

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

```
命令提示字元
Microsoft Windows [版本 10.0.18363.1440]
(c) 2019 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\Users\曾靖驊>ipconfig

Windows IP 設定

乙太網路卡 乙太網路:

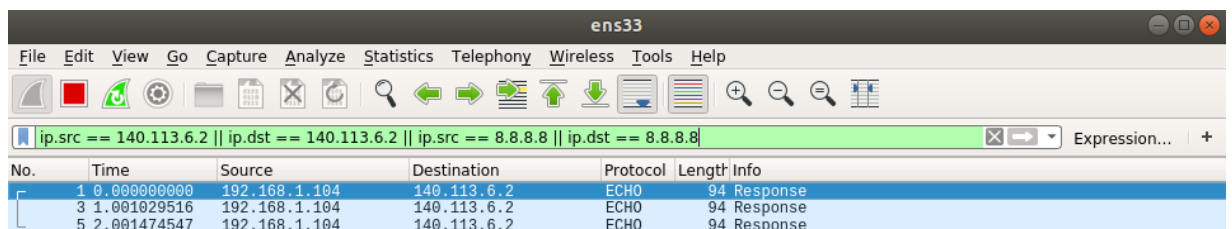
    連線特定 DNS 尾碼 . . . . . : 
    IPv6 位址 . . . . . : 2001:b011:70a0:33f5:384d:f08:b190:b23f
    臨時 IPv6 位址 . . . . . : 2001:b011:70a0:33f5:a0fa:109f:8a1b:15c2
    連結-本機 IPv6 位址 . . . . . : fe80::384d:f08:b190:b23f%9
    IPv4 位址 . . . . . : 192.168.1.104
    子網路遮罩 . . . . . : 255.255.255.0
    預設閘道 . . . . . : fe80::8202:9cff:fe20:de07%9
                        192.168.1.1
```

2. Make

```
cs2021@ubuntu:~/Desktop/ICSHW1$ make
gcc dns_attack.c -o dns_attack
sudo setcap cap_net_admin,cap_net_raw=eip dns_attack
cs2021@ubuntu:~/Desktop/ICSHW1$
```

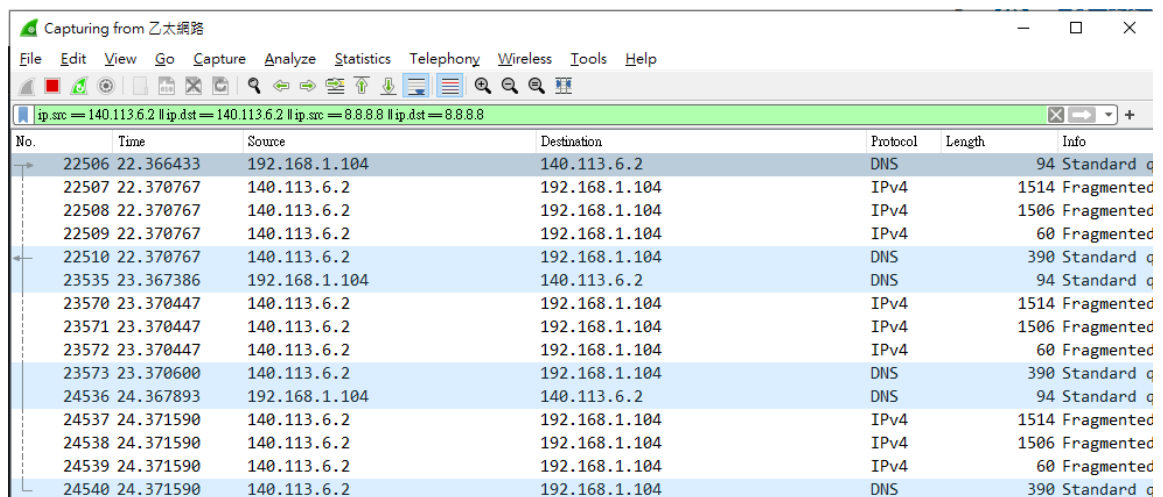
3. Execute `./dns_attack 192.168.1.104 7 140.113.6.2`

- Attacker



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.104	140.113.6.2	ECHO	94	Response
3	1.001029516	192.168.1.104	140.113.6.2	ECHO	94	Response
5	2.001474547	192.168.1.104	140.113.6.2	ECHO	94	Response

- Victim



No.	Time	Source	Destination	Protocol	Length	Info
22506	22.366433	192.168.1.104	140.113.6.2	DNS	94	Standard q
22507	22.370767	140.113.6.2	192.168.1.104	IPv4	1514	Fragmented
22508	22.370767	140.113.6.2	192.168.1.104	IPv4	1506	Fragmented
22509	22.370767	140.113.6.2	192.168.1.104	IPv4	60	Fragmented
22510	22.370767	140.113.6.2	192.168.1.104	DNS	390	Standard q
23535	23.367386	192.168.1.104	140.113.6.2	DNS	94	Standard q
23570	23.370447	140.113.6.2	192.168.1.104	IPv4	1514	Fragmented
23571	23.370447	140.113.6.2	192.168.1.104	IPv4	1506	Fragmented
23572	23.370447	140.113.6.2	192.168.1.104	IPv4	60	Fragmented
23573	23.370600	140.113.6.2	192.168.1.104	DNS	390	Standard q
24536	24.367893	192.168.1.104	140.113.6.2	DNS	94	Standard q
24537	24.371590	140.113.6.2	192.168.1.104	IPv4	1514	Fragmented
24538	24.371590	140.113.6.2	192.168.1.104	IPv4	1506	Fragmented
24539	24.371590	140.113.6.2	192.168.1.104	IPv4	60	Fragmented
24540	24.371590	140.113.6.2	192.168.1.104	DNS	390	Standard q

```

> User Datagram Protocol, Src Port: 53, Dst Port: 931
▼ 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

$$\text{Ratio} = (1514 + 1506 + 60 + 390) / 94 = 36.9$$

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.