Computer Security Capstone_project1_DNS Reflection & Amplification Attack

group member：0516067 曾靖驊、309460027 施楷平

File：

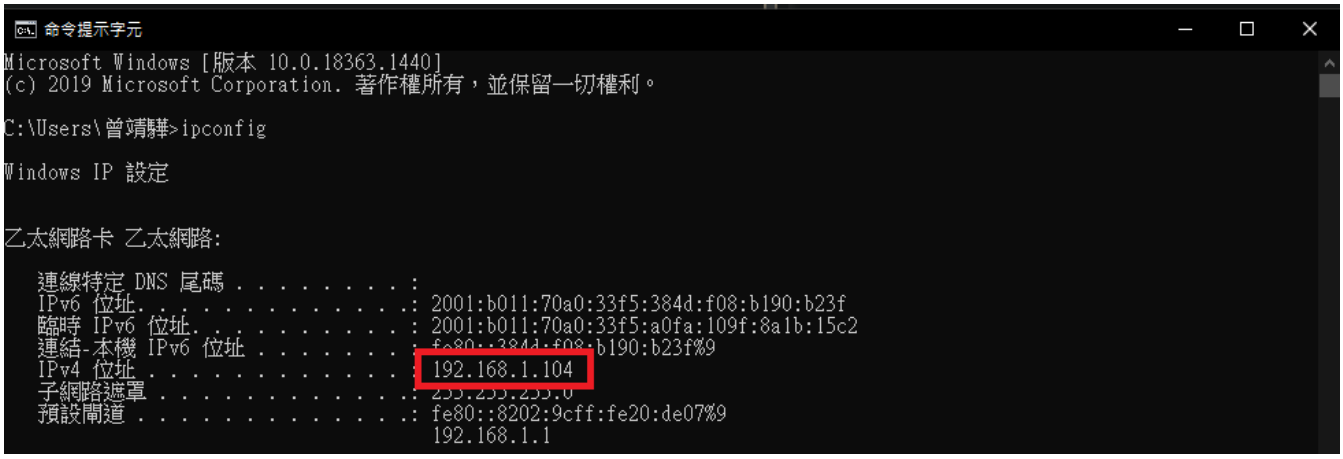
dns_attack.c

Makefile

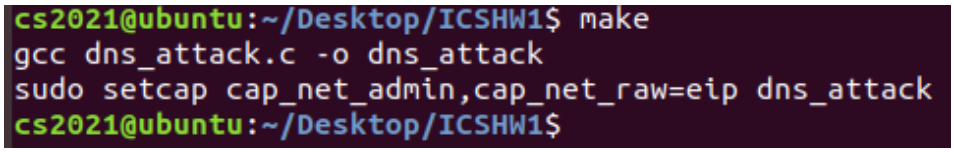
ITEM 1：

Steps:

