DNS nézőpontok

Pásztor Miklós

2014. április, Pécs

Tartalom

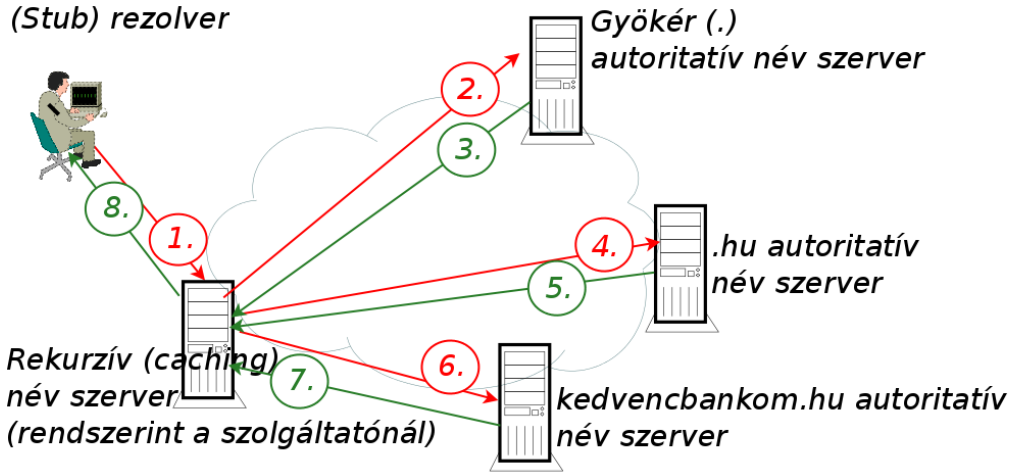
(Pécsett, a Networkshopon 2014-ben elhangzott előadás bővített változata.)

1. Bevezetés

Az internet DNS egy osztott, hierarhikus adatbázis internet nevek tárolására. Elsősorban arra szolgál, hogy **nevekhez** IP címeket rendeljünk. A protokollt még az internet kezdeteinél, 1984-ben alkották meg. Nem csak IP címek, hanem számos egyéb domain nevekhez köthető információ tárolható DNS rekordokban. Sokáig egy-egy DNS kérdésre adott válasz független volt attól, hogy honnan, az internet milyen környezetéből tettük fel a kérdést. Manapság egyre gyakoribb, hogy a DNS válasz, amit kapunk függ a **kérdezőtől** is: más-és más választ kapunk attól függően, honnan **nézzük** a DNS-t. Beszélhetünk tehát DNS nézőpontokról. Ez az írás ismertet néhány jelenséget, okot, ami indokolhatja a nézőpontok különbözőségét, és bemutat néhány eszközt, amivel az ilyen manipulálásokat bevezethetjük, kezelhetjük, másik oldalról viszont felfedezhetjük és kikerülhetjük.

1.1. Az internet DNS

A továbbiak megértéséhez szükséges tudni, hogyan is működik az internet DNS. A feloldás folyamatában a **stub rezolver**, **rekurzív névszerver** és az **autoritatív névszerverek** vesznek részt. Az alábbi ábra szemlélteti a folyamatot:



1. www.kedvencbankom.hu ?
2. www.kedvencbankom.hu ?
3. Nem tudom, de itt vannak a .hu név szerverei!
4. www.kedvencbankom.hu ?
5. Nem tudom, de itt vannak kedvencbankom.hu név szerverei!
6. www.kedvencbankom.hu ?
7. www.kedvencbankom.hu A rekordja: 111.22.33.44 (autoritatív válasz)
8. www.kedvencbankom.hu A rekordja: 111.22.33.44 (nem autoritatív válasz)

A feloldás egyes lépéseit itt nem fejtjük ki, arról sok helyen lehet olvasni, például itt.

