Lab1 Report

B07902066 黃禹喆 B07902062 張彧瑋 B07902068 陳柏豪 B07902080 黃義峰

1. Environment:
   Language: C
   Operating system: Ubuntu 18.04
   VM platform: Virtual box

2. How to detect and defend traceroute?
   Detect:

   Since ttl of traceroute packets increase from 0 , the values are always small compared to normal packets, which have bigger values of max_ttl. For example, default max_ttl in linux is 64. If a packet's ttl is small, there is a high probability that it's a traceroute packet.

   Defend:

   Configure the firewall to block all ICMP echoes, or do not reply to ICMP packets. For UDP, reject UDP packets that are received by ports that are unlikely to be used, especially ports in range 33434~33523, which are the default ports used in linux traceroute. For well-known ports, drop the packets if you are not likely to be targeted, for example, drop all packets to port 53 if the device is not a DNS server.

3. Why traceroute cannot show the full route?

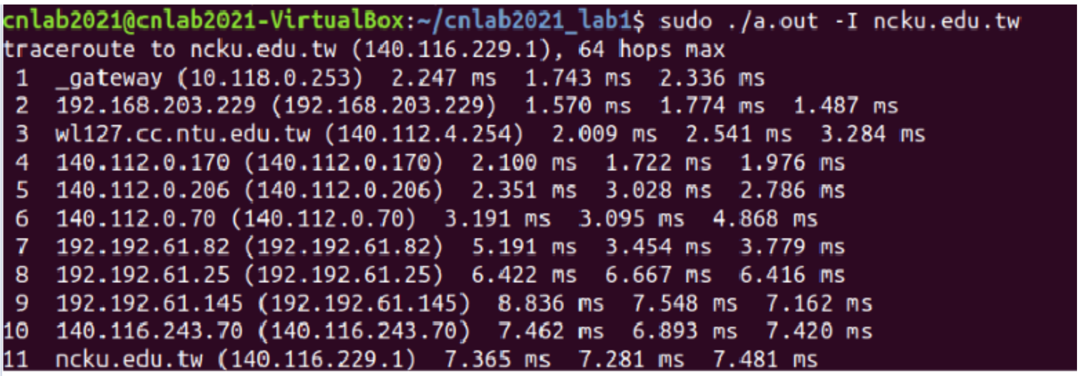
   Some devices disable normal TTL decrementing. For example, some LSPs push a label on the packets when it enters, and only decrements the TTL value twice: upon entering and leaving, using the MPLS method. This is done in order to hide the network topology.

   In addition, ICMP and UDP packets are frequently used for attack, such as DDOS attack using icmp flood or udp flood. Therefore, some routers may reject these two kinds of packets. When the network is busy, routers may also discard packets of traceroute.

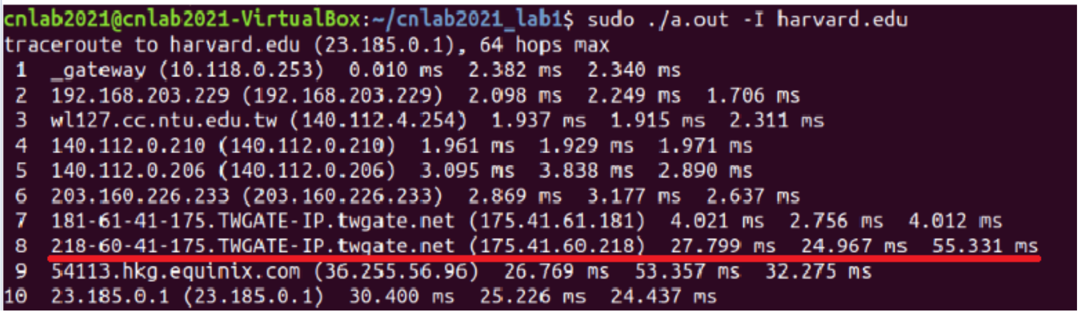
4. Why the result may not always be the same?

   Network is multipath mode. There are mutual paths between source and destination, and network operators reduce the burden on the network by loadblance. Router's forwarding table keeps on changing through network status. In spite of receiving the same packet, one router may choose a different path to forward since the table has changed. That's the reason why the result may not always be the same.

