NEW dnsmeter

DNS-OARC is pleased to announce that we are the new home of dnsmeter, a software tool for DNS server high performance measurement developed by Patrick Fedick at DENIC eG.

One key feature is that the sender address can be spoofed from a given network or from PCAP file.

```
$ sudo dnsmeter -p payload.txt -s 10.0.0.0/24 -z 192.168.100.2:53
INFO: Loading and precompile payload. This could take some time...
INFO: 2 queries loaded
################################################################################
# Start Session with Threads: 1, Queryrate: unlimited
00:00:01 Queries send:   63041, rcv:   59022, Data send:   3570 KB, rcv:   3112 KB
00:00:02 Queries send:   76085, rcv:   74820, Data send:   4309 KB, rcv:   3945 KB
00:00:03 Queries send:   93531, rcv:   92560, Data send:   5297 KB, rcv:   4881 KB
00:00:04 Queries send:   97172, rcv:   93525, Data send:   5503 KB, rcv:   4931 KB
00:00:05 Queries send:   97847, rcv:   93605, Data send:   5542 KB, rcv:   4936 KB
00:00:06 Queries send:  102129, rcv:   95323, Data send:   5784 KB, rcv:   5026 KB
00:00:07 Queries send:  100967, rcv:   98675, Data send:   5718 KB, rcv:   5203 KB
00:00:08 Queries send:   99331, rcv:   94753, Data send:   5626 KB, rcv:   4996 KB
00:00:09 Queries send:   93829, rcv:   86842, Data send:   5314 KB, rcv:   4579 KB
00:00:10 Queries send:   98861, rcv:   94496, Data send:   5599 KB, rcv:   4983 KB
00:00:11 Queries send:   67306, rcv:   64271, Data send:   3812 KB, rcv:   3389 KB
00:00:12 Queries send:       0, rcv:       0, Data send:      0 KB, rcv:      0 KB
================================================================================
network if  Pkt send: 0, rcv: 0, Data send: 0 KB, rcv: 0 KB
DNS Queries send:     990099, Qps:   99009, Data send:   56079 KB =      5 MBit
DNS Queries rcv:      947892, Qps:   94789, Data rcv:    49986 KB =      4 MBit
DNS Queries lost:      42207 = 4.263 %
DNS rtt average: 1.1269 ms, min: 0.1000 ms, max: 32.9000 ms
DNS truncated: 0
DNS RCODES: REFUSED: 947892,
```

DNS-OARC

Domain Name System Operations Analysis and Research Center

dnsperf; Now with TCP & TLS

Moved to DNS-OARC early 2019 from Nominum/Akamai, these tools make it simple to gather accurate latency and through-put metrics for DNS services.

dnsperf “self-paces” the query load to simulate network conditions and resperf increases the query rate and monitors the response rate to simulate caching DNS services.

```
$ echo "dns-oarc.net A" | dnsperf -v -s 192.168.100.2 -p 53 -m tcp
DNS Performance Testing Tool
Version 2.3.2

[Status] Command line: dnsperf -v -s 192.168.100.2 -p 53 -m tcp
[Status] Sending queries (to 192.168.100.2)
[Status] Started at: Mon Oct 21 14:08:49 2019
[Status] Stopping after 1 run through file
> NOERROR dns-oarc.net A 0.226935
[Status] Testing complete (end of file)

Statistics:

  Queries sent:         1
  Queries completed:    1 (100.00%)
  Queries lost:         0 (0.00%)

  Response codes:       NOERROR 1 (100.00%)
  Average packet size:  request 30, response 259
  Run time (s):         0.227346
  Queries per second:   4.398582

  Average Latency (s):  0.226935 (min 0.226935, max 0.226935)
```

DNS-OARC

Domain Name System Operations Analysis and Research Center

dnsjit

dnsjit is a combination of parts taken from dsc, dnscap, drool, and put together around Lua.

