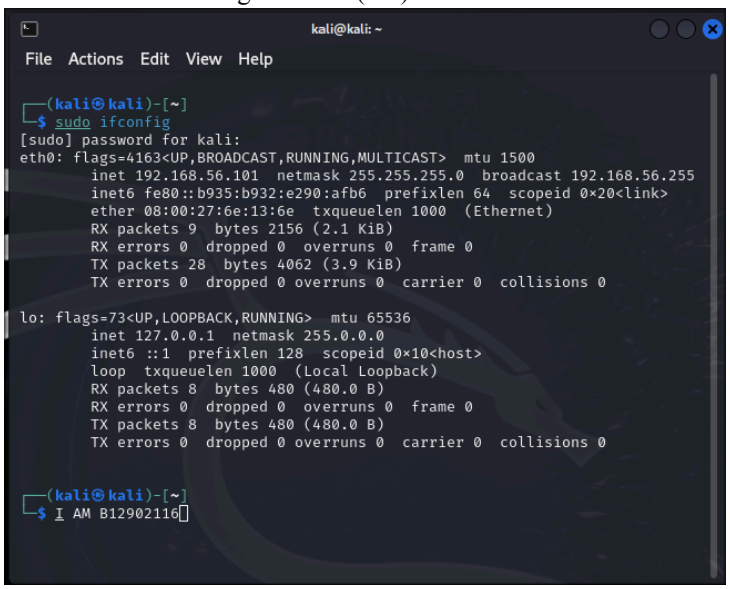
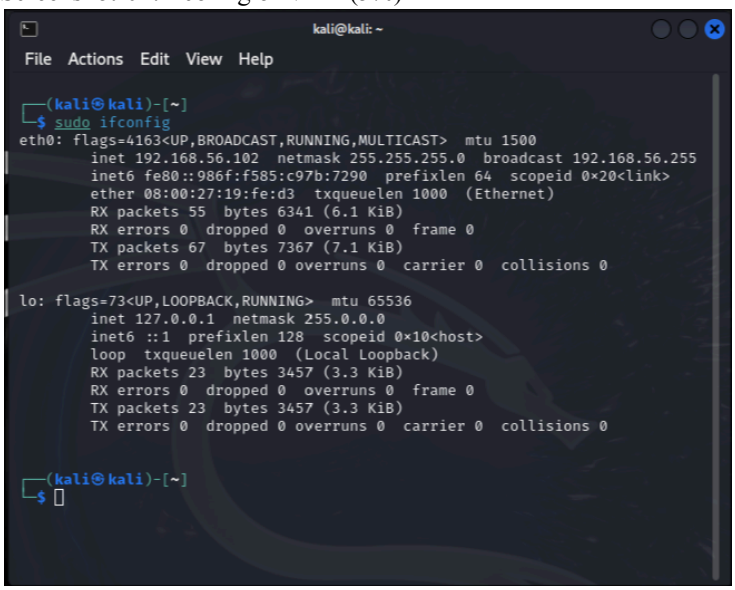
Lab02 Report

1. Name: 林靖昀　Student ID: B12902116

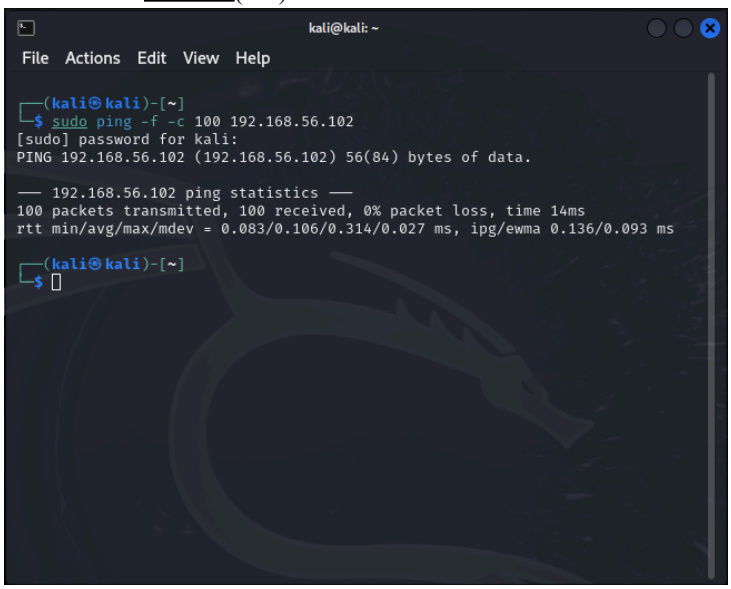
2. Proof of your lab work (clearly label each screenshot)
   a. Screenshot-01: ifconfig of VM1 (5%)



