# 实 验 报 告


课程名称 《网络攻击与防御技术》

学　　院 计算机科学技术学院

专　　业 信息安全

姓　　名 黄　　力

学　　号 **15307130275**

开 课 时 间 **2018** 至 **2019** 学年第 **1** 学期

| | | | |
|---|---|---|---|
| 实验项目名　　称 | 从一个针对 WEB Mail 的网络嗅探数据中提取信息 | 成绩 | |

## 一、实验目的

（1）理解在网络中嗅探数据的原理，掌握使用 wireshark 抓包的方法

（2）掌握从网络嗅探数据中还原和提取简单数据信息和数据文件的方法

## 二、实验内容

（1）从老师给予的网络嗅探文件中获取收件人邮箱、发件人邮箱、邮件标题、邮件正文、邮件附件（一个 pdf 文件）、邮箱中存在的邮件列表、sina.cn 发来的.docx 附件

## 三、实验步骤

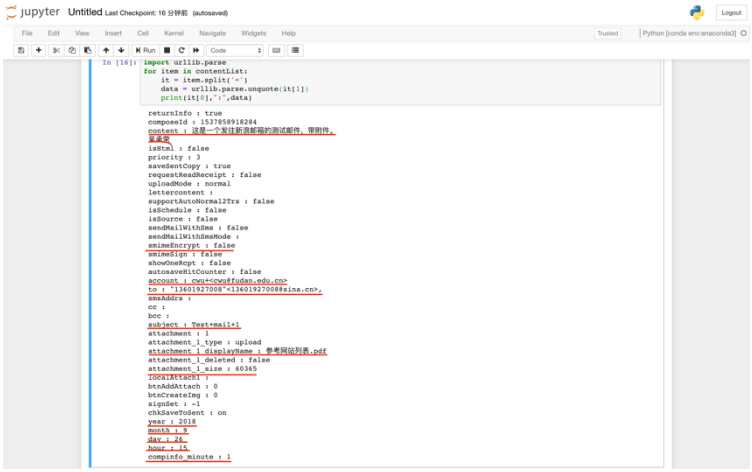
（1）使用 wireshark 软件打开网络嗅探数据文件 fudanwebmail.cap

（2）利用 wireshark 的过滤功能过滤得到 http 的数据分组，使用 wireshark 的流跟踪功能跟踪客户端与邮件服务端的 TCP 流（共有 16 个 TCP 流），并从其中逐个分析得出是哪些数据分组含有提取信息和文件。

（3）从（2）中分析筛选得到的数据分组中成功提取出信息，方法是在 wireshark 的 file 选项中选择 export objects，再在子选项中选择 http，最后根据数据分组的组号提取 pdf 文件和 word 文件并更改文件名和文件后缀名。使用 python 编写脚本解码得到收件人邮箱、发件人邮箱、邮件标题、邮件正文等信息。

## 四、实验结果

（1）发往 sina 邮箱的信息：（第 9 个 tcp 流中，使用 tcp.stream eq 9 过滤）




从截图中可得：

发件人为：cwu@fudan.edu.cn

收件人为：13601927008@sina.cn

邮件标题为：Test+mail+1

邮件正文内容为：这是一个发往新浪邮箱的测试邮件，带附件。吴承荣

附件标题为：参考网站列表.pdf

附件大小为：60365 字节

邮件加密方式为：无

发送邮件的时间为：2018 年 9 月 26 日 15:01

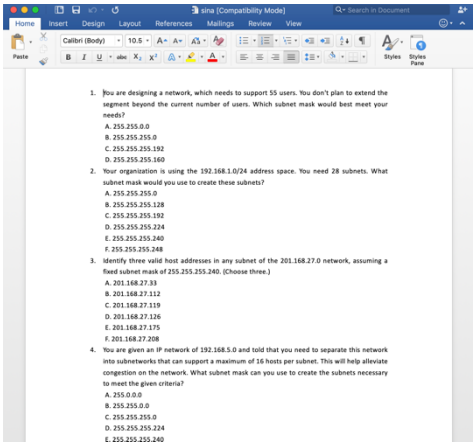
（2）获取到的 pdf 文件（第 9 个 tcp 流中，使用 tcp.stream eq 9 过滤）和 word 文件（第 11 个 tcp 流中，使用 tcp.stream eq 11 过滤）截图（提取到的源文件已随本报告一同提交）：

pdf 文件名为：参考网站.pdf

页面截图：


word 文件名为：IP 基础题.docx

页面截图：




（3）接收到 sina 邮箱的信息：（第 11 个 tcp 流中，使用 tcp.stream eq 11 过滤）

邮件正文内容：这是一个课程测试邮件。请查收。


收件人为：cwu@fudan.edu.cn

发件人为：13601927008@sina.cn

附件标题为：课程测试邮件

邮件加密方式为：无

发送邮件的时间为：2018 年 8 月 25 日 14:59:12

接收邮件的时间为：2018 年 8 月 25 日 15:01:57

（4）邮箱中存在的邮件列表：

邮箱中总共有 200 封邮件，由于本报告篇幅有限，以下仅截了列表中的前 10 封邮件，全部邮件信息可在随本报告一同提交的文件中（ab1_Network_Attacks_and_Countermeasures_黄力.pdf）获取

（5）通讯录：（第 4 个 tcp 流中，使用 tcp.stream eq 4 过滤）

邮箱中总共有 272 个联系人，由于本报告篇幅有限，以下仅截了列表中的前 16 个联系人，全部联系人信息可在随本报告一同提交的文件中（ab1_Network_Attacks_and_Countermeasures_黄力.pdf）获取

（6）其它信息：

老师邮箱容量上限为 2G，已使用 1.12G（第 1 个 tcp 流中，使用 tcp.stream eq 1 过滤）

```
        <span class="">
            <span class="capacity
                <span style="widt
            </span>
        </span>
        <span class="nfMaxSize">

1.12 G/

2 G
        </span>
```

老师邮件附件上传最大为 43M（第 4 个 tcp 流中，使用 tcp.stream eq 4 过滤）

```
        <div class="infoPanel">
            <span class="info">总容量超过43M，$file$等$number$个附件将上传至文件中转站，7天内有效，若被删除或者过期，收件人将无
法下载</span>
            <span class="closePanel" onclick="C.hideInfoPanel()"></span>
        </div>
```

老师的邮箱密码为：ABC12345XYZ（在“密码.jsp”文件中）

## 五、实验总结

通过本次实验，我经过分析，成功从网络嗅探数据文件 fudanwebmail.cap 提取出了重要的信息。由于这次实验的数据报文都是明文，未进行加密，因此实验过程比较顺利，没有遇到解决不了的难题。