# **Lab02 Report**

1. Name: Student ID:
2. Proof of your lab work (clearly label each screenshot)
3. Screenshot-01: ifconfig of VM1 (5%)
4. Screenshot-02: ifconfig of VM2 (5%)
5. Screenshot-03: ping session (VM1 to VM2) of communications on the same host

Note: RTT = \_\_\_\_\_\_\_ (5%)

1. Screenshot-04: ping session (VM1 to VM2) of communication between bridged hosts

Note: RTT = \_\_\_\_\_\_\_ (5%)

1. Screenshot-05: ARP cache result from VM1 (5%)
2. Screenshot-06: Result of “traceroute google.com” (5%)
3. Screenshot-07: Result of “traceroute facebook.com” (5%)
4. Screenshot-08: Result of “traceroute cnn.com” (5%)
5. Screenshot-09: Result of “traceroute ntu.edu.tw” (5%)
6. Screenshot-10: A full path from your VM to *cnn.com* or [*www.ntu.edu.tw*](http://www.ntu.edu.tw)(5%)
7. Screenshot-11: Web page of VM2 from the VM1 Browser (FireFox) (5%)
8. Screenshot-12: Web page of VM1 from the VM2 Browser (FireFox) (5%)
9. Question: Is it possible for VM1 to ping VM2 in the NAT configuration on different hosts?

YES or NO. Justify your answer. (10%)

Question: In Task7 Step2, can you successfully find a path to *cnn.com* or *www.ntu.edu.tw* with traceroute? If not, why? Explain the root cause and your observation in detail. Also provide a method to solve this problem. (10%)

1. Please leverage a hacker tool in kali VM and write down the progress you do. There are many attack type you can choose on below: (20%)
   * *Information Gathering*
   * *Wireless Attack*
   * *Vulnerability Analysis*
   * *Password Attack*
   * *Exploitation Tools*