Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií
Ilkovičova 2, 842 16 Bratislava 4

Počítačové a komunikačné siete

Zadanie 1: Analyzátor sieťovej komunikácie

Matej Belluš

AIS ID:	70495
Študijný program:	PKSS
Ročník:	3
Krúžok:	Piatok 08:00
Predmet:	Počítačové a komunikačné siete
Ak. rok:	2014/15, LS

Zadanie úlohy

Navrhnite a implementujte programový "post" analyzátor Ethernet siete, ktorý analyzuje komunikácie v sieti zaznamenané v súbore a poskytuje nasledujúce informácie o komunikáciách.

1) Výpis všetkých komunikácií, t.j. všetkých rámcov v hexadecimálnom tvarepostupne tak, ako boli zaznamenané v súbore.
   Pre každý rámec uveďte:
   - Poradové číslo rámca v analyzovanom súbore.
   - Dĺžku rámca v bajtoch poskytnutú paketovým drajverom, ako aj dĺžku tohto rámca prenášaného po médiu.
   - Typ rámca – Ethernet II, IEEE 802.3 (IEEE 802.3 - LLC, IEEE 802.3- LLC – SNAP, IEEE 802.3 – Raw).
   - Zdrojovú a cieľovú fyzickú (MAC) adresu uzlov, medzi ktorými je rámec prenášaný.
   - Na konci výpisu uveďte IP adresy všetkých vysielajúcich uzlov, ako aj IP adresu uzla, ktorý sumárne odvysielal (bez ohľadu na príjemcu) najväčší počet bajtov. Počet bajtov taktiež uveďte. Uvažujte iba IP adresy vnorené v rámci Ethernet II.

Vo výpise jednotlivé bajty usporiadajte po 8, 16 alebo 32 v jednom riadku. Pre Prehľadnosť výpisu je vhodné použiť neproporcionálny font.

2) Študent musí vedieť vysvetliť, aké informácie sú uvedené v jednotlivých rámcoch Ethernet II, t.j. vnáranie protokolov ako aj ozrejmiť dĺžky týchto rámcov.

3) V súboroch so zachytenými komunikáciami analyzujte zadané typy komunikácií. Analýzu cez jednotlivé vrstvy vykonajte len pre rámce Ethernet II a protokoly rodiny TCP/IPv4.
Analyzované komunikácie s protokolmi:
a) HTTP komunikácie
b) HTTPS komunikácie
c) TELNET komunikácie
d) SSH komunikácie
e) FTP riadiace komunikácie
f) FTP dátové komunikácie
g) Všetky TFTP komunikácie
h) Všetky ICMP komunikácie
i) Všetky ARP dvojice (request – reply).

Vo všetkých výpisoch treba uviesť aj IP adresy a pri transportných protokoloch aj porty komunikujúcich uzlov.

V prípadoch komunikácií so spojením vypíšte iba jednu kompletnú komunikáciu – Obsahuje otvorenie (SYN) a ukončenie (FIN na oboch stranách alebo ukončenie FIN a RST alebo ukončenie iba s RST) spojenia a aj prvú nekompletnú komunikáciu, ktorá obsahuje iba otvorenie spojenia.Pri výpisoch vyznačte, ktorá komunikácia je

kompletná.

Pre nájdenú a vypísanú kompletnú komunikáciu urobte štatistiku výskytu dĺžky rámca Ethernet II v bajtoch, a to pre dĺžky 0 až19, 20 až 39, 40 až 79, atď. (postupne x až (2x-1)).

V prípade výpisu h) uveďte aj typ ICMP správy (pole Type v hlavičke ICMP), napr. Echo request, Echo reply, Time exceeded, a pod.

V prípade výpisu i) uveďte pri ARP-Request IP adresu, ku ktorej sa hľadá MAC (fyzická) adresa a pri ARP-Reply uveďte konkrétny pár - IP adresa a nájdená MAC adresa. V prípade, že bolo poslaných viacero rovnakých rámcov ARP-Request, vypíšte všetky.