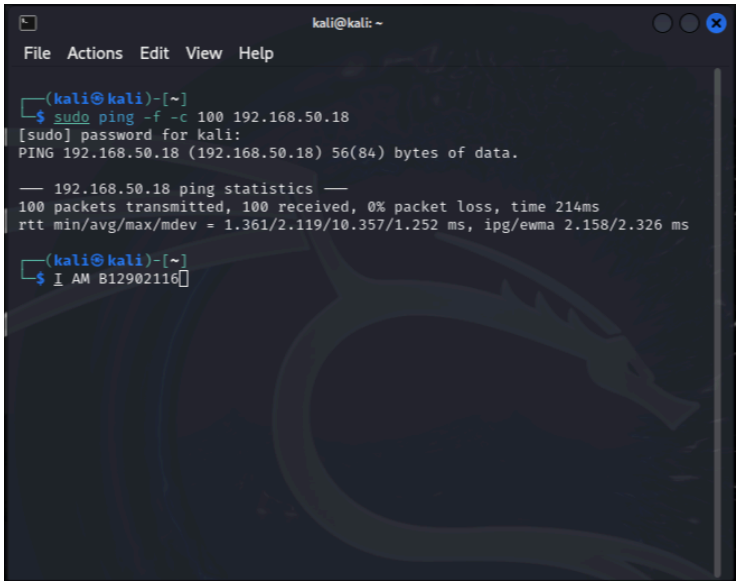
   b. Screenshot-02: ifconfig of VM2 (5%)



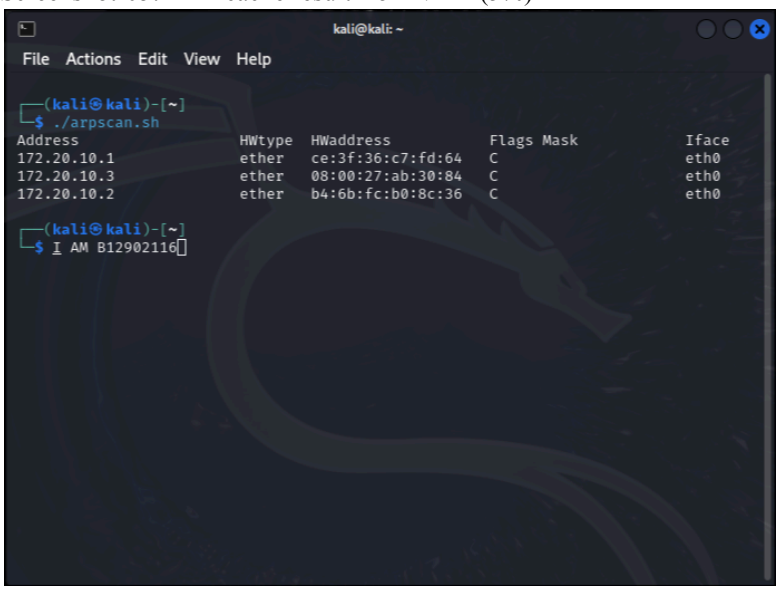
c. Screenshot-03: ping session (VM1 to VM2) of communications on the same host
Note: RTT = 0.106ms(5%)



