

**DNS, esa “cosa” que anda...
(hasta que no) ...**



Quienes somos:

Pablo Carboni (pcarboni@gmail.com) @pcarboni

DevOps @Modernizacion, padre, y cosas raras: RegExp, protocolos nivel bit, leo RFCs, parches *BSD/Linux, asm x86, etc.

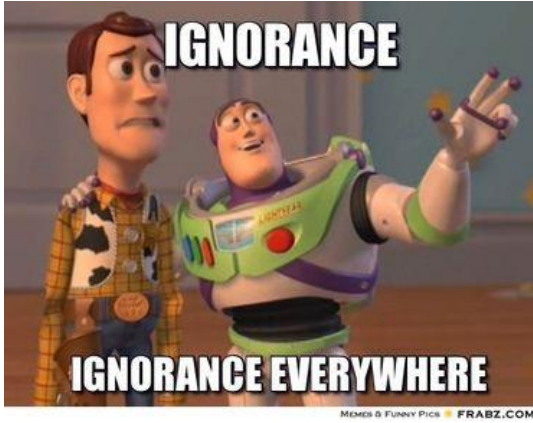
Eduardo Casarero (ecasarero@gmail.com) @jedux

Sysadmin @Percona, CM y N° 2½ de @sysarmy, “Arruino todo”™

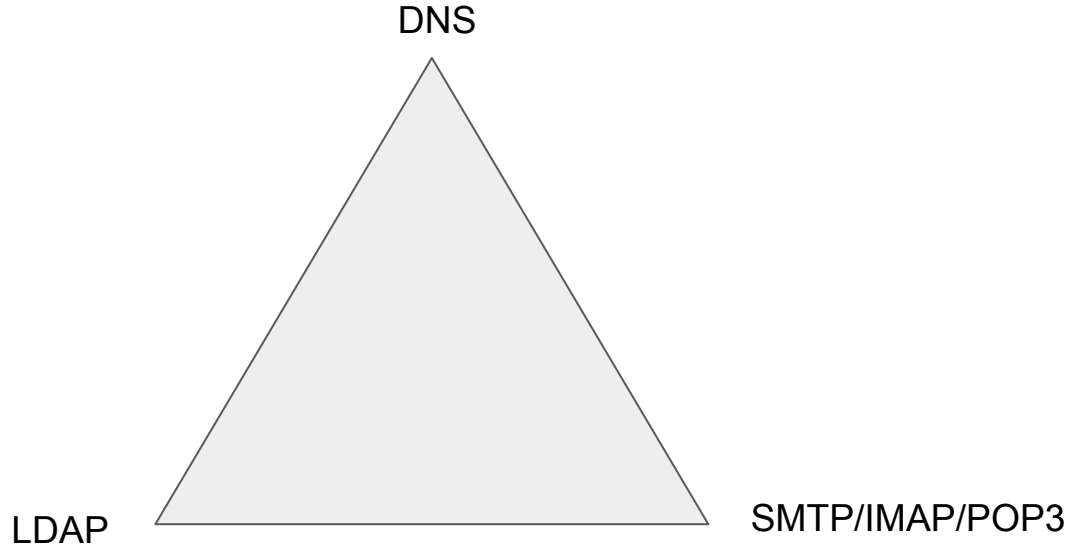
Avisos varios...

- Por razones de tiempo, no incluimos DNSSEC ni DNS en IPv6.
- Elegimos los peores gráficos que pudimos encontrar.
- Por el momento no hay vulnerabilidades nuevas graves de SSL o BIND, verificaremos si sigue así al final de la charla.

Triángulo de la ignorancia



(viejos protocolos pero aun vigentes, y que cada vez menos se conocen en detalle)



Cuencos tibetanos armonizadores de chakras



Para pensar y compartir después...

Recuerdan el momento y cuál fue el primer problema de DNS que tuvieron en sus vidas?

Hi, my name is Bob, and I have DNS issues.



