Team 8

B07902002 連崇安 B07902034 王昱凱 B07902126 謝宗儒

---Environment :

We use Mac OS as the testing environment.

---How to detect and defend traceroute :

Since attacker needs to send traceroute to investigate the topology around the targeted region before attack starts and disconnect the target area, we can detect it by finding rapid increase of traceroute or analyzing hop count to the destination (The destination of attacker’s traceroutes are concentrated within several hops while legitimate user’s ones are distributed normally).
Also, we can defend traceroute by disabling the ICMP functionality of the targeted router, computer or other device(disable its ability to send and receive any requests using the ICMP) from administrative interface(ex. Using firewall) to make the device unresponsive to traceroute requests.

---Why traceroute can’t show the full route :

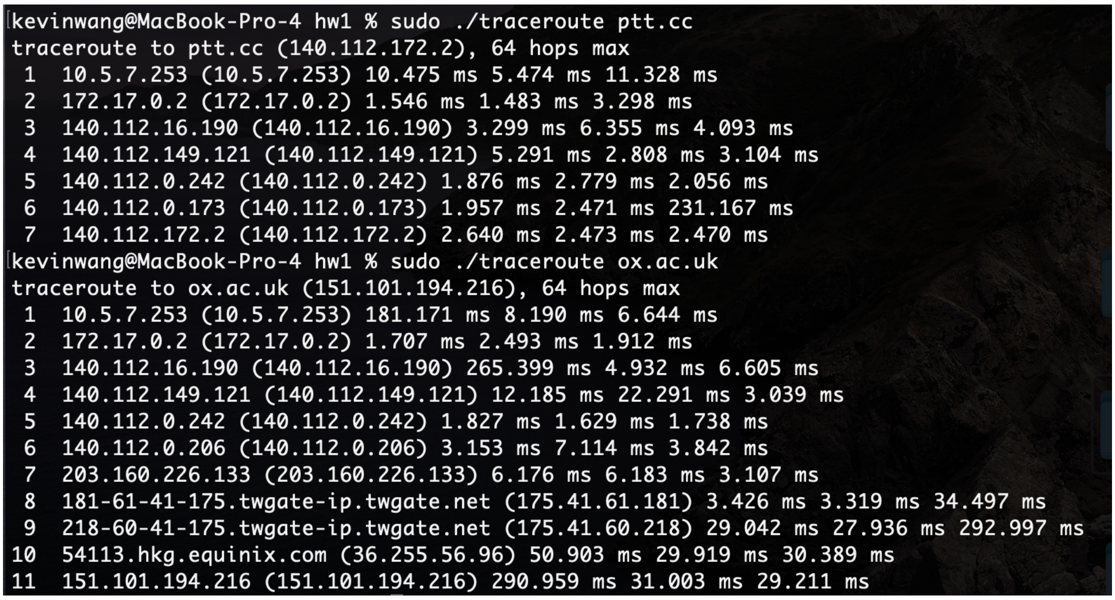
Traceroute can’t show the full route because the router has a firewall that is blocking the ICMP TTL exceeded messages that the intermediate hops generate, but the ICMP message for the echo reply for the last hop is not blocked. It is a (off-topic because it is consumer-grade equipment) router/firewall configuration problem.

---Why the result may not always be the same：

Some domains may use DNS load balancing to redirect requests to one server of a group of server machines to distribute loading. Therefore we may get different results even when we're executing the very same request.

---Compare the results between local and foreign：

It takes longer to get a traceroute result when the destination IP address is located in foreign country compared to domestic IP addresses. Initially, they go through similar paths (routers), however, in order to access to foreign IP, the packet needs to arrive at a domestic gateway. In the following image, we can observe that the domestic gateway of Taiwan is twgate.net, which is established by Chunghwa Telecom. By this gateway, the packet is able to reach foreign IP, since the path is quite long, it needs more time to respond.



```
kevinwang@MacBook-Pro-4 hw1 % sudo ./traceroute ptt.cc
traceroute to ptt.cc (140.112.172.2), 64 hops max
 1  10.5.7.253 (10.5.7.253) 10.475 ms 5.474 ms 11.328 ms
 2  172.17.0.2 (172.17.0.2) 1.546 ms 1.483 ms 3.298 ms
 3  140.112.16.190 (140.112.16.190) 3.299 ms 6.355 ms 4.093 ms
 4  140.112.149.121 (140.112.149.121) 5.291 ms 2.808 ms 3.104 ms
 5  140.112.0.242 (140.112.0.242) 1.876 ms 2.779 ms 2.056 ms
 6  140.112.0.173 (140.112.0.173) 1.957 ms 2.471 ms 231.167 ms
 7  140.112.172.2 (140.112.172.2) 2.640 ms 2.473 ms 2.470 ms
kevinwang@MacBook-Pro-4 hw1 % sudo ./traceroute ox.ac.uk
traceroute to ox.ac.uk (151.101.194.216), 64 hops max
 1  10.5.7.253 (10.5.7.253) 181.171 ms 8.190 ms 6.644 ms
 2  172.17.0.2 (172.17.0.2) 1.707 ms 2.493 ms 1.912 ms
 3  140.112.16.190 (140.112.16.190) 265.399 ms 4.932 ms 6.605 ms
 4  140.112.149.121 (140.112.149.121) 12.185 ms 22.291 ms 3.039 ms
 5  140.112.0.242 (140.112.0.242) 1.827 ms 1.629 ms 1.738 ms
 6  140.112.0.206 (140.112.0.206) 3.153 ms 7.114 ms 3.842 ms
 7  203.160.226.133 (203.160.226.133) 6.176 ms 6.183 ms 3.107 ms
 8  181-61-41-175.twgate-ip.twgate.net (175.41.61.181) 3.426 ms 3.319 ms 34.497 ms
 9  218-60-41-175.twgate-ip.twgate.net (175.41.60.218) 29.042 ms 27.936 ms 292.997 ms
10  54113.hkg.equinix.com (36.255.56.96) 50.903 ms 29.919 ms 30.389 ms
11  151.101.194.216 (151.101.194.216) 290.959 ms 31.003 ms 29.211 ms
```

---Explain the difference by using TCP, UDP, and ICMP：

- ICMP: ICMP traceroute sends raw ICMP echo requests, while receives ICMP echo reply when the packet reaches the destination.
- UDP: UDP traceroute sends UDP packets, while receives ICMP destination unreachable when the packet reaches the destination.
- TCP: TCP traceroute sends TCP SYN packets, therefore it has a greater chance to bypass firewall.

Reference :
https://ieeexplore.ieee.org/abstract/document/8304023
https://www.cloudflare.com/zh-tw/learning/ddos/ping-icmp-flood-ddos-attack/
https://networkengineering.stackexchange.com/questions/16530/traceroute-doesnt-print-entire-route-sometimes
https://zhuanlan.zhihu.com/p/101810847
https://stackoverflow.com/questions/58273223/traceroute-returning-different-results-on-the-same-network