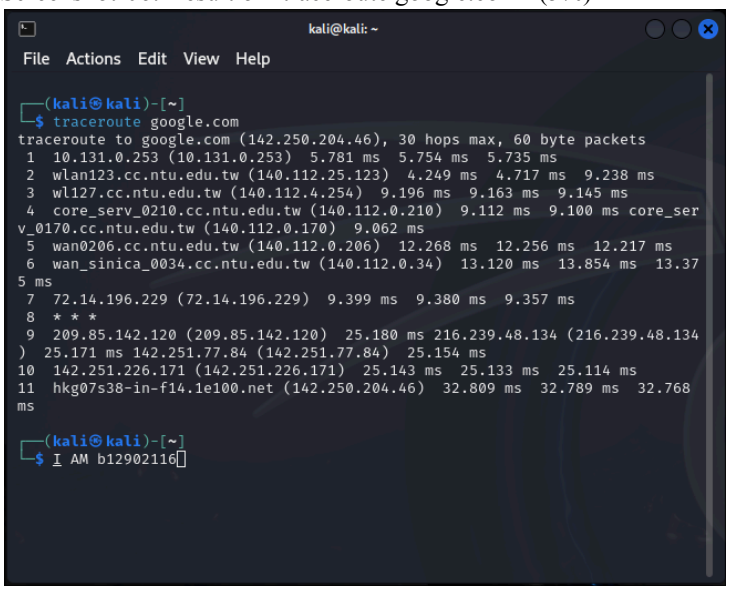
d. Screenshot-04: ping session (VM1 to VM2) of communication between bridged hosts
Note: RTT = 2.119ms (5%)



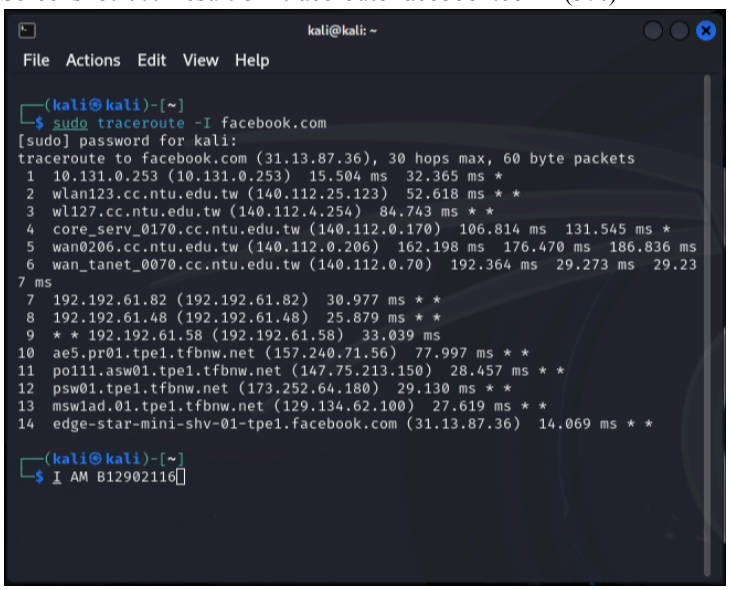
e. Screenshot-05: ARP cache result from VM1 (5%)



