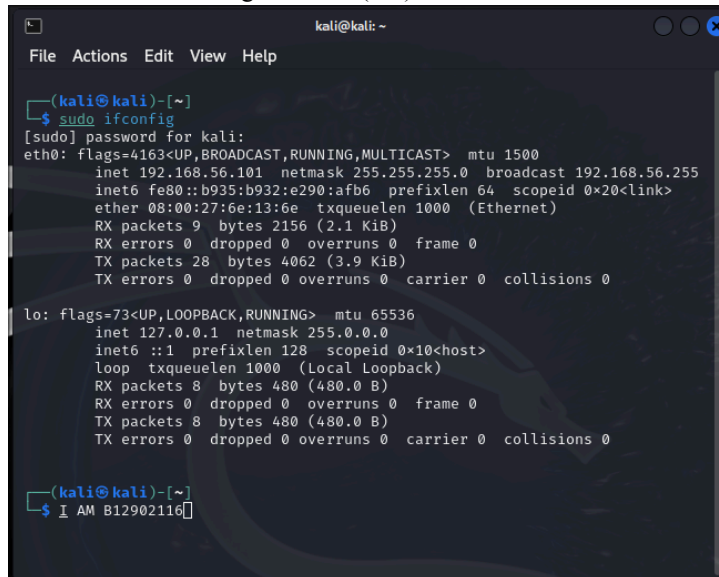


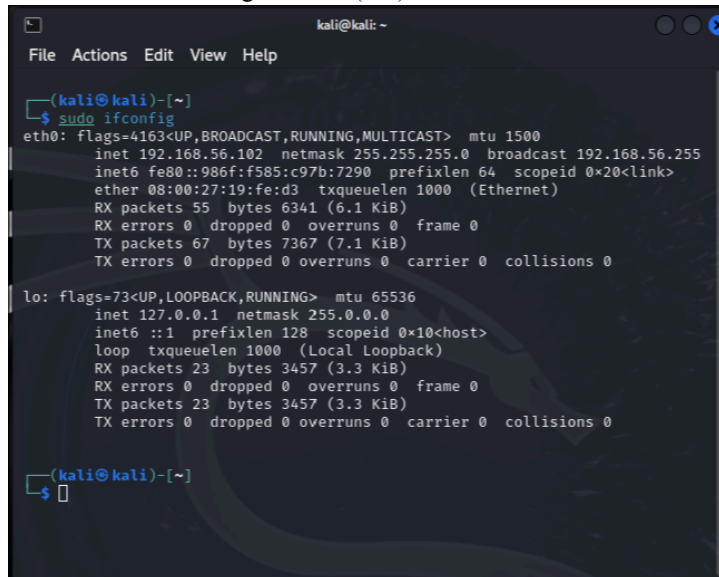
Lab02 Report

1. Name: 林靖昀 Student ID: B12902116
2. Proof of your lab work (clearly label each screenshot)
 - a. Screenshot-01: ifconfig of VM1 (5%)



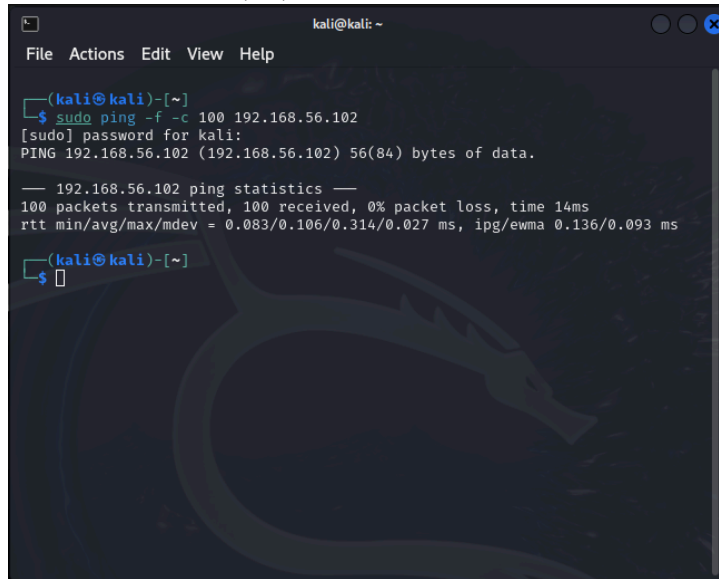
```
kali@kali: -  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo ifconfig  
[sudo] password for kali:  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255  
    inet6 fe80::b935:b932:e290:afb6 prefixlen 64 scopeid 0<20<link>  
    ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)  
    RX packets 9 bytes 2156 (2.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 28 bytes 4062 (3.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$ I AM B12902116
```

