Computer Security Project 1

0816146 Yung-Hsiang Wei

(1) The evidence that I have finished the Tasks

The DNS payload is 48 bytes in the UDP payload. The DNS response is 4096 bytes.
(Length 90 bytes = DNS 48 bytes + UDP header 8 bytes + IP header 20 bytes + Ethernet header 14 bytes)

The amplification ratio is 85 times.

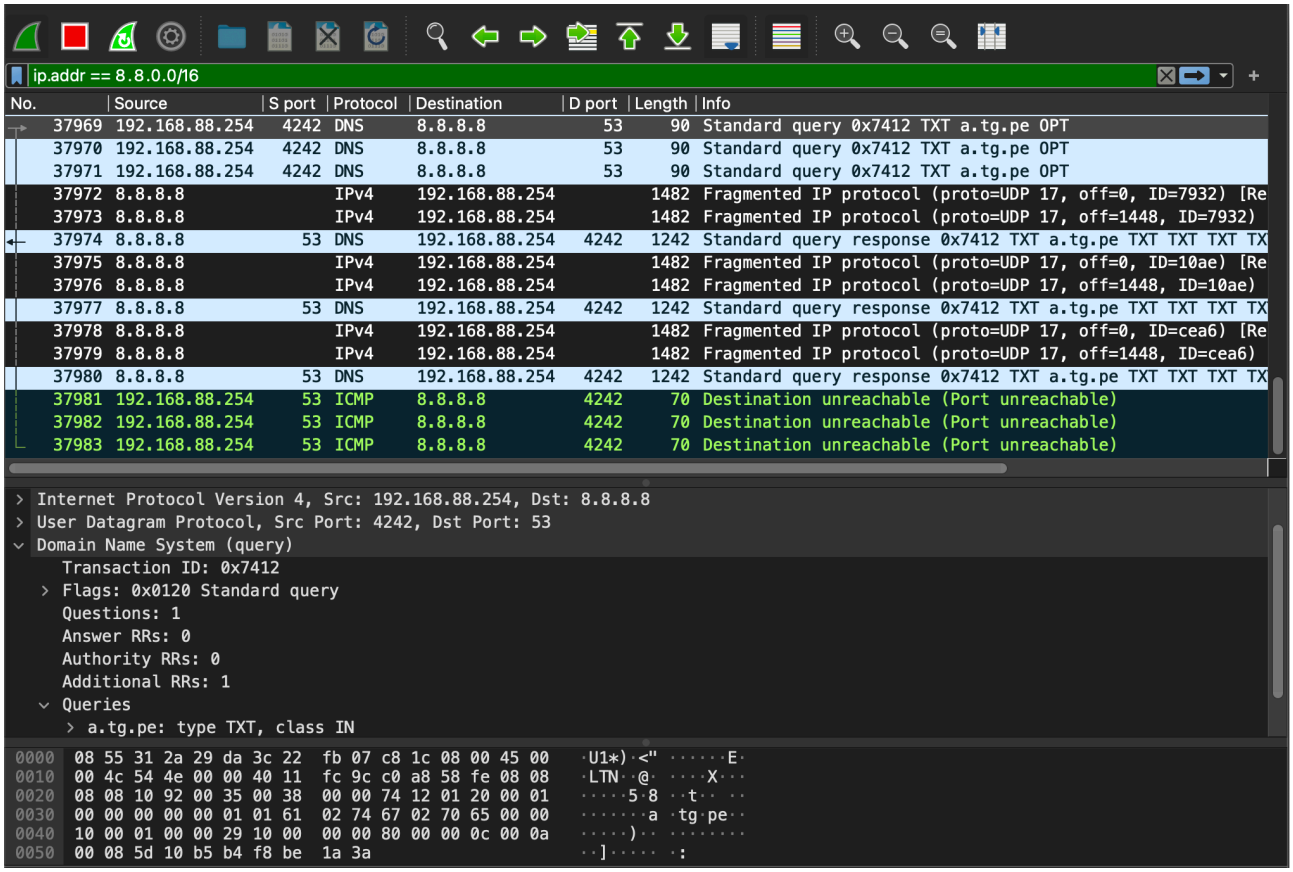

Fig 1. WireShark Screenshot

(2) How I amplify the DNS response

The maximum size for Google DNS in UDP is 4096 bytes (larger answers will be switched to TCP), so I crafted a domain (a.tg.pe) that the response is exactly 4096 bytes.

My method to craft a large response is to add many TXT records into one domain name.

(3) Solution to defend

Coordinate with ISPs/IXPs, drop spoofed IP packets from the sources.
When being attacked from a single source, ask ISP to filter traffic from certain IP address ranges.
Contact the reflect point that the attacker leverages, ask them to block my IP addresses.