

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）

```

In [10]: import urllib.parse
for item in contentList:
    it = item.split("=")
    data = urllib.parse.unquote(it[1])
    print(it[0],":",data)

returnInfo : true
composeId : 1537858918284
content : 这是一个发往新浪邮箱的测试邮件，带附件。
isHtml : false
priority : 3
saveSentCopy : true
requestHeader : false
uploadMode : normal
letterContent :
supportAutoNormal2Text : false
isSchedule : false
isSource : false
sendMailWithIdem : false
sendMailWithIdemMode :
onlineEncrypt : false
uncompress : false
showOutMsg : false
autoconvertCounter : false
account : cwu@fudan.edu.cn
to : 13601927008@13601927008@sina.cn
cc :
bcc :
subject : Test+mail+1
attachment : 1
attachment_type : upload
attachment_displayName : 参考网站列表.pdf
attachment_deleted : false
attachment_size : 60365
TOGETHER :
broadcastTime : 0
bbsCreateTime : 0
skiped : 1
checkOutdent : on
year : 2018
month : 9
day : 28
hour : 14
minute : 1
compileMinute : 1

```

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

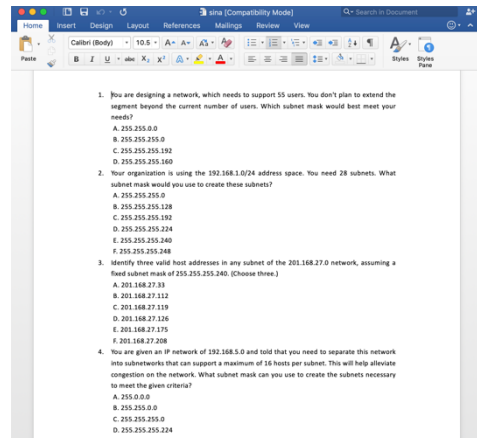
附件大小为：60365 字节

发送邮件的时间为：2018 年 9 月 26 日 15:01

pdf 文件名为: 参考网站.pdf

word 文件名为: IP 基础题.docx

页面截图:



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

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，全部邮件信在随本报告一同提交的文件中 (ab1 Network Attacks and Countermeasures 黄力.pdf) 获取

```

第 4 个组件:
id: 1.13b13qz9f879f4a688a42
name: "测试器"
type: "test"
url: "http://www.baidu.com"
subJexl: 测试器是否支持正则表达式
monitorData: 2018042202181
createTime: 2018042202181

第 5 个组件:
id: 1.13b13qz9f879f4a688a42
name: "测试器"
type: "test"
url: "http://www.baidu.com"
subJexl: "isEqual"
monitorData: "isEqual"
createTime: 2018042202181
第 6 个组件:
id: 1.13b13qz9f879f4a688a42
name: "测试器"
type: "test"
url: "http://www.baidu.com"
subJexl: "isEqual"
monitorData: "isEqual"
createTime: 2018042202181
第 7 个组件:
id: 1.13b13qz9f879f4a688a42
name: "测试器"
type: "test"
url: "http://www.baidu.com"
subJexl: "isEqual"
monitorData: "isEqual"
createTime: 2018042202181
第 8 个组件:
id: 1.13b13qz9f879f4a688a42
name: "测试器"
type: "test"
url: "http://www.baidu.com"
subJexl: 测试器是否支持正则表达式
monitorData: 2018042202181
createTime: 2018042202181

第 9 个组件:
id: 1.13b13qz9f879f4a688a42
name: "测试器"
type: "test"
url: "http://www.baidu.com"
subJexl: 测试器是否支持正则表达式
monitorData: 2018042202181
createTime: 2018042202181

第 10 个组件:
id: 1.13b13qz9f879f4a688a42
name: "测试器"
type: "test"
url: "http://www.baidu.com"
subJexl: 测试器是否支持正则表达式
monitorData: 2018042202181
createTime: 2018042202181

```

(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

第 1 个联系人: id: 154 姓名: jpsong 邮件地址: jpsong@fudan.edu.cn	第 9 个联系人: id: 32 姓名: 12101310181 邮件地址: 12101310181@fudan.edu.cn
第 2 个联系人: id: 62 姓名: 魏峰 邮件地址: cangp@fudan.edu.cn	第 10 个联系人: id: 30 姓名: 1211020012 邮件地址: 1211020012@fudan.edu.cn
第 3 个联系人: id: 34 姓名: 复旦大学国际商学院 邮件地址: ccc@fudan.edu.cn	第 11 个联系人: id: 61 姓名: 1210240001 邮件地址: 1210240001@fudan.edu.cn
第 4 个联系人: id: 35 姓名: 朱海峰 邮件地址: jzhaif@fudan.edu.cn	第 12 个联系人: id: 62 姓名: 1210240002 邮件地址: 1210240002@fudan.edu.cn
第 5 个联系人: id: 78 姓名: 孙家庆 邮件地址: sunjiaqing@fudan.edu.cn	第 13 个联系人: id: 63 姓名: 1210240004 邮件地址: 1210240004@fudan.edu.cn
第 6 个联系人: id: 79 姓名: 王慧敏 邮件地址: wanghui@fudan.edu.cn	第 14 个联系人: id: 64 姓名: 1210240006 邮件地址: 1210240006@fudan.edu.cn
第 7 个联系人: id: 33 姓名: 张雪松 邮件地址: zhangxuesong@fudan.edu.cn	第 15 个联系人: id: 65 姓名: 1210240007 邮件地址: 1210240007@fudan.edu.cn
第 8 个联系人: id: 36 姓名: 徐国治 邮件地址: xuguo@fudan.edu.cn	第 16 个联系人: id: 66 姓名: 1210240008 邮件地址: 1210240008@fudan.edu.cn

(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="width: 100%;>  
  </span>  
</span>  
<span class="nfMaxSize">
```

1.12 G/

2 G

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。