VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Export DNS informací pomocí protokolu Syslog

ISA - Síťové aplikace a správa sítí

19. listopadu 2018 Matěj Mitaš (xmitas02)

Obsah

1 Zadání

Úkolem bylo vytvořit nástroj pro zpracování DNS komunikace s výstupem ve formát pro nástroj `Syslog`. Projekt obsahuje spustitelný soubor `dns-export` s následující konvencí volání:

```
./dns-export [-s server] [-t timeout] [-i interface] [-r file]
```

- s (server) - adresa serveru, na jehož portu `514` je spuštěn naslouchač zpráv typu Syslog
- r (read) - zpracuje soubor typu `.pcap`, obsahující log sítě
- i (interface) - sťové rozhraní, nad níž je realizováno odposlouchávání
- t (timeout) - volitelný přepínač pro nastavení intervalu odeslání zpráv na serveru (pouze při odchytávání živé komunikace, standartně 60s)

1.1 Příklady použití

Jak vyplývá z výše zmíněného, program lze sputit ve dvou módech (*živé odchytávání* a *čtení ze souboru*). První zmíněný mód může být volán takto:

```
./dns-export -s syslog.mujserver.cz -r /logs/2_12_2017-en1.pcap
```

Na server `syslog.mujserver.cz` zašlu pro zpracování všech paketů v souboru `/logs/2_12_2017-en1.pcap` jejich rozparsovaný výpis.

```
./dns-export -s syslog.mujserver.cz -i en1 -t 3
```

Na server `syslog.mujserver.cz` zašlu pro s periodou `3s` rozparsované odchycené pakety z rozhraní `en1`.

2 Teoretický úvod

Díky přednáškám jsem měl obecnou představu, jak je protokol DNS navržen. Nicméně pro praktickou implementaci bylo třeba prozkoumat více zdrojů. (viz sekce Reference).

DNS Query obecně nabývá dvou hodnot, dotaz a odpověd. Pro svůj přenos používá protokol UDP, jelikož v množství požadavků by jakékoliv aplikace či obecněji programy pracující s touto technologií byly neúměrně zdržovány ať již tvořením, či dekodováním. Obecně je maximální délka `512B`.

2.1 Linková vrstva

Ještě než je možno přistoupit k samotnému DNS paketu, jen nutno prostoupit nižšími vrstvami `ISO/OSI`. Nejnižší vrstva ke které lze přistoupit, `MAC adresy` nás nezajímají, z hlediska programu použita celková délka paketu.

2.2 Síťová vrstva

Podporuji pouze `IP` a to ve verzích `v4` i `v6`. Z hlediska výsledného výstupu zprávy `Syslogu` je zajímavá pouze zdrojovou adresou, viz. sekce o Syslogu.

2.3 Transportní vrstva

Zde řešíme transportní protokol. Naprostá většina DNS komunikace je řešena pomocí transportního protokolu `UDP`. V mém řešení jsem vzal na vědomí i `TCP`, nicméně nutnost identifikace paketů a jejich vzájemná fragmentace mě odradila od tohoto řešení.

2.4 Syslog

...

2.5 Aplikační vrstva

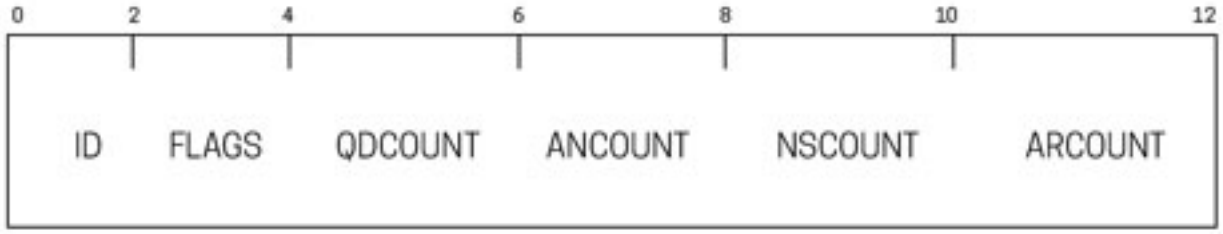
V našem případě běží aplikace na aplikačním protokolu DNS, který je dopodrobna rozepsán níže.