- b. Screenshot-02: ifconfig of VM2 (5%)



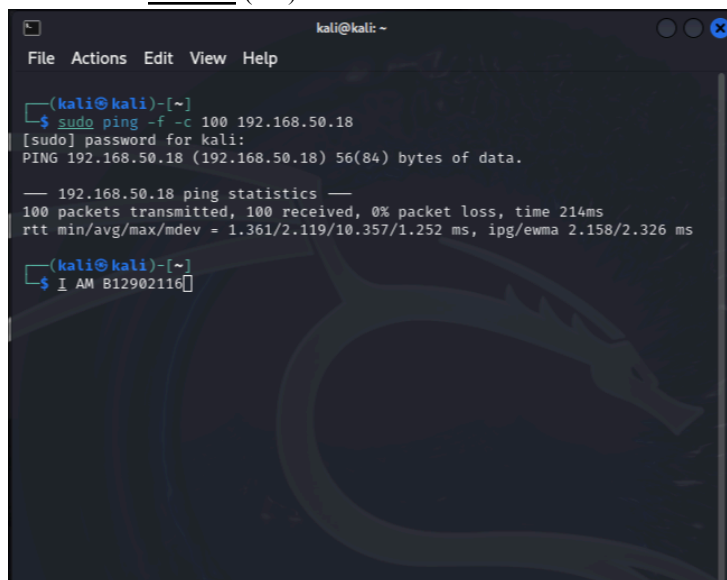
```
kali@kali: -  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255  
    inet6 fe80::986f:f585:c97b:7290 prefixlen 64 scopeid 0<20<link>  
    ether 08:00:27:19:fe:d3 txqueuelen 1000 (Ethernet)  
    RX packets 55 bytes 6341 (6.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 67 bytes 7367 (7.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 23 bytes 3457 (3.3 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 23 bytes 3457 (3.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

- c. Screenshot-03: ping session (VM1 to VM2) of communications on the same host
Note: RTT = 0.106ms(5%)



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo ping -f -c 100 192.168.56.102  
[sudo] password for kali:  
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.  
  
— 192.168.56.102 ping statistics —  
100 packets transmitted, 100 received, 0% packet loss, time 14ms  
rtt min/avg/max/mdev = 0.083/0.106/0.314/0.027 ms, ipg/ewma 0.136/0.093 ms  
  
(kali@kali)-[~]  
$
```

- d. Screenshot-04: ping session (VM1 to VM2) of communication between bridged hosts
Note: RTT = 2.119ms (5%)



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo ping -f -c 100 192.168.50.18  
[sudo] password for kali:  
PING 192.168.50.18 (192.168.50.18) 56(84) bytes of data.  
  
— 192.168.50.18 ping statistics —  
100 packets transmitted, 100 received, 0% packet loss, time 214ms  
rtt min/avg/max/mdev = 1.361/2.119/10.357/1.252 ms, ipg/ewma 2.158/2.326 ms  
  
(kali@kali)-[~]  
$ I AM B12902116
```

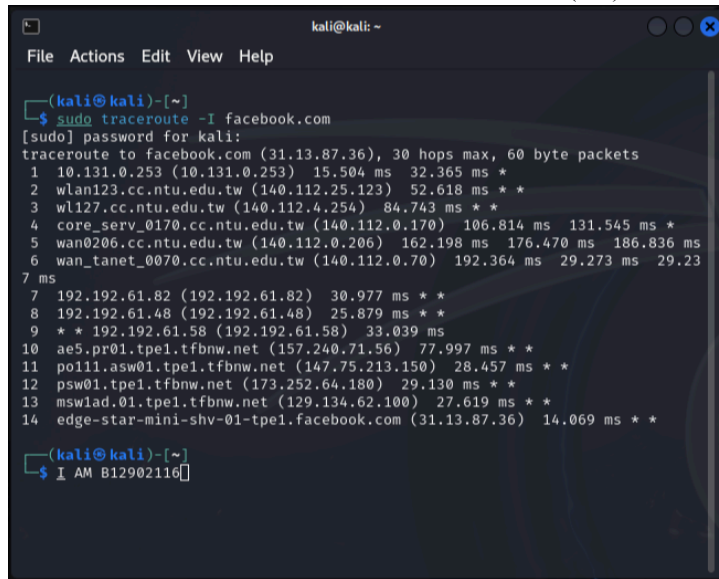
- e. Screenshot-05: ARP cache result from VM1 (5%)

