PC Press

Država: Srbija

Doseg: 25,897

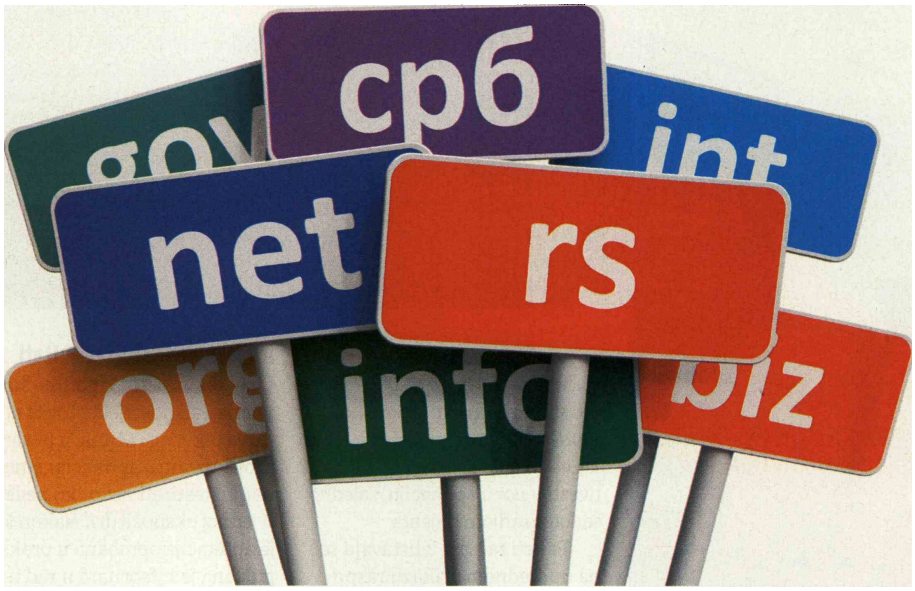
Strana: 90

Površina: 963 cm^2

09.05.2017
utorak

1 / 2

Komunikacije



Od naziva do adrese

Kako se nazivi domena koje otkucate u komandnoj liniji browser-a transformišu u brojeve koji omogućavaju vezu sa željenim sajtom? Nije to samo pitanje iz opšte računarske kulture već i informacija neophodna da biste sajt učinili bezbednim. Kroz nekoliko tekstova upoznaćemo rad DNS servera i njegovo sigurno konfigurisanje

Žarko Kecić

Internet je globalna računarska mreža s nekoliko stotina miliona računara koji međusobno komuniciraju i razmenjuju informacije. Za korisnika, svaki od ovih računara ili servisa koji oni pružaju može biti identifikovan preko jedinstvenog imena – naziva domena. S druge strane, računari i elementi mreže, koji omogućavaju komunikaciju preko Interneta, koriste nizove brojeva – IP *(Internet Protocol)* adrese.

DNS u korenu

Svi korisnici Interneta koriste DNS *(Domain Name System)* da bi se povezali sa odgovarajućim internet servisom. Sistem naziva domena (DNS) distribuirana je baza podataka o nazivima računara i servisa na Internetu. Uloga DNS-a je da korisnicima omogući povezivanje računara na Internetu, a da pri tome oni koriste slovne izraze koji se lako pamte. Mnogi od vas već znaju, ili su čuli, da računari međusobno komuniciraju preko numeričkih IP adresa. Pojednostavljeno, DNS je „IP imenik" koji nazive računara i servisa povezuje sa odgovarajućim IP adresama (brojevima).

DNS sistem mora da bude uvek dostupan, pouzdan, brz, fleksibilan i proširiv. On, kao i mnogi drugi distribuirani računarski sistemi, ima svoje bezbednosne slabosti. Specifičnost DNS sistema, njegova globalna uloga i namena da pruža uslugu svim korisnicima interneta, uticala je da se prilikom njegovog razvoja ne obrati velika pažnja na njegovu bezbednost. Povećanje broja korisnika, naročito

DNS je „IP imenik" koji nazive računara i servisa povezuje sa odgovarajućim IP adresama (brojevima)

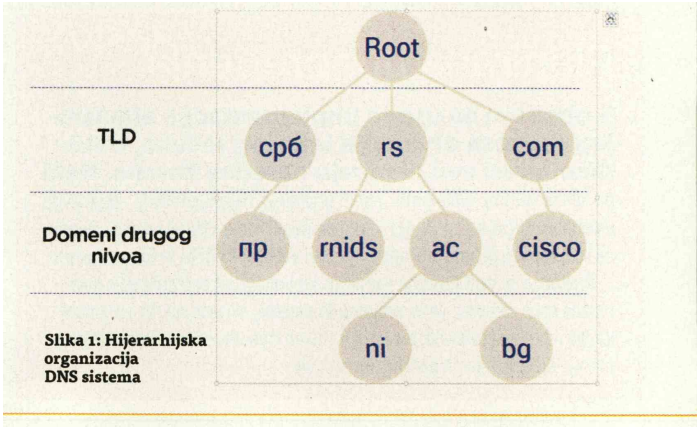
onih zlonamernih, poslednjih godina dovelo je u fokus bezbednost DNS-a.

