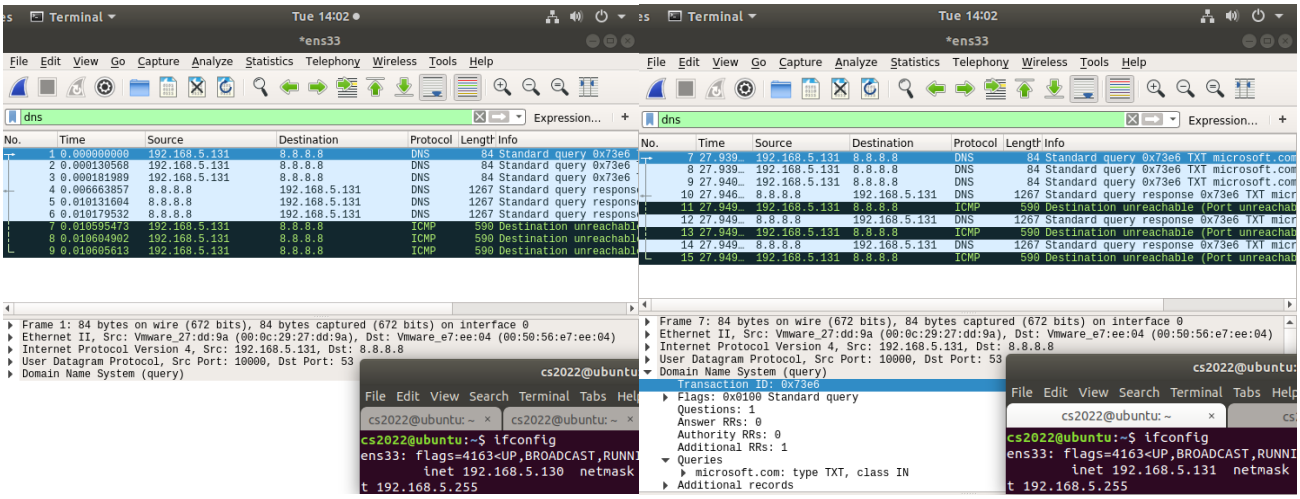
Computer Security Capstone Project 1 Report - 0816102 陳品戎

Item 1:

(Left: attacker 192.168.5.130, Right: victim 192.168.5.131)

command: ./dns_attack 192.168.5.131 10000 8.8.8.8



Packet sent from 192.168.5.130 had spoofing IP 192.168.5.131. The size of DNS query packet is 84 bytes, and the size of response is 1267 bytes.

Amplification ratio: 15

Item 2:

I referred to the query packet of the Linux's 'dig' command, and found that turning 'additional records' into 1 can let the responding packet carry extra data and that TXT type query can often trigger the longest response including multiple TXT records. I entered the command many times with some well-known domain name, looking for the longest response. Finally, 'microsoft.com' responded the most TXT records of the domain names I tried with, giving the amplification ration over 10.

Item 3:

DNS servers should detect quickly whether there are strange packets flow which can possibly be the reflection attack, and limit the rate of packet source or just block the source IP if necessary. There can be a mechanism between victim and DNS server. If a victim is under attack, it can tell DNS server. DNS server will stop sending respond and deny the query from the source for a while.