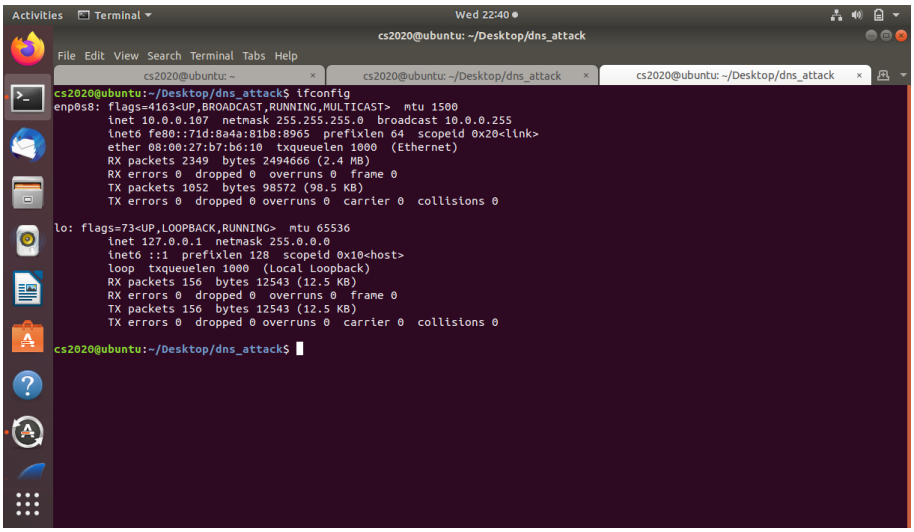
Project 1: DNS Reflection and Amplification Attacks

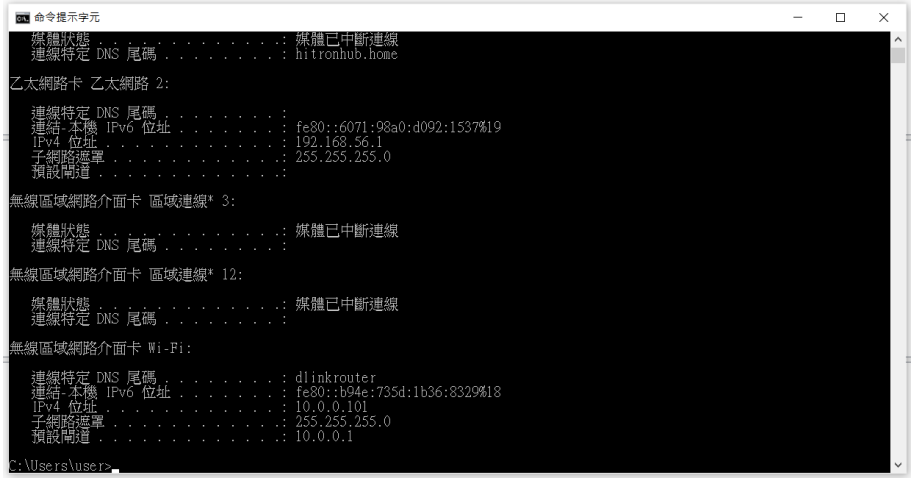
Student ID: 0716085

Part1: DNS Reflection and Amplification Attacks

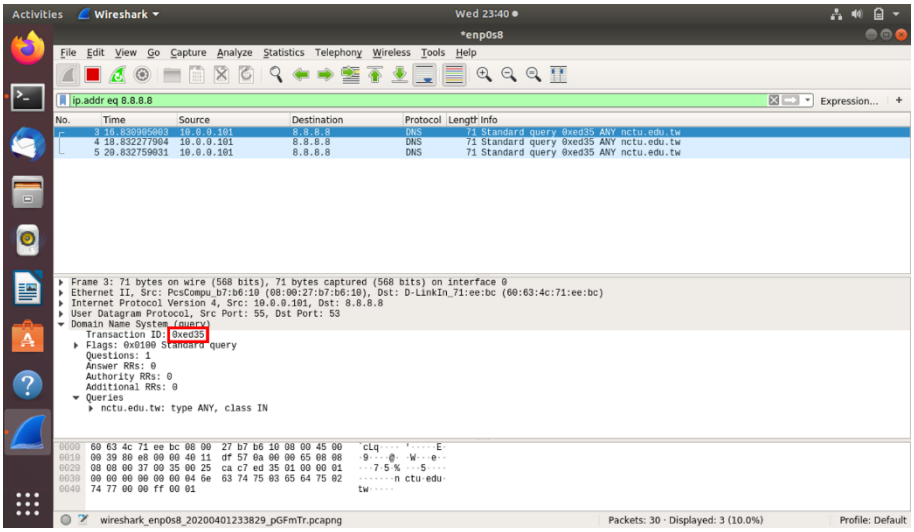
Task I: DNS reflection attack:



