Arhitektura sigurnog DNS sustava

Domain Name System servis (dalje: DNS) jako se dobro uklapa u poznatu metaforu o malenom kotačiću kao neprimjetnom, zamalo-pa-nevažnom djeliću Velike Mašinerije, na kojeg nitko ne obraća pozornost dok ne zaglavi... i time dovede u pitanje funkcionalnost cjeline. Mi sistemci znamo zašto je tomu tako – bez DNS-a nema prevođenja imena računala/servisa u IP adrese, bogme, i obratno u slučaju *reverznog* resolvinga. Nažalost, znadu to i „mangupi u našim redovima“, pa osmisliše napad poznat kao (D)DoS rekurzivnih DNS servera. Riječ je o vjerojatno najučinkovitijoj varijanti ***amplification attack*** napada.

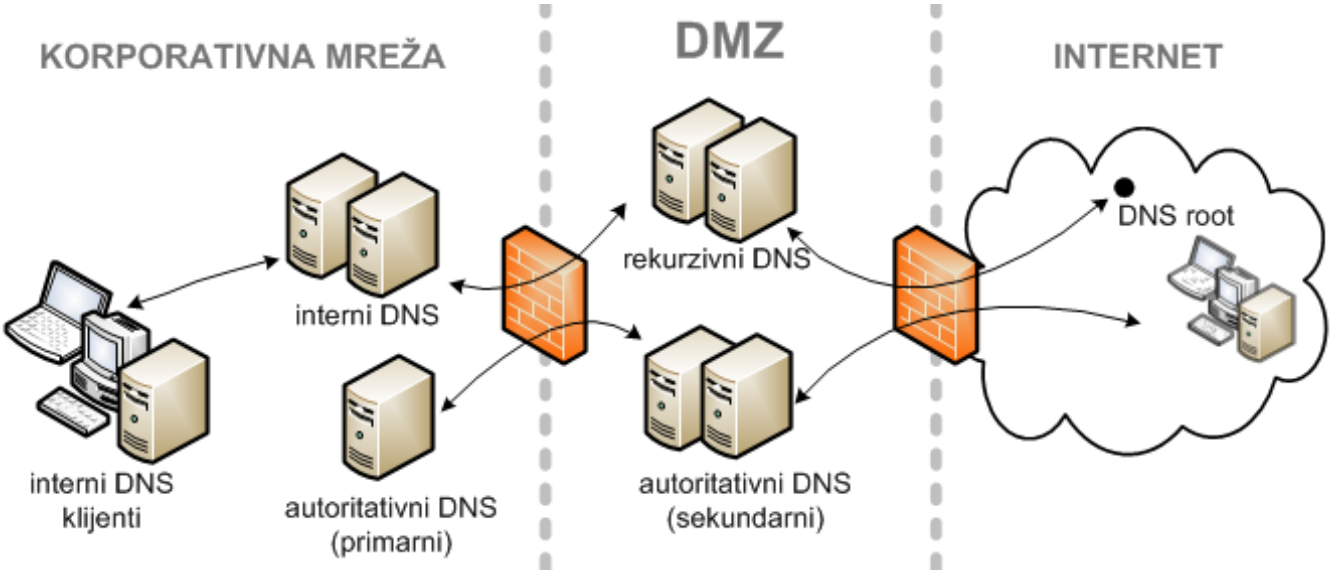
Razmotrimo standardnu implementaciju s Interneta dostupnog sloja DNS sustava (interni DNS ogranak je nebitan u ovoj priči). Fiktivno poduzeće Corp ima svoj internetski identitet, dakle, registriranu domenu corp.hr, i vlastite DNS servere. U standardnoj implementaciji, s Interneta dostupan sloj DNS-a ima ove značajke:

a) U DMZ su dva DNS servera, zbog visoke raspoloživosti tog servisa, dakako.
b) Jedan server obnaša ulogu primarnog, znači, na njemu se upisuju ili mijenjaju domene i zapisi; drugi je sekundarni, njegova baza je read-only i on samo „cica“ podatke sa primarnog servera.
c) Oba servera su autoritativna za sve javne (public) zapise u domeni corp.hr, pa odgovaraju na upite drugih internetskih DNS servera odnosno, šire gledano, DNS klijenata.
d) Oba servera su i rekurzivna tj. ako ne znaju odgovor na upit – a taj upit može se odnositi na bilo koje ime formatirano po FQDN standardu - oni će pitati Internet DNS servere kako bi svom klijentu podastrijeli najbolji mogući odgovor.

Točka d) omogućuje taj stvarno učinkovit (D)DoS napad. U tekstu koji slijedi nećemo se baviti detaljima tog napada – to se lako nađe na Internetu - nego opisom DNS arhitekture otporne na ovakav napad, s nekim pratećim opaskama kojima se povećavaju i sigurnost i funkcionalnost DNS servisa. Rješenje kojega izlažem generičkog je tipa, naime, nebitno je kakav DNS održavate ili dižete – BIND, Microsoft, nešto treće.

Osnovno je, kako niža slika ilustrira, razdvojiti uloge autoritativnosti i rekurzivnosti. Da, želimo li izbjeći predmetnu ranjivost, neizbježan je trošak na dodatne servere. Srećom, DNS je odavno prepoznat kao idealan kandidat za virtualizaciju. K tomu, najpopularnije OS-ove za Intel/AMD serversku platformu – Linux i Windows – možemo instalirati bez GUI-a, uostalom, to je i preporučeni način instalacije. Budući da sam DNS kao servis troši malo serverskih resursa, virtualne mašine mogu biti zaista skromnih tehničkih gabarita.

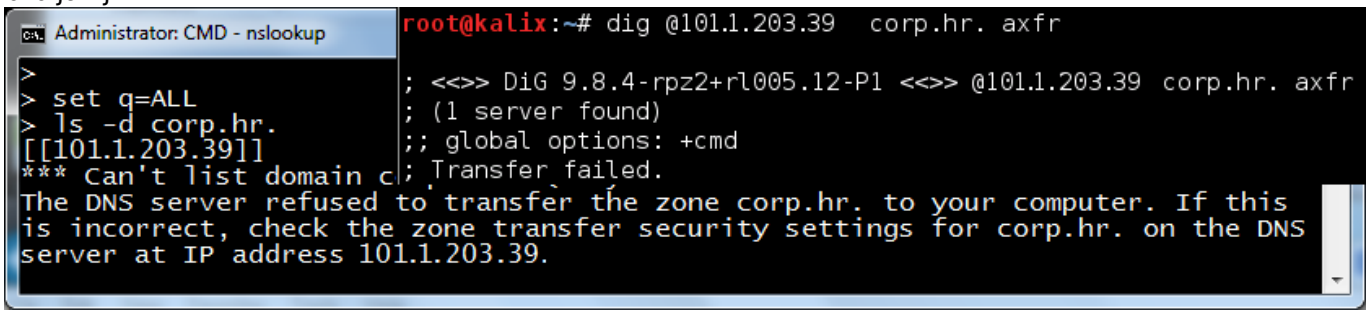
Ako ćemo pravo, trošak na dodatne servere nije baš neizbježan ukoliko rabimo BIND jer on nam, za razliku od Microsfot DNS-a, omogućuje definiranje ***trusted*** odn. ***untrusted*** mreža. Nedostatak je ovog pristupa što je stvarno koristan samo za manje implementacije te ne otklanja neke ranjivosti koje sigurna arhitektura ili umanjuje ili sprečava u potpunosti.