1. Find the Victim's IPv4 address

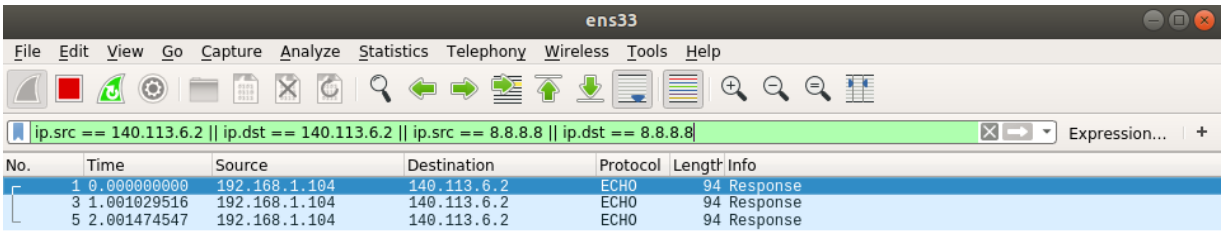


2. Make

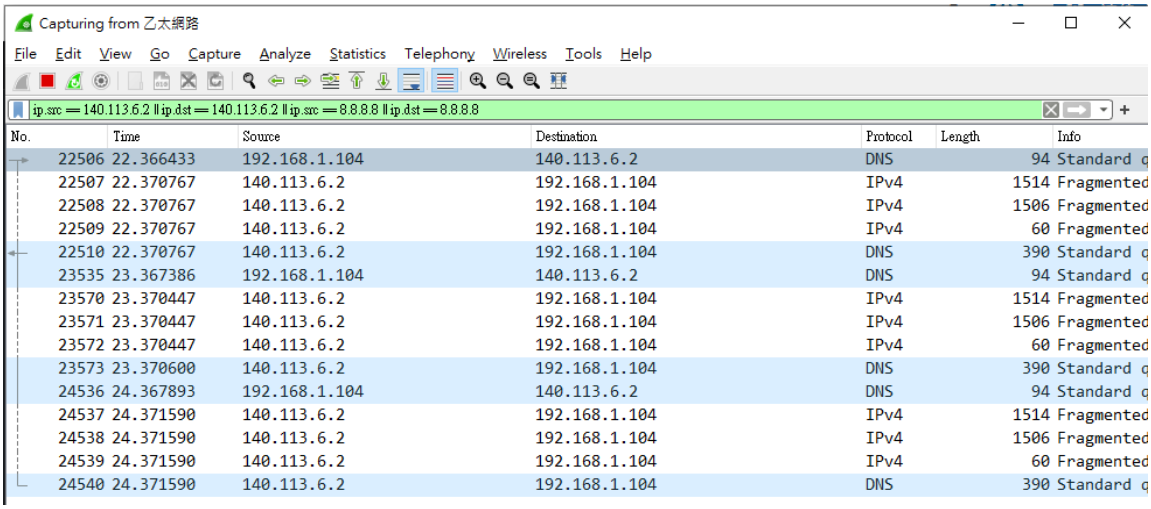


3. Execute ./dns_attack 192.168.1.104 7 140.113.6.2

- Attacker

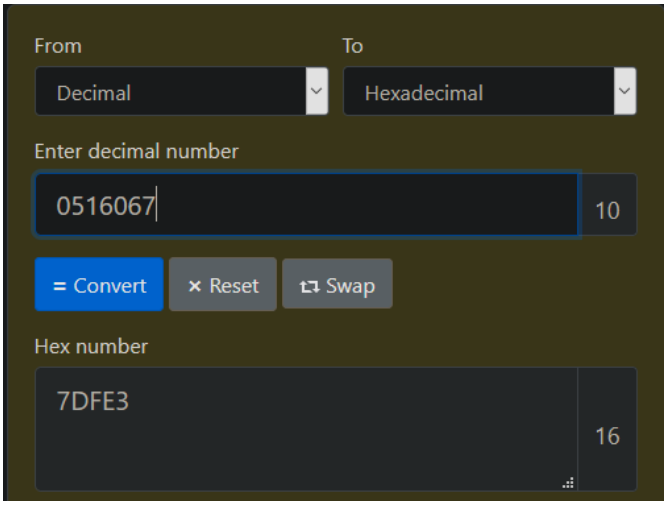


- Victim



```
> User Datagram Protocol, Src Port: 53, Dst Port: 931
v Domain Name System (response)
    Transaction ID: 0xdfe3
  > Flags: 0x8500 Standard query response, No error
    Questions: 1
    Answer RRs: 18
```

Transaction ID: 0xdfe3 = 0516067 last 2byte



22507、22508、22509、22510 are actually one response for request 22506, fragmented into 4 packets

Ratio = (1514+1506+60+390)/94 = 36.9

ITEM 2:

Use **dig +dnssec example.com ns** to check if the DNS Server supports EDNS, try to find the the most effective combination of Domain Name and DNS server(nctu.edu.tw, 140.113.6.2), and we simulate the DNS packet, found that we need to append Additional Records after the DNS query, set type = 41(OPT, allow edns), Z:DO bit = 1(allow dnssec), actively tell the server we can accept more information.

ITEM 3:

1. DNS servers should limit the frequency of request of ANY type, which means once the servers find the client sending identical ANY request, server should only response IPv4 address instead of all informations.

2. Gateway should check if the packets source IP, deny the packets which IP address is not in the subnet. So the attacker won't be able to spoof the IP address.