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



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

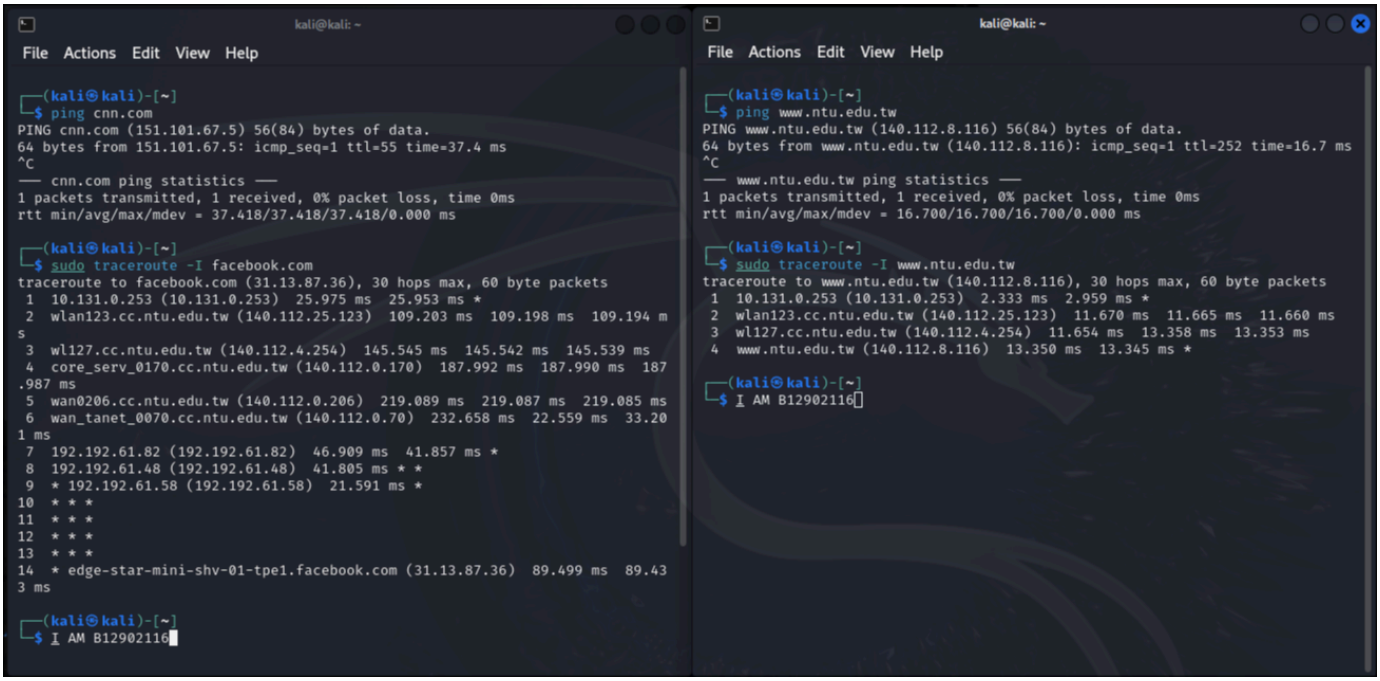


h. Screenshot-08: Result of “traceroute cnn.com” (5%)

