the 'ip a' command to show the IP address and MAC address of this VM. Write the result to your lab report. (Hint: look for the result from the output for Ethernet interface ‘eth0’)
   - 4.2 Use the command 'ss -ant' to determine which TCP ports are listening. Write the result to your lab report.
   - 4.3 Here you will notice that the result is very different from those of the previous two VMs. **Explain this difference** in your report after reading the **Kali Network Service Policy**, which can be found at: https://www.kali.org/docs/policy/kali-linux-network-service-policies/. (This site may be blocked in campus network, but accessible in your home network.) You only need to read the first paragraph of this policy.
   - 4.4 Use the command 'ip r' to determine the default gateway for this VM. Write the result to your lab report.
   - 4.5 Ping the Win7 VM. Press 'Ctrl + C' to stop the ping. Note: In Linux, if you want to limit the number of pings, use 'ping -c <count> <destination IP>', where <count> is the number of ping probes (Eg, ping -c 6 192.16.0.2). Write the result to your lab report. If you cannot reach the Win7 VM, try to fix the problem.
   - 4.6 Ping the Metasploitable2 VM. Press 'Ctrl + C' to stop the ping. Write the result to your lab report. If you cannot reach the Metasploitable2 VM, try to fix the problem.

5. Still in the Kali terminal, execute the following three commands in a row:
   'cd /usr/share/metasploit-framework', 'pwd', and 'ls -l'.
   - 5.1 Grab a screenshot for the results of these three commands respectively, and save the screenshots to your lab report.
   - 5.2 In your report, also explain the meanings of these three commands, especially, the option '-l' in 'ls -l'. (Hint: you can execute 'man ls' to find out)

6. In the Kali desktop, search and run the Wireshark program. Since Wireshark needs root privilege to run, you need to authenticate as ‘kali’ to gain the root privilege.



Authentication is required to run /usr/bin/wireshark as root

An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

Password: ••••

Then, click the **Capture** in the top menu bar and then **Options** to choose the interface **eth0** (the Ethernet interface)**.** Click the **Start** button to start capture network traffic.

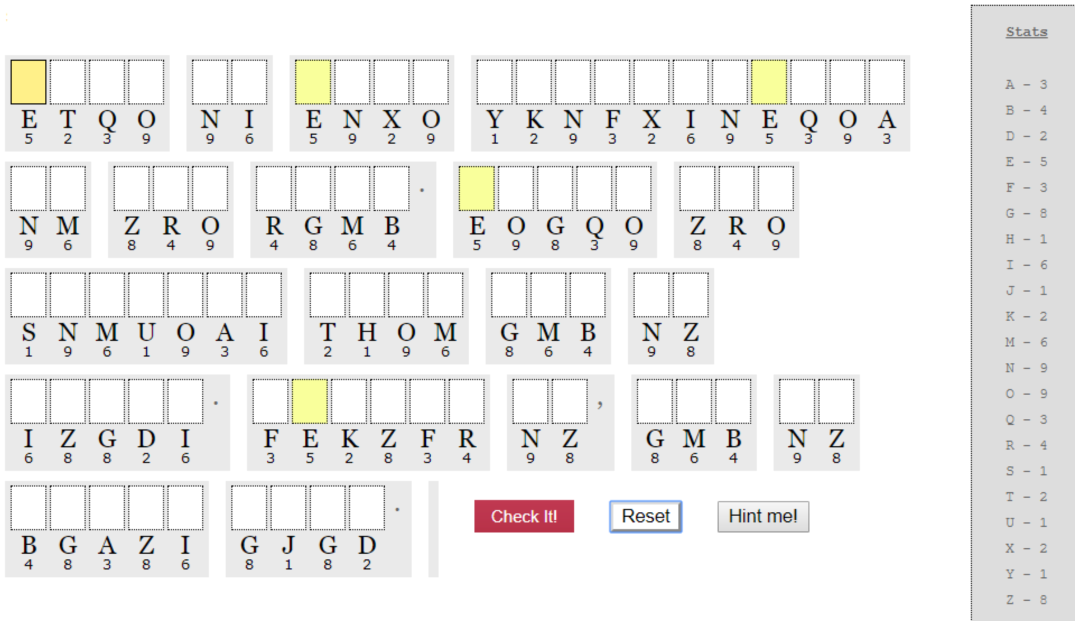
6.1 Switch to a terminal to ping the default gateway. Press 'Ctrl + C' to stop the ping. Include a screenshot for this in your lab report.

6.2 Stop the Wireshark capture and observe the captured ping traffic. Include a screenshot about this in your lab report.