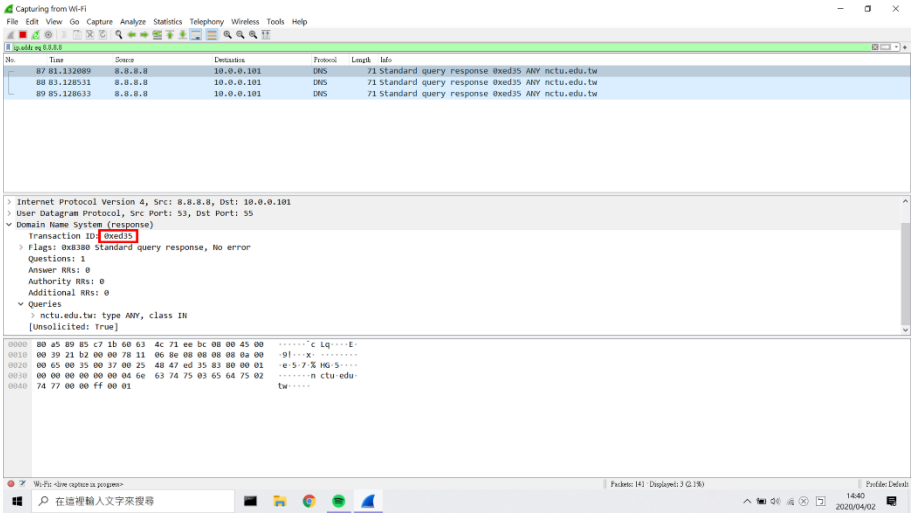
(1) Attacker machine, ip addr = 10.0.0.107



(2) Victim machine, ip addr = 10.0.0.101



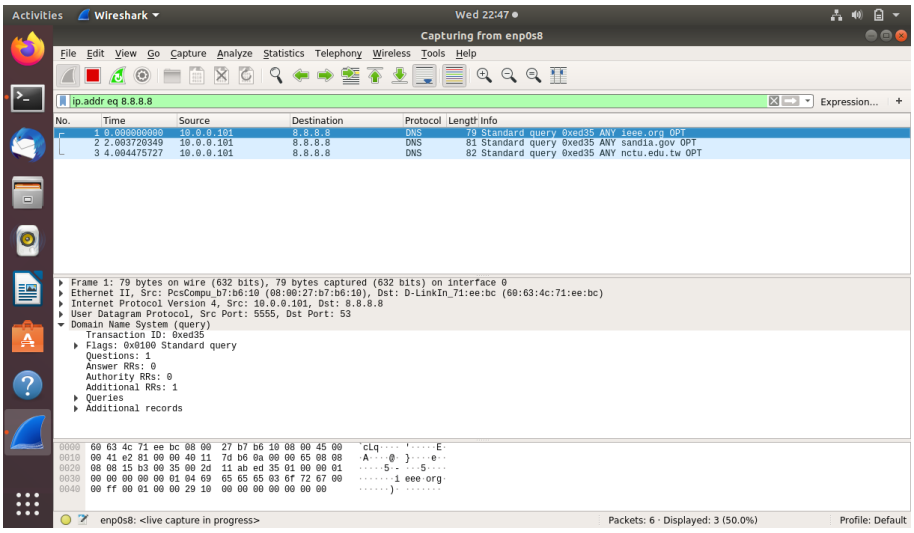
(3-1) Capture packet at attacker machine