5. Compare the results between local and foreign, and explain what causes the difference?



```
cnlab2021@cnlab2021-VirtualBox:~/cnlab2021_lab1$ sudo ./a.out -I ncku.edu.tw
traceroute to ncku.edu.tw (140.116.229.1), 64 hops max
 1  _gateway (10.118.0.253)  2.247 ms  1.743 ms  2.336 ms
 2  192.168.203.229 (192.168.203.229)  1.570 ms  1.774 ms  1.487 ms
 3  wl127.cc.ntu.edu.tw (140.112.4.254)  2.009 ms  2.541 ms  3.284 ms
 4  140.112.0.170 (140.112.0.170)  2.100 ms  1.722 ms  1.976 ms
 5  140.112.0.206 (140.112.0.206)  2.351 ms  3.028 ms  2.786 ms
 6  140.112.0.70 (140.112.0.70)  3.191 ms  3.095 ms  4.868 ms
 7  192.192.61.82 (192.192.61.82)  5.191 ms  3.454 ms  3.779 ms
 8  192.192.61.25 (192.192.61.25)  6.422 ms  6.667 ms  6.416 ms
 9  192.192.61.145 (192.192.61.145)  8.836 ms  7.548 ms  7.162 ms
10  140.116.243.70 (140.116.243.70)  7.462 ms  6.893 ms  7.420 ms
11  ncku.edu.tw (140.116.229.1)  7.365 ms  7.281 ms  7.481 ms
```



```
cnlab2021@cnlab2021-VirtualBox:~/cnlab2021_lab1$ sudo ./a.out -I harvard.edu
traceroute to harvard.edu (23.185.0.1), 64 hops max
 1  _gateway (10.118.0.253)  0.010 ms  2.382 ms  2.340 ms
 2  192.168.203.229 (192.168.203.229)  2.098 ms  2.249 ms  1.706 ms
 3  wl127.cc.ntu.edu.tw (140.112.4.254)  1.937 ms  1.915 ms  2.311 ms
 4  140.112.0.210 (140.112.0.210)  1.961 ms  1.929 ms  1.971 ms
 5  140.112.0.206 (140.112.0.206)  3.095 ms  3.838 ms  2.890 ms
 6  203.160.226.233 (203.160.226.233)  2.869 ms  3.177 ms  2.637 ms
 7  181-61-41-175.TWGATE-IP.twgate.net (175.41.61.181)  4.021 ms  2.756 ms  4.012 ms
 8  218-60-41-175.TWGATE-IP.twgate.net (175.41.60.218)  27.799 ms  24.967 ms  55.331 ms
 9  54113.hkg.equinix.com (36.255.56.96)  26.769 ms  53.357 ms  32.275 ms
10  23.185.0.1 (23.185.0.1)  30.400 ms  25.226 ms  24.437 ms
```

There are multiple possible reasons for the situation:

1. There are few routers that are capable of forwarding oversea packets. Therefore, a huge amount of packets accumulate at the router, so the router may be busy processing other packets, or set the icmp packets to a lower priority.
2. Oversea hops result in larger distance and latency due to long physical transmission.

6. Explain the difference by using TCP, UDP, and ICMP.
   a. For sending packets, ICMP, UDP and TCP traceroute methods send ICMP, UDP, TCP packets respectively.
   b. If the TTL of the packet sent reaches 0 but it doesn't arrive at the destination IP address, all the three methods will receive ICMP packets with type 11, which means "ICMP time exceeded", from the intermediate router/host.
   c. For termination, ICMP traceroute waits for an ICMP packet with type 0 from the destination IP address, which refers to "echo reply". UDP traceroute waits for type 3 instead, which means "destination unreachable", as UDP traceroute is done by setting the destination port to an unlikely port number, which is usually between the range 33434~33525. TCP traceroute, on the other hand, will only terminate after the source receives a SYN+ACK packet from the destination.
   d. To check the sequence of received ICMP packets, the ICMP method checks the sequence number and identity by reading the ICMP header of the original data within the packet. For the UDP method, however, since the sequence isn't reliable, we need to check the destination port contained in the UDP header within the received ICMP data.The

destination port number identifies the sequence number of the packet, since we increment the destination port number along with the number of probes. For TCP, since the transfer sequence is reliable, we only need to make sure that the final SYN+ACK is from our target destination.

e. Since UDP and ICMP packets are more likely to be blocked by firewalls, using TCP traceroute can help break through securities to retrieve information, as it camouflages as a normal connection request.

References:

DNSLookup: https://www.binarytides.com/hostname-to-ip-address-c-sockets-linux/
Checksum: https://jyhshin.pixnet.net/blog/post/31173960
Receive all ip packets:
https://www.opensourceforu.com/2015/03/a-guide-to-using-raw-sockets/?fbclid=IwAR0OCx8fegc72LUaaJWLgS3ef9wYPF3CWAM4WO-0ljs_brlqGDdnsuOgb3k
Send TCP syn packet: https://www.programmersought.com/article/17703477628/
UDP traceroute:
https://blog.csdn.net/C3080844491/article/details/77817028?fbclid=IwAR0Dv8fDxqCReHVhNbukc5r2onsTEgx_D2Qxt2jfxG5IzTRwp0r31h2BCF0
Send & receive ICMP packet using raw socket:
http://chriswenyuan.blogspot.com/2017/05/c-sockraw-ping.html
Set ttl:
https://stackoverflow.com/questions/31066061/setting-ttl-on-outgoing-udp-packets?fbclid=IwAR3yAztguS8Gzc5x7YSigNKtkrejyHnfo_zpYU0OjkaM7whcV0UEGwGgMLM