2.5.1 Obecná struktura DNS dotazu

Délka jednotlivých částí se může lišit, avšak jde hlavně o to, aby dotaz měl maximálně $512B$.

- **HEADER** Obsahuje identifikační a příznakovou část dat.
- **QUESTION** Sekce dotazů, zde je to nejdůležitější pro dotazy.
- **ANSWER** Sekce odpovědí, zde je to nejdůležitější pro odpovědi.
- **AUTHORITY** Informace o autoritativních serverech.
- **ADDITIONAL** Další informace.

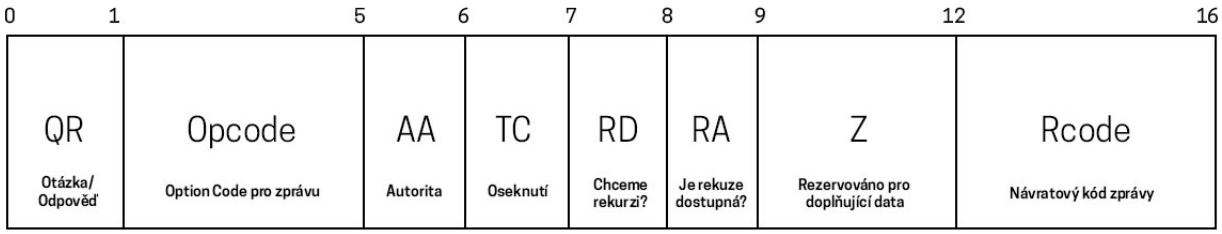
2.5.2 DNS Header (hlavička)



pozn. uvedené hodnoty v grafu značí počet BAJT Ů určených pro jednotlivé části protokolu.

- **ID** - *2B* - Unikátní id, které posíláme v každém dotazu (zde použito *43951*) pro zpětnou kontrolu odpovědí. V případě nesouladu vypíšeme chybu.
- **Sekce příznaků** - *2B* - Příznaky, kterými ovládáme vlastní zprávu (viz níže).
- **QDCOUNT** - *2B* - Počet dotazů.
- **ANCOUNT** - *2B* - Počet odpovědí.
- **NSCOUNT** - *2B* - Počet jmenných serverů.
- **ARCOUNT** - *2B* - Počet doplňjících informací.

2.5.3 DNS Header Flags (příznaky)



pozn. uvedené hodnoty v grafu značí počet BITŮ určených pro jednotlivé části protokolu.

- **QR** - *1b* - 0: query (dotaz), 1: response (odpověď).
- **Opcode** - *4b* - 0: query (standartní dotaz), více než 1, jsou poté speciální typ, které jsou mimo rozsah tohoto projektu (IQUERY, STATUS, UPDATE, NOTIFY).
- **AA** - *1b* - 0: odpověď od neautoritativního serveru, 1: odpověď od autoritativního serveru.
- **TC** - *1b* - 0: bez oseknutí (překročíme $512B$), 1: oseknutí, použij TCP pro komunikaci.
- **RA** - *1b* - Dostupnost rekurze (pro rekurzivní a iterativní vyhledávání).
- **RD** - *1b* - Chceme rekurzi (pouze pro rekurzivní).
- **Z** - *3b* - Další informace (zpravidla prázndné)
- **Rcode** - *1b* - Návratové kódy operace.
  0 - V pořádku.
  1 - Chybný dotaz.
  2 - Server neumí odpovědět
  3 - Jméno neexistuje.
  4 - Nepodporovaný typ dotazu.
  5 - Refused od serveru.

