

《信息安全技术》课程设计报告

**成 绩：**

**学 号： 1604270126**

**姓 名： 王君豪**

**班 级： 信科11602**

**指导教师： 孔维广**

**报告日期：2019年5月29日**

**一、实验1（网络抓包）**

1. 设计任务

**实验目的：**

使用wireshark对网络传输中的数据包进行抓取、分析，以此来理解数据在网络中传输的过程，了解TCP/IP协议，http协议以及加密的http协议：HTTPS，深刻认识到网络安全的重要性。

**工具：**

wireshark，Apache，Java集成开发环境

**亮点说明：**

使用wireshark对本地http传输进行抓包，本地tcp传输进行抓包。

**问题：**

windows系统中，本地向自身发送数据包没有经过真实的网络接口，而是通过环路（loopback interface）接口发送，所以直接使用wireshark抓取本地的数据包是无法实现的。

**解决问题：**

以管理员身份运行cmd---->route add 本机ip mask 255.255.255.255 网关ip，例如route add 10.181.174.183 mask 255.255.255.255 172.16.1.1，这样可以使得本机报文都经过网卡出去走一圈再回来，然后通过wireshark直接抓取。

**抓取结果：**

拿到了10.181.174.183:80（注意：这里不能用localhost:80以及127.0.0.1:80,必须用本机IP+端口）下表单登录的用户名以及密码（明文形式），和用Java模拟的tcp服务端与客户端交互的数据（简单的client发送数据到server，server在转发回client）。

1. 实现过程

**首先抓取http协议的数据包：**

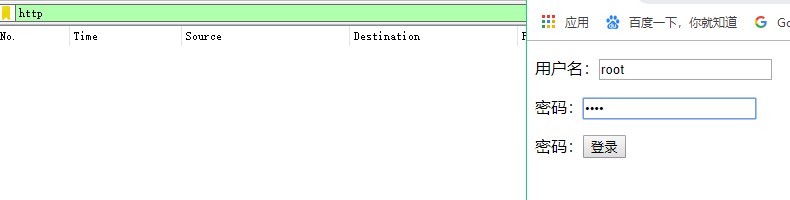
思路：直接抓取http的数据包会导致数据包过多，所以这里通过端口来过滤，过滤条件：port:80

