Vysoké Učení Technické v Brně

Fakulta Informačních Technologií

Dokumentace k projektu z předmětu ISA

Export DNS informací pomocí protokolu Syslog

16. listopadu 2018

Autor: Adam Petráš, xpetra19@stud.fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Obsah

1 Úvod 3

2 Důležité pojmy 3

2.1 Dns-export 3

2.2 Typy DNS záznamů 3

2.2.1 Záznam typu A 3

2.2.2 Záznam typu AAAA 3

2.2.3 Záznam typu MX 4

2.2.4 Záznam typu CNAME 4

2.2.5 Záznam typu TXT 4

2.2.6 Záznam typu NS 4

2.2.7 Záznam typu SOA 4

2.2.8 Záznam typu RRSIG 5

2.2.9 Záznam typu NSEC 5

3 Návrh programu 6

4 Implementace 6

4.1 Offline sniffing 6

4.2 Online sniffing 6

5 Použití aplikace 7

Reference 7

1 Úvod

Dokumentace k projektu z předmětu síťové aplikace a správa sítí. Dokument se ve zkratce zabývá představením a vysvětlením funkce DNS a dále popisuje návrh, implementaci a použití výsledné aplikace. Tato aplikace může být využívaná pro analýzu DNS packetů na počítačové síti.

2 Důležité pojmy

Pro návrh a implementaci programu dns-export je důležité mít alespoň částečné znalosti, co se týká funkčnosti aplikace, a síťovému provozu. V této části je popsán základní princip aplikace dns-export, typy dns záznamů, které jsou na sítí odchytávány.

2.1 Dns-export

Program dns-export se používá především pro analýzu DNS zpráv na počítačové síti. Aplikace sbírá packety, které obsahují DNS záznamů. Ty poté rozbaluje z jednotlivých hlaviček, do kterých je packet zapouzdřen. Packet může mít více odpovědí, ty aplikace parsuje jednotlivě po sobě a sbírá všechny potřebné informace o každé odpovědi. Následně po přeparsování odpovědí jsou odpovědi odeslány pomocí UDP spojení na syslog server.

2.2 Typy DNS záznamů

2.2.1 Záznam typu A

DNS záznam typu A je určen, pro nastavení konkrétní IP adresy, to je tam kam má být doména nebo subdoména nasměrována. Je možné nasměrovat doménu nebo subdoménu na jakoukoliv IP adresu. Do tohoto typu záznamu lze zadat pouze **IP adresa** ve formátu **IPv4**.

2.2.2 Záznam typu AAAA

DNS záznam typu AAAA je alternativou k záznamu typu A. Používají se, pokud má cílový server **IP adresu** ve formátu **IPv6**.

2.2.3 Záznam typu MX

DNS záznam typu MX slouží k nastavení mail serveru, na který se má doručovat pošta pro danou doménu. Před názvem se uvádí priorita (celé kladné číslo), která se využívá v případě více MX záznamů. Obecně platí, že nejvyšší prioritu má server s nejnižším číslem. Pokud server neodpoví tak se zkouší další. Tyto servery slouží jako záložní a využijí se pouze tehdy, pokud není k dispozici server s nejvyšší prioritou. Pokud mají servery stejnou prioritu tak je jedno, kterému z nich se pokusíme zprávu doručit.

2.2.4 Záznam typu CNAME

DNS záznam typu CNAME je určen k nasměrování domény nebo subdomény na libovolnou jinou doménu nebo subdoménu. Do tohoto typu záznamu lze zadat pouze text (například domena.cz). Výhodou záznamu typu CNAME je že pokud se zamění IP adresa cílového serveru tak tento záznam bude stále fungovat na rozdíl od záznamu typu A

2.2.5 Záznam typu TXT

DNS záznam typu TXT slouží k zapsání libovolného textového řetězce. Používá se například k ověření vlastníka domény, kdy poskytovatel hostingových služeb požádá o vložení TXT záznamu s určitým textem aby ověřil majitele domény. Často se také využívá pro záznamy typu **SPF**.

2.2.6 Záznam typu NS

DNS záznam typu NS slouží ke sdělení seznamu **autoritativních DNS serverů** pro danou doménu. Uváděny jsou názvy serverů (tedy jejich doménová jména), nikoliv IP adresy. Chce-li se zařízení spojit s autoritativním DNS serverem nějaké domény, nejprve si na DNS server vyšší úrovně zjistí všechny záznamy typu NS pro hledanou doménu, vybere si jeden z nich a zjistí si k němu IP adresu, teprve pak může dojít ke komunikačnímu spojení přes protokol DNS.