Samotná hlavička je v mé implementaci reprezentována níže uvedenou strukturou, všimněme si položky *opt*, práce s ním bude vysvětlena v implementační sekci.

```
typedef struct ipk18_dns_Header {
        uint16_t id;
        uint16_t opt;
        uint16_t qdcount; // kolik vet ma dotaz
        uint16_t ancount; // kolik vet ma odpoved
        uint16_t nscount; // sekce pro odkazy na autoritativni servery
        uint16_t arcount; // doplnujici informace
} ipk18_dns_Header;
```

2.5.4 DNS Query (dotaz)

Je třeba vyplnit pole dotazu, na specifikace práce s *QNAME* narážím v části Implementace. V projektu použitelné tyto možnosti *QTYPE* a *QCLASS*.

- **QNAME** - *1B * počet znaků* - Doménové jméno, či IP adresa (viz Implementace)
- **QTYPE** - *2B* - Typ požadavku

  1 - A (IPv4 adresa).

  28 - AAAA (IPv6 adresa).

  2 - NS (jmenný server).

  5 - CNAME (CNAME záznam).

  12 - PTR (Reverzní překlad).
- **QCLASS** - *2B* - 1: IN, třída internet

2.5.5 DNS Response (odpověď)

Pole odpovědí (může být i více než jedna, vždy však v rámci $512B$), DNS používá komprimaci, proto tedy při dotazu na QNAME *www.matejmitas.com* nekopíruje do každé odpovědi celý string. Místo toho na jeho pozici vloží konstantu $0xc0$ a přímo za ní uloží adresu skoku (zde $0x0c$ což odpovídá indexu 12, tedy místa, kde je daný string uložený pro zmenšení datové náročnosti.

```
08 00 45 00   ...'.z.. ......E.
08 08 64 41   .PB...:. ......dA
81 80 00 01   C..5...< qP......
61 74 65 6a   .......w ww.matej
00 01 c0 0c   mitas.co m.......
69 52         ........ ....iR
```

Níže je struktura odpovědi (je třeba brát na vědomí, že se vždy vrací celý blok, u dotazu je to [hlavička + dotaz] a u odpovědi [hlavička + dotaz + odpověď].

- **Kopie** - *6B* - QNAME, QTYPE, QCLASS
- **TTL** - *2B* - Time-To-Live, doba platnosti
- **RDLENGTH** - *2B* - Délka nasledující datové části.
- **RDATA** - *1B * RDLENGTH* - Datová část

3 Implementace projektu

Jelikož byl k implementaci projektu použit programovací jazyk *C*, bylo potřeba přistoupit k některým kompromisům, hlavně co se týče práce s pamětí.

Reference

BUSH, R. *Clarifications to the DNS Specification* [online]. 1997. [cit. 9. 4. 2018]. Dostupné z: `https://tools.ietf.org/html/rfc2181`.

FROM WIKIPEDIA, t. f. e. *Domain Name System* [online]. 2018. [cit. 9. 4. 2018]. Dostupné z: `https://en.wikipedia.org/wiki/Domain_Name_System`.

LIBOR DOSTALEK, A. K. *Velky pruuvodce protokoly TCP/IP a systemem DNS*. 5. vydani. Computer Press, 2012. ISBN 978-80-251-2236-5.

MOON, S. *DNS Query Code in C with Linux sockets* [online]. [cit. 9. 4. 2018]. Dostupné z: `https://www.binarytides.com/dns-query-code-in-c-with-linux-sockets/`.

RYSAVY, O. – RAB, J. *IPK - Sitova vrsta - 4. prednaska* [online]. 2018. [cit. 12. 3. 2018]. Dostupné z: `https://wis.fit.vutbr.cz/FIT/st/course-files-st.php?file=%2Fcourse%2FIPK-IT%2Flectures%2FIPK2017L-04-IPv4.pdf`.