2. Jelenségek

2.1. Rosszindulatú DNS nevek

Gyakran eleve rosszindulatú tevékenység számára jegyeznek be egy-egy DNS nevet. A bejegyzett nevet használhatják aztán például fertőzött kód terjesztésére, vagy warez szolgáltatás számára. Botnetek (fertőzött gépek távolról irányított nagy halmaza) is használnak DNS-t, hogy a vezérlő (C&C, Command and Control) szervert elérjék. A Conficker nevű rosszindulatú kóddal fertőzött gépek például napról napra más

és más véletlennek tűnő karaktersorozatokat tartalmazó DNS neveken keresték a C&C szervert. Például 2009. június 30-án a `.hu` alatt ezeket: `ckgtkln.hu, limu.hu, skog.hu, wbox.hu`. A Conficker „gazdái" persze próbáltak gondoskodni arról, hogy a kiválasztott domain nevek a megfelelő napon az ő kezelésükben legyenek. Az a gép, ahol a C&C szerver működik rendszerint szintén fertőzött gép, nem közvetlenül a támadó birtokában levő eszköz. A botnetek gazdái sok szervert is birtokba vesznek, és magát a DNS bejegyzést is gyorsan váltogatják, így egy-egy C&C proxy szerver pár percig működik csak, a feladatát átadja egy következőnek. Az ilyen, gyorsan változó, fertőzött gépekre mutató DNS bejegyzések a **fast-flux** nevek. Paul Vixie szerint az új DNS bejegyzések túlnyomó része évek óta rosszindulatú tevékenységet szolgál.

Érdemes tudni, hogy a `.hu` alatt nem jellemzők az ilyen nevek a szigorú regisztrálási feltételek miatt.

2.2. NXDOMAIN hijacking

NXDOMAIN hijacking az a jelenség, amikor a „nincs ilyen rekord" (NXDOMAIN) válasz helyett valamilyen hamis választ kapunk, gyakran pl. olyan IP címet, aminek web szerverén reklámokat találunk. A rekurzív és az autoritatív névszerverek is élhetnek ezzel. Az NXDOMAIN hijacking azért is veszélyes, mert nem csak a web használ DNS-t, hanem sok más szolgáltatás, amik kárát látják annak, hogy hamis válaszokat kapnak. Nevezetes a Verisign 2003-as esete: a böngészőkben minden nemlétező `.net` és `.com` név helyett reklámokat láthattak a felhasználók. Hatalmas közfelháborodás után megszüntették ezt a gyakorlatot.

2.3. Cenzúra

Akiknek módjukban áll befolyásolni a hálózati forgalmat, a DNS szervereket, azok dönthetnek úgy, hogy manipulálják a DNS válaszokat. Munkahelyünk dönthet úgy, hogy bizonyos DNS neveket szűr: például az internetes újságok nem, vagy csak 18 óra után érhetők el egy-egy munkahelyi hálózatból. Ez a szűrés megoldható DNS alapján. Vannak bíróságok/hatóságok, akik egy-egy DNS név eltávolítását rendelik el autoritatív névszerverből, vagy rekurzív névszerverekből. Amerikában sokszor előfordul, hogy az FBI vagy bíróság rendeli el egy-egy DNS név, vagy a név-fa egy ágának ideiglenes, vagy végleges megváltoztatását. Az FBI szüntette meg a dvdcolletcs.com vagy a Silkroad nevű főleg kábítószerkereskedésre használt webhelyet. Amerikai bíróság rendelte el 2012-ben a 3222.org, vagy 2014-ben a no-ip.com domain nevek lefoglalását.

Persze sokat lehet vitatkozni azon, hogy a DNS cenzúra általában, vagy egy-egy konkrét esetben mennyire megalapozott erkölcsileg és jogilag, azonban ez nem tartozik ebbe az írásba.

2.4. Alternatív DNS szolgáltatók

Rekurzív DNS szervert általában a szolgáltatónk, munkahelyi hálózatunk ad. Nagyon sok IP címen működik azonban olyan DNS szerver, amit használhatunk alternatívaként – feltéve, hogy valamilyen tűzfal nem szűri ezt a forgalmat. Neves cégek is adnak ilyen szolgáltatást. Néhány példa:

- `8.8.8.8, 8.8.4.4` (Google)
- `4.2.2.1` (Verizon)
- `208.67.222.222` (Opendns)
- `185.16.40.143` (OpenNic)

Jó tudni, hogy ezek is gyakran „hazudnak". Például az OpenDNS „veszélyes" DNS neveket szűr és NXDOMAIN hijacking-et alkalmaz. Ez lehet kívánatos számunkra, de lehet, hogy éppen nem az. Érdemes tájékozódni, figyelni. Az Opennic alternatív DNS root-ot használ: a gyökér zónából átveszi a top level domain-okat, de olyan top level domain-okat is szolgáltat, amik nincsenek benne az „igazi" gyökér zónában. Ez szintén valakinél előny, valakinél hátrány lehet. Az alternatív DNS szolgáltatóknak sok gyűjtőhelye található meg a hálózaton, például itt.

2.5. 2014. március: török cenzúra, routing

Törökországban először csak a rekurzív DNS szerverekben hamisították a „veszélyes” DNS neveket. A felhasználók válaszul pl. a `8.8.8.8` IP címet használták rekurzornak. Ezt felfedezve a hatóságok nyomására a szolgálatók a gyakran használt rekurzor IP címeket routing segítségével **eltérítették**. Stephane Bortzmeyer kiderítette, hogy valójában a `195.175.255.66` török címen működő DNS szerver válaszolt az eltérített DNS üzenetekre.

Érdemes tudni, hogy a `whoami.akamai.net` név mindig a rekurzív névszerverünk IP címét adja vissza. Pl. a PPKE hálózatán:

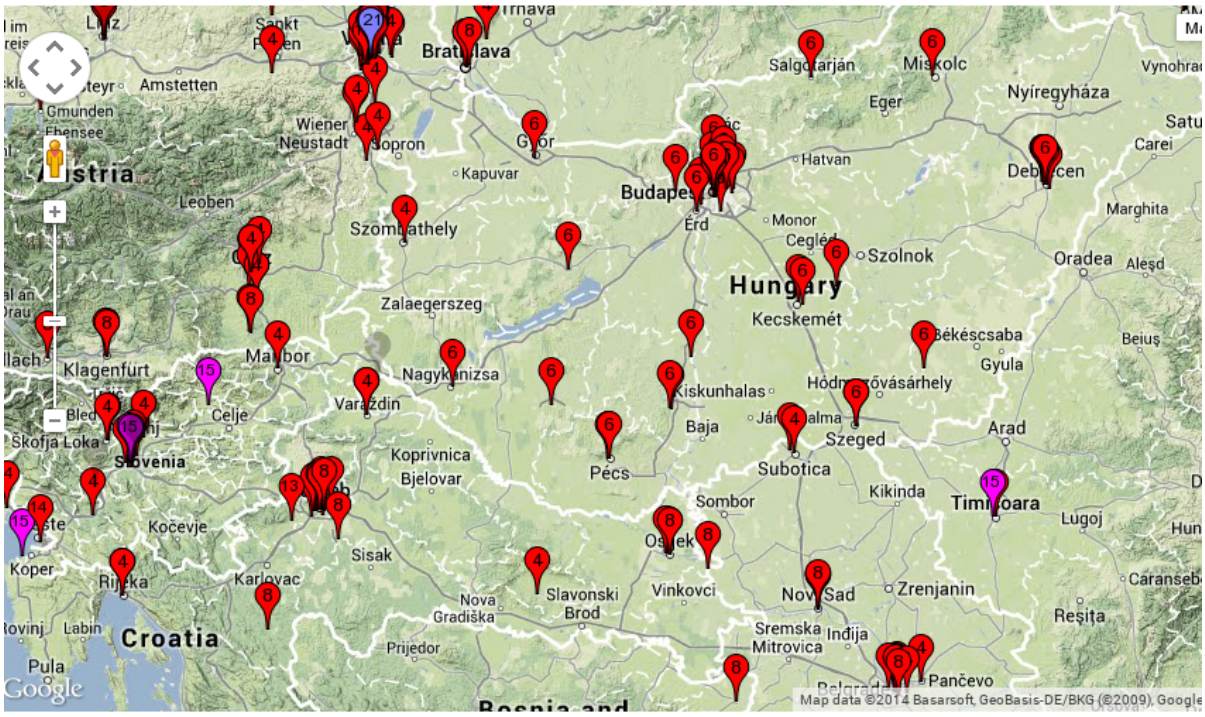
```
%dig +short whoami.akamai.net
193.6.21.45
```

3. Manipulálás a routerekben

3.1. Anycast: máshol látjuk ugyanazt

Amikor a gyökér névszerverek közül pl. a `k.root-servers.net` gépet, annak IP címét (193.0.14.129) kérdezzük, akkor más és más géptől, más és más helyről kapjuk a választ, attól függően, hogy hol vagyunk. Ezt az anycast technológia teszi lehetővé: a 193.0.14.129 címet több helyről több hálózat is hirdeti BGP-vel. Ma már több száz root névszerver szolgáltatja a gyökér zónát. Bővebb információ: `http://root-servers.org/`

A `k.root-servers.net` egy példánya 2005. óta az ISZT hálózatán, Magyarországon van. Az alábbi ábrán a „6”-os cseppek mutatják azokat a Ripe Atlas figyelőpontokat, ahonnan ezt a példányt használják a felhasználók.



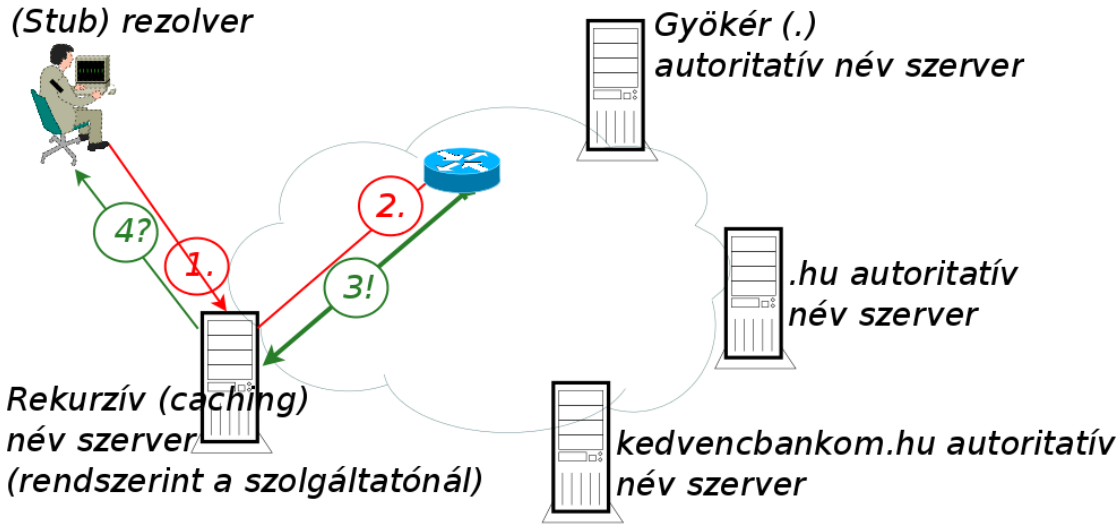
Érdemes ellenőzirzni, hogy IP szolgáltatónk ezt a példányt mutatja-e felénk. Ezt például a `dig` unixos parancs segítségével így tehetjük meg:

```
% dig +short -t txt -c ch id.server @k.root-servers.net
"k2.bix.k.ripe.net"
```

A „`bix`” karaktersorozat mutatja, hogy ez a budapesti, BIX-en levő példány.

3.2. DNS injekció

A DNS kérdést a hálózatban levő bármilyen közbülső doboz (tűzfal, router) elkaphatja, módosíthatja, vagy akár meg is válaszolhatja, ahogy az alábbi ábrán látszik:



1. www.kedvencbankom.hu ?
2. www.kedvencbankom.hu ?
3. www.kedvencbankom.hu A rekordja: 66.66.6.6 (autoritatív válasz)!
4. www.kedvencbankom.hu A rekordja: 66.66.6.6!

Egy ilyen router szintű beavatkozás nagyon sokat tudhat. Egy router válaszolhat **bármelyik** iterációs lépésnél. Egy router elterelheti a forgalmat úgy, hogy a valódi névszervereket sose érjük el. Egy router válaszolhat olyan forrás IP címmel, amivel csak akar: legtöbbször a cél IP címmel válaszol, így próbálja elhitetni, hogy a válasz onnan érkezik, akihez a kérdést intézték. Így működik a kínai nagy DNS fal: a kínai hálózatokon rendszeresen hamis választ adnak a „gyanús” DNS kérdésekre. Jó tudni, hogy a DNSSEC véd az ilyen támadások ellen.

