Doména věc veřejná

aneb jak těžit data z DNS

Petr Krčmář

12. listopadu 2026

Uvedené dílo (s výjimkou obrázků) podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

O mně

- linuxák od roku 1998
- správce serverů
- lektor a konzultant
- šéfredaktor Root.cz
- člen vpsFree.cz
- organizátor LinuxDays
- můj web je petrkrcmar.cz

ROOT.CZ vpsFree.cz

Prezentace už teď na webu

www.petrkrcmar.cz

ROOT.CZ vpsFree.cz

Jmenovky nejsou jen adresy

Doménová jména nejsou jen adresy

- DNS převádí zapamatovatelná jména na technické záznamy
  - doménová jména používají lidé i aplikace každý den
- jmenovka často napoví, k čemu daný systém slouží
  - může odlišit produkční, testovací a vývojové prostředí
  - může odhalit názvy služeb, které organizace provozuje
  - někdy prozradí interní názvosloví nebo strukturu týmu
- název nemusí zůstat interní, pokud se objeví ve veřejných datech
- měli bychom předpokládat, že jmenovku může někdo objevit

ROOT.CZ vpsFree.cz

Jmenovka prozradí víc než adresu

- `vpn.example.com` – odhalí vzdálený přístup
- `mail.example.com` – prozradí roli systému
- `staging.example.com` – odliší testovací prostředí od produkce
- `dev.example.com` – naznačí vývojovou infrastrukturu
- `old.example.com` – může ukazovat na zapomenutou službu
- `admin.example.com` – prozradí administrační rozhraní
- `jmeno-prijmeni.example.com` – odhalí vazbu na konkrétní osobu
- `projekt-x.example.com` – interní název či plánovaná služba

Passive DNS

Passive DNS: pozorování zvenčí

- DNS odpověď zachycuje vazbu mezi jménem a záznamem
- záznam se ukládá spolu s časem pozorování
- záznamy z více senzorů se shromažďují v databázi
- výsledkem je částečný historický pohled na DNS
- lze hledat na jakou IP se doména překládala
- lze také hledat, jaké domény byly spojeny s danou IP adresou
- VirusTotal nabízí rozhraní k prohlížení vlastních dat
  - data získává z analýzy malwaru v sandboxu
  - nebo z vyhledávání uživatelů v jeho rozhraní
  - pokud jméno vidí nebo ho někdo hledá → přidá do DB

Vlastnosti

- DNS dotazy a odpovědi zaznamenávají pozorovací systémy
  - data od uživatelů, různých nástrojů nebo senzorů
- pozorování se ukládají do databáze s časovými značkami
- vlastník domény sběr dat přímo nevidí nevidí
  - vyhledávání v DB neposílá DNS dotaz cílové doméně
- databáze zachycuje jen to, co její zdroje skutečně pozorovaly
- záznamy mohou být neúplné, opožděné nebo zastaralé
- přesto mohou být velmi užitečné a jsou snadno dostupné

Příklad VirusTotal

- přístup k passive DNS nabízí VirusTotal
  - například pohled na slu.cz (mají i API) odhaluje 254 subdomén
- 8 domén obsahuje test, 1 doména old, dále Eset, Zabbix...

