Hot news: dnsperf + resperf

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 ns.dns-oarc.net -p 53
DNS Performance Testing Tool
Version 2.2.1

[Status] Command line: dnsperf -v -s ns.dns-oarc.net -p 53
[Status] Sending queries (to 64.191.0.65)
[Status] Started at: Mon Apr 29 10:44:38 2019
[Status] Stopping after 1 run through file
> NOERROR dns-oarc.net A 0.161037
[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 38, response 46
Run time (s):         0.161095
Queries per second:   6.207517
Average Latency (s):  0.161037 (min 0.161037, max 0.161037)
```
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.
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.
**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.
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.
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.
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."]
  ]
}
```
Now hosting: 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.
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.
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 its members through the use of a small fleet of analysis machines.

<table>
<thead>
<tr>
<th>participant</th>
<th>mbytes</th>
<th>queries_millions</th>
<th># DITL 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>a-root</td>
<td>532,827</td>
<td>10,694</td>
<td>10,694</td>
</tr>
<tr>
<td>afilias</td>
<td>708,960</td>
<td>16,046</td>
<td>16,046</td>
</tr>
<tr>
<td>as112-yow</td>
<td>2,246</td>
<td>57</td>
<td>57</td>
</tr>
<tr>
<td>b-root</td>
<td>152,971</td>
<td>2,729</td>
<td>2,729</td>
</tr>
<tr>
<td>c-root</td>
<td>401,484</td>
<td>10,134</td>
<td>10,134</td>
</tr>
<tr>
<td>cira</td>
<td>56,312</td>
<td>1,218</td>
<td>1,218</td>
</tr>
<tr>
<td>cznic</td>
<td>49,642</td>
<td>1,138</td>
<td>1,138</td>
</tr>
<tr>
<td>d-root</td>
<td>333,263</td>
<td>8,677</td>
<td>8,677</td>
</tr>
<tr>
<td>e-root</td>
<td>223,046</td>
<td>5,027</td>
<td>5,027</td>
</tr>
<tr>
<td>f-root</td>
<td>592,156</td>
<td>17,174</td>
<td>17,174</td>
</tr>
<tr>
<td>h-root</td>
<td>262,623</td>
<td>6,562</td>
<td>6,562</td>
</tr>
<tr>
<td>i-root</td>
<td>518,497</td>
<td>13,263</td>
<td>13,263</td>
</tr>
<tr>
<td>j-root</td>
<td>597,313</td>
<td>12,209</td>
<td>12,209</td>
</tr>
<tr>
<td>k-root</td>
<td>541,347</td>
<td>10,487</td>
<td>10,487</td>
</tr>
<tr>
<td>l-root</td>
<td>616,957</td>
<td>15,721</td>
<td>15,721</td>
</tr>
<tr>
<td>m-root</td>
<td>431,239</td>
<td>7,547</td>
<td>7,547</td>
</tr>
<tr>
<td>nethelp</td>
<td>15,227</td>
<td>293</td>
<td>293</td>
</tr>
<tr>
<td>niccl</td>
<td>21,587</td>
<td>432</td>
<td>432</td>
</tr>
<tr>
<td>switch</td>
<td>28,368</td>
<td>492</td>
<td>492</td>
</tr>
<tr>
<td>tix-or-tz</td>
<td>49</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>wide</td>
<td>16,990</td>
<td>287</td>
<td>287</td>
</tr>
</tbody>
</table>
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.
Check My DNS

Check My DNS is a general-purpose framework for testing DNS resolvers from a client’s 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.
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.