Ak počet rámcov danej komunikácie je väčší ako 20, vypíšte iba 10 prvých a 10 Posledných rámcov.

Pri všetkých výpisoch musí byť poradové číslo rámca zhodné s číslom rámca v Analyzovanom súbore.

4) Program musí byť organizovaný tak, aby čísla protokolov v rámci Ethernet II a v IP pakete ako aj čísla portov v transportných protokoloch boli programom určené z externého súboru a pre známe protokoly a porty boli uvedené aj ich názvy.

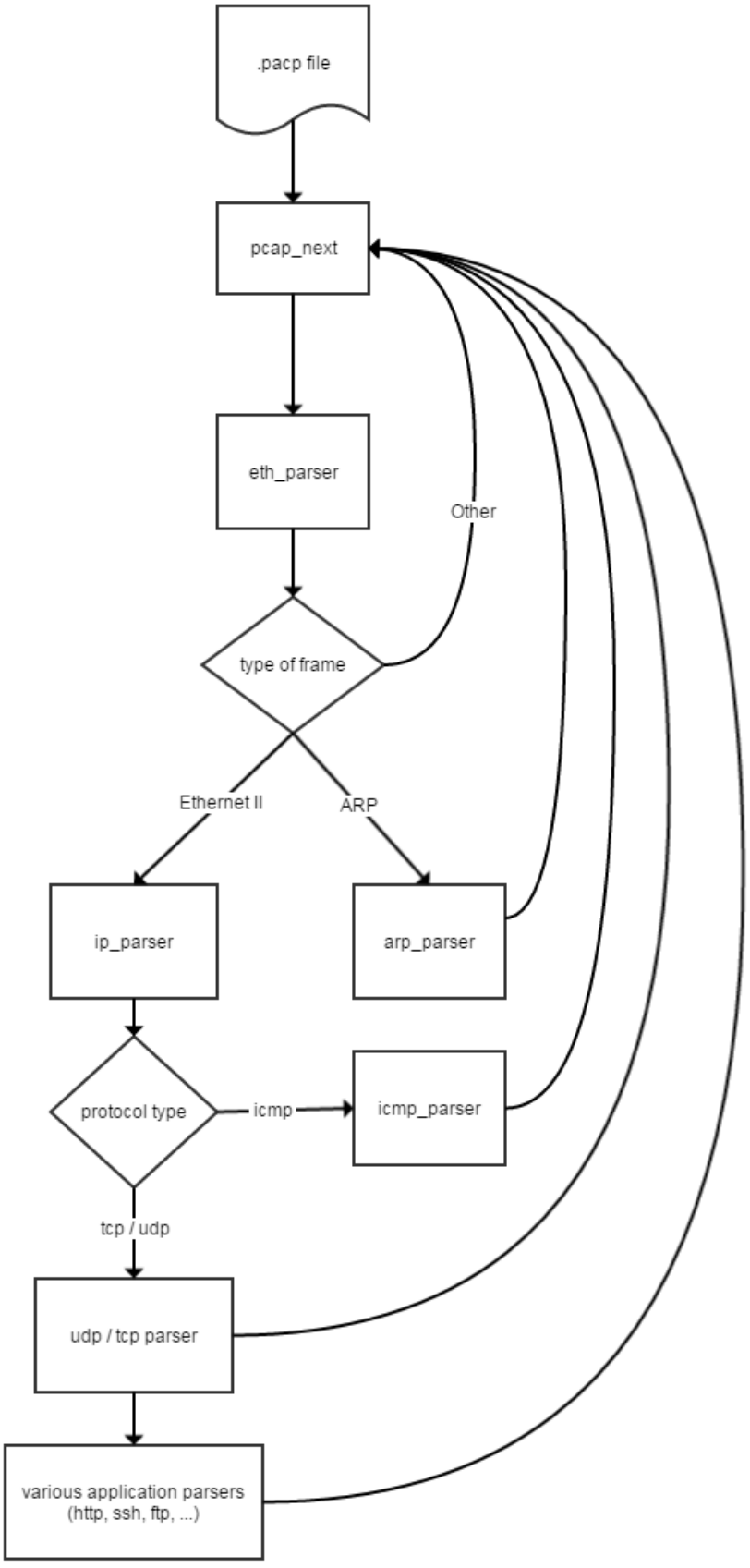
5) V procese analýzy rámcov pri identifikovaní jednotlivých polí rámca ako aj polí Hlavičiek vnorených protokolov nie je povolené použiť funkcie poskytované použitým Programovacím jazykom. Celý rámec je potrebné spracovať postupne po bajtoch.