```
kali@kali: ~  
File Actions Edit View Help  
~  
(kali@kali)-[~]  
$ ./arpscan.sh  
Address          HWtype  HWaddress      Flags Mask    Iface  
172.20.10.1      ether   ce:3f:36:c7:fd:64  C           eth0  
172.20.10.3      ether   08:00:27:ab:30:84  C           eth0  
172.20.10.2      ether   b4:6b:fc:b0:8c:36  C           eth0  
~  
(kali@kali)-[~]  
$ I AM 812902116
```

- f. Screenshot-06: Result of “traceroute google.com” (5%)

```
kali@kali: ~  
File Actions Edit View Help  
~  
(kali@kali)-[~]  
$ traceroute google.com  
traceroute to google.com (142.250.204.46), 30 hops max, 60 byte packets  
 1  10.131.0.253 (10.131.0.253)  5.781 ms  5.754 ms  5.735 ms  
 2  wlan123.cc.ntu.edu.tw (140.112.25.123)  4.249 ms  4.717 ms  9.238 ms  
 3  wl127.cc.ntu.edu.tw (140.112.4.254)  9.196 ms  9.163 ms  9.145 ms  
 4  core_serv_0210.cc.ntu.edu.tw (140.112.0.210)  9.112 ms  9.100 ms  core_ser  
v_0170.cc.ntu.edu.tw (140.112.0.170)  9.062 ms  
 5  wan0206.cc.ntu.edu.tw (140.112.0.206)  12.268 ms  12.256 ms  12.217 ms  
 6  wan_sinica_0034.cc.ntu.edu.tw (140.112.0.34)  13.120 ms  13.854 ms  13.37  
5 ms  
 7  72.14.196.229 (72.14.196.229)  9.399 ms  9.380 ms  9.357 ms  
 8  * * *  
 9  209.85.142.120 (209.85.142.120)  25.180 ms  216.239.48.134 (216.239.48.134  
)  25.171 ms  142.251.77.84 (142.251.77.84)  25.154 ms  
10  142.251.226.171 (142.251.226.171)  25.143 ms  25.133 ms  25.114 ms  
11  hkg07s38-in-f14.1e100.net (142.250.204.46)  32.809 ms  32.789 ms  32.768  
ms  
~  
(kali@kali)-[~]  
$ I AM b12902116
```

g. Screenshot-07: Result of “traceroute facebook.com” (5%)



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~  
$ sudo traceroute -I facebook.com  
[sudo] password for kali:  
traceroute to facebook.com (31.13.87.36), 30 hops max, 60 byte packets  
 1  10.131.0.253 (10.131.0.253)  15.504 ms  32.365 ms *  
 2  wlan123.cc.ntu.edu.tw (140.112.25.123)  52.618 ms * *  
 3  wl127.cc.ntu.edu.tw (140.112.4.254)  84.743 ms * *  
 4  core_serv_0170.cc.ntu.edu.tw (140.112.0.170)  106.814 ms  131.545 ms *  
 5  wan0206.cc.ntu.edu.tw (140.112.0.206)  162.198 ms  176.470 ms  186.836 ms  
 6  wan_tanet_0070.cc.ntu.edu.tw (140.112.0.70)  192.364 ms  29.273 ms  29.23  
 7  ms  
 7  192.192.61.82 (192.192.61.82)  30.977 ms * *  
 8  192.192.61.48 (192.192.61.48)  25.879 ms * *  
 9  * * 192.192.61.58 (192.192.61.58)  33.039 ms  
10  ae5.pr01.tpe1.tfbnw.net (157.240.71.56)  77.997 ms * *  
11  po111.asw01.tpe1.tfbnw.net (147.75.213.150)  28.457 ms * *  
12  psw01.tpe1.tfbnw.net (173.252.64.180)  29.130 ms * *  
13  mswlad.01.tpe1.tfbnw.net (129.134.62.100)  27.619 ms * *  
14  edge-star-mini-shv-01-tpe1.facebook.com (31.13.87.36)  14.069 ms * *  
kali@kali:~  
$ I AM B12902116
```

