Vysoké učení technické v Brně

Fakulta informačních technologií

Síťové aplikace a správa sítí

2020/2021

Oficiální dokumentace projektu

Filtrující DNS resolver

Žák Jiří (xzakji02)

13. Listopadu 2020

Obsah

Úvod

Zadání

Úkolem je napsat program dns, který bude filtrovat domény a poddomény v rámci dodaného seznamu. Nevyfiltrované dotazy bude zasílat specifikovanému dns serveru, který je bude překládat a posílat zpět tomuto serveru. Tyto odpovědi bude server zasílat zpět původnímu tazateli. Program by měl podporovat pouze UDP komunikaci a dotazy typu A.

Problematika

DNS neboli Domain name system je systém doménových jmen s informacemi na kterém serveru se domény nachází. Jedná se o „překladač“ doménových jmen na IP adresy a obráceně. DNS toho samozřejmě podporuje více, ale v našem případě stačí uvažovat pouze o překladu doménového jména na IP adresu.

Požadovaný výstup

Samotná aplikace nevypisuje nic. Klient, po obdržení odpovědi, může vypsat zachycený paket, ale to záleží čistě na implementaci klienta.

Spuštění aplikace

Program je navržen primárně pro systémy Linux. Po přeložení projektu pomocí přidaným Makefilem se vytvoří binární soubor dns(příkazem make). Pro spuštění zadáme příkaz. /dns. Program musíme spustit s příslušnými argumenty, jinak nebude fungovat.

1. –s <server> - povinné
2. –p <port> - nepovinné
3. –f <filter_file> - povinné

Vysvětlení argumentů:

-s <server>
- server, na který bude resolver zasílat nevyfiltrované dotazy
- lze zadat jako IPv4, IPv6 nebo jako doménové jméno

-p <port>
- port, na kterém bude resolver poslouchat a zachytávat pakety
- implicitně je nastaven port 53

-f <filter_file>
- soubor s doménovými jmény, která budou vyfiltrována

Implementace

Program je implementován v jazyce C++. Původně byl vytvářen v jazyce C, ale po přehodnocení byl přepracován do C++.Hlavní důvody tohoto kroku jsou datový typ string a unordered map na případné filtrování poddomén. V jazyce C by implementace této mapy zabrala zbytečně čas navíc.

Parsování argumentů

Program po spuštění nejprve kontroluje vstupní argumenty od uživatele. Pokud uživatel nezadá povinné argumenty, tak se téměř hned vypne. Pokud však jsou zadané, tak se zapíší do připravené globální struktury a program může pokračovat. V dalším kroku se provádí kontrola argument -s, u kterého se zjišťuje v jakém formátu je zadán a případný překlad doménového jména na IPv4 adresu. Nakonec se otevře zadaný soubor a přečtou se z něho doménová jména, která se zapíší do **hashovacího stromu**, který využijeme na rychlé vyfiltrování domén a jejich poddomén.

DNS

Hlavní část programu začíná otevřením spojení pro klienta pomocí funkce **socket** a **bind**. Pomocí funkce socket otevřeme UDP spojení a pomocí funkce bind nastavíme odposlech na zadaný port. Poté program vstoupí do nekonečné smyčky, kde čeká na příchozí pakety s dotazy. Jakmile přijde nějaký paket, tak se zavolá funkce **parsePacket**, která ho zpracuje a rozdělí na dvě základní části, DNS hlavičku a otázku. Z flagů v dns hlavičce zjistí, jestli je dotaz validní, a podle toho ho pošle dál ke zpracování. Pokud z hlavičky zjistí, že dotaz není validní, tak nastaví flag rcode na NOT IMPLEMENTED, flag qr na answer a pošle paket s odpovědí zpět ke klientovi[3]. Dotaz není validní, pokud je jiného typu než A typ. Pokud je dotaz validní, tak se z otázky vyjme doménové jméno[4], a funkce **filterDomain** zkontroluje, jestli náhodou není ve vyfiltrovaných jménech. Pokud ano, tak program posílá zpět paket s odpovědí, kde se nastaví flag rcode na REFUSED a flag qr na answer[4]. Pokud je však adresa nevyfiltrována, tak se zjistí, jestli zadaný server má IPv4 nebo IPv6 adresu a podle toho se pošle do příslušné funkce. Tyto dvě funkce se liší pouze tím, že jedna vytváří spojení pro IPv4 a druhá pro IPv6 adresou. Jinak obě vytváří nový DNS paket s daným doménovým jménem, který zasílají na uživatelem zadaný server a čekají na odpověď. Poté co přijde odpověď, tak změní id v DNS hlavičce a posílají zpět paket původnímu klientovi. Poté server čeká na další paket a následně po přijetí paketu se tato akce opakuje.

Ukončení

Pokud program ukončíme pomocí CTRL + C(SIGINT), tak po sobě uvolní alokovanou paměť a validně skončí. Pokud ho násilně ukončíme (SIGKILL), tak skončí, ale neuvolní si po sobě alokované zdroje.