6) Program musí byť organizovaný tak, aby bolo možné jednoducho rozširovať jeho Funkčnosť o výpis rámcov podľa ďalších požiadaviek na protokoly v bode 3) - pri Doimplementovaní jednoduchej funkčnosti na cvičení.

7) Študent musí byť schopný preložiť a spustiť program v miestnosti, v ktorej má cvičenia! V danom týždni, podľa harmonogramu cvičení, musí študent priamo na cvičení doimplementovať do funkčného programu (podľa vyššie uvedených požiadaviek) ďalšiu prídavnú funkčnosť.

V danom týždni, podľa harmonogramu cvičení, musí študent priamo na cvičení doimplementovať do funkčného programu (podľa vyššie uvedených požiadaviek) ďalšiu prídavnú funkčnosť.

Blokový návrh riešenia:



Mechanizmus analyzovania protokolov na jednotlivých vrstvách:

Linková vrstva

Na linkovej vrstve sa pozerá na 13 a 14 bajt rámca a podla ich hodnoty sa určí typ rámca. 13 a 14 bajt sa volá etherhetype alebo length. Payload je to, čo nasleduje, 15+ bajt.

Frame type	Ethertype or length	Payload start two bytes
Ethernet II	≥ 1536	Any
Raw IEEE 802.3	≤ 1500	0xFFFF
IEEE 802.2 LLC	≤ 1500	Other
IEEE 802.2 SNAP	≤ 1500	0xAAAA

Ak rámec nieje typu Ethernet II, nemá zmysel ho ďalej analyzovať.

Internetová vrstva

Na internetovej vrstve sa analyzujú len pakety typu IPv4 a ARP. Teda len tie, kde ethernet type je 0x0800 (IPv4) alebo 0x0806 (ARP). O ARP pakert sa stará samostatný modul progrmau. Ďalej sa kontroluje IP hlavička a typ vnoreného protokolu. Typ je 10. Bajt. Aj je typ 1 ide o ICMP paket, ak je typ 6 ide o TCP paket. Ostané typy sa neanalyzujú, nakoľko to nevyžaduje zadanie.