3.3. Router szintű beavatkozások felderítése

Az IP csomagok TTL-jéből lehet sejteni, ha ilyen támadás történik: tudhatjuk, hogy egy-egy névszerver hány hop távolságra van, és ha annál közelebbről kapunk választ, sejthető, hogy a válasz router által hamísított. Még biztosabbak lehetünk, ha nem DNS szerverhez intézünk DNS kérést, és mégis választ kapunk. DNS injekció esetén akkor is kapunk (hamis) választ, ha a **célcím** nem DNS szerver címe. Ezzel a trükkel éltek a Sigcomm konferencia előadói. Cikkükben megállapították, hogy az ilyen DNS hamisítás **kiterjedt** és **kiszámíthatatlan** károkat okoz: gyakran olyan routereken mehet át a forgalmunk, amik ilyen hamisítással élnek: pl. chilei felhasználó európai webhelyet akar elérni, és a DNS csomagja kínai hálózaton át utazik az iteráció valemelyik lépésénél – Kínában levő root szervert kérdez.

A kínai DNS hamisításokról halvány képet alkothatunk, ha megkérdezzük a cenzúrázott www.facebook.com címét a pekingi 123.123.123.123 IP címtől:

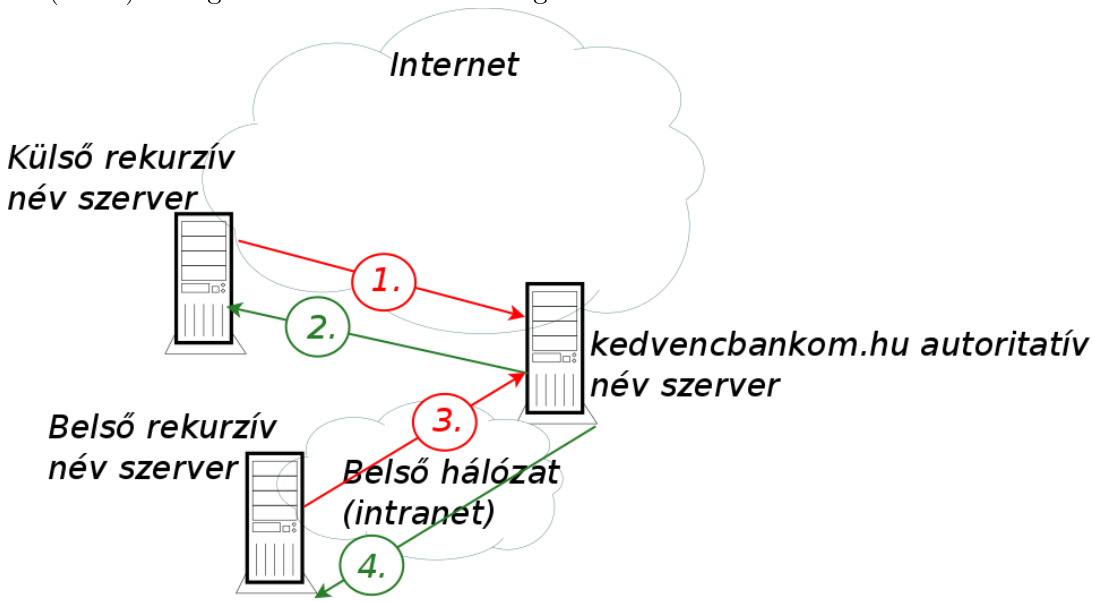
```
dig www.facebook.com  @123.123.123.123 +short
59.24.3.173
```

Ebben a példában a visszakapott cím nyilvánvalóan hamisított, Koreában levő IP cím.

4. Manipulálás az autoritatív névszervernél

4.1. Bind view

A Bind klasszikus DNS szerver implementáció, ami még mindig a legnépszerűbb. A kérdezőtől függően más és más választ adhat az autoritatív névszerver. A leggyakoribb felhasználása ennek az, hogy a belső hálózatunkból a belső web szerverre irányítjuk DNS szinten a a felhasználókat, kintről pedig a nyilvános web lapra. Persze ilyen konfiguráció nem csak Bind névszerver programmal lehetséges. Bind-nál ehhez a „view” (nézet) konfigurációs kulcsszót kell megadni:



1. www.kedvencbankom.hu ?
2. www.kedvencbankom.hu A rekordja: 111.22.33.44 (autoritatív válasz)
3. www.kedvencbankom.hu ?
5. www.kedvencbankom.hu A rekordja: 192.168.1.44 (autoritatív válasz)

A Bind konfigurációban ilyesféleképpen lehet megadni:

```
view "bent" {
 match-clients { 192.168.0.0/16; 10.0.0.0/8; 172.16.0.0/12};
  zone "kedvencbankom.hu" {
   type master;
   file "bent/kedvencbankom.hu";   };  };
view "kint" {
 match-clients {"any"; };
 zone "kedvencbankom.hu" {
   type master;
   file "kint/kedvencbankom.hu";   };  };
```

A `kedvencbankom.hu` zónafájlnak annyi példányban kell léteznie, ahány view van. Mindegyiket karban kell tartani. . .

