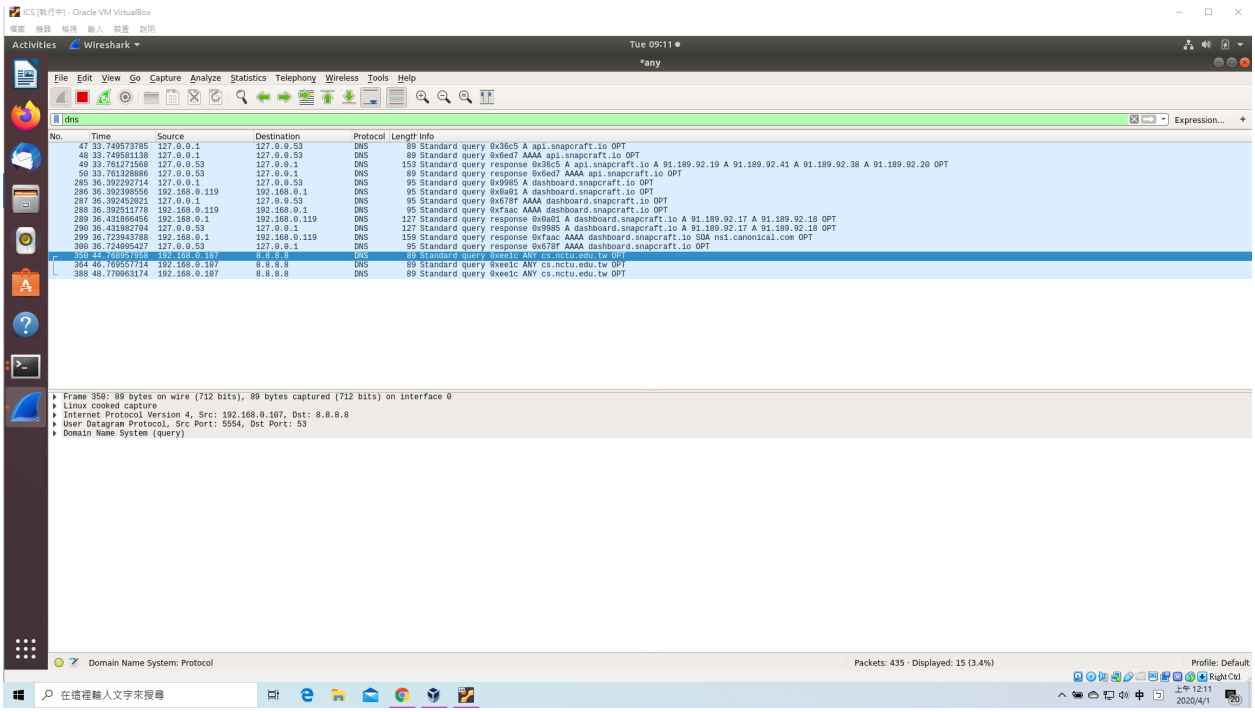

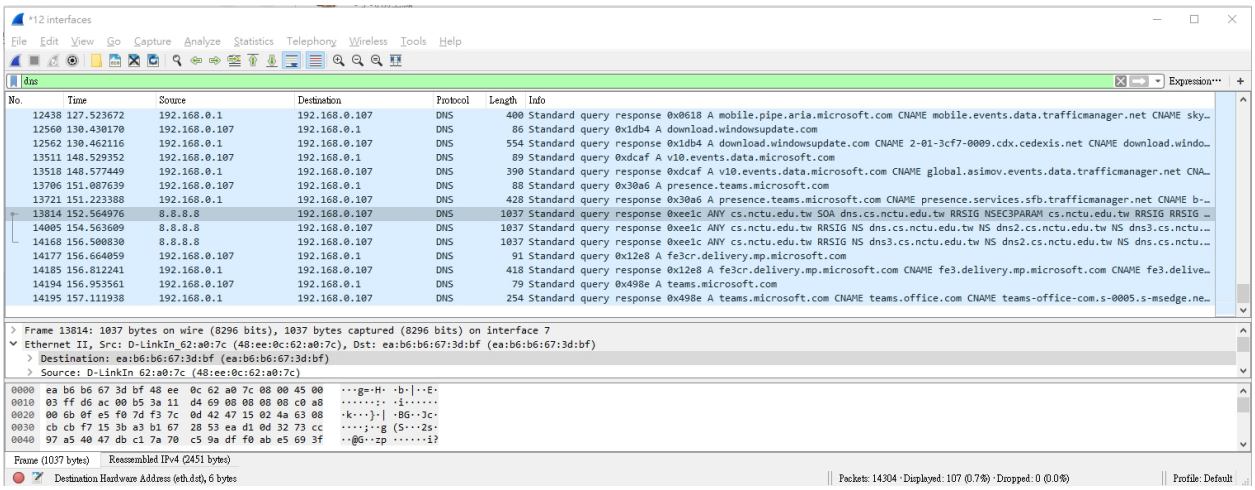

According to the screenshot, firstly I sent the DNS query from my virtual machine(IP:192.168.0.119) and my teammate's computer received the responses (IP:192.168.0.107), which denotes that we have successfully launched reflection attack. Next, we can also tell from the screenshot that the DNS query with query ID 0XEE1C has the length of 89. However, we receive response size of 1037. To sum up, the Amplification ratio of our program is 1037/89 = 11.65.

II

1.Setting query type to 0x00ff to make DNS server return all records of all types known to the name server.

2.We added an additional resource record right after the DNS question field, and set the RR's type to 41(OPT) to enable extension of the space for the response code. Next, set the payload size to 4096 to allow larger UDP payload in the response.

3.Lastly, we attempted to find the website containing most information in the 8.8.8.8 DNS server in order to obtain the largest response.

III solution

Anti-spoofing, directed broadcast, and rate limiting filters should have been implemented. Ideally have network monitors and IDS to detect and notify abnormal traffic patterns

1. Anti-spoofing

(1)source address validation

Filter invalid source ip address by ACL or uRPF check.

(2)BCP38

If the ISP has BCP38 implemented on their customer routers, only packets originating from their customers range would be allowed to pass.

2. DPI

Deep packet inspection (DPI) uses granular analysis to cross-examine the content of different packet headers , being able to uncover metrics for identifying and filtering out malicious traffic.

3. Disable directed-broadcast and open recursive DNS server

Contents DNS server should accept queries from everyone, but service of resolver (cache) DNS server should be restricted to its customer only

4. Rate Limiting

(1)Implement especially on infrequent request types (such as UDP ANY)

(2)Firewall

Can be configured to block specific packets or address range

(3)DNS dampening :

Collect penalty points per address range based on query type, size of the response… . Once the penalty points reach the configured limit, the server drops queries from the IP.

(4)Response Rate Limiting(RRL) :

Limiting the amount of unique responses returned by a DNS server.