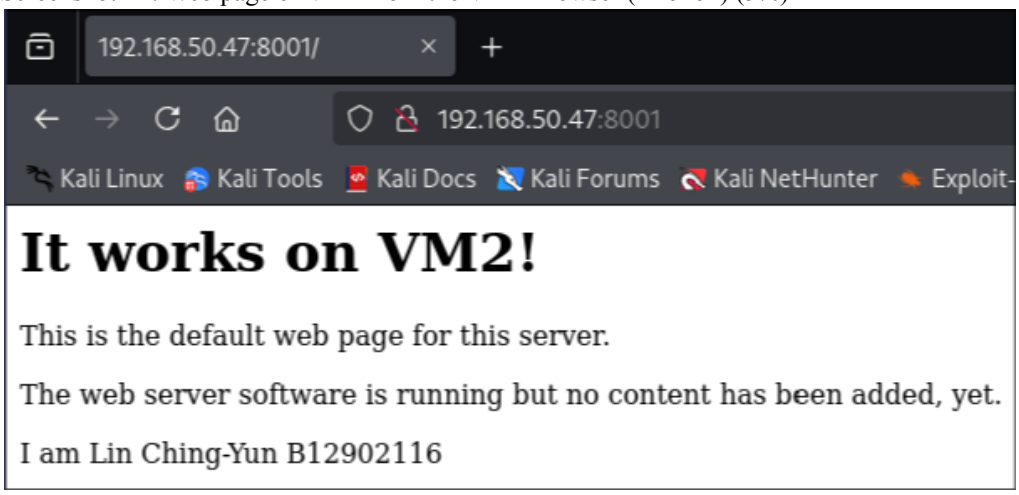
```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(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%)

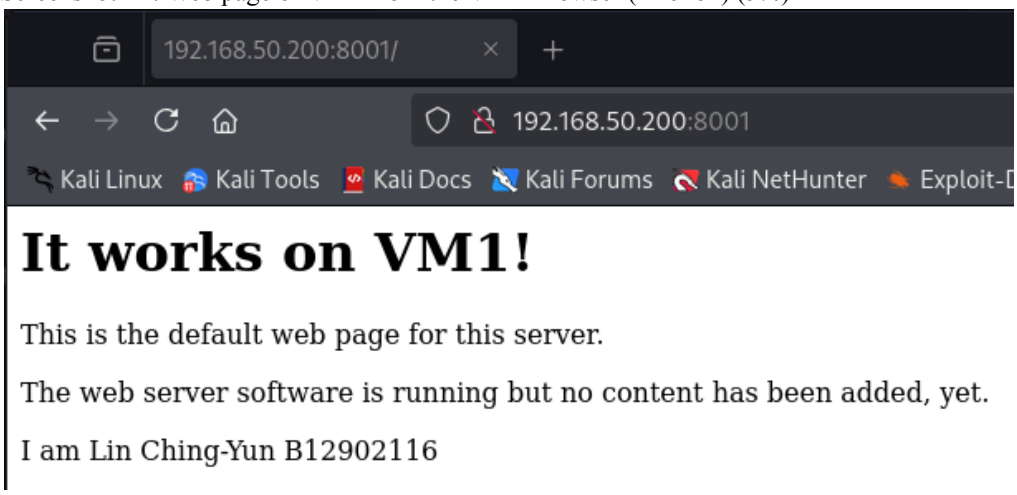
j. Screenshot-10: A full path from your VM to *cnn.com* or www.ntu.edu.tw (5%)



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 .

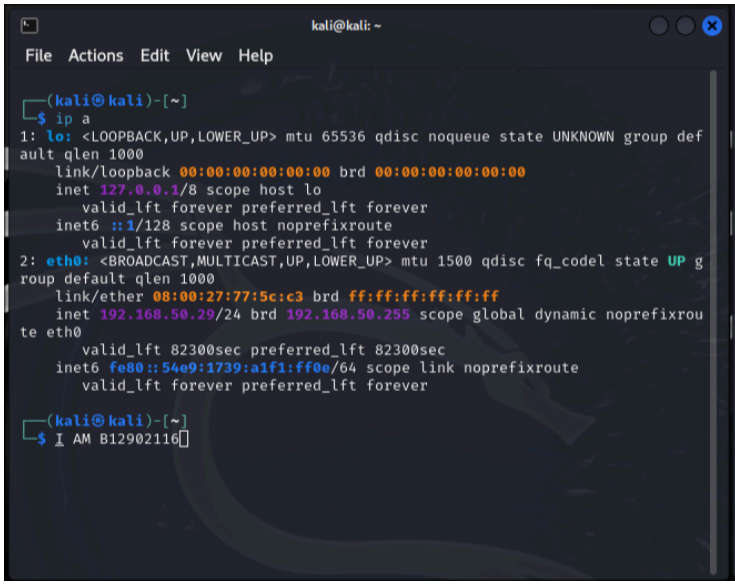
Question: In Task7 Step2, can you successfully find a path to *cnn.com* or *www.ntu.edu.tw* with traceroute? If not, why? Explain the root cause and your observation in detail. Also provide a method to solve this problem. (10%)
Answer: By default, traceroute sends UDP probes, which might be blocked by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