7. This question doesn't involve the use of VMs. It trains you to understand how hackers think in achieving an attack. It uses a game called 'cryptogram' as an example. In cryptogram, you try to decrypt messages encrypted by a cipher similar to the Caesar cipher, probably the first cipher humans have ever invented. You should first understand how this game is played by reading through the following page: https://cryptograms.puzzlebaron.com/faq.php. Then, you should familiarize yourself with it by playing some games at: https://cryptograms.puzzlebaron.com/play.php. In playing this game, you'll often need to find a word with certain pattern. You can get help with this at website: https://www.morewords.com/.

   7.1 In your lab report, give your answer to the following cryptogram. Since you cannot play it using the website (you have to use paper and pencil instead), we offer you a hint that the first letter is 'L'.

   7.2 Describe at least two techniques you use for finding out the answer quickly.



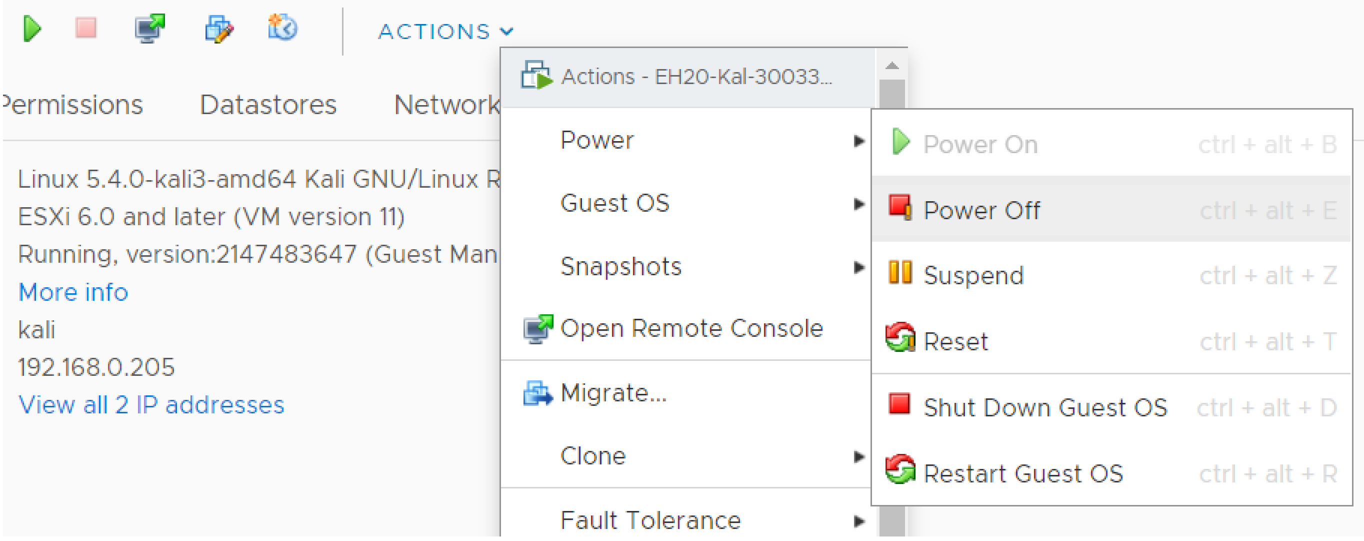
```
E T Q O   N I   E N X O   Y K N F X I N E Q O A
5 2 3 9   9 6   5 9 2 9   1 2 9 3 2 6 9 5 3 9 3

N M   Z R O   R G M B .   E O G Q O   Z R O
9 6   8 4 9   4 8 6 4     5 9 8 3 9   8 4 9

S N M U O A I   T H O M   G M B   N Z
1 9 6 1 9 3 6   2 1 9 6   8 6 4   9 8

I Z G D I .   F E K Z F R   N Z ,   G M B   N Z
6 8 8 2 6     3 5 2 8 3 4   9 8     8 6 4   9 8

B G A Z I   G J G D .
4 8 3 8 6   8 1 8 2
```

Stats

```
A - 3
B - 4
D - 2
E - 5
F - 3
G - 8
H - 1
I - 6
J - 1
K - 2
M - 6
N - 9
O - 9
Q - 3
R - 4
S - 1
T - 2
U - 1
X - 2
Y - 1
Z - 8
```

Powering off all your VMs

After completing all tasks above, **you should first shutdown and then power off all your three VMs.** Our school's cloud is under heavy load, as you can see your VMs may not respond quickly. Therefore, if you are not using them, you should have them power off. To power off, you can use the 'ACTIONS' menu → 'Power' → 'Power Off' as shown below.