Napravimo li kako je gornjom slikom sugerirano, rekurzivni DNS sloj će u stvari postati cache-only, dakle, bez ikakvih lokalno konfiguriranih domena; ti DNS serveri trebaju omogućiti resolviranje Internet servisa klijentima s korporativne mreže. Njih ne moramo registrirati kod nacionalne DNS službe, što znači da su upravo ta dva cache-only servera nove instance korporativne DNS hijerarhije. DNS-ovi autoritativni za corp.hr su, dakako, registrirani, stoga se njihova IP adresa ne mijenja; oni nastavljaju obnašati svoju časnu ulogu informiranja „vanjskog svijeta“ o Internet servisima poduzeća Corp.

Uvođenjem rekurzivnih DNS servera zaštitili smo autoritativne DNS servere od spomenutog DDoS napada, ali sada se isti taj napad može usmjeriti na njih, rekurzivne servere. Budući da oni samo pitaju druge DNS servere, tome ćemo doskočiti tako da na firewallu postavimo pravilo koje će onemogućiti sav UDP/TCP 53 ***unsolicited*** promet, znači, onaj promet kojega nisu oni sami inicirali.

Glede sloja autoritativnih DNS-ova: na prvoj slici možete primijetiti da smo primarni (upisiv) DNS izmjestili u korporativnu mrežu. Ovaj server dostavlja svoje podatke o domenama i zapisima sabraći u DMZ, koja imaju read-only baze. Ovim rješenjem povećali smo zaštitu autentičnosti zapisa na autoritativnim DNS serverima. Tim sekundarnim serverima onemogućit ćemo rekurziju i konfigurirati ih tako da odbijaju upite koji od njih traže isporuku svih zapisa domene. Na nižoj slici je primjer dobro konfiguriranog DNS-a u tom smislu, i *nslookup* i *dig* reagiraju jednako, samo je *nslookup* nešto brbljaviji.



Od važnijih a lako provedivih dodatnih mjera zaštite DNS servera, još je potrebno onemogućiti napad tipa ***cache poisoning***. BIND v9 je prošle godine imao nezgodanciju s time. U najboljoj namjeri primijenjen je tzv. SRTT algoritam obrade NS zapisa a manguparija je nanjušila kako ga zlorabiti... DNSSEC ekstenzija je atraktivna mjera zaštite ali, heh, nije lako provediva.

Na kraju, nek' bude spomenuto i ovo: sigurne arhitekture DNS-a nema bez ispravno konfigurirane mreže. Aktivna mrežna oprema regulira kako će vanjski svijet pristupati našim DNS serverima, štoviše, njena je uloga ključna u „rezanju“ napada poput TCP/UDP SYN flood. Ne osujeti li se takav napad, DNS server će postati neupotrebljiv nakon najviše dvije do tri minute. Na nižoj slici je namjerno odabran napad na TCP 53 jer je informativniji. U praksi se više napada UDP 53 kako bi se DNS server zagušio.

```
TCP    101.1.203.39:53        223.255.176.16:29758   SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.176.201:58654  SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.177.49:8669    SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.178.188:7481   SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.180.92:56827   SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.183.235:46006  SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.184.96:29835   SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.186.160:24098  SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.188.51:27119   SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.188.162:30807  SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.189.125:3783   SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.195.187:58882  SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.195.212:473    SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.197.255:56156  SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.200.212:4485   SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.205.207:42669  SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.208.13:893     SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.212.42:7477    SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.222.145:30646  SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.223.44:49214   SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.224.88:57835   SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.224.228:48222  SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.225.99:28408   SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.226.146:23212  SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.229.48:60239   SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.229.183:34976  SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.229.235:6209   SYN_RECEIVED    1556
TCP    101.1.203.39:53        223.255.234.67:17206   SYN_RECEIVED    1556
```

Vezani članci:

DNS – optimizacija "resolvinga" internih i eksternih imena [1]

uto, 2014-04-08 07:19 - Ratko Žižek**Kategorije:** Sigurnost [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1380

Links
[1] https://sysportal.carnet.hr/node/1395
[2] https://sysportal.carnet.hr/taxonomy/term/30