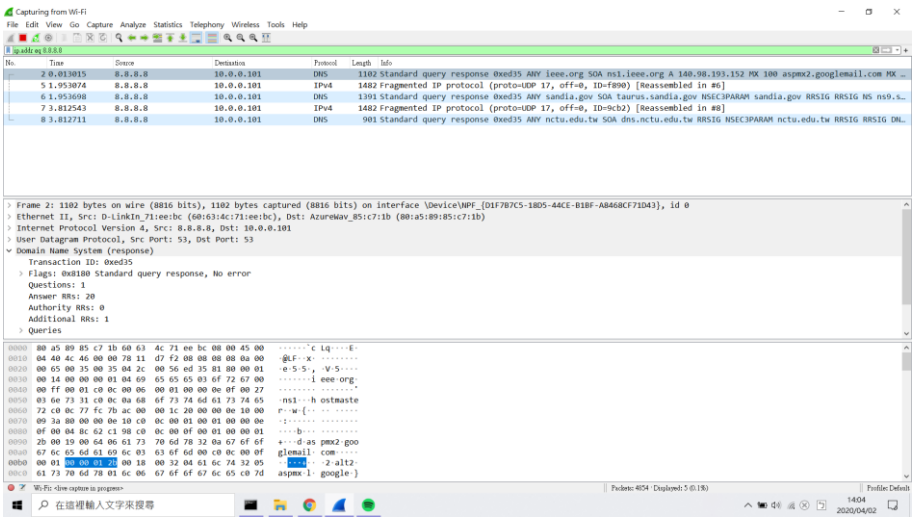
(3-2) Capture packet at victim machine

By picture (3-1) and (3-2), it can show that DNS reflection attack is success.

Task II: DNS amplification attack:



(4-1) DNS request sent by attacker machine

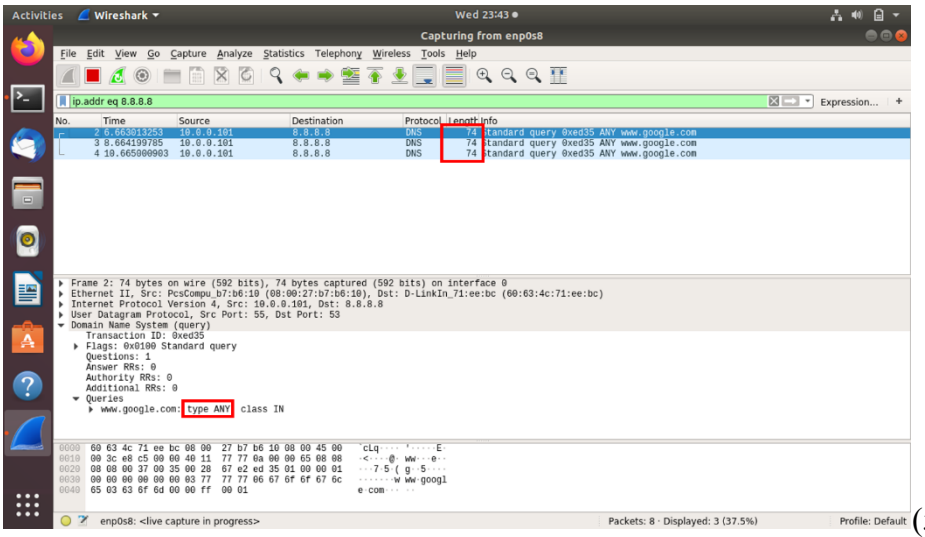


(4-2) DNS response received by victim machine

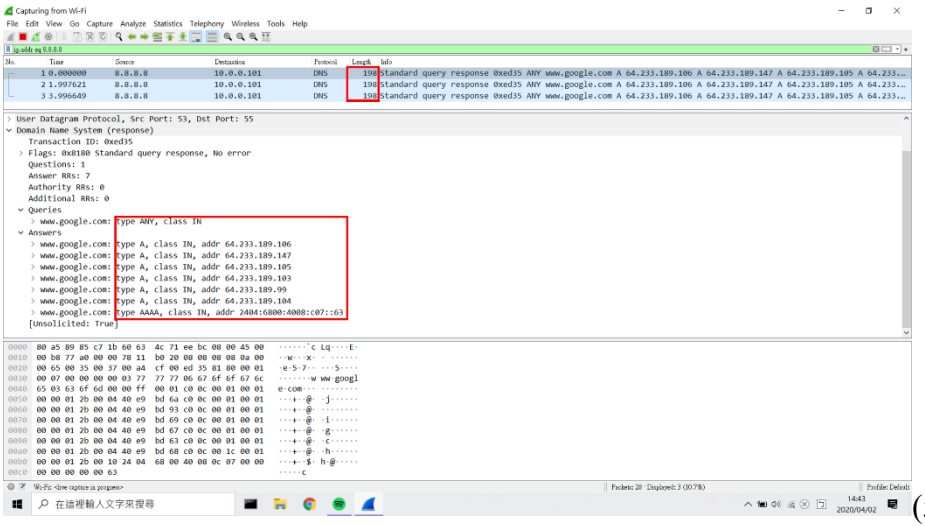
By picture (4-1) and (4-2), it can show that DNS amplification attack is success.

Part 2: Way to amplify the DNS response

In DNS query, different query type will return different response. There is a query type called ANY, which will return all records of all types known. By using this type, response packet may be larger than request packet.