Transportná vrstva

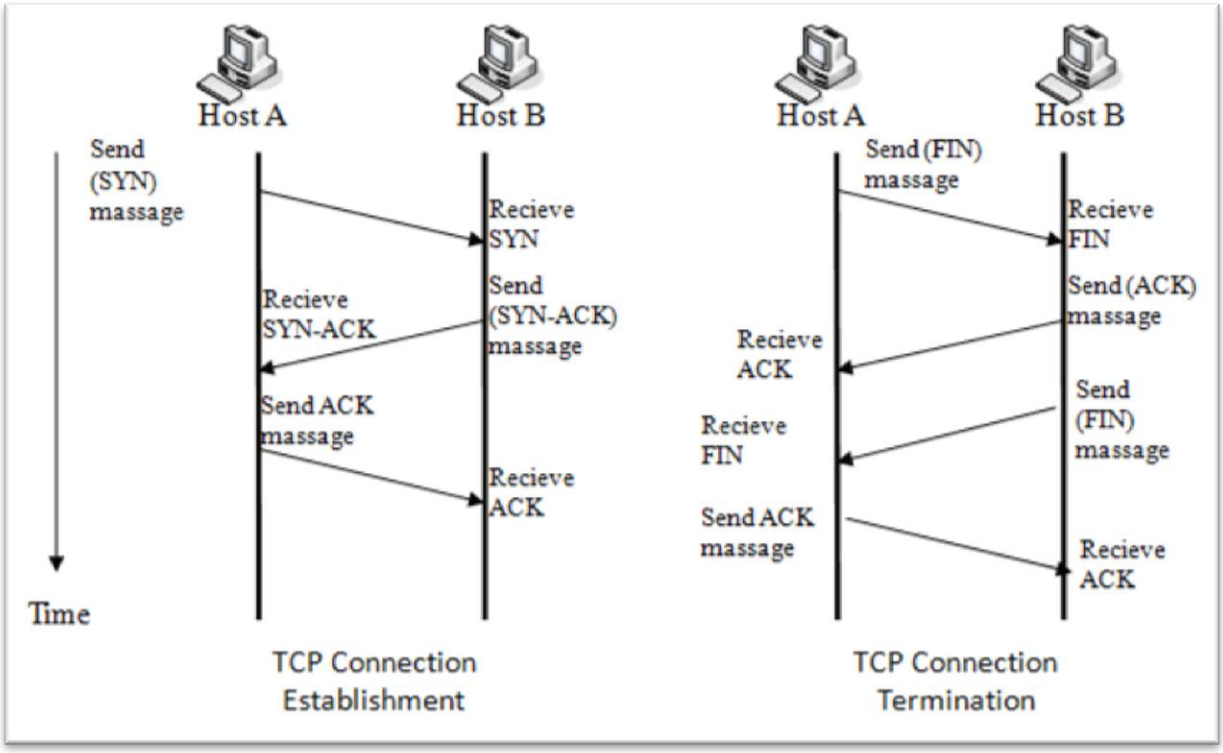
Na transportnej vrstve sa tým pádom analyzuje len TCP hlavička. Podľa prvých 2 bajtov – zdrojový port a druhých 2 bajtov, cielový port sa určuje typ aplikaného protokolu. Relevantné porty sú: 20, 21, 22, 23, 80, 443.

Aplikačná vrstva

Následne sa analyzujú samotné aplikačné dáta, podla typu aplikácie sa zavolá príslušný parser.

Postup pri analýze komunikácie so spojením:

Pri analýze komunikácie so spojením je zásobník protokolov nasledoný:
Ethernet II -> Ipv4 -> TCP. Nadviazanie a ukončenie spojenia:



Nadviazanie spojenia sa relalizuje v 3 krokoch. SYN, SYN-ACK a ACK. Ak sa v kominukácii nájdu tieto flagy v takom to poradí medzi 2 uzlami, môžme prehlásit, že spojenie bolo nadviazanš.

Ukončenie spojenia sa realizuje v 4 krokoch. FIN, ACK, FIN, ACK. Ak sa v kominukácii nájdu tieto flagy v takom to poradí medzi 2 uzlami, môžme prehlásit, že spojenie bolo ukončené.

Lubovolné dáta poslané v čase medzi nadviazaním a ukončením spojenia sú kompetné.

Obsah externých súborov pre určenie protokolov a portov:

Formát:

<číslo portu> <tablátor> <názov>

Príklad:

20 FTP data transfer
21 FTP control (command)
22 The Secure Shell (SSH) Protocol
23 Telnet protocol—unencrypted text communications
80 Hypertext Transfer Protocol (HTTP)
443 Hypertext Transfer Protocol over TLS/SSL (HTTPS)
... ...

Implementačného prostredia a používateľské rozhranie:

Program je naprogramovaný v jazyku C a používa knižnicu pcap. Spúšťa sa cez konzolu a využíva textové rozhranie. Syntax progrmau:

```
analyzer –f file.pcap
```

Vývoj a testovanie sa realizuje na operačnom systéme Ubuntu 14.04 LTS. Fuknčnost na systéme Windows nieje zaručená.

Zdrojový kód

Program je možné stiahnuť z verejného repozitára na adrese:

https://github.com/Horkyze/packet-analyzer