Pored činjenice da je DNS jedan od ključnih internet servisa, njemu se ne pridaje dovoljno pažnje. Pre svega to ne rade sistem administratori i ostali ljudi koji su zaduženi za bezbednost računarskih sistema. DNS je veoma moćan, sveprisutan i uglavnom ignorisan, što je veoma opasna kombinacija.

Organizacija domenskog prostora

Osnovni razlog postojanja DNS-a jeste da omogući dodeljivanje jedinstvenog internet naziva servisima i računarima. Jasna korist ovakvog pristupa jeste lako pamćenje internet naziva servisa, kao što su veb strane ili adrese elektronske pošte, umesto niza brojeva sadržanih u IP adresama tih servisa.

Jednako je važna i činjenica da DNS omogućava odvajanje naziva servisa od njegove lokacije. Servisi mogu da menjaju fizičku lokaciju, a da pri tome ne menjaju svoj internet naziv. Ista veb stranica jednog dana može



Slika 1: Hijerarhijska organizacija DNS sistema

da se nalazi u Beogradu, a već sledećeg u Tokiju ili Melburnu, a da korisnici to i ne primete. Promena se (osim prebacivanja sadržaja veb stranice na drugu lokaciju) ogleda jedino u promeni IP adrese u DNS zapisu internet naziva tog servisa.

Struktura DNS-a sastoji se od velikog broja globalno raspoređenih računarskih i komunikacionih uređaja. Na samom vrhu DNS strukture nalaze se *root* serveri koji sadrže podatke o domenima najvišeg nivoa (TLD), kao što su: *.rs, .ca, .se, .com, .net* itd. Za svaku TLD zonu postoji DNS struktura koja sadrži podatke o domenima drugog nivoa *(.co.rs, rnids.rs, cisco.com...)*. Analogno, za svaku zonu drugog nivoa postoji struktura sa odgovarajućim DNS podacima za tu zonu, kao na slici 1.

Funkcionisanje DNS-a

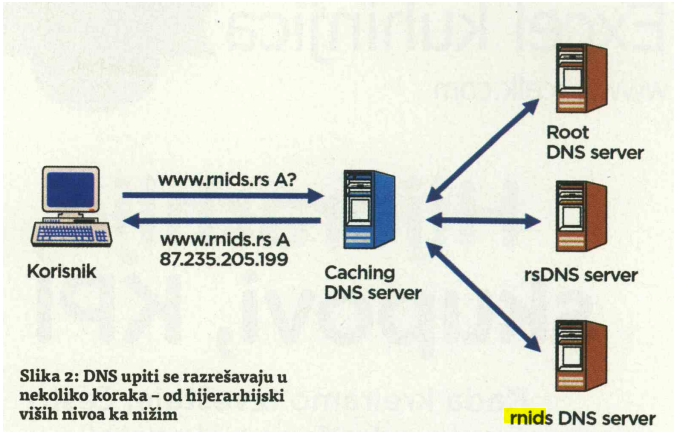
Hajde da ispratimo jedan DNS upit s računara korisnika. Računar korisnika zna adresu nekog DNS servera (to je najčešće DNS server internet provajdera ili DNS server kompanije). Kada korisnik u adresnu liniju veb *browser*-a unese adresu *www.rnids.rs*, računar će poslati upit tom DNS serveru očekujući kao odgovor IP adresu veb strane RNIDS-a. Postoji velika šansa da DNS server vašeg internet provajdera zna IP adresu *www.rnids.rs* jer su mnogi njegovi korisnici pre vas imali isti zahtev i DNS server ju je zapamtio, odnosno keširao (*cached* u DNS terminologiji), i vaš računar će odmah dobiti odgovor. DNS keš ima dvojaku ulogu, da ubrza nalaženje odgovarajuće IP adrese za popularne internet servise, ali i da smanji opterećenje globalnog DNS servisa, jer upiti ne idu dalje od prvog DNS servera koji je poznat vašem računaru.

