dnstap-whoami

Robert Edmonds (edmonds@fsi.io)
Farsight Security, Inc.

Intro

- DNS nameservers that return custom responses
  - Diagnostics
  - Experimentation
- Result passed through to the original client
- Examples:
  - DNS “whoami”
  - OARC port and reply size tests

DNS “whoami”

- Query for type A
- Get resolver IPv4 address in record data

```
$ dig +short @8.8.8.8 whoami.akamai.net
74.125.177.51
```

Anycasted service address

```
$ dig +short @8.8.8.8 whoami.akamai.net
74.125.177.51
```

Unicast resolver address

```
$ dig +short @8.8.8.8 whoami.akamai.net
74.125.177.51
```

OARC port and reply size tests

- Client sends query to resolver
- Nameserver forces resolver to perform multiple queries
- Get information about source port randomization, EDNS buffer size

```
$ dig +short porttest.dns-oarc.net TXT

porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i
.h.g.f.e.d.c.b.a.pt.dns-oarc.net.

"70.89.251.89 is GREAT: 75 queries in 2.1
seconds from 75 ports with std dev 17022"
```

```
$ dig +short rs.dns-oarc.net TXT
rst.x4050.rs.dns-oarc.net.
rst.x4058.x4050.rs.dns-oarc.net.
rst.x4064.x4058.x4050.rs.dns-oarc.net.
"70.89.251.89 DNS reply size limit is at least 4064"
"70.89.251.89 sent EDNS buffer size 4096"
"Tested at 2015-09-23 18:26:16 UTC"
```

dnstap-whoami

- Encode the resolver's wire query (plus metadata) into the response RR
- Makes resolver information visible to client, e.g.:
  - IPv4/IPv6 query source address
  - TCP/UDP query source port
  - EDNS buffer size
  - EDNS0 options (client-subnet, cookies, etc.)
  - 0x20

dnstap-whoami

- Uses dnstap protobuf schema for encoding
  - ✔ Compact, extensible
  - ✘ Not human readable, requires decoder tool

dnstap-whoami

- Query **whoami.dnstap.info** type **NULL** for IPv4

```
$ dig +short whoami.dnstap.info NULL
```