aak.slu.cz, absolventi.slu.cz, ad.slu.cz, akce.slu.cz, amok.slu.cz, apate.slu.cz, aphrodite.slu.cz, apollo.slu.cz, archivsu.slu.cz, asociace.slu.cz, aspsu.slu.cz, athena.slu.cz, aura.slu.cz, bbb.slu.cz, behsezoo.slu.cz, bezpecnost.slu.cz, bodyineuropeanhistory.slu.cz, box.slu.cz, bspace.slu.cz, bydleni.slu.cz, carcopes.slu.cz, carmen.slu.cz, ca.slu.cz, centos.slu.cz, cepis.slu.cz, cep.slu.cz, cit.slu.cz, cmc2023.slu.cz, cro-idp.slu.cz, cro.slu.cz, croutils.slu.cz, cul.slu.cz, czv.slu.cz, demeter.slu.cz, dike.slu.cz, dobrovolnictvi.slu.cz, dotaznik.slu.cz, ects.slu.cz, eden.slu.cz, eduroam.slu.cz, e-fvp.slu.cz, eis.slu.cz, elearning.slu.cz, elisa.slu.cz, elisa-test.slu.cz, english.slu.cz, epis.slu.cz, erasmus.slu.cz, eris.slu.cz, eset.slu.cz, eshop.slu.cz, escher.slu.cz, esport.slu.cz, euros.slu.cz, evidence.slu.cz, evido.slu.cz, files.slu.cz, filmac.slu.cz, forkys.slu.cz, foto.slu.cz, fpf.slu.cz, fsm-msk.slu.cz, funday.slu.cz, fvp.slu.cz, gallery.slu.cz, gitlab.slu.cz, git.slu.cz, go.slu.cz, had.slu.cz, helios.slu.cz, helpdesk.slu.cz, help.slu.cz, hera.slu.cz, hra.slu.cz, hypnos.slu.cz, chaos.slu.cz, iapetus.slu.cz, idp-cro.slu.cz, idp.slu.cz, imap-r1.slu.cz, imap.slu.cz, indico.slu.cz, innlocal.slu.cz, inoviny.slu.cz, intranet.slu.cz, iot.slu.cz, ip.slu.cz, iskam.slu.cz, isois.slu.cz, is.slu.cz, itf-new.slu.cz, jinak.slu.cz, jis.slu.cz, kariera.slu.cz, karty-old.slu.cz, karty.slu.cz, karty-test.slu.cz, keycloak.slu.cz, kiosky.slu.cz, kirke.slu.cz, knihovna.slu.cz, koleje.slu.cz, komunita.slu.cz, konferencehot.slu.cz, kontakty.slu.cz, krouzek-informatika.slu.cz, krus.slu.cz, kulided.slu.cz, kulturni-dejiny.slu.cz, kurzy.slu.cz, laniakea.slu.cz, lcna.slu.cz, ldap.slu.cz, ldap1.slu.cz, login-idp.slu.cz, login.slu.cz, loskutaci.slu.cz, luskouni.slu.cz, luskutaci.slu.cz, magnet.slu.cz, magnet-test.slu.cz, mail.slu.cz, mail-test.slu.cz, mailtrain.slu.cz, manualy.slu.cz, mars.slu.cz, math.slu.cz, mda.slu.cz, mediadejiny.slu.cz, media.slu.cz, merch.slu.cz, merkur.slu.cz, metis.slu.cz, midas.slu.cz, mirror.slu.cz, missu.slu.cz, mixuj.slu.cz, mobility.slu.cz, mobilniflotila.slu.cz, mobily.slu.cz, moje.slu.cz, moje2.slu.cz, msmx1.slu.cz, msmx3.slu.cz, mx1.slu.cz, mx2.slu.cz, novevykazy.slu.cz, noviny.slu.cz, ns1.slu.cz, ns2.slu.cz, opavskypav.slu.cz, opavsky-robocup.slu.cz, openuni.slu.cz, opf.slu.cz, op-vr.slu.cz, orion.slu.cz, orion-test.slu.cz, ors.slu.cz, orthus.slu.cz, osp.slu.cz, ovirt.slu.cz, pandeia.slu.cz, paste.slu.cz, patchman.slu.cz, perses.slu.cz, physics.slu.cz, phys.slu.cz, pkcentrum.slu.cz, plone.slu.cz, podchod.slu.cz, podpora.slu.cz, poll.slu.cz, pontus.slu.cz, popularizacevedy.slu.cz, poradna.slu.cz, portal.slu.cz, post.slu.cz, prihlasit.slu.cz, prijezdy.slu.cz, projekty.slu.cz, proteus.slu.cz, pruvodce.slu.cz, prvaci.slu.cz, radius1.slu.cz, radius2.slu.cz, restartesf.slu.cz, retrobajty.slu.cz, rpa.slu.cz, rustlab-api.slu.cz, saturn.slu.cz, silse.slu.cz, slu.cz, smtp.slu.cz, smtp1.slu.cz, smtp2.slu.cz, soudobe-dejiny.slu.cz, sp-cro.slu.cz, spolu.slu.cz, sport.slu.cz, spp.slu.cz, stag.slu.cz, stag-ws.slu.cz, starseu2026.slu.cz, stats.slu.cz, studentiprotivalce.slu.cz, study-economics.slu.cz, sunet.slu.cz, superstage.slu.cz, suscience.slu.cz, sutalent-api.slu.cz, suudrzitelna.slu.cz, suveda.slu.cz, talent.slu.cz, talent-survey.slu.cz, test-cepis.slu.cz, testvykazy.slu.cz, testweb.slu.cz, thetye.slu.cz, tisk.slu.cz, trainehotel.slu.cz, transfer.slu.cz, tritius.slu.cz, tyrkysovasbirka.slu.cz, ua.slu.cz, uftrt.slu.cz, uchazeci.slu.cz, uk.slu.cz, uks.slu.cz, unisfera.slu.cz, unisphere.slu.cz, upld.slu.cz, utils.slu.cz, u3v.slu.cz, vck.slu.cz, virtuniv.slu.cz, vkop5.slu.cz, vpn.slu.cz, vr.slu.cz, vssp.slu.cz, vybersi.slu.cz, vyjezdy.slu.cz, vykazy.slu.cz, vykazy2.slu.cz, web-auth.slu.cz, webstag.slu.cz, whoo.slu.cz, www.slu.cz, www-static1.slu.cz, www1.slu.cz, www2.slu.cz, zabbix.slu.cz, zakazky.slu.cz, zkp.slu.cz, 30let.slu.cz

