WELCOME TO RISEUP'S ETHERPAD!

WARNING: this pad is accessible by anyone who has the address to this pad, if you used an obvious name for the pad, it could be guessed.
WARNING: This pad will be DELETED if 30 days go by with no edits. There is NO WAY to recover the pad after this happens, so be careful!

Riseup is a collective providing secure online communication tools for people and groups working on liberatory social change. If you appreciate the tools Riseup provides, please contribute! We rely on contributions by users to exist: https://riseup.net/donate

This is the EtherPad for the DNS Measurements Hackathon!

Official info: https://atlas.ripe.net/hackathon/dns-measurements/#!the-event
https://atlas.ripe.net/hackathon/dns-measurements/#!attendee-information

Mailing list address: dns-measurements-hackathon@ripe.net
IRC channel: #ripeatlas on freenode and/or oftc

Emergencies: Vesna: +31 6 2125 8191

Venue address:
VolksHotel
Wibautstraat 150
1091 GR Amsterdam

Our rooms names: **Beton + vilt** (ground floor)

Schedule Thursday:
09:00 Welcome
09:30 Presentations by RIPE NCC: Logistics,thanks to sponsors, timeline (vesna)
09:40 Round of introductions (All)
* Round of personal introductions (1 minute per person)
* RIPE NCC Projects, Data Sources etc
* Ideas suggestion (2 minutes per person/team/idea)

10:30 Brainstorm & teams-forming
* RE-ARRANGE THE TABLES!!

11:00 - 13:00 WORK on projects (2 hours)
13:00 LUNCH break
14:00 - 19:00 WORK (5 hours)
19:00 dinner in VolksHotel
21:00 - midnight: OPTIONAL - continue working! (3 hours, OPTIONAL)

Schedule Friday:
9:00 arrive & start working
09:00 - 11:00 WORK (2 hours)
11:00 (15 minutes) all: Presenting progress
11:15 - 13:15 WORK (2 hours)
13:15 LUNCH break
14:00 - 17:00 WORK (3 hours)
17:00 wrap-up: presenting final results & planning follow-up steps
17:45 - JURY gathers in a smoke-filled room & comes up with feedback & a "winner" of stroopwafels!
18:00 - closing ceremony
18:30 - LEAVE FOR DINNER
19:00 dinner : De Bekeerde Suster, beer-brewery-restaurant, NieuweMarkt
http://debekeerdesuster.nl Kloveniersburgwal 6 1012 CT Amsterdam 020 423 0112

the Introduction webinar recording is available here: (no, plugin downloadable if you have flash?)

http://meet95212513.adobeconnect.com/p5sih9ji0zx/

Slides are available here:
https://wiki.techinc.nl/index.php/File:Pdf_DNS_Measurements_hackathon_webinar_v1_.pdf

Code released and coded during the hackathon:

- https://github.com/adulau/passive-dns-atlas - Passive DNS collection (and statistics) from RIPE Atlas Sensors
- https://github.com/DNS-OARC/ripe-hackathon-dns-caching - Everything you ever wanted to know about caching resolvers but were afraid to ask
- https://github.com/ripe-dns-anomaly - Anomaly detection, brough to you by the Anomalizers™

Possible projects:

* DNS (root? ccTLD?) server observatory (Emile) (maybe this is multiple small projects that we can bundle together at the end of the hackathon?)
    * take multiple data-sets (RIS, new Atlas DNS measurements, Atlas traceroutes) and see if we can create a public observatory of the DNS root/ccTLD server system. Goal is to provide additional transparency to the lower levels of the DNS server system, and detect anomalies in how users see the DNS server system, so DNS/network operators have an easy interface into how to optimise things for accessing the root name server system.
        * multiple views: a global view , and possibly per-country, per-ASN views?, per-"public resolver provider"?
        * do time series (see https://labs.ripe.net/Members/emileaben/iran-and-k-root-the-rest-of-the-story fig 1 for an example)
        * do time series anomaly detection (giovane) -- anycast catchments are suppose to be very stable (http://www.isi.edu/~johnh/PAPERS/Wei17a.html), what happens when there are anomalies in their the number of probes each site responds? (site offline, ddos, etc).