Ako internet adresa koju je korisnik tražio, u ovom slučaju *www.rnids.rs*, nije poznata vašem DNS serveru ili hijerarhijskim serverima za keširanje, upit koji je njegov računar poslao stići će do samog korena globalnog

Servisi mogu da menjaju fizičku lokaciju, a da ne menjaju naziv internet domena

```
;; global options:  printcmd
.                   16730   IN      NS      a.root-servers.net.
.                   16730   IN      NS      l.root-servers.net.
.                   16730   IN      NS      h.root-servers.net.
.                   16730   IN      NS      b.root-servers.net.
.                   16730   IN      NS      k.root-servers.net.
.                   16730   IN      NS      f.root-servers.net.
.                   16730   IN      NS      c.root-servers.net. …
;; Received 228 bytes from 82.117.194.2#53(82.117.194.2) in 12 ms
rs.                 172800  IN      NS      l.nic.rs.
rs.                 172800  IN      NS      k.nic.rs.
rs.                 172800  IN      NS      h.nic.rs.
rs.                 172800  IN      NS      g.nic.rs.
rs.                 172800  IN      NS      f.nic.rs.
rs.                 172800  IN      NS      d.nic.rs.
rs.                 172800  IN      NS      b.nic.rs.
rs.                 172800  IN      NS      a.nic.rs.
;; Received 460 bytes from 198.41.0.4#53(a.root-servers.net) in 18 ms
rnids.rs.           3600    IN      NS      ns1.nic.rs.
rnids.rs.           3600    IN      NS      ns2.rnids.rs.
rnids.rs.           3600    IN      NS      odisej.telekom.rs.
rnids.rs.           3600    IN      NS      ns1.rnids.rs.
;; Received 221 bytes from 194.146.106.114#53(l.nic.rs) in 0 ms
rnids.rs.           3600    IN      A       87.237.205.199
rnids.rs.           3600    IN      NS      ns1.nic.rs.
rnids.rs.           3600    IN      NS      odisej.telekom.rs.
rnids.rs.           3600    IN      NS      ns1.rnids.rs.
rnids.rs.           3600    IN      NS      ns2.rnids.rs.
;; Received 262 bytes from 147.91.8.6#53(ns1.nic.rs) in 14 ms
```

Slika 3: Put kojim korisnik stiže do IP adrese servera



Slika 2: DNS upiti se razrešavaju u nekoliko koraka – od hijerarhijski viših nivoa ka nižim

DNS je veoma moćan, sveprisutan i uglavnom ignorisan, što je veoma opasna kombinacija

DNS sistema, do *root* servera, tačnije do jednog od trinaest *root* servera. *Root* serveri predstavljaju poseban set hijerarhijski najviših DNS servera koji znaju adrese autoritativnih DNS servera za hijerarhijski najviše delove internet naziva, tj. za deo adrese sdesna nalevo do tačke. To je u našem slučaju .RS, ali *root* serveri znaju i IP adrese autoritativnih DNS servera i za ostale domene najvišeg nivoa, ili TLD *(Top Level Domain)*, kao što su: *.com, .net, .org, .edu, .it, .uk, .se, .de, .срб, .rf...*

Kada računar pošalje DNS upit, vaš DNS server, ukoliko mu nije poznata adresa servisa koju ste tražili, pokušaće da razreši *(resolve)* tu IP adresu i poslaće upit jednom od *root* servera. *Root* server neće proslediti odgovor sa IP adresom za *www.rnids.rs*, pošto mu ona nije poznata, već će DNS serveru *(resolver*-u) korisnika poslati listu DNS servera koji su autoritativni za .RS. Tada će DNS server korisnika poslati nov upit prvom s liste DNS servera koji su autoritativni za .RS, ali ni od njega neće dobiti IP adresu za *www.rnids.rs*, već listu autoritativnih DNS servera za *rnids.rs*. DNS server ponovo šalje upit prvom s liste autoritativnih DNS servera za *rnids.rs*, i od njega dobija IP adresu za *www.rnids.rs*, koju smešta u svoju memoriju (kešira je za slučaj da se u nekom određenom intervalu ponovi isti upit) i prosleđuje je računaru korisnika. Treba napomenuti da proces razrešavanja IP adrese obično traje manje od 100 milisekundi i da krajnji korisnik to vreme praktično i ne primeti i nije ni svestan koliki je put u stvari prešao njegov DNS upit (slika 2).

DNS servis je jedini centralizovan i hijerarhijski organizovan servis na Internetu

Sada i računar korisnika zna IP adresu računara na kome se nalazi veb strana RNIDS-a i povezuje se sa veb servisom na adresi 87.237.205.199 i u korisnikovom *browser*-u prikazuje traženu veb stranu (slika 3).

DNS servis je jedini centralizovan i hijerarhijski organizovan servis na Internetu. Uz to, od svog nastanka DNS servis veoma se malo menjao i stoga je razumljivo da DNS serveri, zbog svog značaja, predstavljaju stalnu metu zlonamernih korisnika Interneta. Ciljevi napadača mogu biti različiti, od političkih i verskih do materijalnih ili jednostavno destruktivnih. O napadima na DNS servere i odbrani od njih govorićemo u sledećem broju našeg časopisa.

Tekst je realizovan u saradnji s Registrom nacionalnog internet domena Srbije, RNIDS