h. Screenshot-08: Result of “traceroute cnn.com” (5%)



```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ traceroute cnn.com
traceroute to cnn.com (151.101.131.5), 30 hops max, 60 byte packets
 1 10.131.0.253 (10.131.0.253)  3.971 ms  3.951 ms  7.930 ms
 2 wlan123.cc.ntu.edu.tw (140.112.25.123)  13.845 ms  13.827 ms  13.813 ms
 3 wl127.cc.ntu.edu.tw (140.112.4.254)  32.715 ms  32.698 ms  32.684 ms
 4 core_serv_0170.cc.ntu.edu.tw (140.112.0.170)  32.670 ms  core_serv_0210.cc
.ntu.edu.tw (140.112.0.210)  32.651 ms  core_serv_0170.cc.ntu.edu.tw (140.112.
0.170)  41.529 ms
 5 wan0206.cc.ntu.edu.tw (140.112.0.206)  41.504 ms  41.472 ms  48.726 ms
 6 175-41-63-53.twgate-ip.twgate.net (175.41.63.53)  48.705 ms  15.247 ms  1
5.217 ms
 7 203-78-181-217.twgate-ip.twgate.net (203.78.181.217)  17.482 ms  203-78-18
1-209.twgate-ip.twgate.net (203.78.181.209)  17.435 ms  17.420 ms
 8 203-78-181-54.twgate-ip.twgate.net (203.78.181.54)  46.580 ms  203-78-181-
58.twgate-ip.twgate.net (203.78.181.58)  46.524 ms  46.508 ms
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

(kali@kali)-[~]
$ I AM B12902116
```

i. Screenshot-09: Result of “traceroute ntu.edu.tw” (5%)

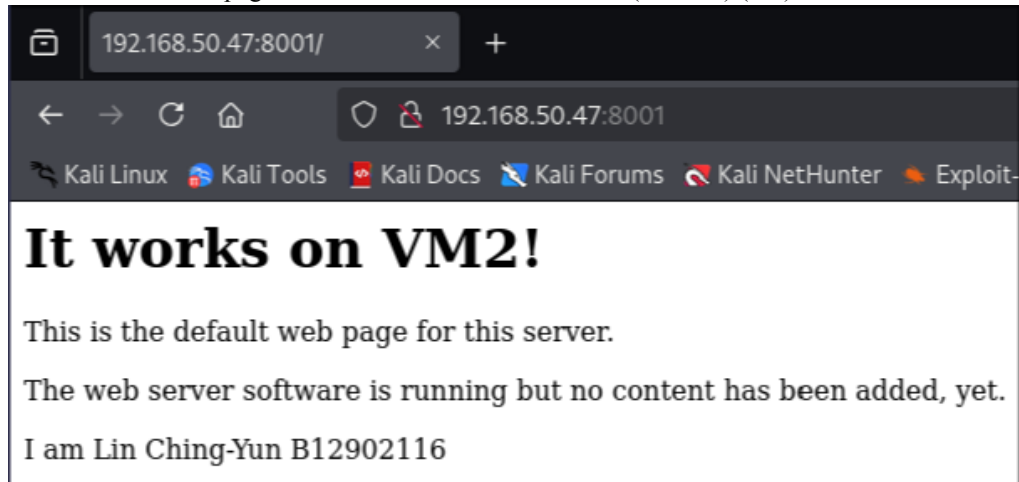
```
kali@kali: ~  
File Actions Edit View Help  
❏(kali@kali)-[~]  
$ traceroute www.ntu.edu.tw  
traceroute to www.ntu.edu.tw (140.112.8.116), 30 hops max, 60 byte packets  
1 10.131.0.253 (10.131.0.253) 5.611 ms 15.129 ms 16.901 ms  
2 wlan123.cc.ntu.edu.tw (140.112.25.123) 33.520 ms 33.503 ms 33.433 ms  
3 wl127.cc.ntu.edu.tw (140.112.4.254) 41.386 ms 66.346 ms 66.335 ms  
4 * * *  
5 * * *  
6 * * *  
7 * * *  
8 * * *  
9 * * *  
10 * * *  
11 * * *  
12 * * *  
13 * * *  
14 * * *  
15 * * *  
16 * * *  
17 * * *  
18 * * *  
19 * * *  
20 * * *  
21 * * *  
22 * * *  
23 * * *  
24 * * *  
25 * * *  
26 * * *  
27 * * *  
28 * * *  
29 * * *  
30 * * *
```

j. Screenshot-10: A full path from your VM to cnn.com or www.ntu.edu.tw (5%)