4.2. GeoIP

A GeoIP olyan szolgáltatás, illetve program, ami IP címekhez földrajzi helyet, országot rendel. A Maxmind (`http://www.maxmind.com`) terméke. Ingyenes és pénzért vehető változata is van. Két GeoIP Debian csomag van: `geoip-database` és `goip-bin`. A GeoIP adatfájlból dolgozik:

- `/usr/share/GeoIP/GeoIP.dat`
- `/usr/share/GeoIP/GeoIPv6.dat`

Persze sok országokon átívelő szolgáltató van, és az IP címek kiosztása gyorsan változik, a GeoIP tehát gyakran téved. Ezt tudomásul kell venni. (Kevesebbet téved, ha rendszeresen frissítjük.)

4.3. GeoIP és Bind

Az egyes view-khoz tartozó IP címeket nem csak CIDR alakban, hanem országra való hivatkozással is megadhatjuk:

```
view "hu" {
        match-clients { country_HU; };
```

Ez módot ad terhelés elosztásra: a közelebb levő szerver IP címét adhatjuk vissza. Persze amit a rekurzív névszerverből látunk, az **nem** a kliens, hanem a **rekurzív névszerver** IP címe, ezt tudjuk GeoIP segítségével figyelembevenni: ha valaki Ázsiából afrikai rekurzív névszervert használ, afrikai szerver címet kaphat vissza. Gyakran messze lehet a tényleges kliens a rekurzív névszervertől. Ahogy az pl. `alternatív DNS szolgáltatók` bekezdésben olvasható, vannak az egész világról használt rekurzív névszerverek (Google, Verizon stb.). Ha ezek kérdeznek egy autoritatív névszervert, nem lehet tudni, mi az optimális válasz.

4.4. EDNS client subnet extension

A „rekurzív névszerver elrejti a valódi kliens IP címét az autoritatív névszerver elől” problémára megoldás lehet az „edns client subnet extension" internet draft. Ez egy Google kezdeményezés, a fő szerző Google munkatárs. Az elképzelés lényege, hogy a rekurzív névszerver elküldi a **kérdező** stub resolver címét (hálózatát) egy EDNS mezőben. Az autoritatív névszerver ezt a mezőt nézi a válasznál, és eszerint válaszol. Ilyen módon a rekurzív névszerverben egy-egy rekordhoz több cache-elt entry tartozhat! A Google, az Opendns és néhány nagy CDN vállalat támogatja (Akamai nem). Nem egyszerű a használata: az autoritatív névszervernek jelentkezni kell a rekurzív névszerver vállalatánál (whitelisting), hogy ezt a szolgáltatást használhassa. Így is sok a tévedési lehetőség — pl. VPN-ek, proxy-k zavarhatják, megtévesztehetik a válaszoló névszervereket.

4.5. GeoIP (view-k) és DNSSEC

Elsőre azt hihetnénk, hogy a DNSSEC nem fér össze azzal, hogy különböző kérdezőknek másképpen válaszolunk. De ha különböző válaszokat adunk ugyanarra a kérdésre, attól még mindegyiket aláírhatjuk! Példa erre a `security.debian.org`. Ha ezt az `A` rekordot kérdezzük, akkor más és más választ kapunk attól függően, hogy milyen kontinensen vagyunk. Van egy `TXT` rekord is, ami megmondja, hogy mi melyik „view”-t nézzuk:

```
;; ANSWER SECTION:
security.debian.org.    3600    IN      TXT     "EU view"
security.debian.org.    3600    IN      RRSIG   TXT 8 3 3600 20140516113403 20140416113403 7554 sec
```

Ebben az esetben tehát európainak tekint minket az autoritatív név szerver. De például az USA hálózataiból (jó esetben) '`NA view`' a `TXT` rekord tartalma.

5. Manipulálás a rekurzív névszervernél

A mai rekurzív névszerverek módot adnak arra, hogy a DNS válaszokat a rekurzív névszerverben módosítsuk, felülírjuk. Természetesen a rekurzív névszervernél alkalmazottr hamisítások DNSSEC-cel nem férnek össze.