  Challenge: In Atlas we can't measure actual user-experience (only user->caching resolver, or user-network to authoritative, not user->resolver->auth)

    * (merc) Let's chat about the user->resolver->auth. I've been experimenting with an extension of geodns and the ability to generate custom hashed-timestamped hostnames to cause mostly-unique user->resolver->auth queries and short TTLs resulting in some pretty rich data. From the corporate end, this typically isn't measured since AuthNS is delegated to third-party and cost-per-query becomes a factor.
    * (jerry) I would like to join the chat about user->resolver->auth since I'm working on CheckMyDNS https://cmdns.dev.dns-oarc.net/

  * (Wouter) It would be interesting to keep track of some sort of "state" for a given host (root/ccTLD). When any significant (by some definition) changes occur an event can be triggered. Maybe users can attach actions to these events? (E.g. send an e-mail, post a twitter, feed the dog).

  An event would be a significant change in routing, latency, anycast instance<->user mapping.

  * Automatically categorize events? E.g. localized (an ISP suddenly has poor routing to a ccTLD), global (a ccTLD/root has poor routing to (a part of) the Internet). Impact of the event? (Latency has increased by 0.5s across all measurements -> high impact).

* Root DNS Anycast Map (from Tom Arnfeld, possibly as part of the above?)
    * could use hostname.bind queries as a source of relatively low resolution geo data from some roots?

      There are measurements/maps on the RIPE Atlas website already:
      https://atlas.ripe.net/results/maps/root-instances/
    * find ways to visualise the geographical relationship between Atlas probes and anycast root providers
    * v4 routes vs. v6 routes would be particularly interesting

      (Ricardo) I have been working on that, might be something to talk about ;)
    * are there any obvious inefficiencies in the routes root queries are taking? and why?

* Atlas DNS measurement result streaming to dedicated (key-value, metric) storage backends

by INIGO

* InfluxDB's Telegraf supports customisations (https://github.com/influxdata/telegraf/blob/master/CONTRIBUTING.md) and integrates with plenty of sources (https://www.influxdata.com/integrations)

An input plugin can be written in Go to stream results and store them in influxDB.

Metrics can be made multi-dimensional (not just response latency) by embedding RCODEs as metric labels to be leveraged for querying and presentation

* Elasticsearch' libbeats is, similarly, extensible (https://www.elastic.co/guide/en/beats/libbeat/current/new-beat.html)

A new beat (atlasbeat! :) can be written in Go to stream results and store them in Elasticsearc

* Alternatively, a python application can be written leveraging ripe.atlas.cousteau and elasticsearch-py (Iñigo has a proof of concept for this: https://github.com/ioc32/atlas-es-indexer)

* Bonus nachos if the project delivers a Kibana5/Grafana dashboard!
  * go->redis/influxdb/kafka->logstash/(maybe beats)->elastic is doable and could be finished relatively quickly.
  * If we're ok with a simple hack, go->logfile->filebeat->elastic is super simple and could be accomplished in a day.
    * (merc) I have experience with both items above and am happy to help.
    * (jerry) Beats seem fairly easy to write so I'm happy to help also, would like to get more Go-coding-time in
    * (ulrich) I have written a telegraf plugin before and would like to dive into this further (https://github.com/ulrichwisser/telegraf/tree/master/plugins/inputs/dns_query)
  * (konstantin) Stream data into clickhouse analytics database, column-oriented (https://clickhouse.yandex/)
    * (tom arnfeld) +9001 ClickHouse. Feel free to reach out if you have any questions.

* Zone authority consistency check (from Shane):

I have a small program which checks the serial number of the root zone at each root server every few seconds (or maybe every second?). It tracks the first and last time a serial appears at each server, storing this information in an SQLite database. This can detect how long the zone is inconsistent (not yet updated at every server, or returning different serials from one server).

I'd like to make this more general (so it can be used for any zone), more distributed (right now it just runs on a single server, and I would like to run it from several locations and collate the data), and provide a better UI (right now it just has a curses interface and reports generated from some SQL and gnuplot).

I can give a very short presentation (10 minutes, no slides, showing the code & database & running system) about where it is now at the start if anyone is interested.
(jerry) this sounds like it can be part of the "DNS (root? ccTLD?) server observatory"
What we have so far:

* Modified Shanes original tooling so it spits out json in atlas probe compatible format
* Atlas probe format is now importable into elastisearch and shows graphs
* Atlas output scanner [Tom] that tries to generate the same output as Shane's original tools.
  This enables us to look at the same data from a wider perspective and a longer timespan.
  https://github.com/tarnfeld/ripe-ncc-hackathon-2017
* Shane suggested "it would be interesting to see how these *weird serials* show up in the probe results"
  example: 1997022727 by dns.dnsmadeeasy.com.