Tcp也是通过端口过滤。

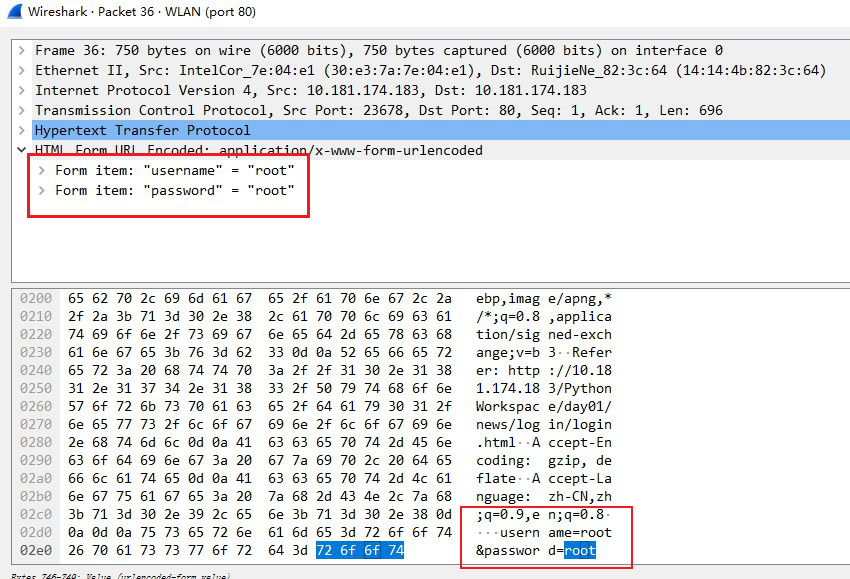
1. 设计结果

**抓取http：**

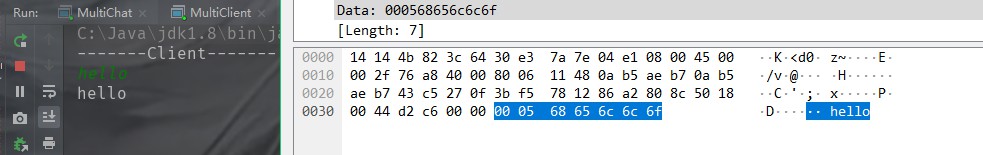
没提交之前



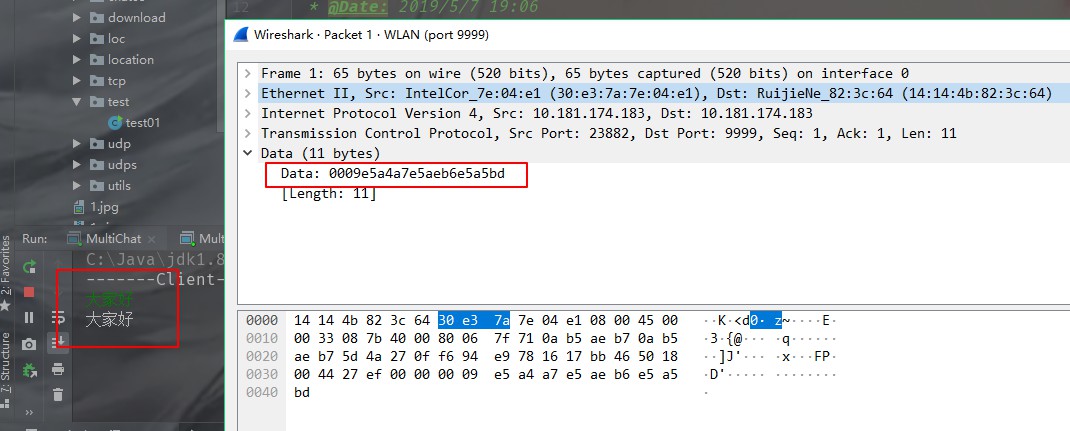
**提交之后：**



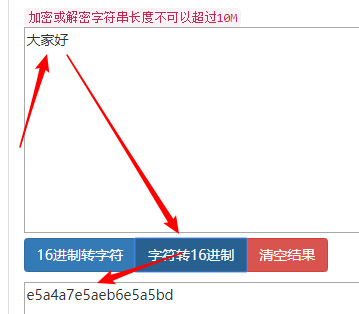
**抓取tcp：**



**抓取tcp传输中的中文：**



由上图可以看出wireshark不会主动解析中文而是以16进制显示



比对两串16进制字符可以看出抓取的数据没有问题，至于字节数是因为发送tcp数据需要回车换行即”hello\r\n”和”大家好\r\n”。

**二、总结**

**遇到的问题：**

抓取的数据太多时不好区分和处理；无法抓取本地传输中的数据。

解决方法：设置合理的过滤条件；使本机报文都经过网卡出去走一圈再回来。

**学习心得：**

掌握了wireshark的基本使用，能抓取简单的数据包，并进行分析。加深了对tcp/ip，http协议理解。从我抓取的数据包中可以看出数据不经过加密就在网络中传输是极不安全的，所以在网络传输中要注意对重要数据进行加密后再进行传输，也认识到https协议在网络传输的重要性。

**二、实验2（加密应用）**

（1）设计任务

**目的：**

使用加密算法实现一个加密系统（网站），以此熟悉加密解密算法的使用，了解异或加密解密的原理。

**工具：**

IDEA Java集成开发环境、Java JDK

**亮点说明：**

自己实现了一个加密系统，包括几种加密算法：异或加密解密，base64加密解密，md5加密，shx256加密。

（2）实现过程

异或算法：使用Java操作符“^”，明文字符串中的每个字符与指定秘钥进行异或得到字节数组，通过字节数组转字符串的到密文。

其他算法是直接调用别人的加密算法，其中base64加密解密是Javajdk自带的加密解密算法，md5和shx256是使用commons-codec-1.10.jar中的加密算法。

（2）设计结果

**Xor加密：秘钥12345678**



**Xor解密：秘钥12345678**



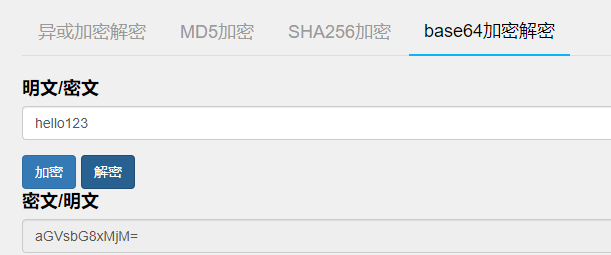
**Md5加密：**



**SHA256加密：**



**Base64加密:**



**Base64解密：**



**二、总结**

**学习心得：**

了解加密算法的使用，学会使用第三方加密算法。认识到学习加密算法的重要性：对传输过程中的重要数据第一时间进行加密而不是存入数据库时才使用数据库自带加密算法进行加密，否则数据传输过程可能会被别抓取，如上一个实验中使用wireshark抓取的用户名和密码。也了解了MD5加密算法和sha256加密算法的区别，MD5加密算法更快但是安全度较低（32位密文），而sha256加密算法速度较慢但是安全度较高（64位密文）。对于日常通信MD5加密算法的安全度已经足够。