5.1. Unbound

Az Unbound népszerű rekurzív névszerver, az Nlnetlabs terméke. Itt két egyszerű és hatékony eszköz áll rendelkezésre a manipulálásra:

- `local-zone`
- `local-data`

Mindkét eszközt lehet alkalmazni a konfigurációs fájlban (`unbound.conf`) és parancssorból (`unbound-control`).

5.1.1. Unbound – zónák elrejtése

A következő példák szemléltetik az Unbound néhány lehetőségét zónák elrejtésére:

- `local-zone gonosz.org static`
  - Nincs ilyen rekord (NXDOMAIN) lesz a válasz, **kivéve** ha `local-data` felülírja.
- `local-zone gonosz.org deny`
  - Csendben eldobja a kérést, **kivéve** ha `local-data` felülírja.
- `local-zone gonosz.org refuse`
  - Visszautasítja a kérdést, **kivéve** ha `local-data` felülírja.
- `local-zone gonosz.org transparent`
  - Normális lesz a válasz, **kivéve** ha `local-data` felülírja.

5.1.2. Unbound – rekordok felülírása

Azt is megtehetjük, hogy a rekurzív névszerverben más IP címre irányítjuk a kérdezőket: a gonosz helyett egy jóságos helyre:

- `local-data www.gonosz.org A 195.56.172.143`

Ebben a példában egye `A` rekordot a az `fsf.hu` IP címére irányítunk. Persze nem csak `A` rekordot, hanem bármilyen más típusú rekordot is definiálhatunk.

5.2. Bind: RPZ (Response Policy Zones)

A Bind 9.8 változata óta rugalmas, sokat tudó megoldást kínál a rekurzív névszerver oldalán történő manipulálásra, ennek neve RPZ (Response Policy Zones). DNS „tűzfal” szabályokat DNS **zónákban** írjuk le. Különös, hogy a **rekurzív** szerverben autoritatívként definiálnunk kell ehhez egy (vagy több) zónát, ilyesféleképpen:

```
zone "my-rpz"
  {
  type master;
  file "my-rpz";
  allow-query { none; };
  allow-transfer { none; };
};
```

Deklarálnunk kell, hogy RPZ-t használunk, és milyen zóná(k)ban van(nak) az átírt rekordok:

```
response-policy { zone "my-rpz"; };
```

Egy RPZ zónában levő rekordok **triggereket** és **action-öket** tartalmaznak. A triggerek egy-egy feltételt tartalmaznak, ami szerint szűrhetünk, manipulálhatunk. Trigger lehet:

- A kérdezett név (Ez felel meg a `local-zone`-nak unbound-nál)
  - Az RPZ zónában egyszerűen a névvel kell megadni
- A **válasz** IP cím, hálózat !
  - Az RPZ zónában `prefixlength.B4.B3.B2.B1.rpz-ip` alakban kell megadni
- Az autoritatív névszerver neve vagy címe, ami felelős a kérdezett névért
  - Az RPZ zónában az `rpz.nsdomain` alzónában kell megadni

5.2.1. RPZ „akciók”

Ha egy feltétel teljesül, akkor a megfelelő RPZ zónában levő rekordban kell megadni, hogy mit is tegyen a rekurzív névszerver. Lehet:

- `NXDOMAIN` (nincs ilyen rekord a válasz. Ezt egy olyan `CNAME` mutatja, aminek jobb oldalán a gyökér zónát jelentő `.` van. Például:

```
*.gonosz.org    CNAME .
15.0.0.68.124.rpz-ip CNAME .
```

Az első sor azt jelenti, hogy minden `valami.gonosz.org`-ra vonatkozó kérdésre `NXDOMAIN` legyen a válasz, a másik pedig azt, hogy a minden olyan válasz helyett, ami a `124.68.0.0/15` hálózatban levő IP címet eredményezne, `NXDOMAIN`-t válaszoljunk.