Linux 5.4.0-kali3-amd64 Kali GNU/Linux R
ESXi 6.0 and later (VM version 11)
Running, version:2147483647 (Guest Man
More info
kali
192.168.0.205
View all 2 IP addresses

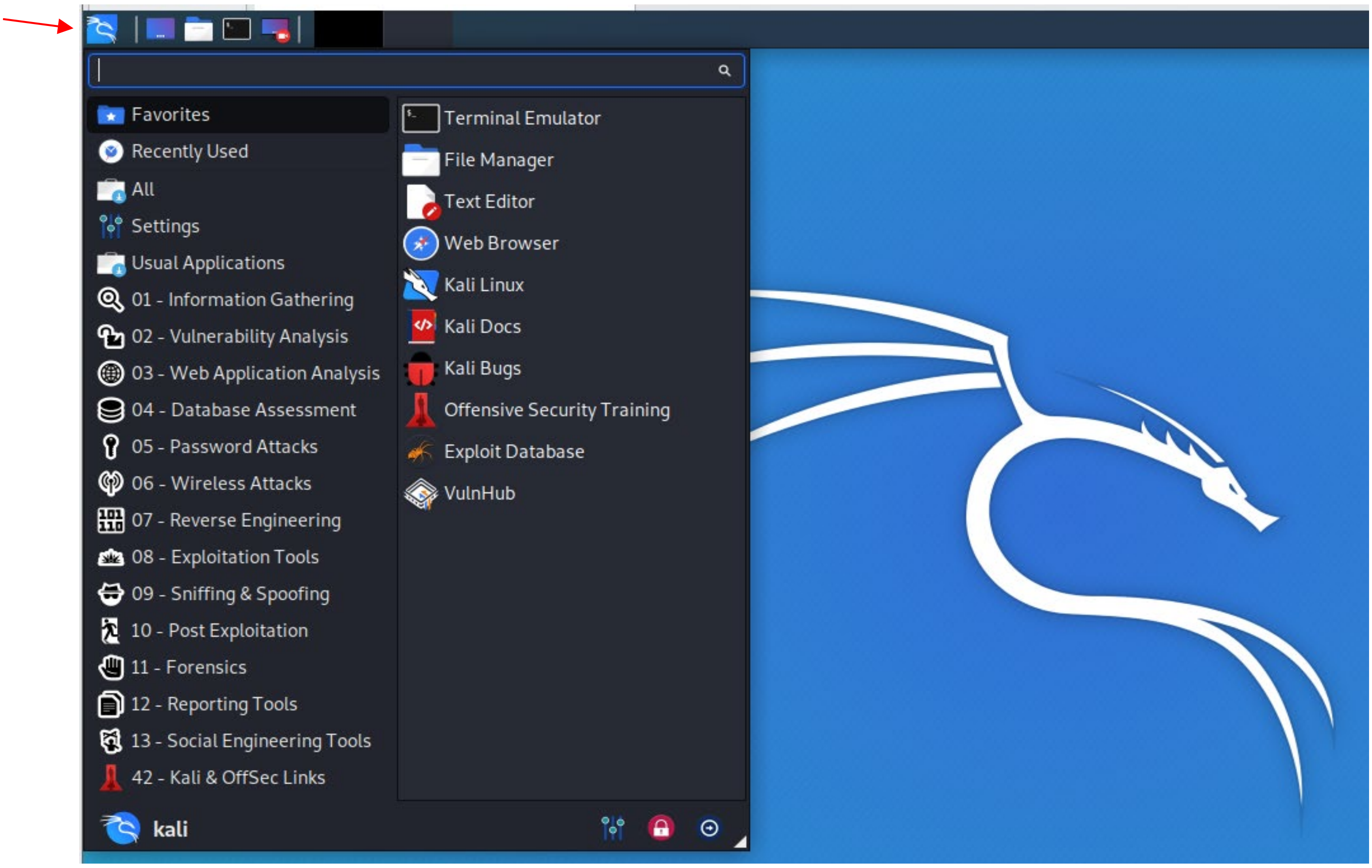
Before you power off a VM, it is better to shut it down first.

- To shutdown Kali, click the 'log off' button in the top bar and then follow the dialogs.
- To shutdown Win7, click 'Start' and then 'Shutdown'.
- To shutdown Metasploitable2, execute the command 'sudo shutdown now -h'.
  Note: The '-h' option means to halt the system instead of rebooting the system. If you leave it out, the 'shutdown' command will reboot the system by default.

Appendix A: How to use Kali's desktop environment: Xfce

There are a number of desktop environments that can be used on Kali Linux. The default one for Kali Linux after 2020 is **Xfce**. Note that, before 2020, Kali uses GNOME or KDE as its default desktop environment. The reasons for this switch are twofold: (1) Xfce is simple and fast; (2) Kali does not need a comprehensive desktop environment such as GNOME. Xfce is basically similar to the interface of Microsoft Windows, but still has some significant differences.

Below is an example screenshot of the Xfce. When you press the Windows key ⊞ in the keyboard or click the Kali icon in the top-left corner, all installed applications and a Search Box will be displayed. The Search Box can be used to search for Applications.



In this unit, the Linux terminal, the fourth one in the top bar, will often be run to provide a command-line interface. Other programs can be easily found and run using the Search Box.

More detailed usage of Xfce can be found at: https://www.xfce.org/.