* Improve operational excellence with RIPE DNSMON (Stefan Jakob, Manuel Domke (not attending) from DENIC the .de ccTLD provider)
  As a RIPE DNSMON User, we would like to explore ways using the Atlas API

to make our everyday work automated aka easier.
That specifically targets manual analysis of the visually rendered output or crunching the raw API data.

Our goal is to make an intelligent system, that utilizes RIPE atlas data to detect time series anomalies or unusual events. The tool should help to classify the results and support useful alerting.

Some considerable aspects based on response time violations:
* Design should be easy usable by common monitoring tools as item/trigger.
* The influence of a probes dataset on the total result set should be configurable. Design should be able to use/ignore/weigh data sets by pattern to influence result set, e.g. ignore results from probe X. Use default weight per probe and influence result/trigger by probe individual weights.
* Result dependant reports of additional data should be configurable, f.e. provide trace information for all probes violating threshold over given time series. Add proactive data analyis e.g. are there common path attributes like AS or Hop.

Some considerable aspects on path and GeoIP attributes:
* Geo-fence a probe based on "radius" based on probes source IP. Detect probes which show an insane geoIP location. (emile: we've done some research on this, lets talk during the hackathon!)
* Path stability over time, based on trace AS field.
* Path changes over time, based on trace AS fields.

* monitor the availability of DNS resolution for end users (caching resolvers and/or further upstream) (Emile)w

An ISP will have problems if their users can't resolve. We can use RIPE Atlas to monitor this (I've done a prototype of this for a Dutch ISP that had it's caching resolvers under DDoS). Do alerting based on this signal? "How is my probe doing relative to others in the same network?" (see probe dashboard)

* Everything you ever wanted to know about caching resolvers but were afraid to ask (Jeery, Willem, Andrea, Petros, Teemu, Emile)
https://pad.riseup.net/p/hackathon-dns-caching

* BGP Monitoring of anycasted DNS services (Emile)
* (possibly as part of other projects?)
* If we annotate BGP data with geolocation data (from bgp communities), we have much more insight into where we receive anycasted BGP prefixes (much of the root and ccTLD system for instance, but also caching resolvers).
* potential to re-analyse "the Dyn attack" to see how things were re-routed geographically
* hijacks (more specifics in PCH data for instance)?
* (merc) let's talk more about this. Coming from a large website, we were left in the dark about actions being taken during "Dynocalypse" and only had vague information from their RCA. This almost didn't matter as we were running dual-provider nameservers. I can envision a heatmap + time-playback plugin on kibana.

* "Lia's Probe dashboard" (Emile)
* DNS diagnostics for individual ripe atlas probe hosts (learn from internet.nl)
* is your resolver working (under DDoS maybe?) / are you behind something that does DNSSEC?
* education tool for probe hosts?
* "get through 1st-line" support quickly-feature: My atlas probe says this is the problem (saves time for ISPs if we get it right)

* Monitor response time and unanswered queries for DNS servers that are authoritative for

revserse zones (Sofía)
  * Similar to what DNSMON does for high level zones

* Automatically check Reverse DNS Consistency using RIPEstat API (Sofía)
  * Basic tool that daily checks consistency for a set of IP prefixes
  * In case of errors of not found for any sub-prefix, inform which is the prefix/sub-prefix that presents problems

* Integration DNSMON/Atlas into existing Threat Intelligence Platform like MISP (Alex CIRCL)
  * Many DNS measurement or collection are also interesting for security analysts.
  * Providing additional DNS measurement in addition to existing Passive DNS to better support an investigation.
  * Extending MISP modules https://github.com/MISP/misp-modules - https://github.com/MISP/MISP
    * Atlas measurement API
    * RIPEStat API

* Reviewing existing Passive DNS Internet-Draft to review compatibility with existing Atlas/DNSMON format (https://datatracker.ietf.org/doc/draft-dulaunoy-dnsop-passive-dns-cof/) (Alex CIRCL)

* Are DNS measurement done by others accessible via the Streaming API (beside the ? To use it as a way to feed Passive DNS collectors (Alex CIRCL)
  * At least I can test the streaming import in ardb(https://github.com/yinqiwen/ardb) along with the geolocation of the sensor.
  * Works via streaming API - https://atlas.ripe.net/docs/result-streaming/ (thanks to Chris)

* "DNS map" - probably as a part of one of the above (Maciej A.)
  * a tool to visualise root/ccTLD reachability (RTT, AS Path) from different countries, ASes, ...
  + an extra feature that after providing data about "real" DNS traffic (i.e. observed on a root/ccTLD servers) would suggest the best location for DNS servers (in terms of RTT, AS path, ...)

