

网络安全实验报告

题 目 基于 libnet 的程序设计

专 业 信息安全

学 号 1190201012

学 生 张中界

指 导 教 师 王彦

# 一、实验目的

掌握 libnet 数据包的构造原理。

**二、实验内容**

1. 掌握 libnet 数据包的构造原理
2. 编程实现基于 libnet 的数据包构造，结合前面实验给出验证过程。能够对源码进行解释。

# 三、实验过程

**基于 libnet 的数据包构造实验基本信息：**

实验环境：Ubuntu16.04 x64 编程语言：C

## 1. 需求分析

需要使用 libnet 构造并发送一个数据包，并验证这个数据包被成功发送了。验证这一过程需要用到实验二中的捕包程序 pcap，将生成的数据包从虚拟机 B 发送到虚拟机 A，虚拟机 A 中的捕包程序会自动将其捕获，通过检查各项信息，证明捕获的数据包就是从虚拟机 B 此程序 createPac 中发送的数据包。

追加：在虚拟机 A 中编写接收来自相应端口 udp 数据包的程序 recvUDP，验证该数据包确实可以被正确接收。

## 程序结构

1. 定义协议参数

首先要明确各层协议要用到的参数，这里对一些需要格式转换的参数进行说明：

IP地址：调用libnet\_name2addr4()函数将字符串形式的IP地址转换为long型的网络字节序的IP地址；

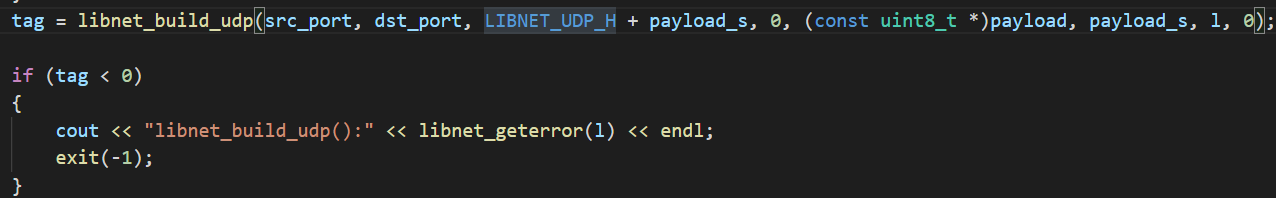
MAC地址：6字节，存储在字节数组中。

1. libnet\_init()

使用libnet\_init()函数得到一个libnet句柄，在参数中指定网卡和错误输出。

1. 构造UDP数据报

调用libnet\_build\_udp()函数

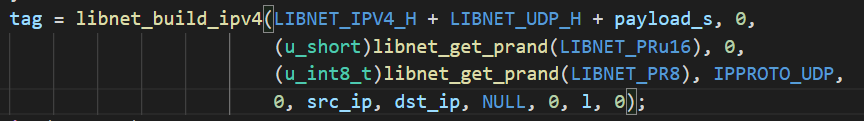


UDP协议的总长度字段为UDP头部的长度+负载payload的长度；

最后一个参数为0表示新建数据报；

1. 构造IP数据报

调用libnet\_build\_ipv4()函数

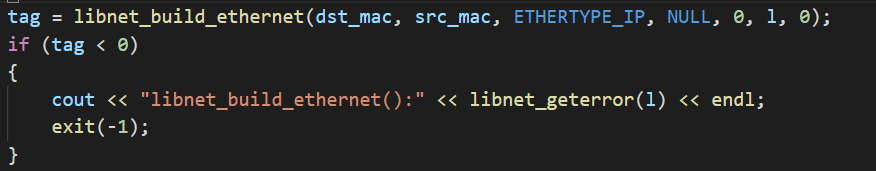


总长度字段为IP头部长度+UDP头部长度+负载长度；

标识和TTL字段使用随机数；

1. 构造MAC数据报

调用libnet\_build\_ethernet()函数



源和目的mac地址为字节数组；

ETHERTYPE\_IP指定上一层为IP协议；

1. 发送数据报

调用libnet\_write(l)将构造好的数据包发送到网络上，l为libnet句柄。

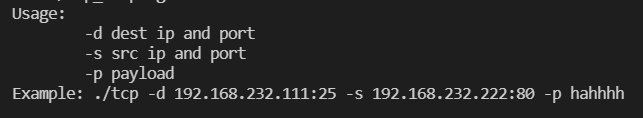
1. 释放资源

libnet\_destroy(l).

## 3. 进一步验证

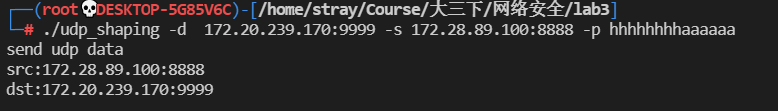
本例在windows下运行udp服务器（9999端口），在wsl下运行udp数据包生成程序，并使用wsl下的sniffer监听。

udp\_shaping程序的参数说明：

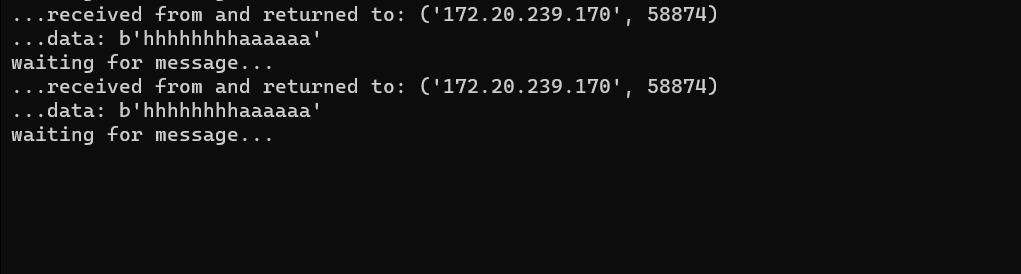


首先需要得到udp服务器的mac地址，在wsl中使用udp客户端向udp服务器发送数据，在sniffer中得到udp服务器的mac地址。

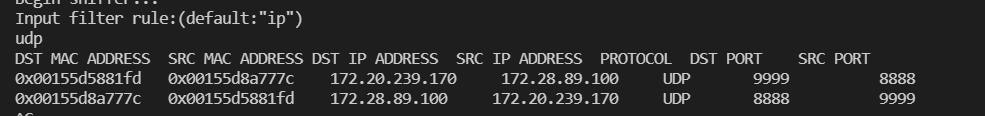
运行数据包生成程序：



服务端收到数据包：



sniffer监听的结果：



# 四、心得体会 （出现问题分析）

1. 问题：数据包已经发出但是服务器收不到

原因：数据包的目的mac地址错误，先用udp客户端与服务端通信，然后抓包查看mac地址；