ISA

Export DNS informací

2018/2019

Jméno: Petr Medek
Login: xmedek07

Obsah

1. Úvod

Tento dokument byl vytvořen jako dokumentace k projektu do předmětu ISA (Síťové aplikace a správa sítí). Základem programu je knihovna libpcap pomocí které program zpracovává pakety. Komunikace se syslog serverem je zajištěna pomocí BSD socketu.

2. Implementace

Pro implementaci jsem zvolil jazyk c++ ale bez využití objektových vlastností. Výhodou oproti jazyku C byla jednoduší práce s textem. Aplikace je vytvořena pro OS Linux, byla vyvíjena a testována na Ubuntu 16.04. Výstup byl kontrolován pomocí programu wireshark.

3. Knihovny

V programu jsou využívány funkce, konstanty a struktury z následujících knihoven:

```
#include <pcap.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <arpa/inet.h>
#include <netinet/in.h>
#include < netinet/ip.h>
#include < netinet/tcp.h>
#include < netinet/udp.h>
#include <string>
#include <sstream>
#include <iostream>
#include <stdio>
#include <cstdlib>
#include <net/ethernet.h>
#include <getopt.h>
#include <cstring.h>
#include <signal.h>
#include <unistd.h>
#include <netdb.h>
#include <ctime>
#include <chrono>
#include <climits>
```

4. DNS

Pro komunikaci na internetu se používají IP adresy k identifikaci komunikujících uzlů. Pro člověka je však IP adresa těžko zapamatovatelná, a proto byl vymyšlen systém, který umožňuje pro IP adresu zavést doménové jméno. Toto doménové jméno lze pak používat tam kde je možno použít IP adresu. Vazba mezi doménovým jménem a IP adresou je definována v celosvětově distribuované databázi DNS. Části této databáze jsou umístěny DNS serverech. Pro komunikaci s DNS serverem se používá TCP/UDP protokol na portu 53 (UDP protokol se vyskytuje častěji).

5. TCP fragmentace

Při přenosu souboru hraje roli jeho velikost. Maximální velikost Ethernet paketu je 1500B, pokud by paket měl překročit tuto velikost je rozdělen na více segmentů, jednotlivé segmenty dat opatří sekvenčním číslem a odešlou se. To znamená že přenášený soubor je rozdělen na části, které odpovídají maximální velikosti. Na straně klienta se tyto části složí dohromady. Aplikace dns-export podporuje spojování TCP paketů.

6. Popis programu

Program dns-export zpracovává data protokolu DNS a statistiky posílá na zadaný syslog server. Pokud aplikace zpracovává pcap soubor a není zadaný syslog server na vypíše statistiky na STDOUT. Aplikace zasílá statistiky defaultně každých 60s, pokud je aplikaci zaslán signál SIGUSR1 vypíše všechny statistiky na STDOUT.

7. Zpracování paketů

Program buď naslouchá na daném síťovém rozhraní nebo zpracovává zadaný soubor. Zpracování jednotlivých paketů probíhá v obou případech stejně. Pro každou hlavičku mám vytvořenou strukturu, která odpovídá dané části paketu. Nejprve se načte Frame, Ethernet hlavička a IP hlavička. V IP hlavičce se nachází informace o protokolu, který bude následovat, tímto zjistíme, zda bude následovat UDP nebo TCP. Dále načteme hlavičku odpovídajícího protokolu, zde pomocí portu zjistíme, zda následuje DNS hlavička (DNS používá port 53).

Frame
Ethernet
IP
TCP/UDP
DNS

8. DNS zpráva

Všechny DNS zprávy mají stejný formát. V DNS hlavičce můžeme najít ID, Flags nebo také počty všech druhů odpovědí. Podle Flagu QR můžeme zjistit, zda se jedná o DNS dotaz/odpověď. V DNS odpovědi se může nacházet několik typů RR, aplikace podporuje všechny vypsané v následující tabulce.