Ejemplo #1: Lame delegation + baja inadvertida de dominio en servidor recibiendo delegación

Lo que puede fallar a causa del DNS:

En una jugada podemos romper:

- www,
- mobile(red celular),
- apps,
- emails,
- servicios varios,
- smart phone,
- hasta IoT!
- botnets

D'oh!



¿Quién/es usan el DNS y para qué sirve?

- Lo usan computadoras, servicios o cualquier otro dispositivo conectado a internet (skynet, mirai)
- Asocia info variada con nombres de dominio asignados a c/u de las entidades participantes, por ejemplo servicios de mail, msg, telefonía.
- Traduce fácilmente nombres memorizados de dominio a direcciones IP numéricas.



DNS: ¿Cuál es su (no aburrida) historia?

- El archivo de la muerte “hosts.txt” (o similar), usado y mantenido por Jon Postel en una universidad, se transformó en inmantenible por su tamaño y su carácter de centralizado...

```
➔ ~ wc -l /etc/hosts
42000000000000948584 /etc/hosts
```

- El “Domain Name System” se pensó en un principio para soportar el crecimiento de las comunicaciones vía e-mail (ARPANET). Luego empezó a soportar Internet a escala mundial.

The conclusion in this area was that the current "user@host" mailbox identifier should be extended to "user@host.domain" where "domain" could be a hierarchy of domains.

- J. Postel; *Computer Mail Meeting Notes*, [RFC 805](#); 8 Feb 1982.

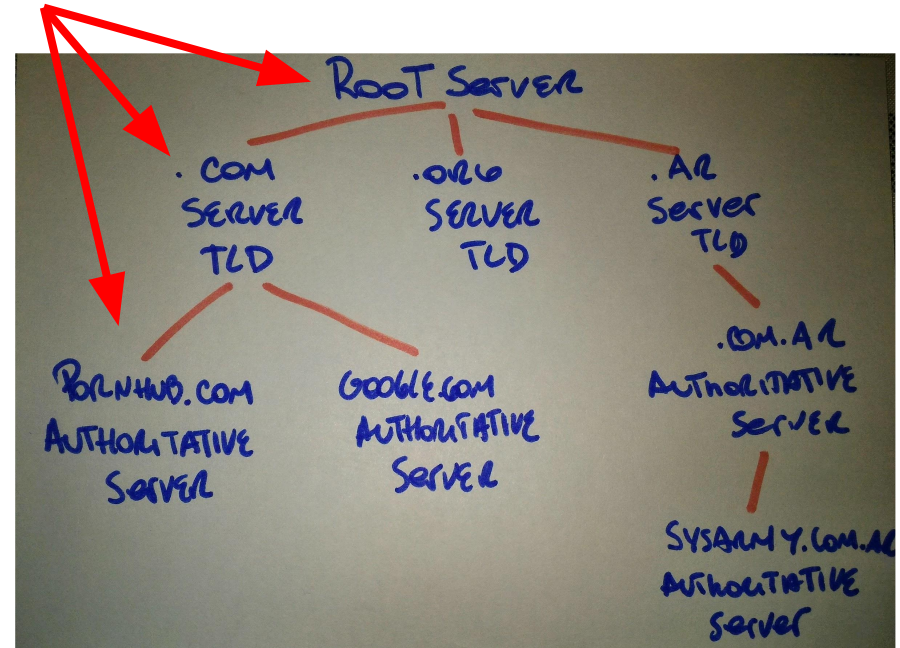
DNS autoritativos

- Jerárquico de arriba hacia abajo. Se lee(interpreta) de derecha a izquierda, incluyendo el punto final, “zona root”.

nada.masomenos.bastante.mucho.