**一、实验3（病毒程序设计）**

（1）设计任务

**实验目的：**

设计简单整蛊病毒程序

**亮点说明：**

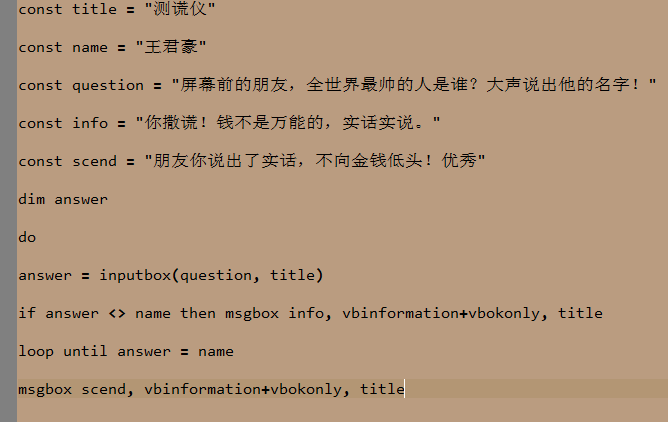
自己使用简单的VBScript代码设计了一个简单的整蛊测谎仪程序，并将其图标改为腾讯QQ的图标，当点击QQ图标是就会进入vbs程序，达到整蛊的目的。

（2）实现过程

**实验过程：**

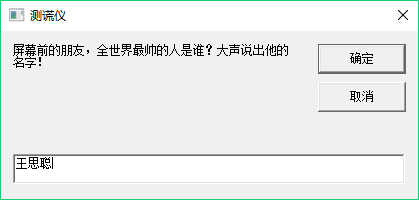
**首先新建vbs程序并写入代码，将该vbs程序新建快捷方式，然后修改快捷方式的图标。**

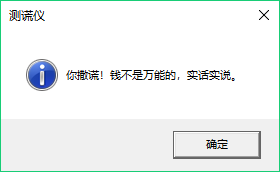
（3）设计结果

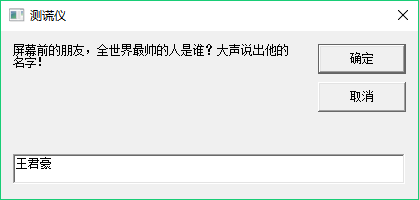


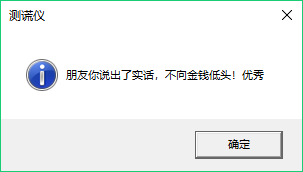
 

**将源文件隐藏后双击“腾讯QQ”**









**二、总结**

**学习心得：**

通过简单的病毒代码设计，了解了病毒的危害，虽然本事例只是简单的整蛊程序，但是通过vbs也可以写出对计算机有一定危害的的脚本程序，例如点击脚本直接关机，导致无法正常工作，或者无限弹窗直到电脑死机，影响电脑性能等等。所以我们要加强对病毒的防护，定期杀毒。提升自己计算机技术的同时也要提升自己的道德水平，不恶意制造病毒，不传播病毒，创造出文明安全的网络环境。

**一、实验4（网站安全评级）**

（1）设计任务

**实验目的：**

对知乎网进行安全等级评估

（2）实现过程

**1.知乎网简介：**

知乎是网络[问答](https://baike.baidu.com/item/%E9%97%AE%E7%AD%94/3009834" \t "https://baike.baidu.com/item/%E7%9F%A5%E4%B9%8E/_blank)社区，连接各行各业的用户。[用户](https://baike.baidu.com/item/%E7%94%A8%E6%88%B7/3621489" \t "https://baike.baidu.com/item/%E7%9F%A5%E4%B9%8E/_blank)分享着彼此的[知识](https://baike.baidu.com/item/%E7%9F%A5%E8%AF%86/74245" \t "https://baike.baidu.com/item/%E7%9F%A5%E4%B9%8E/_blank)、[经验](https://baike.baidu.com/item/%E7%BB%8F%E9%AA%8C/4315" \t "https://baike.baidu.com/item/%E7%9F%A5%E4%B9%8E/_blank)和见解，为中文[互联网](https://baike.baidu.com/item/%E4%BA%92%E8%81%94%E7%BD%91/199186" \t "https://baike.baidu.com/item/%E7%9F%A5%E4%B9%8E/_blank)源源不断地提供多种多样的[信息](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF/111163" \t "https://baike.baidu.com/item/%E7%9F%A5%E4%B9%8E/_blank)。