This creates a script-based engine for easy capturing, parsing and statistics gathering of DNS messages while also providing facilities for replaying DNS traffic.

```
#!/usr/bin/env dnsjit
require("dnsjit.core.objects")
local input = require("dnsjit.input.pcap").new()
local layer = require("dnsjit.filter.layer").new()
local dns = require("dnsjit.core.object.dns").new()

input:open_offline(arg[2])
layer:producer(input)
local producer, ctx = layer:produce()

while true do
    local object = producer(ctx)
    if object == nil then break end
    if object:type() == "payload" then
        dns.obj_prev = object
        if dns:parse_header() == 0 then
            print(dns.id)
        end
    end
end
```

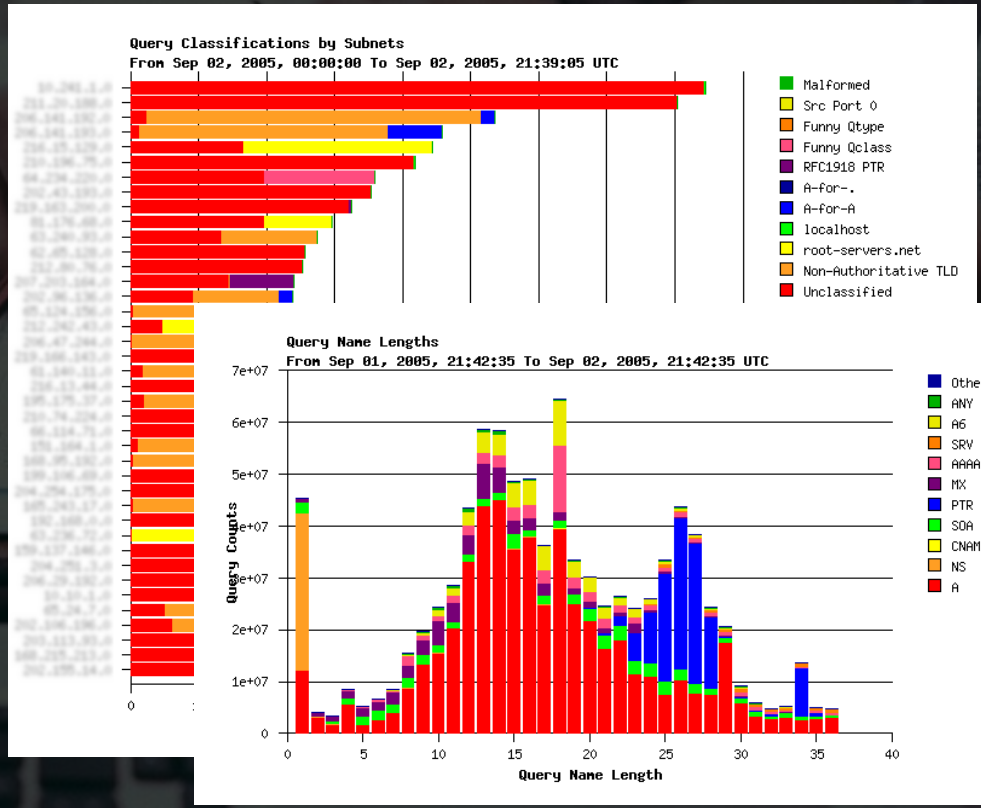
DNS-OARC

Domain Name System Operations Analysis and Research Center

dsc

DSC is a system for collecting and exploring statistics from busy DNS servers. It uses collectors running on or near name-servers and the data can be presented as shown.

DSC is configurable to allow the administrator to capture all kinds of DNS data.



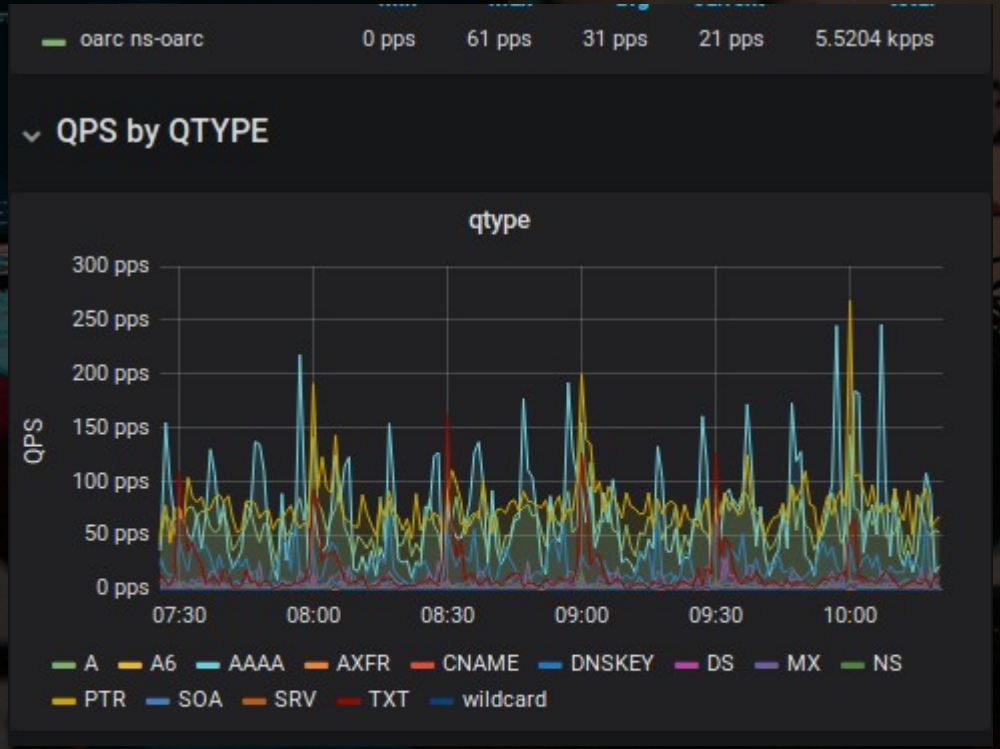
DNS-OARC

Domain Name System Operations Analysis and Research Center

dsc-datatool

dsc-datatool can be used to convert, export, merge or transform DSC data.

It was created to convert DSC XML to Graphite / InfluxDB so DSC data can be displayed by more modern analytical and monitoring tools such as Grafana.



DNS-OARC

Domain Name System Operations Analysis and Research Center

dnscap

dnscap is a network capture utility designed specifically for DNS traffic. It produces binary data in PCAP format.

This utility is similar to tcpdump, but has a number of features tailored to DNS transactions and protocol options. OARC uses dnscap for DITL data collections.

```
$ dnscap -i eth0 -g
[58] 2019-04-25 13:50:44.067926 [#0 eth0 4095] \
    [172.17.0.11].42169 [172.17.0.1].53  \
    dns QUERY,NOERROR,12744,rd \
    1 dns-oarc.net,IN,A 0 0 0
[287] 2019-04-25 13:50:44.071254 [#1 eth0 4095] \
    [172.17.0.1].53 [172.17.0.11].42169  \
    dns QUERY,NOERROR,12744,qr|rd|ra \
    1 dns-oarc.net,IN,A \
    1 dns-oarc.net,IN,A,120,64.191.0.198 \
    4 dns-oarc.net,IN,NS,95,ns.dns-oarc.net \
    dns-oarc.net,IN,NS,95,ns2.dns-oarc.net \
    dns-oarc.net,IN,NS,95,ns3.dns-oarc.net \
    dns-oarc.net,IN,NS,95,sns-pb.isc.org \
    6 ns.dns-oarc.net,IN,A,95,64.191.0.65 \
    ns2.dns-oarc.net,IN,A,95,192.211.126.36 \
    ns3.dns-oarc.net,IN,A,95,77.72.225.243 \
    ns.dns-oarc.net,IN,AAAA,95,2620:ff:c000:0:1::65 \
    ns2.dns-oarc.net,IN,AAAA,95,2604:1f80:5eb::3 \
    ns3.dns-oarc.net,IN,AAAA,95,2a01:3f0:0:57::243
```

DNS-OARC

Domain Name System Operations Analysis and Research Center

drool

drool can replay DNS traffic from PCAP files and send it to a server, with options such as to manipulate the timing between packets, as well as loop packets infinitely or for a set number of iterations.

The goal is to produce a high amount of UDP packets and TCP sessions on common hardware.

```
$ drool replay --json ~/dns.pcap 172.17.0.1 53
<< dnsjit v0.9.7 https://github.com/DNS-OARC/dnsjit/issues >>
{
  "runtime": 0.00211226,
  "finish": 1.522e-06,
  "packets": 133,
  "queries": 41,
  "sent": 41,
  "received": 41,
  "responses": 41,
  "timeouts": 0,
  "errors": 0
}
$ drool replay ~/dns.pcap 172.17.0.1 53 --timing keep -vvvv
<< dnsjit v0.9.7 https://github.com/DNS-OARC/dnsjit/issues >>
input.mmpcap[0x41dd1318] debug: pcap v2.4 snaplen:65535
filter.timing[0x556551403b00] debug: init with clock_nanosleep() now is
99396.752531287, diff of first pkt -1476877585.676538287
filter.timing[0x556551403b00] debug: init mode keep
replay info: sending udp query
replay info: got response
filter.timing[0x556551403b00] debug: keep mode, sleep to 99396.754520287
filter.timing[0x556551403b00] debug: keep mode, sleep to 99396.754975287
filter.timing[0x556551403b00] debug: keep mode, sleep to 99396.759086287
```

DNS-OARC

Domain Name System Operations Analysis and Research Center

packetq

packetq is a command line tool to run SQL queries directly on PCAP files, the results can be outputted as JSON (default), CSV and XML.

PacketQ was previously known as DNS2db but was renamed in 2011 when it was rebuilt and could handle protocols other than DNS among other things.

```
$ packetq -s "select id, qname from dns limit 10" ~/dns.pcap
[
  {
    "table_name": "result-0",
    "query": "select id, qname from dns limit 10",
    "head": [
      { "name": "id","type": "int" },
      { "name": "qname","type": "text" }
    ],
    "data": [
      [1,"google.com."],
      [2,"google.com."],
      [5,"206.218.58.216.in-addr.arpa."],
      [6,"206.218.58.216.in-addr.arpa."],
      [7,"google.com."],
      [8,"google.com."],
      [14,"google.com."],
      [15,"google.com."],
      [18,"206.218.58.216.in-addr.arpa."],
      [19,"206.218.58.216.in-addr.arpa."]
    ]
  }
]
```

