POČÍTAČOVÉ SIETE – cvičenia
ak. rok 2007/08, letný semester

Téma 1) **Sieťový analyzátor**

Zadanie projektu

Navrhnite a implementujte programový "post" analyzátor Ethernet siete, ktorý analyzuje komunikáciu v sieti zaznamenanú do súboru a poskytuje informácie o vnorených protokoloch získané analýzou Ethernet_II rámcov resp. rámcov 802.3.

Riešenie projektu je rozdelené do dvoch častí, implementácia každej časti je hodnotená samostatne. Každá časť predstavuje istú časť z celkovej implementácie "post" analyzátora.

1. časť (5 bodov)

Výpis celej komunikácie - všetkých rámcov v hexadecimálnom tvare, postupne tak ako boli zaznamenané, t.j.
rámec 1,
rámec 2, …….atď.
s uvedením:
poradové číslo rámca,
dĺžka rámca v bajtoch,
typ rámca: Ethernet II alebo 802.3,
MAC adresa zdroja a cieľa.

Napr.
rámec 1
00 04 76 13 97 df 00 00 c0 d7 80 c2 08 00 45 00
00 30 0c 12 40 00 80 06 01 81 93 af 62 ee 93 af
62 e8 04 6f 00 8b 7d d8 e2 e0 00 00 00 00 70 02
40 00 f0 36 00 00 02 04 05 b4 01 01 04 02
dĺžka: 62 bajtov
Ethernet II
SA MAC: 00 00 c0 d7 80 c2 DA MAC: 00 04 76 13 97 df

rámec 2
ff ff ff ff ff ff 00 e0 29 05 51 2b 08 06 00 01
08 00 06 04 00 01 00 e0 29 05 51 2b 93 af 62 1e
00 00 00 00 00 00 93 af 62 0b 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00
dĺžka: 60 bajtov
Ethernet II
SA MAC : 00 e0 29 05 51 2b DA MAC: ff ff ff ff ff ff

atď.

2. časť (15 bodov)

a) Výpis celej komunikácie podľa bodu 1) rozšírený o výpis:
typ vnoreného protokolu zo sieťovej a transportnej vrstvy ako aj zdrojový acieľový port.
V prípade, ak je vnorený IP protokol, treba vypísať aj IP adresy (logické adresy), a to v desiatkovo-bodkovej notácií.
Vnorené protokoly treba, v maximálne možnej miere, uviesť menom a nie iba číslom určeným z rámca.

Napr.

rámec 10
00 00 c0 d7 80 c2 00 04 76 13 97 df 08 00 45 00
00 30 15 79 40 00 80 06 f8 19 93 af 62 e8 93 af
62 ee 00 8b 04 6f 34 dc 19 51 7d d8 e2 e1 70 12
ff ff e1 f8 00 00 02 04 05 b4 01 01 04 02
dĺžka: 62 bajtov
Ethernet II
DA MAC: 00 00 c0 d7 80 c2 SA MAC: 00 04 76 13 97 df
IP,
DA IP: 147.175.98.238 SA IP: 147.175.98.232
TCP,
SA port: 00 8b – netbios-ssn DA port: 04 6f

atď.

b) V zaznamenanej komunikácii nájdite jednu kompletnú TCP komunikáciu a vypíšte ju v tvare a so všetkými informáciami ako je uvedené v časti 2a). Poradové číslo rámca musí zodpovedať číslu rámca v zaznamenanej komunikácii.
Vo výpise uveďte aj dôležité príznaky z hlavičky TCP protokolu. Ak názov príznaku bude uvedený, znamená, že nadobúda hodnotu 1.
Kompletná TCP komunikácia: komunikácia od nadviazania spojenia až po normálne ukončenie spojenia – nie ukončenie s reset, abort a pod. (rámce, ktoré do tejto komunikácie nepatria sa vo výpise nesmú vyskytovať).

Napr.

rámec 10
00 00 c0 d7 80 c2 00 04 76 13 97 df 08 00 45 00
00 30 15 79 40 00 80 06 f8 19 93 af 62 e8 93 af
62 ee 00 8b 04 6f 34 dc 19 51 7d d8 e2 e1 70 12
ff ff e1 f8 00 00 02 04 05 b4 01 01 04 02
dĺžka: 62 bajtov
Ethernet II
DA MAC: 00 00 c0 d7 80 c2 SA MAC: 00 04 76 13 97 df
IP,
DA IP: 147.175.98.238 SA IP: 147.175.98.232
TCP,
SA port: 00 8b – netbios-ssn DA port: 04 6f
príznaky: SYN, ACK

atď.

Formát súborov so zaznamenanou komunikáciou je libpcap formát. Obsahuje data zachytených rámcov v binárnom tvare. Tento formát je štandardne používaný mnohými sieťovými analyzátormi, napr. Ethereal, WinDump, atď. (súbory boli zaznamenané analyzátorom Ethereal).

Formát súboru treba zistiť (WinPcap\docs\ ), súbor nezačína výpisom obsahu zachyteného rámca!

Pri riešení použite moduly Winpcap knižnice. WinPcap je voľne dostupný systém pre priame sieťové prístupy pod OS Windows.