Testování

Při vytváření programu byl vytvořen test.sh, pro usnadnění testování. Tento soubor využívá program dig k vytváření dotazů. Makefile podporuje **make test**, který využívá právě test.sh a soubor s filtrovanými doménovými jmény. Oba tyto soubory jsou k projektu přiloženy. Program byl dále testován na studentském serveru merlin. Jak už bylo řečeno, tak samotný server nic nevypisuje a tak výstup z testování je výpis od klienta.

Výstupy z testování

Ukázka validního nevyfiltrovaného dotazu. Odpověď přišla s rcode flagem NOERROR.

```
; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @127.0.0.1 -p 3333 www.seznam.cz
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3712
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.seznam.cz.                 IN      A

;; ANSWER SECTION:
www.seznam.cz.          137     IN      A       77.75.75.176
www.seznam.cz.          137     IN      A       77.75.74.172
www.seznam.cz.          137     IN      A       77.75.74.176
www.seznam.cz.          137     IN      A       77.75.75.172

;; Query time: 3 msec
;; SERVER: 127.0.0.1#3333(127.0.0.1)
;; WHEN: Tue Nov 10 22:58:44 CET 2020
;; MSG SIZE  rcvd: 95
```

Ukázka dotazu s vyfiltrovanou doménou či poddoménou. Odpověď přišla s rcode flagem REFUSED.

```
; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @localhost -p 3333 wow.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 5536
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: bbf11e94a9b53893 (echoed)
;; QUESTION SECTION:
;wow.com.                       IN      A

;; Query time: 0 msec
;; SERVER: 127.0.0.1#3333(127.0.0.1)
;; WHEN: Tue Nov 10 22:58:44 CET 2020
;; MSG SIZE  rcvd: 48


; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @localhost -p 3333 asda.wow.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 57748
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 963399df1ff74a1e (echoed)
;; QUESTION SECTION:
;asda.wow.com.                  IN      A

;; Query time: 0 msec
;; SERVER: 127.0.0.1#3333(127.0.0.1)
;; WHEN: Tue Nov 10 22:58:44 CET 2020
;; MSG SIZE  rcvd: 53
```

Ukázka dotazu, která má typ, který není na server implementován. Odpověď přišla s rcode flagem NOTIMP.

```
; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @127.0.0.1 -p 3333 -x 216.58.220.110
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOTIMP, id: 21318
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a7ac221f8eefb18b (echoed)
;; QUESTION SECTION:
;110.220.58.216.in-addr.arpa.   IN      PTR

;; Query time: 0 msec
;; SERVER: 127.0.0.1#3333(127.0.0.1)
;; WHEN: Tue Nov 10 22:58:44 CET 2020
;; MSG SIZE  rcvd: 68


; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @127.0.0.1 -p 3333 mx fit.vutbr.cz
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOTIMP, id: 44291
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 1956b9a671ec9cfb (echoed)
;; QUESTION SECTION:
;fit.vutbr.cz.                  IN      MX

;; Query time: 0 msec
;; SERVER: 127.0.0.1#3333(127.0.0.1)
;; WHEN: Tue Nov 10 22:58:44 CET 2020
;; MSG SIZE  rcvd: 53
```

Ukázka dotazu nevyfiltrované domény a poddomény, která neexistuje. Odpověď přišla s rcode flagem NXDOMAIN.

```
; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @127.0.0.1 -p 3333 gooasdasdagle.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 47372
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;gooasdasdagle.com.             IN      A

;; AUTHORITY SECTION:
com.                    560     IN      SOA     a.gtld-servers.net. nstld.verisign-grs.com. 1605045155 1800 900 604800 86400

;; Query time: 12 msec
;; SERVER: 127.0.0.1#3333(127.0.0.1)
;; WHEN: Tue Nov 10 22:58:44 CET 2020
;; MSG SIZE  rcvd: 108


; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @127.0.0.1 -p 3333 www.seznam.cz/adsa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 44023
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.seznam.cz/adsa.            IN      A

;; AUTHORITY SECTION:
.                       86395   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2020111001 1800 900 604800 86400

;; Query time: 12 msec
;; SERVER: 127.0.0.1#3333(127.0.0.1)
;; WHEN: Tue Nov 10 22:58:44 CET 2020
;; MSG SIZE  rcvd: 111
```

Použité zdroje

[1] *DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION* [online]. Listopad 1987 [cit. 2020-11-15]. Dostupné z: https://tools.ietf.org/html/rfc1035

[2] *DNS - Protocol and Format* [online]. [cit. 2020-11-15]. Dostupné z: http://www-inf.int-evry.fr/~hennequi/CoursDNS/NOTES-COURS_eng/msg.html

[3] *Deep dive into DNS messages. AMRIUNIX* [online]. [cit. 2020-11-15]. Dostupné z: https://amriunix.com/post/deep-dive-into-dns-messages/

[4] *DNS Query Code in C with linux sockets* [online]. [cit. 2020-11-15]. Dostupné z: https://gist.github.com/fffaraz/9d9170b57791c28ccda9255b48315168

[5] *Stack overflow* [online]. [cit. 2020-11-15]. Dostupné z: https://stackoverflow.com/