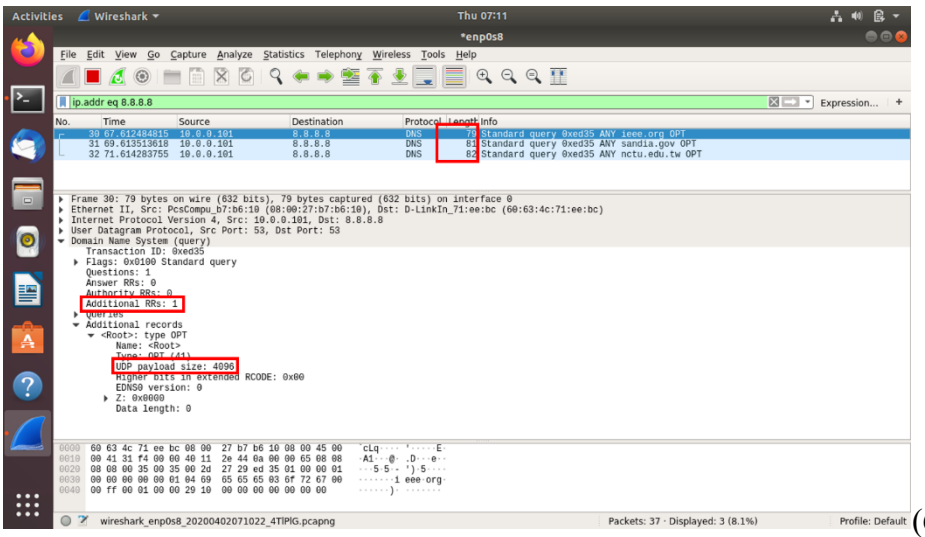
(5-1)



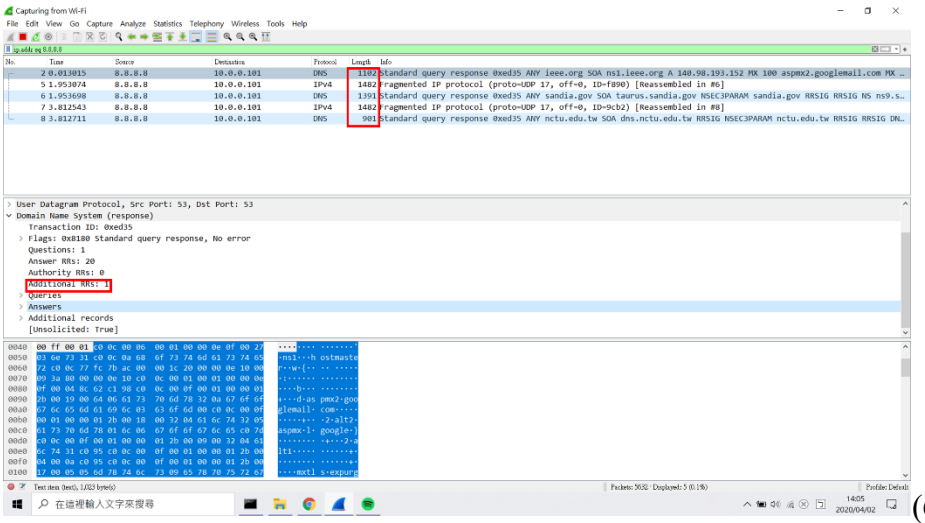
(5-2)

Picture (5-1) and (5-2) are the example of using type ANY and query name is "www.google.com". It shows that amplification ratio is 198/74 = 2.0.

Although the above method can amplify the response packet, the amplification ratio is quite small. To make the response packet much larger, we can use the additional section in DNS structure to increase the upper limit of UDP payload size.



(6-1)



(6-2)

Picture (6-1) and (6-2) are the example of using additional section and using 3 different query name “ieee.org”, “sandia.gov”, “nctu.edu.tw”. Their amplification ratio is 1102/79 = 13.9, 1391/81 = 17.2, 901/82 = 11.0 (only calculate DNS protocol). It is clearly that the second method’s response packet is larger than the first method. By the way, I don’t use the “www.google.com” as query name in second method is because the amplification ratio has only 2.5, it can’t see a big different between two methods.

Part 3: Solution to defend against DoS attack based on the DNS reflection

We can’t completely defend the DNS reflection attack because of the importance of the DNS service. However, we can try to mitigate this kind of attack. One of the methods is disable the recursive query or setting access control list (ACL) to allow the trusted ip address on the list can use recursive query. Another way is once the server detected the DNS reflection attacks, the server can block these specific DNS servers that are used by the attacker.