ROOT.CZ vpsFree.cz

Certifikáty

HTTPS je dnes všude

- HTTPS chrání spojení mezi prohlížečem a webovým serverem
  - odposlouchávání a modifikace nejsou možné
- server se při navazování spojení prokáže certifikátem
- certifikát spojuje doménové jméno s veřejným klíčem
  - vystavuje autorita po ověření žádosti
- certifikát **obsahuje jména**, pro která platí
- tato jména mohou zahrnovat i subdomény
- všechny certifikáty pro veřejný web se zveřejňují
  - kvůli transparentnosti, hlídání autorit, odhalení chyb

ROOT.CZ vpsFree.cz

Certificate Transparency

- CT je systém **veřejných logů** vydaných certifikátů
  - certifikační autority do logů zapisují **všechny certifikáty**
- logy jsou veřejně prohledávatelné a průběžně se doplňují
  - záznam obsahuje mimo jiné doménová jména uvedená v certifikátu
- kdokoli může logy procházet nebo využít monitorovací službu
  - správci mohou sledovat certifikáty pro své domény
  - kdokoliv tam může hledat libovolné informace
- pro vystavení musí existovat záznam v DNS
- hvězdičkový certifikát neprozradí konkrétní subdomény

ROOT.CZ vpsFree.cz

Veřejná rozhraní

- veřejné rozhraní nabízí například CRT.sh nebo CertKit.io
- lze vyfiltrovat jen platné domény
  - maximální platnost dnes 200 dnů
  - Let’s Encrypt vydává na 90 dnů
  - budeme zkracovat až na 47 dnů (2029)
  - data bývají velmi aktuální
- pohled na `slu.cz` odhalil **434 subdomén**
  - přibylo 46 subdomén s www
  - přibyly tři hvězdičkové certifikáty
  - přibylo pět dalších domén „test“
- tohle je výrazně přesnější metoda
- co když ale doména nebude mít veřejně platný certifikát?