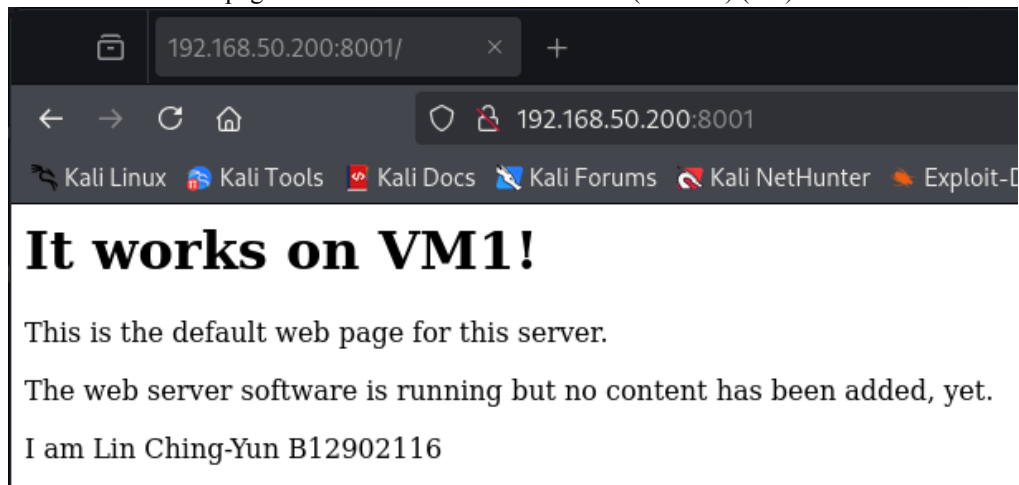
```
kali@kali: ~  
File Actions Edit View Help  
❏(kali@kali)-[~]  
$ ping cnn.com  
PING cnn.com (151.101.67.5) 56(84) bytes of data:  
64 bytes from 151.101.67.5: icmp_seq=1 ttl=55 time=37.4 ms  
^C  
— cnn.com ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 37.418/37.418/37.418/0.000 ms  
❏(kali@kali)-[~]  
$ sudo traceroute -I facebook.com  
traceroute to facebook.com (31.13.87.36), 30 hops max, 60 byte packets  
1 10.131.0.253 (10.131.0.253) 25.975 ms 25.953 ms *  
2 wlan123.cc.ntu.edu.tw (140.112.25.123) 109.203 ms 109.198 ms 109.194 ms  
3 wl127.cc.ntu.edu.tw (140.112.4.254) 145.545 ms 145.542 ms 145.539 ms  
4 core_serv_0170.cc.ntu.edu.tw (140.112.0.170) 187.992 ms 187.990 ms 187.987 ms  
5 wan0206.cc.ntu.edu.tw (140.112.0.206) 219.089 ms 219.087 ms 219.085 ms  
6 wan_tanet_0070.cc.ntu.edu.tw (140.112.0.70) 232.658 ms 22.559 ms 33.201 ms  
7 192.192.61.82 (192.192.61.82) 46.909 ms 41.857 ms *  
8 192.192.61.48 (192.192.61.48) 41.805 ms * *  
9 * 192.192.61.58 (192.192.61.58) 21.591 ms *  
10 * * *  
11 * * *  
12 * * *  
13 * * *  
14 * edge-star-mini-shv-01-tpe1.facebook.com (31.13.87.36) 89.499 ms 89.433 ms  
❏(kali@kali)-[~]  
$ I AM B12902116
```

```
kali@kali: ~  
File Actions Edit View Help  
❏(kali@kali)-[~]  
$ ping www.ntu.edu.tw  
PING www.ntu.edu.tw (140.112.8.116) 56(84) bytes of data:  
64 bytes from www.ntu.edu.tw (140.112.8.116): icmp_seq=1 ttl=252 time=16.7 ms  
^C  
— www.ntu.edu.tw ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 16.700/16.700/16.700/0.000 ms  
❏(kali@kali)-[~]  
$ sudo traceroute -I www.ntu.edu.tw  
traceroute to www.ntu.edu.tw (140.112.8.116), 30 hops max, 60 byte packets  
1 10.131.0.253 (10.131.0.253) 2.333 ms 2.959 ms *  
2 wlan123.cc.ntu.edu.tw (140.112.25.123) 11.670 ms 11.665 ms 11.660 ms  
3 wl127.cc.ntu.edu.tw (140.112.4.254) 11.654 ms 13.358 ms 13.353 ms  
4 www.ntu.edu.tw (140.112.8.116) 13.350 ms 13.345 ms *  
❏(kali@kali)-[~]  
$ I AM B12902116
```

