VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Síťové aplikace a správa sítí

Filtrující DNS resolver (Dr. Polčák)

16. listopadu 2020

Lukáš Perina

Obsah

1 DNS resolver a DNS

1.1 DNS resolver

DNS resolverom sa rozumie program určený na prekladanie doménových adries na IP adresy. Jedná sa o klientskú časť DNS ktorá prekladá užívatelské dotazy. Robí to v spolupráci s DNS serverom ktorý je serverová časť tohto programu. [3]

1.2 DNS

Je to hierarchický a decentralizovaný menný systém pre počítače, služby a ostatné zariadenia pripojené na internet. DNS je esenciálnym komponentom internetu už od 1985 a odoberá nám povinnosť pamätať si IP adresy ako také, takže nám stačí pamätať si len ich doménové reprezentácie. [3]

1.3 Filtrujúci DNS resolver

Filtrujúci DNS resolver sa rozumie DNS resolver ktorému je zadaný blacklist, na základe ktorého sa DNS resolver rozhoduje či danú adresu preloží a odošle užívatelovi odpoved alebo nie. Jedným zo známejších príkladov pri použití s Raspberry pi je program pi-hole, ktorý slúži ako filtrujúci DNS resolver určený na zachytávanie reklamy. `https://pi-hole.net/`

2 Návrh aplikácie

Aplikácia bola navrhnutá tak aby bola robustná a nespôsobovala samovolné pády a dokázala sa vysporiadať s rôznymi situáciami.

2.1 Popis implementácie

Aplikácia bola implementovaná na systéme Manjaro Linux a následne testovaná na tomto systéme a serveroch eva.fit.vutbr.cz a merlin.fit.vutbr.cz. Aplikácia využíva na komunikáciu esenciálne funkcie recvfrom a sendto ktorými komunikuje s klientom a so serverom. Aplikácia najskôr prijme požiadavku od klienta ktorú následne skontroluje a porovná s dotazovanú adresu s blacklistom. Následne pošle príkaz na predom zadaný DNS server, prijme odpoved a túto odpoved pošle klientovi. V prípade zachytení domeny blacklistom sa užívatelovi odošle preddfinovaná chybová hláška.

3 Spustenie DNS resolveru

Po úspešnom preložení aplikácie sa DNS resolver spúšta nasledujúcim jednoduchým príkazom s 3 parametrami: ./dns -s server [-p port] -f blacklist

3.1 Parametre

Program má 3 parametre ktorými je možné upresnovať funkcionalitu DNS resolveru. Tieto parametre sú:

- Parameter -s Určujúci DNS server na ktory sa budu preposielat dotazy.
- Parameter -p je volitený parameter pre zadanie portu na ktorom bude resolver počúvať.
- Parameter -f určuje blacklist ktorý obsahuje zakázané domény.

3.2 Beh programu

Po spustení programu sa zadefinujú základné premenné, skontrolujú sa parametre programu a naviaže sa spojenie s klientom pomocou funkcie bind. Po naviazaní programu je program v režime serveru, čaká na dotazy a pre každý dotaz vytvára child procesy ktoré obslúžia klienta. V prípade zachytenia domény ktorá sa nachádza v blackliste alebo zachytenia iného dotazu ako dotazu typu A sa upraví odpoved pre klienta tak aby bol klient informovaný prečo jeho dotaz bol zamietnutý. Toto nastavenie prebieha pomocou nastavenia error kódu DNS odpovede. [2]

3.3 DNS Header

Pre reprezentáciu DNS Header používam volne dostupnú reprezentáciu dns headeru v podobe štruktúry dostupnú na `https://pcapplusplus.github.io/api-docs/structpcpp_1_1dnshdr.html`[1]

3.4 Getaddrinfo

V projekte je použitá funkcia getaddrinfo, avšak striktne na preklad doménového serveru zadaného parametrom -s.

3.5 Odozva programu

Program v chybových situáciách končí chybou a návratovým kódom -1 s detailnou hláškou na stderr.

3.6 Kontrola blacklist

Na kontrolu domény v blackliste používam funkciu searchFile(string filename,string domain). Po prijatí dotazu na preklad domény túto doménu pošlem na kontrolu do tejto funkcie, ktorá vyhodnotí či je doména na blackliste. Súbor prechádzam pre každú doménu celý a neukladám si jeho obsah kvôli ušetreniu pamati, ked súbory môžu mať aj viac ako 20MB.

4 Testovanie

Testovanie prebiehalo na systémoch Manjaro Linux, merlin a eva. Na testovanie bol použitý program dig a python script ktorý tento program volal zároveň so serverom.

5 Záver

Implementovať DNS resolver bol určite zaujímavý projekt ktorý ma mnohé naučil, ale kedže som už s cpp a so sietovými knihovnami pracoval, dalo sa to zvládať relatívne v poriadku.

Literatura

[1] PcapPlusPlus: pcpp::dnshdr Struct Reference. https://pcapplusplus.github.io/api-docs/structpcpp_1_1dnshdr.html, (Accessed on 11/16/2020).

[2] Iana: Domain Name System (DNS) Parameters. https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-6, (Accessed on 11/14/2020).

[3] Wikipedia: Domain Name System — Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/w/index.php?title=Domain%20Name%20System&oldid=987975972, 2020, [Online; accessed 13-November-2020].