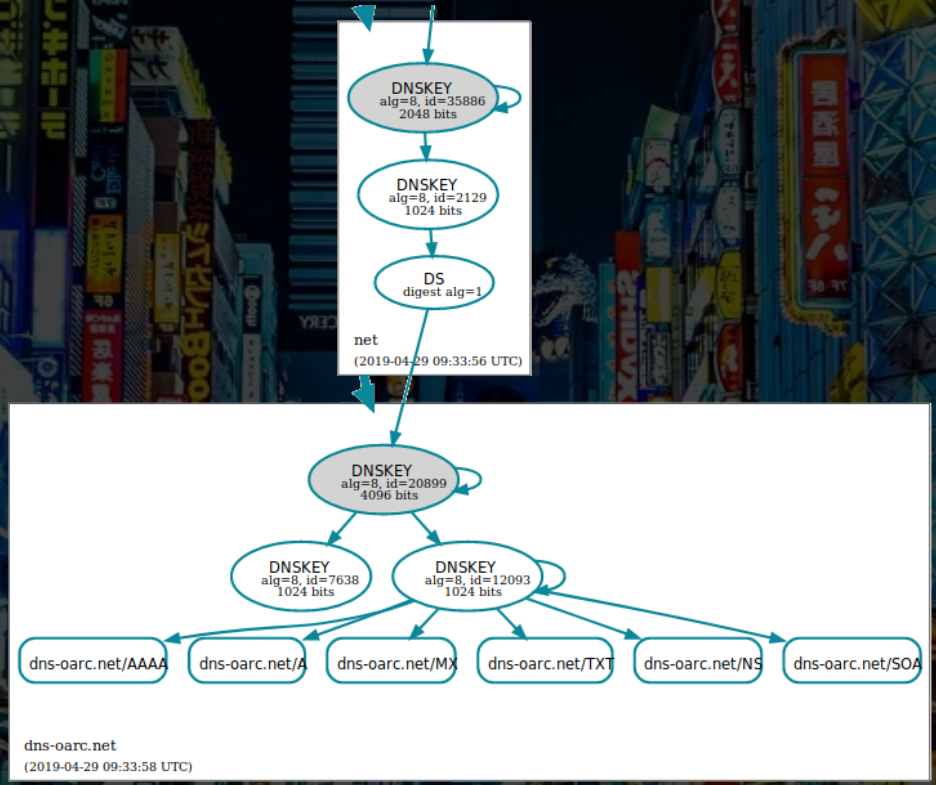
DNS-OARC

Domain Name System Operations Analysis and Research Center

dnsviz

DNSViz is a tool for visualizing the status of a DNS zone, understanding and troubleshooting the deployment of DNSSEC.

It provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace, and lists configuration errors detected.



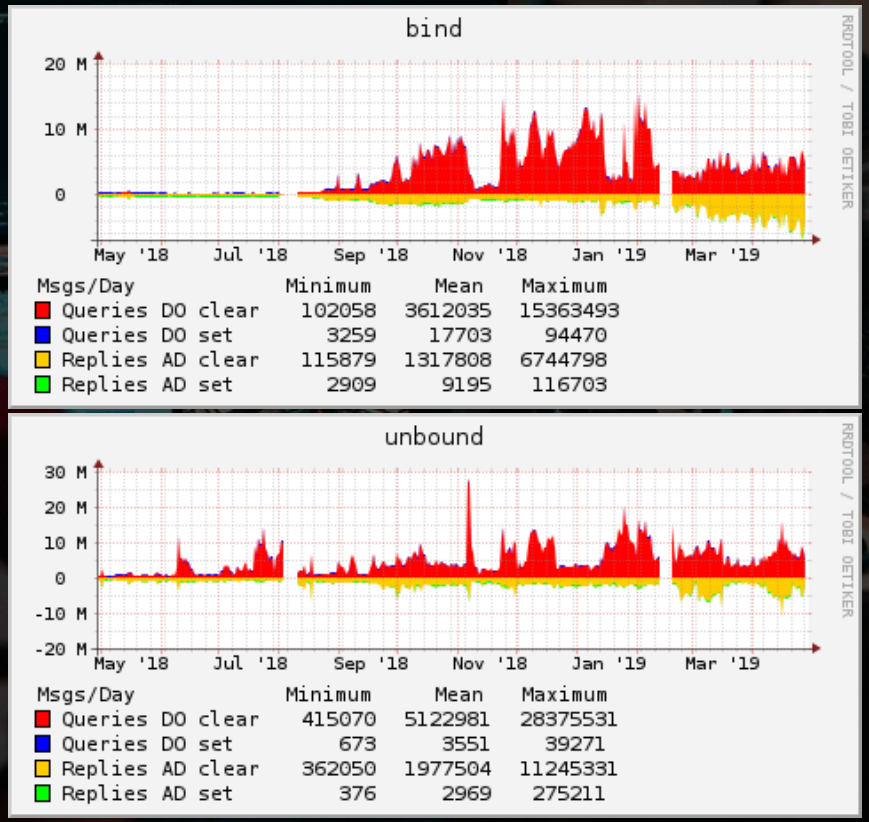
DNS-OARC

Domain Name System Operations Analysis and Research Center

ODVR + DNS Privacy

OARC offers open DNSSEC-validating and DNS Privacy resolvers for experimenting with DNSSEC and DNS over TLS (DoT, RFC 7858).

Data is collected from these services and is available to our members for research purposes



