|  |  |  |  |
| --- | --- | --- | --- |
| **姓名：** | **唐玉涵** | **学号：** | **2014011328** |

**作业要求：**

布置作业时间：2016年12月02日

提交作业期限：2016年12月12日

提交作业方式：网络学堂（请以本文件为模板写作业）

**迟交与未交的作业都按照零分计算**

本次作业在课程最终成绩中记10分

**作业题目：体验认证技术**

基于第一次作业（网络监控），在自己经常使用账号密码登陆的网站中，选择一个使用了加密和认证技术的网站，监测并简要分析其身份认证环节的情况。作业要求阐述三方面的内容：

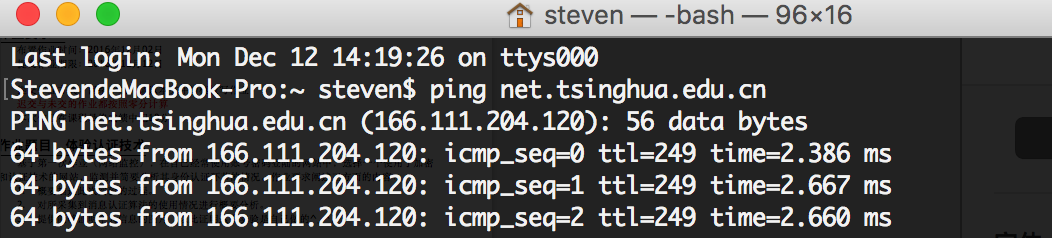
1. 概要描述此次实验的过程。
2. 对所采集到消息认证算法的使用情况进行概要分析。
3. 提供能够证明个人信息的图片（以此证明这个实验是自己做的^\_^）

**答：**

1. 实验过程

我选取的是net.tsinghua.edu.cn，也即校园网连接网站。

首先为了获取其ip地址，先使用了终端中的ping指令，得到其ip地址为：166.111.204.120

操作截图如下：

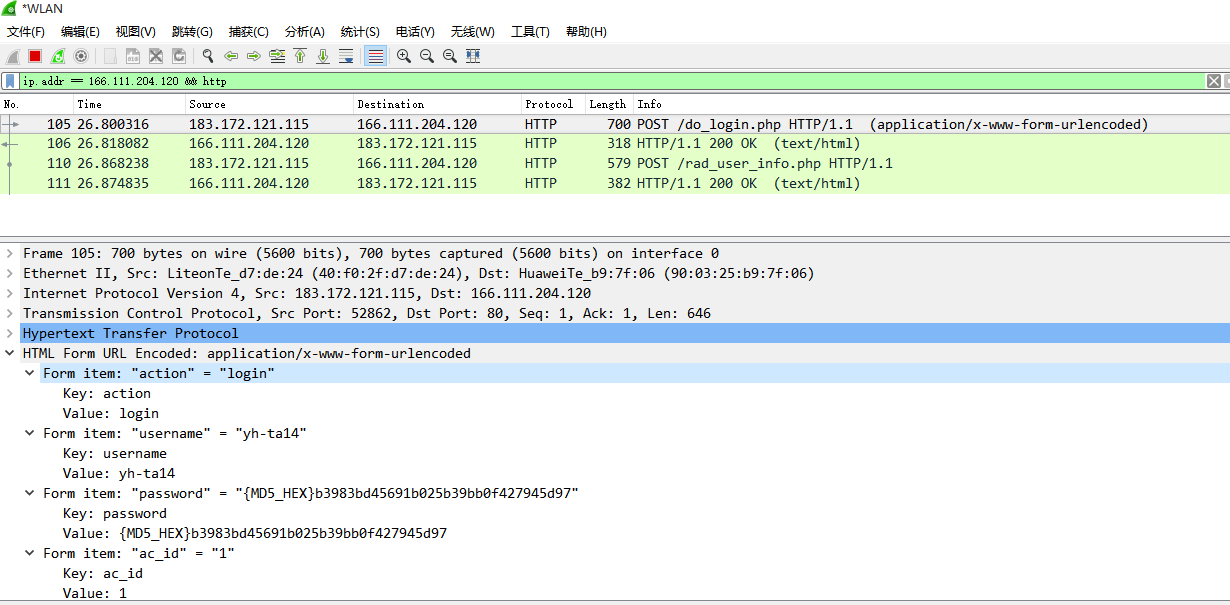
然后打开Wireshark软件，输入限制条件为ip.addr == 166.111.204.120，

结果发现下面的条目过多，故继续加入http的限制。



操作过程是先用浏览器打开net.tsinghua.edu.cn网页，此时处于登录状态，见上图。

故先需要手工断开连接之后重新进行登录操作，此时看到了我们所需的条目，见下图。

发现这个校园网登陆界面使用的是MD5消息摘要算法来进行消息认证。

以上b398…d97即为算法结果。

以上即为实验过程。

1. MD5算法使用情况分析

MD5算法属于消息摘要算法，输入任意长度消息，按照512位分组处理，输出128位消息摘要。其优点在于不易受到弱碰撞性的攻击，但不能对付强碰撞性攻击。在运行速度上MD5结构简单，运行速度快，故在很多网站广泛使用。很多时间比较久远的网站都采用了这样的消息认证算法。

虽然MD5早已被攻破，但是如同二战时期的德军加密仪器ENIGMA一样，MD5如今在日常生活的安全范围内还是能够胜任的。不过，在航空航天，金融相关等领域的消息认证，需要使用安全性更高的方法。

1. 以上截图中的yh-ta14为我（唐玉涵）的用户名，可用来验证身份。谢谢。