- Query **whoami6.dnstap.info** type **NULL** for IPv6

```
$ dig +short whoami6.dnstap.info NULL
```

```
$ dig +short @8.8.8.8 whoami.dnstap.info NULL

\# 89
72550801100122044A7D2A37309FFD03408BEE8BB0054D096A312F52
3A1555001000010000000000010677686F616D6906646E7374617004
696E666F00000A000100002910000000800000B00080007000118004
4659FB7801
```

```
$ dig +short @8.8.8.8 whoami.dnstap.info NULL | \
    cut -f3- -d' ' | xxd -r -p | hd

00000000  72 55 08 01 10 01 22 04  4a 7d 2a 37 30 9f fd 03  |rU....".J}*70...|
00000010  40 8b ee 8b b0 05 4d 09  6a 31 2f 52 3a 15 55 00  |@.....M.j1/R:.U.|
00000020  10 00 01 00 00 00 00 00  01 06 77 68 6f 61 6d 69  |..........whoami|
00000030  06 64 6e 73 74 61 70 04  69 6e 66 6f 00 00 0a 00  |.dnstap.info....|
00000040  01 00 00 29 10 00 00 00  80 00 00 0b 00 08 00 07  |...)............|
00000050  00 01 18 00 46 59 fb 78  01                       |....FY.x.|
00000059
```

```
$ dig +short @8.8.8.8 whoami.dnstap.info NULL | \
    cut -f3- -d' ' | xxd -r -p | \
    protoc --decode=dnstap.Dnstap ./dnstap.proto

message {
  type: AUTH_QUERY
  socket_family: INET
  query_address: "J}*7"
  query_port: 65183
  query_time_sec: 1443034891
  query_time_nsec: 791767561
  query_message:
"\025U\000\020\000\001\000\000\000\000\000\001\00
6whoami\006dnstap\004info\000\000\n\000\001\000\0
00)\020\000\000\000\200\000\000\013\000\010\000\0
07\000\001\030\000FY\373"
}
type: MESSAGE
```

```
$ dig +short @8.8.8.8 whoami.dnstap.info NULL | \
    cut -f3- -d' ' | xxd -r -p | \
    protoc --decode=dnstap.Dnstap ./dnstap.proto

message {
  type: AUTH_QUERY
  socket_family: INET
  query_address: "J}*7"
  query_port: 65183
  query_time_sec: 1443034891
  query_time_nsec: 791767561
  query_message:
"\025U\000\020\000\001\000\000\000\000\000\001\00
6whoami\006dnstap\004info\000\000\n\000\001\000\0
00)\020\000\000\000\200\000\000\013\000\010\000\0
07\000\001\030\000FY\373"
}
type: MESSAGE
```

```
$ dig +short @8.8.8.8 whoami.dnstap.info NULL | \
    dnstap-ldns -xy

type: MESSAGE
message:
  type: AUTH_QUERY
  query_time: !!timestamp 2015-09-23 19:01:31.791767
  socket_family: INET
  query_address: 74.125.42.55
  query_port: 65183
  query_message: |
    ;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 5461
    ;; flags: cd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

    ;; QUESTION SECTION:
    ;whoami.dnstap.info.  IN  NULL

    ;; ANSWER SECTION:

    ;; AUTHORITY SECTION:

    ;; ADDITIONAL SECTION:

    ;; EDNS: version 0; flags: do ; udp: 4096
    ;; Data: \# 11 000800070001180046 59fb
---
```

```
$ dig +short @8.8.8.8 whoami.dnstap.info NULL | \
    dnstap-ldns -xy

type: MESSAGE
message:
  type: AUTH_QUERY
  query_time: !!timestamp 2015-09-23 19:01:31.791767
  socket_family: INET
  query_address: 74.125.42.55
  query_port: 65183
  query_message: |
    ;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 5461
    ;; flags: cd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

    ;; QUESTION SECTION:
    ;whoami.dnstap.info.  IN  NULL

    ;; ANSWER SECTION:

    ;; AUTHORITY SECTION:

    ;; ADDITIONAL SECTION:

    ;; EDNS: version 0; flags: do ; udp: 4096
    ;; Data: \# 11 000800070001180046 59fb
---
```

```
$ dig +short @8.8.8.8 whoami.dnstap.info NULL | \
    dnstap-ldns -xy

type: MESSAGE
message:
  type: AUTH_QUERY
  query_time: !!timestamp 2015-09-23 19:01:31.791767
  socket_family: INET
  query_address: 74.125.42.55
  query_port: 65183
  query_message: |
    ;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 5461
    ;; flags: cd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

    ;; QUESTION SECTION:
    ;whoami.dnstap.info.  IN  NULL

    ;; ANSWER SECTION:

    ;; AUTHORITY SECTION:

    ;; ADDITIONAL SECTION:

    ;; EDNS: version 0; flags: do ; udp: 4096
    ;; Data: \# 11 000800070001180046 59fb
---
```

```
$ dig +short @8.8.8.8 whoami.dnstap.info NULL | \
    dnstap-ldns -xy

type: MESSAGE
message:
  type: AUTH_QUERY
  query_time: !!timestamp 2015-09-23 19:01:31.791767
  socket_family: INET
  query_address: 74.125.42.55
  query_port: 65183
  query_message: |
    ;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 5461
    ;; flags: cd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

    ;; QUESTION SECTION:
    ;whoami.dnstap.info.  IN  NULL

    ;; ANSWER SECTION:

    ;; AUTHORITY SECTION:

    ;; ADDITIONAL SECTION:

    ;; EDNS: version 0; flags: do ; udp: 4096
    ;; Data: \# 11 000800070001180046 59fb
---
```

```
$ dig +short @8.8.8.8 whoami.dnstap.info NULL | \
    dnstap-ldns -xy

type: MESSAGE
message:
  type: AUTH_QUERY
  query_time: !!timestamp 2015-09-23 19:01:31.791767
  socket_family: INET
  query_address: 74.125.42.55
  query_port: 65183
  query_message: |
    ;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 5461
    ;; flags: cd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

    ;; QUESTION SECTION:
    ;whoami.dnstap.info.  IN  NULL

    ;; ANSWER SECTION:

    ;; AUTHORITY SECTION:

    ;; ADDITIONAL SECTION:

    ;; EDNS: version 0; flags: do ; udp: 4096
    ;; Data: \# 11 000800070001180046 59fb
---
```

```
$ dig +short @8.8.8.8 whoami.dnstap.info NULL | \
    dnstap-ldns -xy

type: MESSAGE
message:
  type: AUTH_QUERY
  query_time: !!timestamp 2015-09-23 19:01:31.791767
  socket_family: INET
  query_address: 74.125.42.55
  query_port: 65183
  query_message: |
    ;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 5461
    ;; flags: cd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

    ;; QUESTION SECTION:
    ;whoami.dnstap.info.  IN  NULL

    ;; ANSWER SECTION:

    ;; AUTHORITY SECTION:

    ;; ADDITIONAL SECTION:

    ;; EDNS: version 0; flags: do ; udp: 4096
    ;; Data: \# 11 000800070001180046 59fb
---
```

Source code

- Reference decoding tool
  - https://github.com/dnstap/dnstap-ldns
- Custom nameserver
  - https://github.com/dnstap/dnstap-evldns
- Protobuf schema
  - https://github.com/dnstap/dnstap.pb

Special thanks

- Ray Bellis, for his “evldns” DNS server framework
  - https://github.com/raybellis/evldns

Thanks!