DNS debugging

NSRC
Network Startup Resource Center

Some tips and tricks

- We wish there were some magic tools
  - Well ok, there are a couple…
  - The hardest things in computer science are cache invalidation and naming things – Phil Karlton
  - DNS is about ***naming***, **looking up** and ***caching*** ☺
- We're going to be using `dig` as our "swiss army knife"
  - Available on all UNIX/Linux platforms
  - On Windows as well
    - https://help.dyn.com/how-to-use-binds-dig-tool/#installdigwindows

NSRC
Network Startup Resource Center

dig

- Might not always be installed with the default tools
  - On Debian/Ubuntu, part of `dnsutils`, `bind-utils` on RedHat-ish
  - Lots of information the first time!
  - Let’s walk through a dig session

dnstop

- Very useful as a quick “what’s happening” tool on live servers
  - https://www.cyberciti.biz/faq/dnstop-monitor-bind-dns-server-dns-network-traffic-from-a-shell-prompt/
- Works on authoritative or recursive
  - Or set it up on a mirror port, so you don’t use CPU on your DNS server
    - Also called SPAN port
- Can read traffic directly from the interface, or read a tcpdump pcap file
- Let’s have a quick demo…

zonemaster

- Very thorough tool to debug zone configuration, including nameservers, transport, consistency across nameservers, etc.
- https://zonemaster.net/domain_check
- Used by several TLDs

dnsviz

- Best way to debug your DNSSEC zones
  - https://dnsviz.net
- Let's do a live demo…

tcpdump

- When all else fails, look at the network…
- Look at the packets: `tcpdump -ni eth0 -s 0 port 53`

```
08:13:36.784274 IP 100.100.1.2.36822 > 100.100.3.68.53: 45491+ [1au] NS? grp1.lactld.te-labs.training. (69)
08:13:36.784393 IP 100.100.3.68.16322 > 54.173.126.124.53: 51842% [1au] A? grp1.lactld.te-labs.training. (57)
08:13:36.784710 IP 54.173.126.124.53 > 100.100.3.68.16322: 51842- 0/4/5 (442)
08:13:36.784797 IP6 fdd6:7364:3:64::68.35950 > fdd6:7364:1:128::130.53: 56501% [1au] NS? grp1.lactld.te-labs.training. (57)
08:13:37.161422 IP6 fdd6:7364:3:64::68.21045 > fdd6:7364:1:128::130.53: 33445% [1au] NS? grp1.lactld.te-labs.training. (57)
08:13:37.538060 IP 100.100.3.68.36964 > 100.100.1.131.53: 21557% [1au] NS? grp1.lactld.te-labs.training. (57)
08:13:37.538202 IP 100.100.1.131.53 > 100.100.3.68.36964: 21557 Refused- 0/0/1 (57)
08:13:37.538296 IP6 fdd6:7364:3:64::68.46014 > fdd6:7364:1:128::131.53: 7523% [1au] NS? grp1.lactld.te-labs.training. (57)
08:13:37.538395 IP6 fdd6:7364:1:128::131.53 > fdd6:7364:3:64::68.46014: 7523 Refused- 0/0/1 (57)
08:13:37.538443 IP6 fdd6:7364:3:64::68.8462 > fdd6:7364:1:128::131.53: 36925% [1au] NS? grp1.lactld.te-labs.training. (57)
08:13:37.538534 IP6 fdd6:7364:1:128::131.53 > fdd6:7364:3:64::68.8462: 36925 Refused- 0/0/1 (57)
08:13:37.538577 IP 100.100.3.68.32269 > 100.100.1.131.53: 48682% [1au] NS? grp1.lactld.te-labs.training. (57)
08:13:37.538630 IP 100.100.1.131.53 > 100.100.3.68.32269: 48682 Refused- 0/0/1 (57)
08:13:37.538665 IP 100.100.3.68.15013 > 100.100.1.130.53: 23613% [1au] NS? grp1.lactld.te-labs.training. (57)
08:13:37.538803 IP 100.100.1.130.53 > 100.100.3.68.15013: 23613*- 2/0/5 NS ns1.grp1.lactld.te-labs.training., NS ns2.grp1.lactld.te-labs.training. (181)
08:13:37.538934 IP 100.100.3.68.53 > 100.100.1.2.36822: 45491 2/0/1 NS ns1.grp1.lactld.te-labs.training., NS ns2.grp1.lactld.te-labs.training. (93)
```

NSRC
Network Startup Resource Center

Other things to think about

- Remember that the error isn't necessarily on your end
- Middleboxes, misconfigured firewalls, routing problems
  - All can lead to DNS problems
  - DNS UDP filters, MTU size issues, TCP blocked, …
  - Still quite common to see these even at TLD level!
  - Use these tools to help you identify the problem
- Another useful network debugging tools: mtr

Questions?