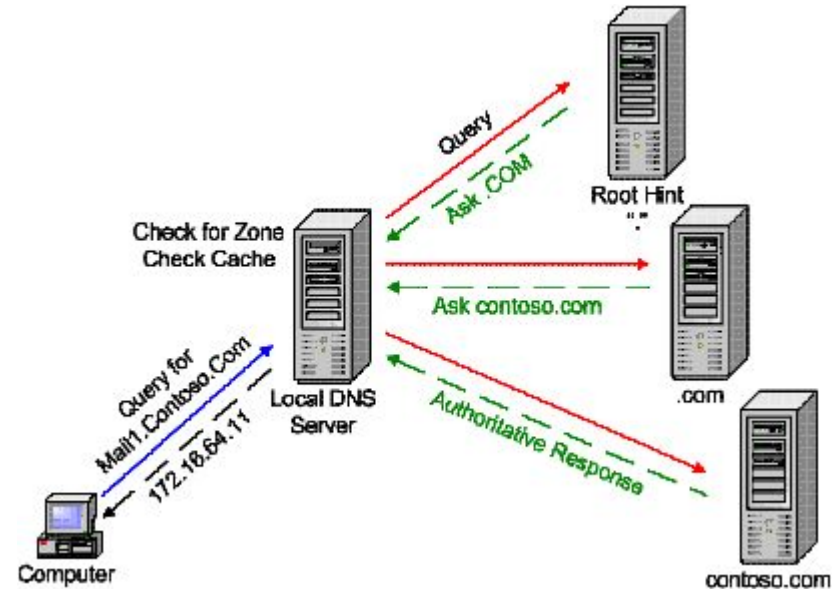
- Están los root servers (hay un mirror en cabase). Luego están los “normales” (con nombres)
- Los Root server son lo unico “hardcoded” en los servers.
- BIND, NSD, PowerDNS y otros

DNS Server(s)



DNSes Recursivos

- Lo usan los clientes de DNS (PCs, cell phones, IoT, servers) para consultar nombres y servicios.
- Se basa en la jerarquía del slide anterior.
- El servidor de dns recursivo, 'pasea' por la misma haciendo preguntas (queries) para llegar a la respuesta que se está buscando.
- El paseo finaliza cuando el último autoritativo responde con los datos de si mismo y el registro deseado.



- BIND, Unbound, PowerDNS Recursor y otros

Registración de dominios.

La registración de dominios, implica que queden configurados en los CCTLD (Country Code Top Level Domain) de cada país, y esto es muy dependiente de sus leyes.

En la gran mayoría de los casos, tener dominios cuesta \$\$\$, pero no siempre esto es así. Organizaciones como gobierno, militar, educativas, y otras, a veces lo tienen de forma gratuita.

En Argentina, la entidad que regula la actividad, es “NIC.AR”, <http://www.nic.ar>.


Tenemos dominios como: .com.ar y .net.ar (comerciales), .org.ar, .gov.ar/.gob.ar, .mil.ar, .edu.ar, .tur.ar, .uba.ar, y otros.



Domain name registration: If you have cash...

Algunos TLD (Top Level Domain) se convirtieron con el tiempo para uso comercial. Particularmente, nombres “a pedido”

https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains



New Generic Top-Level Domains

ICANN

ICANN

APPLICANT GUIDEBOOK

CUSTOMER PORTAL



CUSTOMER SERVICE

About

Applicants

Program Status

News & Media

NEW GTLD AUCTION RESULTS

Search

Reset

You can enter date, eg. 2014-05-21, 21 May 2014 or 05/21/2014

Auction results are listed below. Only contention sets that resolved through Auction are included. This page will be periodically updated within seven (7) days after an Auction or update in status.

Information about the Auction process, Auction proceeds or additional contention set status' can be found on the Auctions page, Auction proceeds page or Contention Set Status page, respectively.

