**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**  1.1.png（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](mailto:cwu@fudan.edu.cn)  收件人为：[13601927008@sina.cn](mailto: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 word文件名为：IP基础题.docx  1.2.png**1.3.png** 页面截图： 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）  1.6.png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](mailto:cwu@fudan.edu.cn)  发件人为：[13601927008@sina.cn](mailto: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：  1.8.png1.7.png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）  1.10.png1.9.png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：  1.4.png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）  1.5.png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）  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。 |