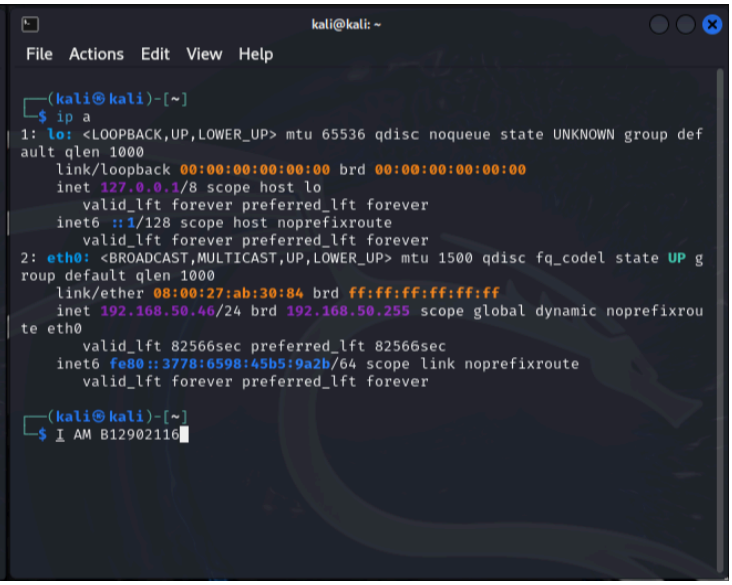
4. Please leverage a hacker tool in kali VM and write down the progress you do. There are many attack type you can choose on below: (20%)
    - *Information Gathering*
    - *Wireless Attack*
    - *Vulnerability Analysis*
    - *Password Attack*
    - *Exploitation Tools*

    Experiment settings:

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

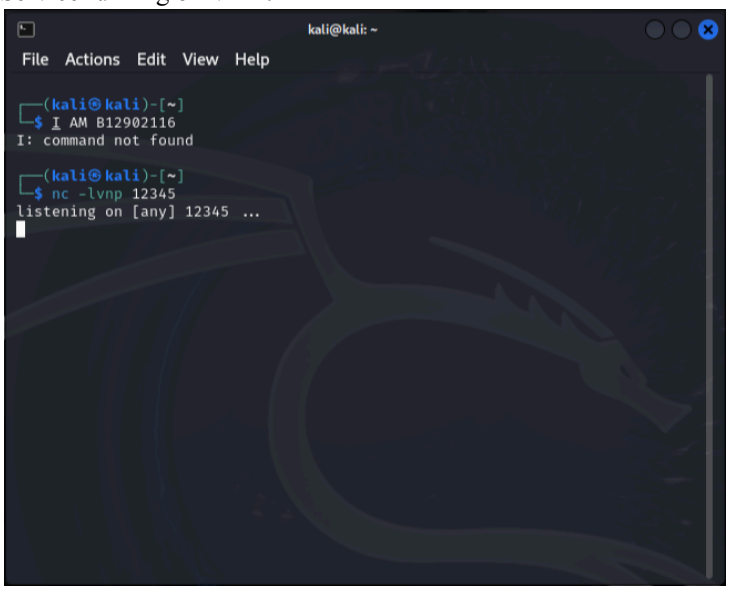
    IP addresses of the two VMs:





VM1: 192.168.50.29 VM2: 192.168.50.46

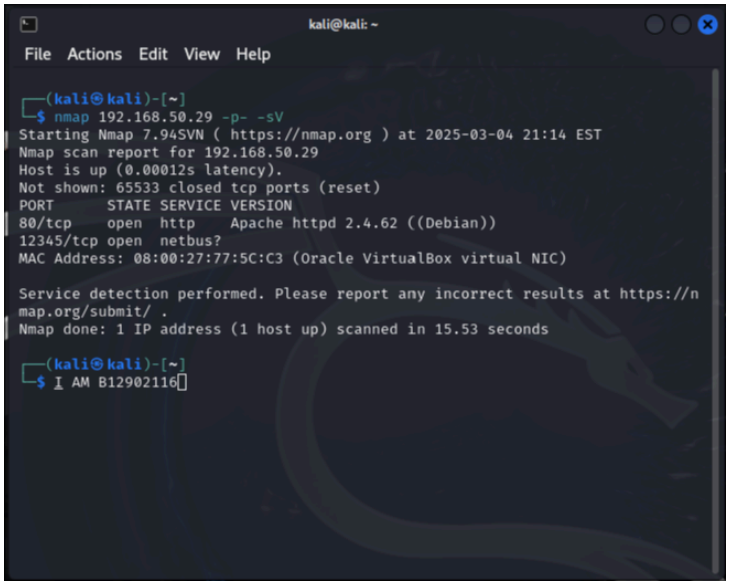
Service running on VM1:



Procedure:

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

Results:



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