- k. Screenshot-11: Web page of VM2 from the VM1 Browser (FireFox) (5%)



- l. Screenshot-12: Web page of VM1 from the VM2 Browser (FireFox) (5%)



3. Question: Is it possible for VM1 to ping VM2 in the NAT configuration on different hosts?

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

Answer: NO, ping sends ICMP messages, which operates at layer 3 in the internet protocol stack. At layer 3, there is no multiplexing with ports, thus we are unable to ping a device behind a NAT, since we aren't able to access their private IP .

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%)

Answer: By default, traceroute sends UDP probes, which might be blocked by firewalls on the route to the destination, however, we see that we can ping both domains successfully, which means ICMP_ECHOs are successfully reaching the destination, we can use the -I flag in traceroute to send ICMP_ECHO probes instead of UDP probes.

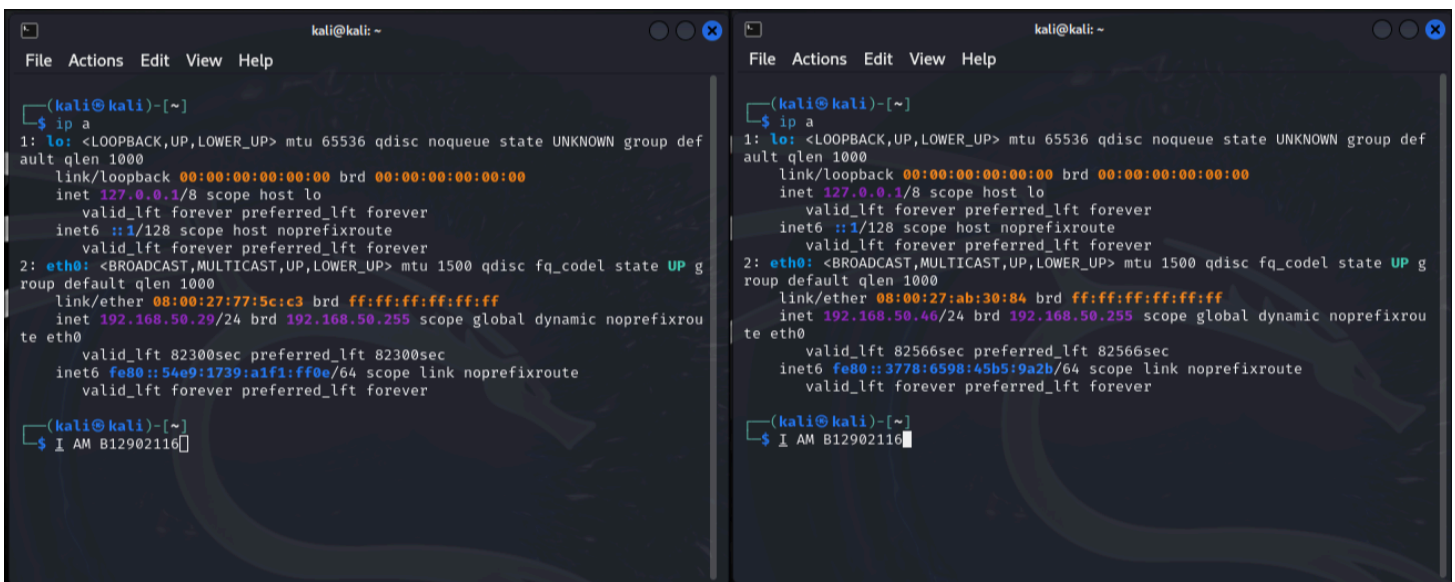
4. Please leverage a hacker tool in kali VM and write down the progress you do. There are many attack type you can choose on below: (20%)

- *Information Gathering*
- *Wireless Attack*
- *Vulnerability Analysis*
- *Password Attack*
- *Exploitation Tools*

Experiment settings:

2 VMs with bridged network adapters, VM1 runs a service on port 12345.

IP addresses of the two VMs:

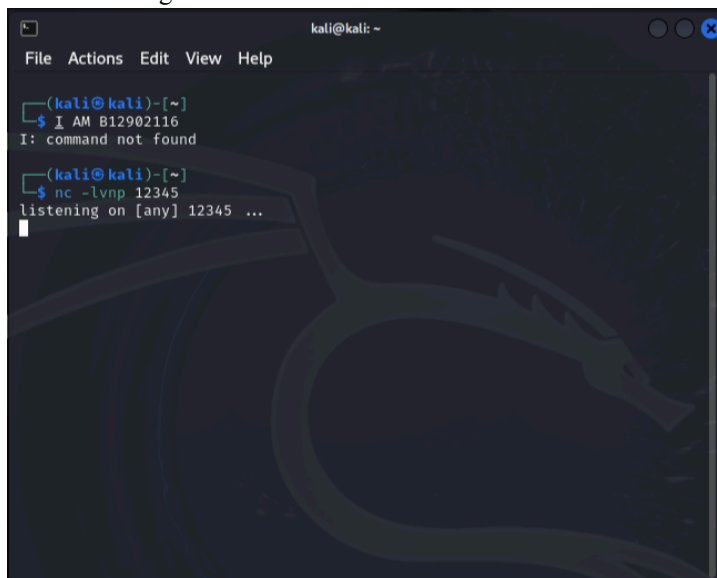


The image shows two terminal windows side-by-side, both titled 'kali@kali: ~'. The left window (VM1) shows the output of the 'ip a' command, highlighting the 'lo' interface with IP 127.0.0.1 and the 'eth0' interface with IP 192.168.50.29. The right window (VM2) shows the output of the 'ip a' command, highlighting the 'lo' interface with IP 127.0.0.1 and the 'eth0' interface with IP 192.168.50.46. Both windows also show the MAC address for 'eth0' as 08:00:27:77:5c:c3 for VM1 and 08:00:27:ab:30:84 for VM2.

VM1: 192.168.50.29

VM2: 192.168.50.46

Service running on VM1:

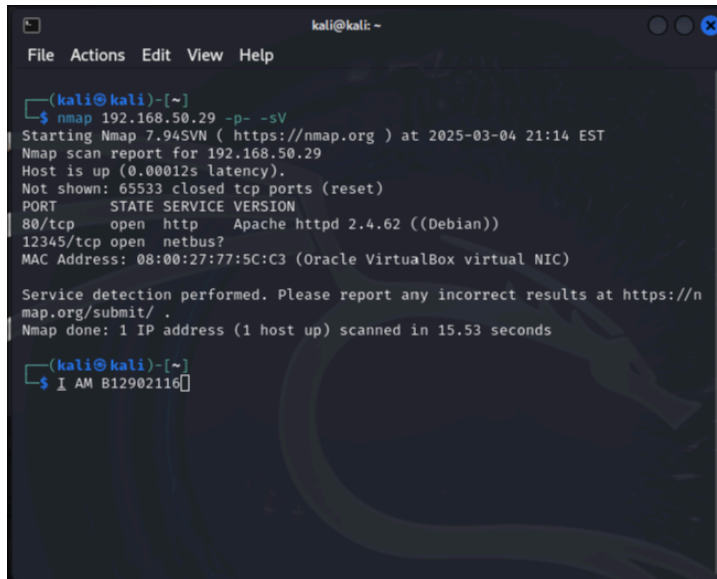


The image shows a terminal window titled 'kali@kali: ~'. It displays the output of the 'nc -lvnp 12345' command, which is 'listening on [any] 12345 ...'. The prompt is ready for an incoming connection.

Procedure:

We use nmap to do a full port scan to look for open ports / services.

Results:



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap 192.168.50.29 -p- -sV  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-04 21:14 EST  
Nmap scan report for 192.168.50.29  
Host is up (0.00012s latency).  
Not shown: 65533 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
80/tcp    open  http    Apache httpd 2.4.62 ((Debian))  
12345/tcp  open  netbus?  
MAC Address: 08:00:27:77:5C:C3 (Oracle VirtualBox virtual NIC)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 15.53 seconds  
  
(kali@kali)-[~]  
$ I AM B12902116
```

We see that port 80 is open, and is running an apache http server, we also find the hidden service running on port 12345.