Fingerprinting DNS

Roy Arends

Jakob Schlyter

RIPE 47 29-01-2004

Telematica Instituut

WHY

- Troubleshooting DNS problems
- Surveys: distribution of implementations
- Surveys: protocol compliance

Telematica
Instituut

HOW: assumptions

- Bogus data handling is unspecified
- Not all DNS spec is required to do DNS
- Not all DNS spec is implemented appropriately
- Implementations have bugs
- Implementations fixed bugs
- Implementations have features
- Implementations stopped having features

HOW: requirements

- REQUIREMENTS
  - Nothing breaks !
  - Independent of data served
  - Independent of configuration
  - In at least possible queries
  - With at least possible log-entries

HOW: assessment

- 16 bit header, we used 14 for classification
  - QR and Z bit are not used.
- Just header, question section: “.” A IN
  - That’s 16K possible headers (14 bit)
  - Responses tied to queries, tied to IP
- The set of equal {Q =>R} strains must be the same implementation….
- What followed was simple reconnaissance

Telematica Instituut

HOW: reconnaisance

- Finding implementations that matched our strains.
    - Version.bind / version.server / etc / etc
    - Set up local installation. Works well with opensource
    - Asking operators at sites.
- LOTS of help. Thanks Peter, Bill, Brad, Mark, Mans, Miek and Jaap

WHAT:different implementations

- BIND 4/8/9
- NSD
- MS NT/2K/2K3
- MaraDNS
- PowerDNS
- MyDNS
- Nominum ANS/CNS
- NonSequitur DNS
- OakDNS
- UltraDNS
- Simple DNS plus
- Net::DNS::Nameserver
- VGRS ATLAS
- TinyDNS
- QuickDNS
- eNom DNS
- Incognito DNS commander
- Pliant DNS server
- Posadis
- PowerDNS
- Rbldnsd
- TotD

WHAT: still looking

- We finally have the original JEEVES sources.
  - Still busy with emulating PDP-10/tops-20
- Cisco stuff
- (running) BSD-4.3-tahoe/4.4-reno BIND versions.
- New breeds

WHAT not

- What does not help fingerprinting:
- Active Load Balancing
- Firewalls checking queries (checkpoint FW1-NGwAI)
- FORWARDERS
- DoS blocks

Extra’s

- Remember the QR bit we didn’t use ?
  - QR bit (indicating query or response)
- Setting the QR bit in a Query (i.e. sending a response) makes some implementations respond anyway
- The latter can causes query storms between implementations.
- All those implementations have been fixed, check for the latest releases of your software.

SURVEYS

- Bill Manning did a survey on .com
- Mark Lottor did a survey on .in-addr.arpa
- Peter Koch did a survey on .de
- I’ll ask them to put their results online (or post them to a list)

Telematica
Instituut

Where:tool / discussion

- The fpdns tool (version 0.9.0) will be made available some time next week at

  www.rfc.se/fpdns

- There will also be a place for surveys and discussions

Where

- Thanks for listening
- Reach us at roy@dnss.ec or jakob@rfc.se