String	Contention Set Number	Auction Date	Application ID	Winning Applicant	Winning Price
WEBS	233	27 July 2016	1-1033-73917	Vistaprint Limited	\$1
WEB	233	27 July 2016	1-1296-36138	NU DOT CO LLC	\$135,000,000
SHOP	229	27 January 2016	1-890-65213	GMO Registry, Inc.	\$41,501,000
APP	39	25 February 2015	1-1138-33325	Charleston Road Registry Inc.	\$25,001,000
TECH	20	17 September 2014	1-1670-76346	Dot Tech LLC	\$6,760,000
REALTY	112	22 October 2014	1-1913-14988	Registry, LLC	\$5,588,888
SALON	28	22 October 2014	1-1618-18834	Outer Orchard, LLC	\$5,100,575
BUY	16	17 September 2014	1-1315-53217	Amazon EU S.à r.l.	\$4,588,888

Tipos de registros.

- Indican qué tipo de información estás buscando.
- **NS** (Name Server - delega autoridad a otro DNS autoritativo)
- **A/AAAA** (Address) - Enlista la(s) IPv4 / IPv6 asignada(s) a un host
- **MX** (Mail Exchanger) - Servidor(es) asignados para recibir mails.
- **SOA** (Start Of Authority) - Indica servidor primario, numero de serie, datos de expiración, y otros en relación a la zona.
- **TXT** (SPF, DMARC, tokens, versiones) - Devuelve texto.
- **SRV** (voip, mobile, xmpp, etc.) - Informa servidor(es) que prestan servicio(s)
- **NSEC/NSEC3/DNSKEY/RRSIG** -> de uso en DNSSEC
- Etc :)

Cómo usan el dns los rusos:



→ ~ dig nix.ru TXT

;; QUESTION SECTION:

nix.ru. IN TXT

;; ANSWER SECTION:

nix.ru. 3600 IN TXT

nix.ru. 3600 IN TXT

"IT dep. +7 (495) 974-3333"

"v=spf1 mx a ip4:91.233.230.4 -all"

Otros usos comunes.

- Spotify usa SRV para que el cliente sepa a donde conectarse:

```
➔ ~ dig +short _spotify-client._tcp.spotify.com SRV
10 10 4070 ap.gslb.spotify.com.
```

- RBLS
- Hash databases
- Calculadora

```
➔ ~ dig @dns.postel.org 2.10.add.calc.postel.org +short
0.12.0.0
```

- Mapping an IP address or prefix to a corresponding BGP Origin ASN :

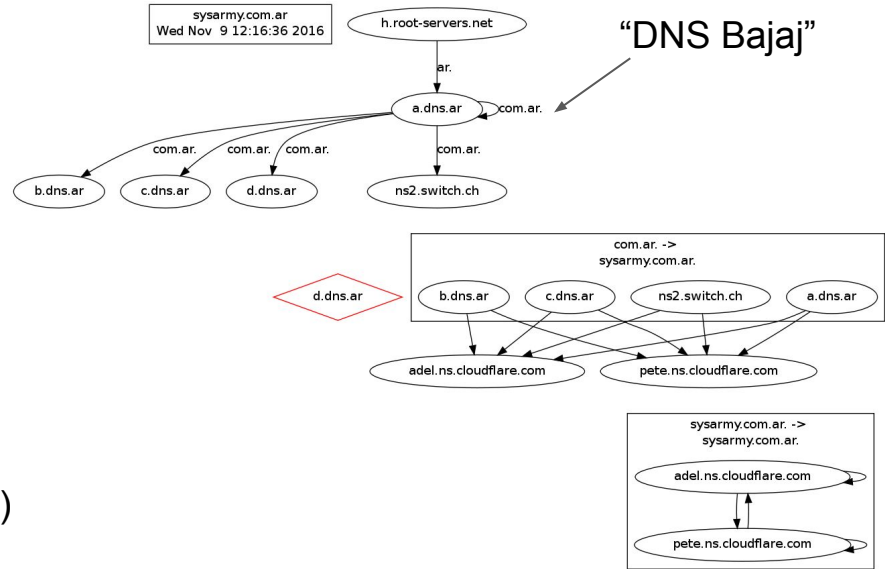
```
➔ ~ dig 31.108.90.216.origin.asn.cymru.com TXT +short
"23028 | 216.90.108.0/24 | US | arin | 1998-09-25"
```

- Getting external IP address via DNS

```
➔ ~ dig myip.opendns.com @resolver1.opendns.com +short
175.45.176.1
```

Toolset para recursión:

- CLI: dig +trace (bind), drill -T (unbound)
- Web - Gráficas: DNS Bajaj
- Web - Texto: dnsstuff, dig web y otros...