* Visualisation of DNSSEC deployment (Maciej A.)
  * use probes' local resolvers to query for DNSSEC-secured domain names (signed using various cryptosystems) and:
    * visualise support for various DNSSEC algrithms (per resolver/proble AS, country,...)
    * check wherther the end-user is indeed DNSSEC-secure (e.g. all the DNS resolvers configured for a probe perform DNSSEC validation)

(Jerry) I did a test measurement and saw that there are a bunch of probes configured to use public resolvers that aren't in it's own network and you don't easily see if the home router is configured the same, need to get figures on this before doing it so you can actually say that it's a good representation of how users see it (need to remember that it's mostly tech ppl running probes that more likely poked at every setting)

(willem) I vaguely remember probes tell if the resolver came from dhcp? Not completely sure; let's check. They don't.

(jerry) from my (first) atlas measurement from 50 probes / 82 results: 19 are google and 34 are localnet; here are some more data abuout it: http://www.dns.pl/dnssec/ecc_support_in_dns_resolvers.pdf (current as of Jan 2016)

* DNS censorship visualisation (Maciej A.)
  * use probes' local resolvers in order to detect:
    * distinctive answers to queries for popular domain names (e.g. RFC6890 - Special-Purpose IP Address)
    * "public DNS resolver" hijack (e.g. something like: `dig whoami.akamai.net +short @8.8.8.8 | xargs whois`)
    * NXDOMAIN redirection

READ: https://labs.ripe.net/Members/kistel/ethics-of-ripe-atlas-measurements

READ: https://labs.ripe.net/Members/stephane_bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes

Google DOC: https://docs.google.com/document/d/1p_41YKmVBJYG-oFtSQuW3lTjIFISjQf7ywnjVe4_fmY/edit?usp=sharing

Slides: https://docs.google.com/presentation/d/1nooCcB_Jv1CxKQT4K7g7fyN05FfiAmw8h3yidxc7U-U/edit?usp=sharing t

* (Willem) Resolver properties and capabilities.
  * As mentioned above in previous proposals already, RIPE Atlas probes have a very nice inside perspective on resolvers in the networks where those probes are. What are the properties and capabilities of those resolvers.

    (Jerry) See my note above on user probes

    (willem) I saw your comment. Maybe it doesn't matter. I know how the big public resolvers respond, It's the other ones that I'm interested in... Also, isn't the origin of the upstream resolver (dhcp or manual entry) in the probes data?

    (jerry) if you dont specify target it will use the probes configured resolver and there is IPs in the result data so you see who answered

    (willem) What about the probes information... so not the result data, but the query for the probe ID.

    Just checked... so it is not in there.

    This hackathon is about giving feedback too. This would be a nice addition. Indicate the origin of the resolver.

    * The IP on the remote end whoami.akamai.net or o-o.myaddr.l.google.com. to inventory the resolver AS'es
    * DNSSEC capabilities
      * Is it validating? (Can we compare with APNIC Google-ad measurements at https://stats.labs.apnic.net/dnssec)
        * Which algorithms can be validated. I know Olafur has a matrix of domains at cloudfare which can be used to test this. He targeted it with his hackathon project in Prague I think... I could check.
      * If not validating, is the provided data usable by a validating stub?
        * Are signatures given?
        * Is valid proof for non-existant answers given?
        * Is valid proof for wildcard answers given?
    * Can it resolve IPv6-only domains / Qname minimisation / TCP support (Jerries cmdns things)

      (Jerry) This really requires a controllable authority to test against, it is possible to integrate Atlas with CheckMyDNS but that's going to be more work then what fits within the hackathon

      (Willem) So I know the anchors serve some domain names for testing PMTU. Perhaps they could be equiped with more dynamic authoritatives as well (for example that echo the contacting IP, or that detect qname minimisation).

      * Yes Jerry, I think we have some of those authorities with internet.nl too... let me check.

        I cannot find it now, I have to ask Ralph again, but we do have queries you can do to test for

        qname minimisation... dig qnamemintest.internet.nl TXT

        (jerry) did a quick measurement, 3 out of 795(500 probes) had qname minimization :)

        Wow! That's not bad!

        I know! Was expecting zero :) maybe I hit all of Stephane's probes :)
    * Are fragmented responses accepted/reassembled (with IPv4 and IPv6)
    * What is the maximum path MTU
    * etc.

* (Willem) Measuring the DNS measurements.
  * Process past measurements on RIPE Atlas.

    Who did them, what did they query, what were the results?

    Can we create a passive DNS database from it?

    How much of the DNS tree can be reconstruct?

Possible Wednesday Social:

It's a tradition to visit a local hackerspace, and one of them has an "open evening" / "Social Event" every Wednesday:

https://wiki.techinc.nl/index.php/Social:2017-04-19

When: 19:00
Where: Technologia Incognita
ACTA Broedplaats
Louwesweg 1
1066 EA

https://wiki.techinc.nl/index.php/ACTA#How_to_Get_Here

Vesna: Adding random notes, to be used later for documentation
https://pad.riseup.net/p/hackathon_dns_anom
: https://docs.google.com/document/d/1p_41YKmVBJYG-oFtSQuW3lTjIFISjQf7ywnjVe4_fmY/edit?usp=sharing

https://github.com/adulau/passive-dns-atlas

https://medium.com/@dominikus/the-superpower-of-interactive-datavis-a-micro-macro-view-4d027e3bdc71

http://system.opendns.com

https://github.com/ioc32/atlas-es-indexer

https://atlas.ripe.net/docs/built-in/

https://github.com/tarnfeld/ripe-ncc-hackathon-2017

https://t.me/joinchat/AAAAAAzBVkPfsqmH0qGu3g

@StroopwafelW Authentic Dutch Stroopwafels in tin, Stroopwafel Liquour, stroopwafel tea and Dutch Food.(http://www.stroopwafelworld.com/en) Also in bulk available.
Amsterdam, The Netherlands
stroopwafelworld.com/en
https://9gag.com/gag/aAdO6Q0?ref=t

Quote => You might like my website: http://www.stroopwafelworld.com Would be nice if you want me to be your partner for the hackathons :).

Emile: adding random notes:

- feature request (wouter) UI to have cloning of measurements
- https://atlas.ripe.net/api/v2/measurements/5001 (paris ID = null ?!)

Beer:

- https://www.google.nl/maps/place/Proeflokaal+Arendsnest/@52.375438,4.8883896,17z/data=!4m5!3m4!1s0x0:0x782e79a7c72de1c4!8m2!3d52.3767343!4d4.8893002
- https://www.google.nl/maps/place/Beer+Temple/@52.3757613,4.8866712,15.97z/data=!4m2!3m1!1s0x47c609c14a6680df:0x643f005113531f15?hl=en

Oh, beer ;-) Let me add some alternative ones ;-)
http://butchers-tears.com/

The *actual* monastery : **brouwerijkleiburg.nl/**
http://amsterdambreweries.com/breweries/kleiburg/

Windmill!! brouwerijhetij.nl/?lang=en

Squat: http://villafriekens.nl/

Amsterdam noord: The Oedipus Brewing Taproom, Gedempt Hamerkanaal 85,
1021 KP AMSTERDAM

The one where our dinner on Friday will be: http://debekeerdesuster.nl

Pubs, near VolksHotel:
BierTuin http://www.debiertuin.nl/linnaeusstraat/index.html
SmokinBarrels http://www.smokinbarrels.nl/menu/20170201-SB-Drinks-web.pdf
Drovers Dog http://drovers-dog.com/dog3/ Wibbautstraat 206 / 020 2213744

Shop: BeerKoning: bierkoning.nl

etc: http://amsterdambreweries.com/
http://www.10best.com/destinations/netherlands/amsterdam/nightlife/brew-pubs/
http://www.iamsterdam.com/en/visiting/what-to-do/eating-and-drinking/bars-and-cafes/beer-sampling-in-amsterdam/best-craft-and-speciality-beer-bars