准确地讲，知乎更像一个[论坛](https://baike.baidu.com/item/%E8%AE%BA%E5%9D%9B/158397" \t "https://baike.baidu.com/item/%E7%9F%A5%E4%B9%8E/_blank)：用户围绕着某一感兴趣的话题进行相关的讨论，同时可以关注兴趣一致的人。对于概念性的解释，网络百科几乎涵盖了你所有的疑问；但是对于[发散思维](https://baike.baidu.com/item/%E5%8F%91%E6%95%A3%E6%80%9D%E7%BB%B4/1437127" \t "https://baike.baidu.com/item/%E7%9F%A5%E4%B9%8E/_blank)的整合，却是知乎的一大特色。

1. **信息系统安全保护等级定级指南**

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全，社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

|  |  |  |  |
| --- | --- | --- | --- |
| 受侵害的客体 | 对客体的侵害程度 | | |
| 一般损害 | 严重损害 | 特别严重损害 |
| 公民、法人和其他组织的合法权益 | 第一级 | 第二级 | 第二级 |
| 社会秩序、公共利益 | 第二级 | 第三级 | 第四级 |
| 国家安全 | 第三级 | 第四级 | 第五级 |

1. **知乎网平台安全等级确定**

**5**个安全等级各自提供的安全能力如下表所示：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 安全能力 | 一级 | 二级 | 三级 | 四级 | 五级 |
| 自主访问控制 | √ | ∈ | ≡ | ≡ | ∈ |
| 强制访问控制 |  |  | √ | ∈ | ≡ |
| 标记 |  |  | √ | ∈ | ≡ |
| 身份鉴别 | √ | ∈ | ∈ | ≡ | ≡ |
| 客体重用 |  | √ | ≡ | ≡ | ≡ |
| 审计 |  | √ | ∈ | ∈ | ∈ |
| 数据完整性 | √ | ≡ | ∈ | ≡ | ≡ |
| 隐蔽信道分析 |  |  |  | √ | ≡ |
| 可信路径 |  |  |  | √ | ≡ |
| 可信恢复 |  |  |  |  | √ |

注；√：新增功能，∈：比上一级功能有扩展，≡：与上一级功能相同。

**3.1业务信息安全**

知乎网是针对知乎用户开放的网上问答社区，网站上的信息属于公开信息，信息被破坏不会对国家利益造成严重损害。如果信息完整性被破坏也不会造成较大范围的社会不良影响。但是知乎用户的每一个回答都受知识产权的保护，此时知乎用户的权益将受到影响。

|  |  |  |  |
| --- | --- | --- | --- |
| 业务信息安全被破坏时所侵害的客体 | 对相应客体的侵害程度 | | |
| 一般损害 | 严重损害 | 特别严重损害 |
| 公民、法人和其他组织的合法权益 | 第一级 | 第二级 | 第二级 |
| 社会秩序、公共利益 | 第二级 | 第三级 | 第四级 |
| 国家安全 | 第三级 | 第四级 | 第五级 |

◇第二级

**3.2系统服务安全**

如果知乎网系统瘫痪，知乎用户将无法提问，也无法回答问题，知乎会员的权益将受到较大影响，而普通用户所受的影响较小。

|  |  |  |  |
| --- | --- | --- | --- |
| 业务信息安全被破坏时所侵害的客体 | 对相应客体的侵害程度 | | |
| 一般损害 | 严重损害 | 特别严重损害 |
| 公民、法人和其他组织的合法权益 | 第一级 | 第二级 | 第二级 |
| 社会秩序、公共利益 | 第二级 | 第三级 | 第四级 |
| 国家安全 | 第三级 | 第四级 | 第五级 |

◇第二级

**3.3 定级对象的安全保护等级**

作为定级对象的信息系统的安全保护等级由业务信息安全保护等级和系统服务安全保护等级的较高者决定。

**二、总结**

本次实验对于知乎网的安全等级评估并不全面和准确。随着互联网的发展，网络安全也必须得到足够的重视，对于网站安全等级的评估也理应交给专业的部门进行评估。互联网本就置我们于透镜之中，如果网络安全的不到保障，更不用说人身安全和国家安全。所以本次实验仅仅是对网站安全等级评估过程的一个了解，真正的等级评估应当更公平、更准确、更严格。