Links útiles:

<http://zonecut.net/DNS> (DNS Bajaj)

<http://www.dnsstuff.com/tools> (DNS stuff)

<https://www.digwebinterface.com/> (Dig web interface)

<http://dns.measurement-factory.com/tools/dnstop/>

Don't DO IT !!!

Error común, que es válido pero NO recomendable:

- Que en el DNS responda queries autoritativos y recursivos, en el mismo puerto, y en la misma IP.
- Se hace difícil separar servicios, que tengan QOS, y por supuesto, SEGURIZARLOS!



Dispararse en el pie: round 1

Caso típico: poner TTL muy bajo (0-5s).

Con esto se expiran los caches rápidamente, aumentando considerablemente las consultas a los DNS recursivos, y por supuesto uso de CPU y BW.



Dispararse en el pie: round 2

Caso: Olvidarse de renovar el dominio.

Y que te lo registre otra persona...

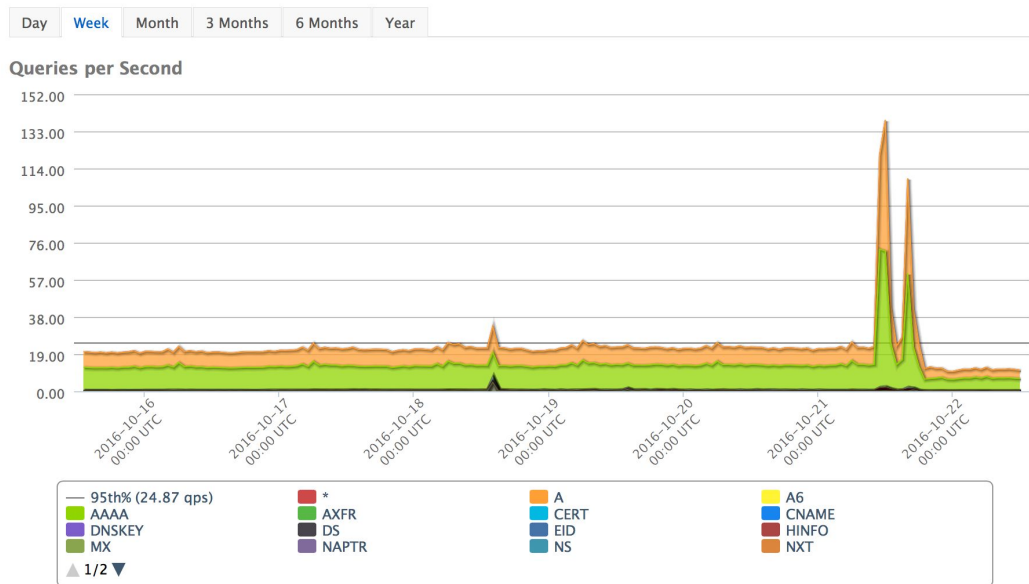
2016: existe el calendar y el registrar suele mandar emails avisando con tiempo que se vence.



Dispararse en el pie: round 3



Caso: No tener AAAA records y tener que pagar por algo que no tenés.



Dispararse en el pie: round 3

Caso: Abrir el firewall solo para udp/53 y no tcp/53

TCP is used if the **size of the packet goes over 512 bytes**. Practically this is only used for **zone transfers**.