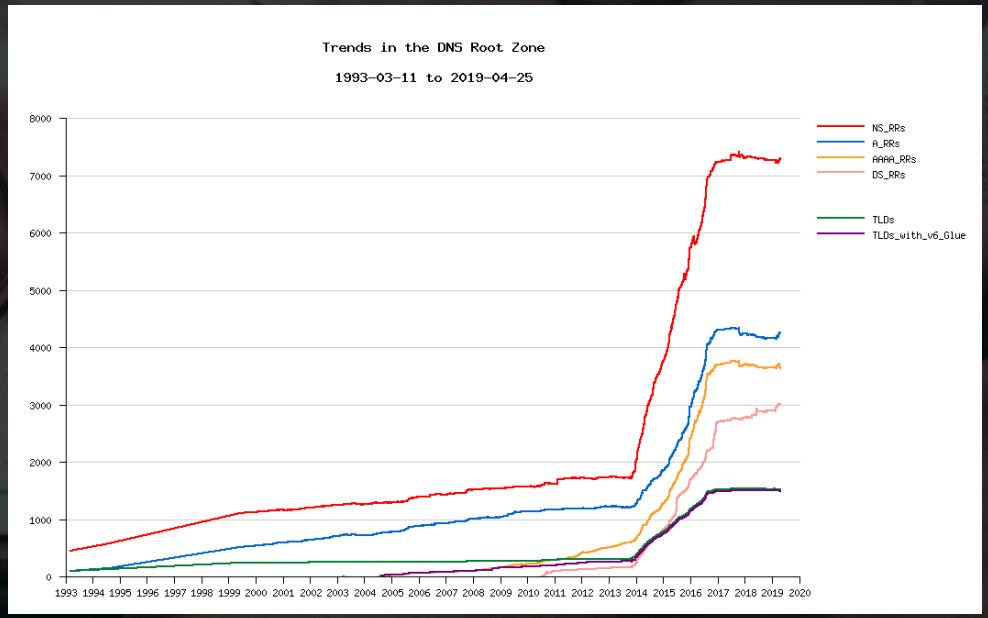
DNS-OARC

Domain Name System Operations Analysis and Research Center

Root Zone Archive

With the assistance of its members and friends DNS-OARC has assembled a historical archive of the DNS root zone dating back to 1993.

This archive is a part of our larger project, the Zone File Repository, where OARC archives copies of TLD zone files on a weekly basis.



DNS-OARC

Domain Name System Operations Analysis and Research Center

Day In The Life of the Internet

OARC collects DNS traces from busy and interesting DNS name-servers through various means, such as the annual Day In The Life of the Internet (DITL) collection effort.

OARC offers access to this data for it's members through the use of a small fleet of analysis machines.

participant	mbytes	queries_millions	# DITL 2018
a-root	532,027	10,694	
afilias	708,960	16,046	
as112-yow	2,246	57	
b-root	152,971	2,729	
c-root	401,484	10,134	
cira	50,312	1,218	
cznic	40,042	1,138	
d-root	333,263	8,677	
e-root	223,046	5,027	
f-root	592,156	17,174	
h-root	262,623	6,562	
i-root	518,497	13,263	
j-root	597,313	12,209	
k-root	541,347	10,487	
l-root	610,957	15,721	
m-root	431,239	7,547	
nethelp	15,227	203	
niccl	21,587	432	
switch	28,360	492	
tix-or-tz	49	2	
wide	10,990	287	

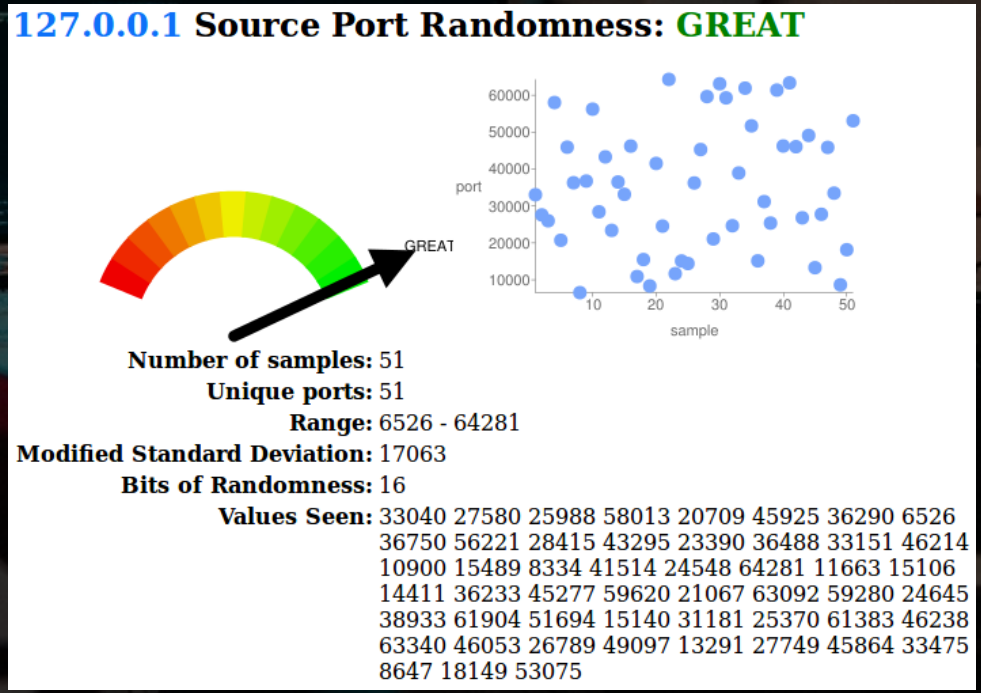
DNS-OARC

Domain Name System Operations Analysis and Research Center

DNS Entropy Test

US-CERT's Vulnerability Note VU#800113 describes deficiencies in the DNS protocol and implementations that can facilitate cache poisoning attacks.

DNS Entropy Test is an online web-based service that can help you learn if your ISP's name-servers are vulnerable to this type of attack.



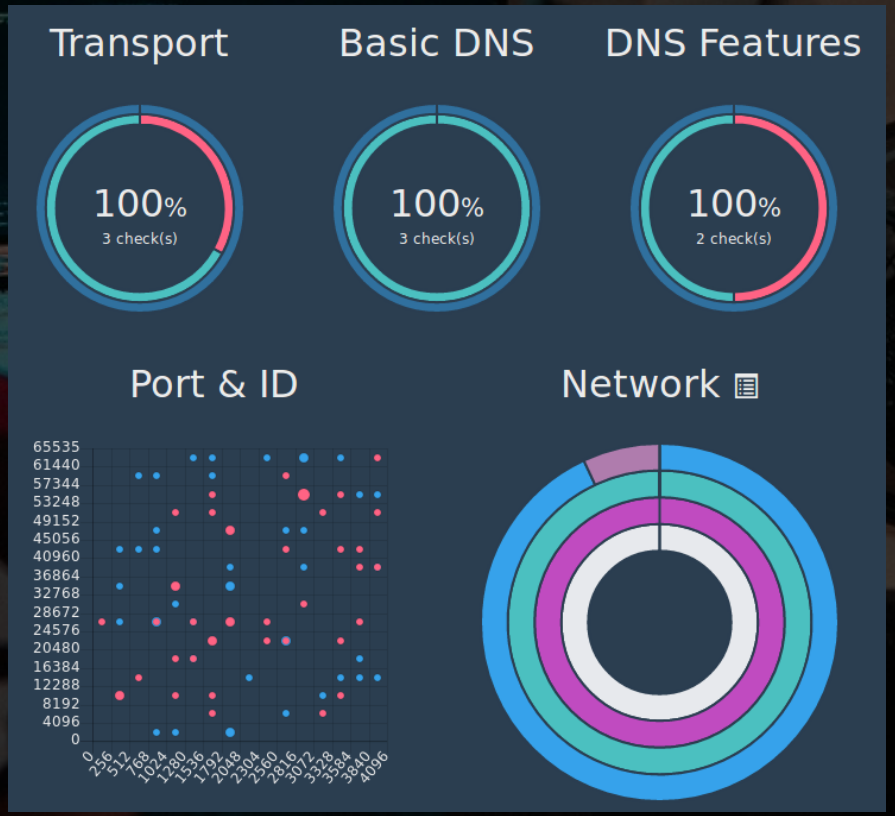
DNS-OARC

Domain Name System Operations Analysis and Research Center

Check My DNS

Check My DNS is a general-purpose framework for testing DNS resolvers from a clients PoV, it includes tests for IPv6 and TCP, DNSSEC, EDNS, QNAME minimization and DNS Entropy.

As a DNS-OARC member you can get access to this data on our analysis servers.



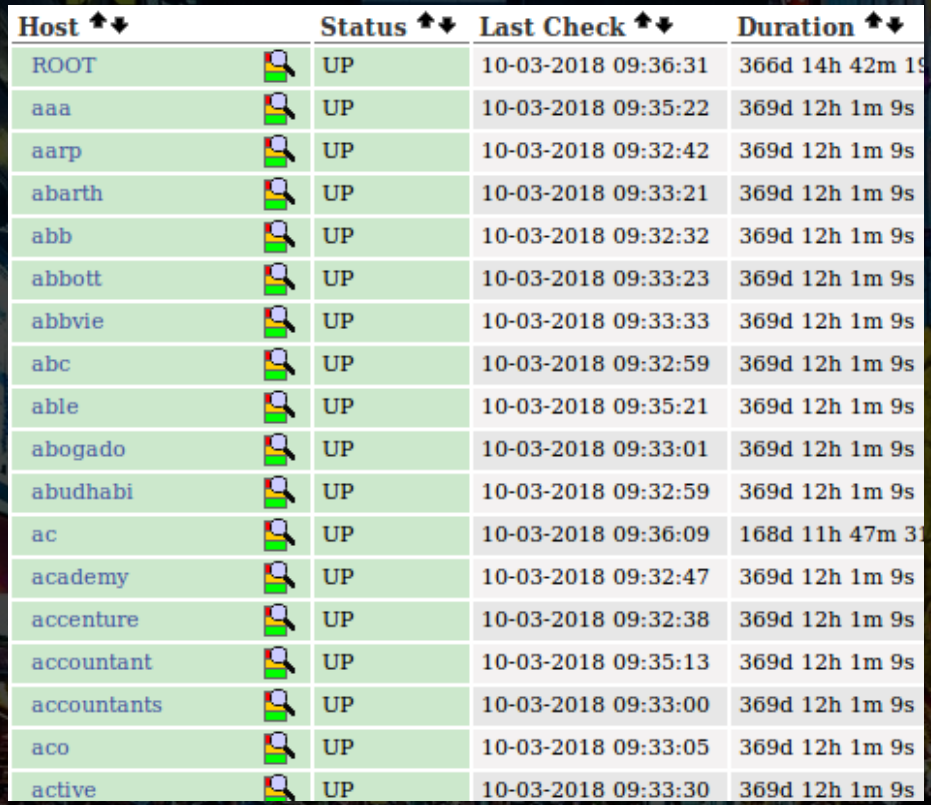
DNS-OARC

Domain Name System Operations Analysis and Research Center

TLDmon

OARC's TLDmon uses Nagios to monitor authoritative name-servers for the Root Zone and all TLDs with checks for authoritative answers, EDNS, TCP, lame delegations, open resolvers, expired RRSIGs, matching serial numbers and more.

As a member you can sign-up to receive notifications for your zones.



Host	Status	Last Check	Duration
ROOT	UP	10-03-2018 09:36:31	366d 14h 42m 19
aaa	UP	10-03-2018 09:35:22	369d 12h 1m 9s
aarp	UP	10-03-2018 09:32:42	369d 12h 1m 9s
abarth	UP	10-03-2018 09:33:21	369d 12h 1m 9s
abb	UP	10-03-2018 09:32:32	369d 12h 1m 9s
abbott	UP	10-03-2018 09:33:23	369d 12h 1m 9s
abbvie	UP	10-03-2018 09:33:33	369d 12h 1m 9s
abc	UP	10-03-2018 09:32:59	369d 12h 1m 9s
able	UP	10-03-2018 09:35:21	369d 12h 1m 9s
abogado	UP	10-03-2018 09:33:01	369d 12h 1m 9s
abudhabi	UP	10-03-2018 09:32:59	369d 12h 1m 9s
ac	UP	10-03-2018 09:36:09	168d 11h 47m 31
academy	UP	10-03-2018 09:32:47	369d 12h 1m 9s
accenture	UP	10-03-2018 09:32:38	369d 12h 1m 9s
accountant	UP	10-03-2018 09:35:13	369d 12h 1m 9s
accountants	UP	10-03-2018 09:33:00	369d 12h 1m 9s
aco	UP	10-03-2018 09:33:05	369d 12h 1m 9s
active	UP	10-03-2018 09:33:30	369d 12h 1m 9s

DNS-OARC

Domain Name System Operations Analysis and Research Center