2.2.7 Záznam typu SOA

je speciální záznam, který se musí v každém zónovém souboru vyskytovat právě jednou. Jedná se o jakousi hlavičku, která obsahuje následující informace:

MNAME – název primárního DNS serveru pro danou zónu

RNAME – kontakt na správce zónového souboru - uvádí se e-mailová adresa, ve které je zavináč nahrazen za tečku (protože znak zavináče má v DNS speciální význam)

SERIAL – sériové číslo zóny – jedná se o číselný údaj, který udává verzi zónového souboru; při změně v záznamech se číslo navýší a sekundární DNS servery si při porovnání s číslem, které mají uložené u sebe, zjistí, že došlo ke změně a že je třeba data aktualizovat

REFRESH - počet sekund, po jejichž uplynutí od poslední kontroly či načtení zóny z primárního DNS provede sekundární server kontrolu sériového čísla

RETRY - po zahájení zjišťování sériového čísla z předchozího bodu opakuje požadavek na primární DNS server po uplynutí RETRY sekund, pokud se předchozí požadavek nezdařil (pokud server neodpověděl)

EXPIRE - pokud se nedaří stáhnout sériové číslo z primárního DNS a od posledního úspěšného pokusu uplynulo EXPIRE vteřin, je zóna považována za neplatnou a sekundární DNS server by ji měl vyřadit ze svých záznamů (zapomenout ji)

2.2.8 Záznam typu RRSIG

DNS záznam typu RRSIG používá veřejný kryptografický klíč pro přihlášení a ověření. Digitální podpisy jsou uloženy v RRSIG záznamu a jsou použity k autentizaci.

2.2.9 Záznam typu NSEC

DNS záznam typu NSEC je RR záznam, který ve svých RDatech obsahuje informaci o následujícím záznamu v setříděné zóně a informaci o všech existujících typech pro vlastníka záznamu. Při dotazu na neexistující záznam vrací autoritativní DNS server takový NSEC záznam, který je před a za dotazovaným doménovým jménem v případě kompletní neexistence takového doménového jména, nebo přímo NSEC záznam se shodným vlastníkem v případě neexistence konkrétního typu RR záznamu.

3 Návrh programu

Aplikace dns-export pracuje a rozbaluje jednotlivé packety, proto používám knihovnu pcap, která mi zajišťuje sběr jednotlivých packetů online (ze síťové komunikace) nebo offline (ze souboru .pcap). Knihovna také nabízí filtrování packetů, které je vhodné proto, aby mi byly posílány z pcap knihovny pouze ty packety, které požaduji. Jako filtr knihovna veme textový řetězec ten poté zkompiluje a nastaví filtr. Packety, které mi pošle knihovna, následně rozříznu, vemu síťovou hlavičku a IP hlavičku. Poté každý packet obsahuje DNS záznam, tu musím však z jednotlivých packetů dostat sám. Každý DNS záznam má v podstatě jinou strukturu, takže musím parsovat každý typ záznamu jinak.

4 Implementace

Program je implementován v jazyce C++. Je navržen objektově spíše jako zapouzdření do jednotlivých tříd. Aplikace využívá standardních knihoven C++ a je vytvořena pro OS Linux, byla vyvíjena a testována na Ubuntu 16.04 .

4.1 Offline sniffing

Offline sniffing, neboli čtení packetů ze souboru .pcap je realizováno tak, že přečte pcap soubor a jeden packet po druhém parsuje a ukládá přeparsované odpovědi do vektoru. Následně pokud skončí čtení souboru pcap aplikace veme všechny záznamy z vektoru a pošle je na syslog server, který je zadán jako IP adresa do přepínače.

4.2 Online sniffing

Online sniffing, neboli čtení packetů přímo ze sítě, je realizováno tak, že aplikace je napojena na zařízení, které je dáno přepínačem a sleduje pohyb packetů. Pokud zachytí packet, který nese záznam DNS tak jej rozbalí. Odpovědi, které získá z packetu poté parsuje stejně jako offline. Poté co se dokončí parsování odpovědí se jednotlivě uloži do vectoru. Následně pokračuje zase sledování pohybu packetů na síti. Pokud přijde signál SIGUSR1 aplikace vypíše statistiky. Pokud přijde signal SIGALRM poté pošle aplikace všechny odpovědi na syslog server.

5 Použití aplikace

Program musí být spuštěn s právy roota, pokud chceme online sniffing, pokud však chceme offline sniffing práva nejsou potřeba.

Parametry spuštění programu jsou následující:

dns-export [-r file.pcap] [-i interface] [-s syslog-server] [-t seconds]

- -h: zobrazí nápovědu
- -r : zpracuje daný pcap soubor
- -i : naslouchá na daném síťovém rozhraní a zpracovává DNS provoz
- -s : hostname/ipv4/ipv6 adresa syslog serveru
- -t : doba výpočtu statistik, výchozí hodnota 60s

Reference

[1] Domain Names – Implementation and specification [Online] https://www.ietf.org/rfc/rfc1035.txt

[2] DNSSEC Resource Records [Online] https://www.ietf.org/rfc/rfc4034.txt

[3] Domain Name Systém [Online] https://cs.wikipedia.org/wiki/Domain_Name_System

[4] List of DNS record types [Online] https://en.wikipedia.org/wiki/List_of_DNS_record_types