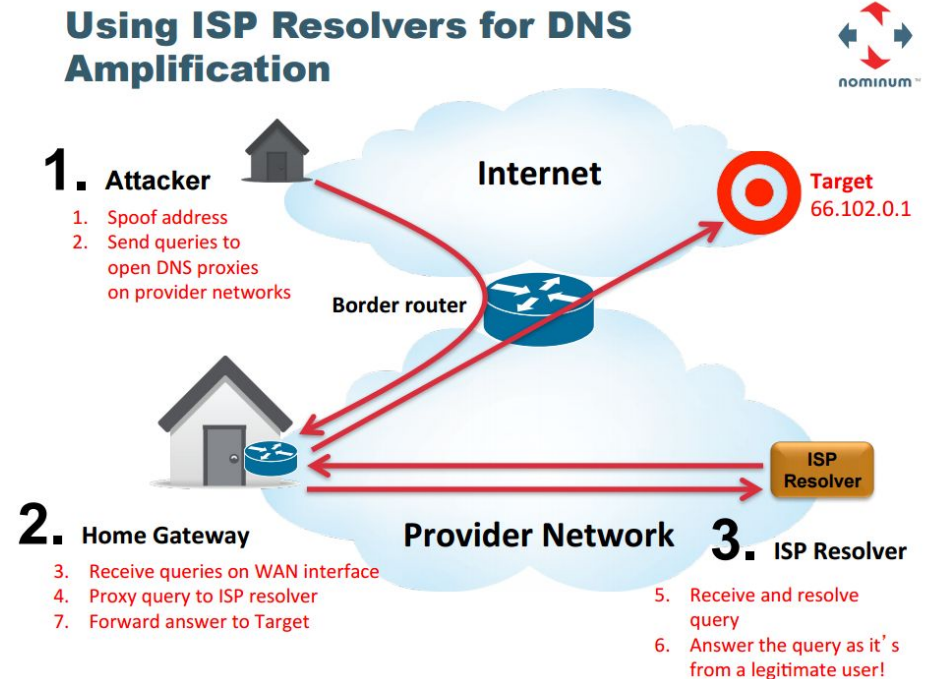
Ataques y abusos más comunes:

- Open resolvers: DNSs recursivos que no tienen configuradas ACLs adecuadas para su uso.
- Bugs en software. El Bind(ISC) es un típico ejemplo de viejas épocas.
- Bugs por naturaleza del protocolo en sí:

Cache poisoning (Glue Records): En las respuestas a los queries, en la info incluye “adicionalmente”, registros intencionalmente fake(attacker) reemplazando los del cache por estos. Sucede en servidores que no hacen chequeos necesarios únicamente. DNSSEC evita este tipo de ataques firmando zonas, registros, etc.

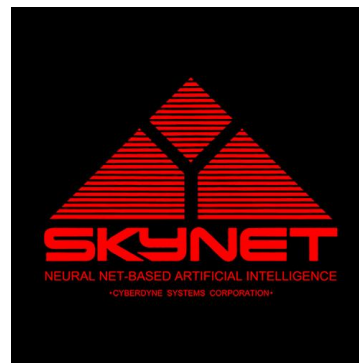
Ataques más comunes(cont.)

- DDOS amplificado: Ataque distribuido a gran escala, usando botnets, empleando además IP spoofing, y como consecuencia “amplificando” respuestas, y consumiendo mucho BW. Se efectúan queries con respuestas “grandes” (64KB - Ej: registros de DNSSEC). Usar URPF/BCP38, Como último recurso, rate limit.



Ataques de importancia (últimamente)

- Hace algunos meses (Sep' 2016) llamó la atención porque consumió 1 terabit p/s. Esto NO fue generado por botnets de PCs. Esto fue generado por dispositivos conectados a Internet (IoT) y una vulnerabilidad, "user y pass por default" explotada por un malware, "Mirai", afectando más de 145.000 cámaras IP.
- El pasado lunes 7/Nov, al menos 2 casas en Finlandia se quedaron sin agua caliente ni calefacción. ¿Motivos? DDOS que saturaron la red en los equipos del proveedor de dichos servicios, haciendo que se rebooten cada 5' los controladores.



¿Preguntas?