Header
Question
Answer
Authority
Additional

ID	Typ	Popis
1	A	IPv4 address
2	NS	Authoritative name server
5	CNAME	Canonical name for an alias
6	SOA	Marks the start of a zone of authority
15	MX	Mail exchange
16	TXT	Text strings
28	AAAA	IPv6 Address.
43	DS	Delegation Signer
46	RRSIG	RR Signature
47	NSEC	Lists of RR types for the RR name
48	DNSKEY	Public key

9. DNS záznam

Name
Type
Class
TTL
Rdata Length
Rdata

Každý RR má variabilní délku, protože obsahuje dvě pole s různou délkou. Prvním polem je „Name“ které vždy končí bytem s hodnotou 0, toto pole také často obsahuje ukazatele viz kapitola o kompresi. Druhým je pole „Rdata“ jehož délku udává pole „Rdata Length“. Obsah pole „Rdata“ záleží na typu záznamu. V další čísti jsou popsány k čemu slouží některé ze zajímavějších záznamů.

1. RRSIG

V RRSIG se nachází DNSSEC podpis pro sadu záznamů (jeden nebo více DNS záznamů se stejným názvem a typem).

2. NSEC

Typ NSEC uvádí všechny typy záznamů, které existují pro dané RR Name. Všechny typy záznamů jsou uloženy v bitovém poli.

3. DNSKEY

Záznam DNSKEY obsahuje veřejný klíč, který se používá k ověření podpisů DNSSEC v záznamech RRSIG.

10. Komprese

Komprese je využívána k redukci velikosti DNS paketu. V paketu se může doménové jméno vyskytnout opakovaně, komprese toto opakující se jméno uvede pouze jednou a každý další výskyt je nahrazen ukazatelem na první výskyt. Jako oddělovač jednotlivých částí doménového jména je použito číslo určující délku následující části. Tento oddělovač je uložen v jednou bajtu. Každá část doménového jména může být dlouhá maximálně 63 znaků. Oddělovací bajt má maximální hodnotu 63. Pokud je v tomto bajtu číslo 192 nebo větší, pak to znamená že nebude uvedeno doménové jméno, ale pouze odkaz na jeho předcházející výskyt.

11. Použití programu

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

-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
-h : nápověda

- **./dns-export -h**

  Vypíše nápovědu k programu.
- **./dns-export -r dns.pcap -s 192.168.1.2**

  Zpracuje soubor *dns.pcap* a odešle statistiky na syslog server který se nachází na adrese *192.168.1.2.*
- **./dns-export -i wlp2s0 -t 20**

  Poslouchá na rozhraní *wlp2s0*.
- **./dns-export -i wlp2s0 -s 192.168.1.2 -t 20**

  Poslouchá na rozhraní *wlp2s0* a každých *20s* posílá statistiky na syslog server na adrese *192.168.1.2.*
- **./dns-export -i wlp2s0 -s 192.168.1.2**

  Poslouchá na rozhraní *wlp2s0* a každých *60s* (Default) posílá statistiky na syslog server na adrese *192.168.1.2.*
- **./dns-export -r dns.pcap**

  Zpracuje soubor *dns.pcap* a odešle statistiky na *STDOUT*.
- **./dns-export -r dns.pcap -i wlp2s0**

  ERROR: Neplatné argumenty.

12. Reference

[1] https://routley.io/tech/2017/12/28/hand-writing-dns-messages.html
[2] http://www.firewall.cx/networking-topics/protocols/domain-name-system-dns/160-protocols-dns-query.html
[3] https://simpledns.com/help/dns-record-types
[4] http://www.networksorcery.com/enp/protocol/dns.htm
[5] https://tools.ietf.org/html/rfc3755
[6] https://tools.ietf.org/html/rfc3225
[7] https://tools.ietf.org/html/rfc2535
[8] https://tools.ietf.org/html/rfc1035
[9] https://tools.ietf.org/html/rfc5424