

# 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.

No.	Source	S port	Protocol	Destination	D port	Length	Info
37969	192.168.88.254	4242	DNS	8.8.8.8	53	90	Standard query 0x7412 TXT a.tg.pe OPT
37970	192.168.88.254	4242	DNS	8.8.8.8	53	90	Standard query 0x7412 TXT a.tg.pe OPT
37971	192.168.88.254	4242	DNS	8.8.8.8	53	90	Standard query 0x7412 TXT a.tg.pe OPT
37972	8.8.8.8		IPv4	192.168.88.254		1482	Fragmented IP protocol (proto=UDP 17, off=0, ID=7932) [Re
37973	8.8.8.8		IPv4	192.168.88.254		1482	Fragmented IP protocol (proto=UDP 17, off=1448, ID=7932) [Re
37974	8.8.8.8	53	DNS	192.168.88.254	4242	1242	Standard query response 0x7412 TXT a.tg.pe TXT TXT TXT TX
37975	8.8.8.8		IPv4	192.168.88.254		1482	Fragmented IP protocol (proto=UDP 17, off=0, ID=10ae) [Re
37976	8.8.8.8		IPv4	192.168.88.254		1482	Fragmented IP protocol (proto=UDP 17, off=1448, ID=10ae) [Re
37977	8.8.8.8	53	DNS	192.168.88.254	4242	1242	Standard query response 0x7412 TXT a.tg.pe TXT TXT TXT TX
37978	8.8.8.8		IPv4	192.168.88.254		1482	Fragmented IP protocol (proto=UDP 17, off=0, ID=cea6) [Re
37979	8.8.8.8		IPv4	192.168.88.254		1482	Fragmented IP protocol (proto=UDP 17, off=1448, ID=cea6) [Re
37980	8.8.8.8	53	DNS	192.168.88.254	4242	1242	Standard query response 0x7412 TXT a.tg.pe TXT TXT TXT TX
37981	192.168.88.254	53	ICMP	8.8.8.8	4242	70	Destination unreachable (Port unreachable)
37982	192.168.88.254	53	ICMP	8.8.8.8	4242	70	Destination unreachable (Port unreachable)
37983	192.168.88.254	53	ICMP	8.8.8.8	4242	70	Destination unreachable (Port unreachable)

> Internet Protocol Version 4, Src: 192.168.88.254, Dst: 8.8.8.8  
> User Datagram Protocol, Src Port: 4242, Dst Port: 53  
v Domain Name System (query)  
Transaction ID: 0x7412  
> Flags: 0x0120 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 1  
v Queries  
> a.tg.pe: type TXT, class IN

0000 08 55 31 2a 29 da 3c 22 fb 07 c8 1c 08 00 45 00 .U1\*) <" .....E.  
0010 00 4c 54 4e 00 00 40 11 fc 9c c0 a8 58 fe 08 08 .LTN.@. ....X..  
0020 08 08 10 92 00 35 00 38 00 00 74 12 01 20 00 01 .....5.8 ..t..  
0030 00 00 00 00 00 01 01 61 02 74 67 02 70 65 00 00 .....a .tg.pe..  
0040 10 00 01 00 00 29 10 00 00 00 80 00 00 0c 00 0a .....).  
0050 00 08 5d 10 b5 b4 f8 be 1a 3a ...].....:

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.