- Van ilyen rekord, de ilyen **típusú** nincs. Ezt a névszerver válaszban onnan tudhatjuk, hogy a válasz kód nem jelez hibát (`NOERROR`) de a válasz szekció üres. Ez a helyzet például, ha egy ipv6-os rekordot kérdezünk, de a kérdezett névhez csak ipv4-es rekord tartozik. Ha azt akarjuk, hogy az RPZ zónában megadott feltétel ilyen választ eredményezzen, akkor egy olyan `CNAME`-t kell megadnunk, aminek jobb oldalán a `*.` wildcard (wildcard TLD) van. Például:

```
*.gonosz.org     CNAME *.
```

- Más, hamis választ is adhatunk. Például a `valami.gonosz.org`-ra vonatkozó `A` rekordokat mind az `fsf.hu`-ra irányíthatjuk így:

```
*.gonosz.org     A 195.56.172.143
```

Ha kivételt akarunk tenni egy domain alatt, azt úgy tehetjük meg, hogy a rekord jobb oldalán az `rpz-passthru.` TLD-t adjuk meg. Például a `gonosz.org` egy aldomain-jával így tehetünk kivételt:

```
ok.gonosz.org  CNAME rpz-passthru.
```

- Ilyenkor „normális” lesz a válasz.

5.3. RPZ providerek

Az RPZ nagy ereje, hogy a felállított feketelistákat közzé lehet tenni. Ilyen RPZ provider például a Spamhaus. A közzé tett zónát zóna transzferrel áthozhatjuk, és így használhatjuk a mások által karbantartott, és közzétett feketelistát. Például:

```
response-policy {
   zone "rpz.spamhaus.org";
};
```

Az `rpz.spamhaus.org` szabadon használható, de regisztrálni kell az IP címet, ahonnan AXFR-t akarunk. Az RPZ providerekről további információ olvasható a `https://dnsrpz.info` webhelyen.

6. Tükör által, homályosan

6.1. DNS looking glass

Az internet routing tanulmányozására régen használatosak BGP looking glass-ok (tükrök). Ezek olyan web szerverek, amik távoli (pl. brazil) hálózatokból mutatják az utat a mi hálózatunk (vagy bármilyen más hálózat) fele. (Ilyenekről egy lista: `http://www.bgp4.as/looking-glasses`.)

Látjuk, hogy a DNS világában hasonló a helyzet: nem nyilvánvaló egy-egy DNS kérdésről sem, hogy milyen választ eredményez különböző hálózatokból. Adódik tehát az ötlet, hogy legyen DNS kérdésekre is looking glass szolgáltatás. Ez Stephane Borztmeyer találmánya és (python) programja. Az egyes looking-glass példányok http felett érhetők el. A választ JSON formában kapjuk. A DNS lookig-glass-okról egy lista: `http://www.dns-lg.com/`. Ez több mint 20 ilyen szolgáltatást nyújtó DNS szervert sorol fel szerte a világban. Például az `nl1` node-tól az `example.org` `NS` rekordját így lehet megkérdezni:

```
wget http://www.dns-lg.com/nl01/example.org/ns
```

6.2. DNSYO

A sok-sok világban elérhető rekurzív szerverről listákat készítenek, és tartanak karban. (Az Open Resolver Project 32 millió (!) nyílt rekurzív névszerverről tud.) A DNSYO egy >1500 rekurzív dns szervert kérdező eszköz pythonban írva. A használt névszerverek listája egy lokális fájlban található, amit időről időre frissíthetünk, és magunk is módosíthatunk. Maga a program elérhető itt: `https://github.com/samarudge/dnsyo`.

Például így tudjuk megkérdezni a `security.debian.org` TXT rekordját az összes dnsyo által ismert névszervertől:

```
dnsyo -x  -q ALL security.debian.org txt
```

A válaszból látjuk, mely névszerverek válaszoltak 'NA view'-t, 'EU view'-t stb. A DNSYO maga is tudni véli, hogy mely névszervernek mi a földrajzi helye. Mivel a példában kérdezett TXT rekord éppen azt mutatja, hogy a security.debian.org gazdái mit gondolnak, melyik kontinensen van a kérdező névszerver, érdekes összevetni a parancs outputjában a két információt.

6.3. Összefoglalva

Láttuk, hogy a DNS válaszokat sokan, sokféle céllal manipulálhatják. Láttunk eszközöket arra, hogy ha mi üzemeltetünk DNS szervert, alkalmasint mi is manipulálhatjuk a válaszokat autoritatív és rekurzív névszervernél is. Vannak módszereink arra is, hogy a DNS manipulálást kiderítsük vagy megkerüljük.