Ответить

Опции темы

01.09.2018, 23:35 #1

sashok_2005
Пользователь
Регистрация: 26.03.2017
Сообщений: 10

C++ Снифер

Здрасте. Пишу снифер на c++ (что-то по типу Wireshark, без WinPcap) вот что пока получилось:

Код:

```
#include <iostream>
#include <winsock2.h>
#include <bitset>

#define SIO_RCVALL          0x98000001

using namespace std;

typedef struct IPPacket //Структура ip пакета
{
    unsigned char  ip_ver_hlen;
    unsigned char  ip_tos;
    unsigned short ip_length;
    unsigned short ip_id;
    unsigned short ip_flag_offset;
    unsigned char  ip_ttl;
    unsigned char  ip_protocol;
    unsigned short ip_xsum;
    unsigned int   ip_srcaddr;
    unsigned int   ip_dstaddr;
    unsigned char  ip_data[];
};

typedef struct TCPHeader // Структура TCP заголовка
{
    unsigned short tcp_srcport;
    unsigned short tcp_dstport;
    unsigned int tcp_sn;
    unsigned int tcp_acksn;
    unsigned char tcp_hlen:4;
    unsigned char tcp_flag_offset:6;
    unsigned char tcp_flags:6;
    unsigned short tcp_window;
    unsigned short tcp_xsum;
    unsigned short tcp_urg_pointer;
    unsigned char tcp_opt_data[];
};

typedef struct UDPHeader // Структура UDP заголовка
{
    unsigned short udp_srcport;
    unsigned short udp_dstport;
    unsigned short udp_length;
    unsigned short udp_xsum;
    unsigned char  udp_data[];
};

void ShowPacketInfo(IPPacket* iph){ // Информация об IP пакете
    cout<<"Version: "<<static_cast<int>(iph->ip_ver_hlen >> 4)<<endl;
    cout<<"Header length: "<<static_cast<int>(iph->ip_ver_hlen & 15)<<endl;
    cout<<"ToS: "<<bitset<8>(iph->ip_tos)<<endl;
    cout<<"Packet length: "<<ciph->ip_length<<endl;
    cout<<"Id: "<<ciph->ip_id<<endl;
    cout<<"Flags: "<<bitset<3>(iph->ip_flag_offset >> 13)<<endl;
    cout<<"Offset: "<<bitset<13>(iph->ip_flag_offset & 8191)<<endl;
    cout<<"TTL: "<<static_cast<int>(iph->ip_ttl)<<endl;
    cout<<"Protocol: ";
    switch(iph->ip_protocol){
case IPPROTO_TCP:
    cout<<"TCP";
    break;
case IPPROTO_UDP:
    cout<<"UDP";
    break;
default:
    cout<<"Unknown";
    break;
    }
    cout<<endl;
    cout<<"Xsum: "<<iph->ip_xsum<<endl;
    IN_ADDR sa;
    sa.s_addr = iph->ip_srcaddr;
    cout<<"Src: "<<inet_ntoa(sa)<<endl;
    sa.s_addr = iph->ip_dstaddr;
    cout<<"Dst: "<<inet_ntoa(sa)<<endl;
}

void ShowPacketData(IPPacket* iph, int type){ // Данные IP пакета
    cout<<"IPData: "<<endl;
    if(type == 1){//HEX
        for(int i = 0; i < iph->ip_length - (iph->ip_ver_hlen & 15) * 32; i++){
            char bf[2];
            itoa(static_cast<short>(iph->ip_data[i]), bf, 16);
            if(bf[1] == 0){
                bf[1] = bf[0];
                bf[0] = '0';
            }
            cout<<bf<<' ';

            if(i%16 == 0 & i != 0){
                cout<<endl;
            }
        }
    }else{//char
        for(int i = 0; i < iph->ip_length - (iph->ip_ver_hlen & 15) * 32; i++){
            if(iph->ip_data[i] == 0){
                cout<<'.';
            }else{
                cout<<iph->ip_data[i];
            }
            if(i%64==0 & i!=0){
                cout<<endl;
            }
        }
    }
    cout<<endl;
}

int main(int argc, char *argv[])
{
    cout<<"Start...\n";
    WSAData wSData;
    WSAStartup(0x202,&WSData);
    SOCKET s;
    char name[128];
    HOSTENT* phe;
    SOCKADDR_IN sa;
    unsigned long flag = 1;
    s = socket( AF_INET, SOCK_RAW, IPPROTO_IP );
    gethostname(name, sizeof(name));
    phe = gethostbyname( name );
    ZeroMemory( &sa, sizeof(sa) );
    sa.sin_family = AF_INET;
    sa.sin_addr.s_addr = ((struct in_addr *)phe->h_addr_list[0])->s_addr;
    bind(s, (SOCKADDR *)&sa, sizeof(SOCKADDR));
    ioctlsocket(s, SIO_RCVALL, &flag);
    int count=0;
    int c = 0;
    while( c == 0 ) // До первого IP пакета
    {
        char Buffer[65500];
        count = recv( s, Buffer, sizeof(Buffer), 0 );
        if( count >= sizeof(IPPacket) )
        {
            c = 1;
            IPPacket* iph = (IPPacket *)Buffer;
            ShowPacketInfo(iph);
            ShowPacketData(iph, 0);
            if(iph->ip_protocol == IPPROTO_TCP){
                TCPHeader* tcp = (TCPHeader *) iph->ip_data;
                cout<<tcp->tcp_srcport; // Вывод IP порта
            }
            if(iph->ip_protocol == IPPROTO_UDP){
                UDPHeader* udp = (UDPHeader *) iph->ip_data;
                cout<<udp->udp_srcport; // Вывод IP порта
            }
        }
    }

    WSACleanup ();
    system("PAUSE");
    return 0;
}
```

Вобщем что эта штука делает:
1: Ловит один IP пакет;
2: Показывает его заголовок(версия, длина, флаги и т.д.);
3: Показывает его данные

Код:

```
char ip_data[];
```

Он показывает заголовок нормально, но у меня всегда выходят слишком длинные пакеты, по 10000, 20000 байт(но в Wireshark'е пакеты максимум длины 100), ещё какоето странное смещение с единицей.
Данные показывает в начале нормально (как видно на 1-ом изображении), но потом долго идут нули (точки). А потом происходит какаята хрень, как видно из 2-го рисунка.
Вобщем помогите, что нужно зделать что бы Ip пакет показывался нормальною

Изображения
wsock1.png (17.5 Кб, 164 просмотров)
wsock2.png (30.1 Кб, 127 просмотров)

Цитата

02.09.2018, 00:29 #2

Black Fregat
Программист
Участник клуба
Регистрация: 23.06.2009
Сообщений: 1,640

Цитата:

> Сообщение от **sashok_2005**
> *у меня всегда выходят слишком длинные пакеты, по 10000, 20000 байт*

Цитата:

> Сообщение от **wiki**
> *The fields in the header are packed with the most significant byte first (big endian)*

Используйте **ntohl**

Цитата:

> Функция ntohl осуществляет перевод целого числа из сетевого порядка байт в порядок байт, принятый на компьютере.

Цитата

02.09.2018, 11:01 #3

sashok_2005
Пользователь
Регистрация: 26.03.2017
Сообщений: 10

Ну вроде всё получилось, ntohl не подошла, зато ntohs самое то. Толбко пакет немного обрывается, но это как нибудь потом. И теперь порт правильно показывается.
В общем СПАСИБО.

Изображения
Sniff1.png (24.1 Кб, 137 просмотров)
Sniff2.png (23.1 Кб, 135 просмотров)
Sniff3.png (17.1 Кб, 124 просмотров)

Цитата

02.09.2018, 17:06 #4

Black Fregat
Программист
Участник клуба
Регистрация: 23.06.2009
Сообщений: 1,640

Цитата:

> Сообщение от **sashok_2005**
> *ntohl не подошла, зато ntohs самое то*

Перепутал, виноват.. Спать хотелось

Цитата

Ответить

Похожие темы

Тема	Автор	Раздел	Ответов	Последнее сообщение
Снифер COM	tarakan1983	Общие вопросы Delphi	2	13.05.2017 16:07
HTTP/S Снифер	EliteDeN	Общие вопросы Delphi	0	27.10.2013 22:08
не реагирует снифер	megostudent	Работа с сетью в Delphi	2	22.04.2012 16:59
Снифер с ведением лога	Ghost of Night	Софт	2	14.07.2011 03:35
Снифер на Delphi.	SuperMooDuck	Работа с сетью в Delphi	7	04.02.2008 19:16