|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **计算机网络与通信实验报告（一）** | | | | | | |
| 学 号 | 姓 名 | | 班 级 | | 报告日期 | |
| 181110315 | 王少博 | | 1811103 | | 2020年6月10日 | |
| 实验内容 | **网络常用命令的使用及DNS层次查询、SMTP协议分析；利用分组嗅探器（Wireshark）进行应用层协议分析** | | | | | |
| 实验目的 | 1. 掌握常用的MS-DOS下的网络命令，对于网络中的时延丢包吞吐率带宽等基本概念有一个自己的认识； 2. 掌握DNS域名解析的原理和使用，配合nslookup对三层结构进行分析； 3. 了解SMTP发送邮件的原理，实现一个MS-DOS下的邮件发送； 4. 掌握Java的TCP/UDP Socket编程，掌握基本的C/S模式； 5. 学会抓包软件Wireshark的使用，并且以此分析网络中包裹分组对应的各个层次的协议，特别是http、dns协议的报文内容 | | | | | |
| 实验预备知识 | 前三章的知识，主要是应用层的几个协议，还有传输层的TCP/IP协议。   1. 深度理解DNS原理和根、顶级、权威三层域名服务器结构还有本地域名服务器和主机的关系； 2. SMTP邮件发送协议报文格式和内容； 3. TCP/UDP编程的java基础知识（这个我在大一年度项目中就写过多线程版本） 4. HTTP协议报文格式和内容 5. wireshark软件使用和dos环境下的命令学习 | | | | | |
| 实验过程描述 | 所有实验的答案已经汇总在两个word文档里，在此我记录一下印象最深刻、遇到困难次数最多的几个实验：   1. **telnet进行SMTP邮件发送** 2. qq邮箱的服务器对应的域名是smtp.qq.com，而并非mail.qq.com所以一开始尝试后者总是失败 3. qq邮箱的授权码需要单独去web邮件管理器中生成，不能直接用qq密码对应的base64编码生成，而应该用base64编码的授权码来使用，在此问题上折腾了一晚最终得到解决。该步骤需要自主前往qq邮箱配置。 4. telnet连接建立是计时的，不能输错太多次（因为每次输错都需要重新输一行），否则会超时。 5. 其余就是严格按照报文格式，注意一下单独一行的“.”即可 6. 另外，我的MS-DOS下的telnet命令是没有办法直接复制过去的，这一点与老师上课时演示的不太一样。不过最后在没有输入错误的情况下还是成功发送了邮件。 7. **nslookup命令对DNS逐层解析** 8. 查找13个根域名服务器。随便用一个查询 com 根域名对应的顶级名称服务器 9. 在给出的顶级名称服务器中，随便用一个来查询 baidu.com 的权威名称服务器 10. 在给出权威名称服务器中，随便用一个来查询xueshu.baidu.com 11. 因为一开始本地域名服务器中有缓存记录，所以没有指明服务器ip的时候也成功了。总体来说这个实验进行的比较顺利。 12. 一开始首选dns的IP错了，备用的没有错，所以能连网但是dns总是失败。修改了配置之后，效果就好了。 13. **wireshark进行抓包实验：** 14. 这一部分主要还是根据实验报告一步一步进行，但是由于wireshark的版本差异比较大，部分操作有所不同。 15. 我用的是chrome浏览器进行分析，这个时候网络环境就非常不好，尽管我每次都清理了缓存，但是我的浏览器插件自动会运行，难免会有一些干扰。另外，只要登录了chrome的谷歌账号，就会有gmail网络应用的各种协议，会有一定的影响，不过后来通过ip和网站具体域名的筛选，成功地分析了结果。 16. 34个问题主要都是对于报文的字段进行一些分析，具体的在结果中说明。 | | | | | |
| 实验结果 | 1. telnet DNS查询   **首先找到13个根域名服务器**  1 198.41.0.4  2 199.9.14.201  3 192.33.4.12  4 199.7.91.13  5 192.203.230.10  6 192.5.5.241  7 192.112.36.4  8 198.97.190.53  9 192.36.148.17  10 192.58.128.30  11 193.0.14.129  12 199.7.83.42  13 202.12.27.33  然后开始三层查询。  根域名服务器：    顶级域名服务器：    权威域名服务器：    本地域名服务器查询：     1. SMTP邮件发送报文：（在vscode下编辑的）      1. wireshark抓包实验（列出8个题目的答案）：   (1) 列出在第7 步中分组列表子窗口所显示的所有协议类型。ARP HTTP UDP TCP DNS  (7) 分析你的浏览器向服务器发出的第一个HTTP GET 请求的内容，在该请求报文中，是否有一行是：IF-MODIFIED-SINCE？  否  (9) 分析你的浏览器向服务器发出的第二个“HTTP GET”请求，在该请求报文中是否有一行是：IF-MODIFIED-SINCE？如果有，在该首部行后面跟着的信息是什么？  有 Date: Mon, 08 Jun 2020 16:13:55 GMT\r\n    (10)服务器对第二个HTTP GET 请求的响应中的HTTP 状态代码是多少？服务器是否明确返回了文件的内容？请解释。  没有。服务器返回了304表示之前发过的包没有修改不继续发了。    (22)检查DNS 查询响应报文，其中提供了多少个“answers”？每个answers 包含哪些内容？  2个；    (Name, Type, Class, TTL)另外还有 Data length和具体给出的Value。  (25)DNS 查询报文的目的端口号是多少？DNS 查询响应报文的源端口号是多少？  53；53      (29)DNS 查询报文发送的目的地的IP 地址是多少？这个地址是你的默认本地DNS 服务器的地址吗？  114.114.114.114； 是的  (34)检查DNS 查询响应报文，其中提供了多少个“answers”？每个answers 包含哪些内  容？  A类型的回答，对应一个answer | | | | | |
| 实验当中问题  及解决方法 | 1. nslookup dns操作的时候，会失败。这个时候有两个解决方案，一个是用wifi接入手机热点，不用以太网，另一个方式就是重新进行配置，把默认的接入变成以太网。  2. 邮件smtp首先是qq邮箱自身的问题，需要获取官方的验证码转成base64，然后就是telnet时间有限制，不能弄的太慢。  3. 捕包里最大的麻烦就是网络环境不太好，这个在实验二里面也有类似情况。chrome的环境会自带一些gmail应用导致的协议，不过在熟悉wireshark之后还是能够通过过滤以及看ip等手段解决，总体来说按照实验步骤不会有特别多的问题。每次进行捕包之前，先清理缓存。新建标签页的时候其实并不会有http连接（这个我不是特别明白原因，可能因为我的新建标签页是自己定制的和大部分浏览器标签页不同，我的新标签页也不是空白页）然后输入网址之后立马能看到http服务。对应着查看数据就行了。环节五最后一个网站DNS解析捕包的时候总有连续访问超时并且访问失败的情况，最后发现是网络环境原因，调整网络之后恢复正常了。 | | | | | |
| 成绩（教师打分） | 优秀 | 良好 | | 及格 | | 不及格 |