

1. please give evidence that you have finished Tasks I and II

The image displays two sequential terminal windows from a Kali Linux system, illustrating a DNS flood attack. The terminal is running on a virtual machine named 'cso2020ubuntu-'. The left window shows the initial setup, including the creation of a network namespace and the start of a DNS flood attack using a script named 'dns_flood.py'. The right window shows the attack in progress, with a large volume of traffic overwhelming the target. Red boxes highlight key IP addresses and command outputs. Labels like 'Attacker IP', 'DNS Response', 'Launch Attack', 'DNS Query', and 'Query Size' are overlaid on the terminal output to identify specific parts of the attack.

Attacker IP

DNS Response

Launch Attack

DNS Query

Query Size

Response Size

The screenshot displays the Wireshark network protocol analyzer interface. At the top, the title bar indicates the active file is "fany.pcap". The main window is divided into several panes:

- Packets List Pane (Top):** Shows a list of captured packets. Packet 8 is selected, which is a DNS Standard query response from 192.168.40.129 to 192.168.40.125.
- Packet Details Pane (Middle):** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II frame, Internet Protocol Version 4 header, User Datagram Protocol header, and Domain Name System (DNS) message details, including flags, questions, answers, queries, and additional records.
- Packet Bytes Pane (Bottom):** Displays the raw hexadecimal and ASCII data of the selected packet.

The status bar at the bottom indicates that 15 packets are displayed, representing 64.0% of the total capture, with 0.0% dropped.

$$Sr = 1279 + 8(\text{UDP header size}) = 1287$$

$$Sq = 56 + 8 = 64$$

$$R = 1287/64 = 20.1$$

2. please explain how you amplify the DNS response

First, I create some personal and large TXT entries in a public domain hosting service (in this case the nctu.me domain hosting service). Then, I query these TXT entries. Since the TXT entries are rather large, I am able to amplify the DNS response.

3. please propose a solution that can defend against the DoS attack based on the DNS reflection

To solve the root cause, the internet service providers should stop packets with spoofed IP from leaving the network. Other than that, DNS resolvers can configure their servers so that they won't respond to deviant query such as the ANY query. Finally, those who run web services can seek protection from large company such as Cloudflare or Akamai since the malicious bandwidth is not likely to overwhelm those companies.