ROOT.CZ vpsFree.cz

DNSSEC

Důvěryhodnější odpovědi z DNS

- DNSSEC rozšiřuje DNS záznamy o digitální podpisy
  - podpisy umožňují ověřit původ dat
- validátor kontroluje, že data nebyla po cestě změněna
  - důvěra se ověřuje řetězcem od důvěryhodného bodu až k doméně
- DNSSEC pomáhá odhalit podvržené nebo pozměněné odpovědi
- zajišťuje také ověřitelné odpovědi o **neexistujících jménech**
  - aby nikdo nemohl neoprávněně zatajit informaci
  - neexistence jmenovky je taky informace a má podpis
  - generuje se předem, servery nemusejí mít klíče

NSEC: důkaz neexistence v řetězci

- DNSSEC musí umět ověřit i to, že dotazované jméno neexistuje
- NSEC propojuje existující jména v zóně podle jejich pořadí
- záznam ukazuje na **následující jméno** v tomto pořadí
  - zároveň uvádí, jaké typy záznamů dané jméno obsahuje
- NSEC dokládá, že mezi dvěma jmény žádné další není
  - *„existuje jméno ananas a pak až citron“*
  - máme potvrzenou neexistenci jména banan
- řetězec lze procházet opakovanými DNS dotazy
- při průchodu se tak mohou odhalit jména v celé zóně
- NSEC tedy **prozrazuje obsah** zóny

ROOT.CZ vpsFree.cz

NSEC3: místo jmen jejich haše

- NSEC3 řeší ověřování neexistence stejně jako NSEC
- místo čitelných jmen pracuje s jejich **hašovanou podobou**
  - záznamy propojují haše v pořadí jmén v zóně
- odpověď zase prokazuje neexistenci jména
  - *„existuje hašované jméno fc2a36b07f5b... a pak až b4a34df68c... “*
  - máme potvrzenou neexistenci mezilehlého haše
- přímý průchod už neukazuje názvy jmenovek v čitelné podobě
- jmenovky ale můžeme **hádat** nebo použít slovník
  - hašování nesmí být moc složité → zatěžuje resolvery
  - vyšší počet iterací zakazuje RFC 9276
- NSEC3 věc komplikuje, ale nezaručuje utajení jmenovek
  - lepší řešení nemáme a mít zřejmě nebudeme

ROOT.CZ vpsFree.cz

Použitelné nástroje

- použít lze nástroje nsec3map a John the Ripper
  - první projde a uloží NSEC3 záznamy ze zóny
  - druhý umí lámat haše podle slovníků nebo náhodně
- lze použít třeba i NSEC3 Walker a Hashcat

```
$ n3map -v --output slu.cz.zone slu.cz
3map 0.8.2: starting mapping of slu.cz.
looking up nameservers for zone slu.cz.
using nameserver: 2001:718:1001:149::9 (decsys.vsb.cz.)
using nameserver: 2001:718:1:1::144:205 (nsa.ces.net.)
using nameserver: 2001:718:2201:209::5 (ns2.slu.cz.)
using nameserver: 2001:718:2601:386::64 (ns1.slu.cz.)
checking SOA...
checking DNSKEY...
detecting zone type...
zone uses NSEC records
starting enumeration in mixed query mode...
;; walking slu.cz.: records = 453; queries = 466; ........................................
finished mapping of slu.cz. in 0:00:46.433080
```

Doménová jména jsou veřejná

- názvy v DNS berme vždy jako **veřejnou informaci**
- subdoména může hodně prozradit
  - službu, prostředí, projekt nebo interní názvosloví
- informace se mohou objevit ve veřejně dostupných zdrojích
- NSEC3 skryje čitelná jména, ale neudělá z nich tajemství
- nepočítejte nikdy s tím, že jmenovku nikdo neobjeví
  - nestavte bezpečnost na utajení názvu domény nebo subdomény
- přístup ke službě chraňme jiným způsobem
  - autentizací, řízením přístupu a správnou konfigurací

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz