|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **计算机网络与通信实验报告（二）** | | | | | | |
| 学 号 | 姓 名 | | 班 级 | | 报告日期 | |
| 2022211972 | 吴俣辰 | | 2211105 | | 2024/10/23 | |
| 实验内容 | **利用分组嗅探器进行应用层协议分析** | | | | | |
| 实验目的 | 1. 分析HTTP协议 2. 分析DNS协议 | | | | | |
| 实验预备知识 | ****基础概念****：****HTTP（Hypertext Transfer Protocol）****：是一种用于分布式、协作和超媒体信息系统的应用层协议，是万维网的数据通信基础。  ****工作原理****：   * 1. ****请求-响应模型****：了解客户端请求和服务器响应的基本流程。   2. ****状态码****：熟悉常见的HTTP状态码（如200、404、500等）及其含义。   3. ****方法（动词）****：了解GET、POST、PUT、DELETE等HTTP方法及其用例。   ****报文结构****：   * 1. ****请求报文****：包含请求行、请求头部字段、空行和可选的请求体。   2. ****响应报文****：包含状态行、响应头部字段、空行和可选的响应体。   ****HTTP版本****：主要包括HTTP/1.0、HTTP/1.1、HTTP/2、HTTP/3等，了解不同版本的改进点，如持久连接、传输层安全改进、多路复用等。  ****安全性****：了解HTTPS及其通过TLS/SSL加密来保障数据传输安全的基本机制。  ****头部字段****：理解常见的HTTP头部字段及其作用，如Host、User-Agent、Accept、Content-Type等。 ****DNS（Domain Name System）****：是一种用于将域名解析为IP地址的分布式数据库系统。 ****DNS结构****：****层次结构****：包括根域（Root）、顶级域（TLD）、二级域及子域。  ****域名解析****：理解域名解析的递归和迭代过程。  ****DNS缓存****：DNS缓存对于提高查询效率的重要性，以及可能产生的问题（如缓存污染）。  ****协议详解****：理解DNS协议使用的传输层协议（通常是UDP，在53端口），以及在某些情况下使用TCP的机制。  ****工具与实战****：使用工具如nslookup、dig来进行DNS查询和故障排查。  掌握以上预备知识，可以帮助更深入地理解和分析HTTP和DNS协议在网络通信中的应用和机制。 | | | | | |
| 实验过程描述 | **1、HTTP GET/response交互**  首先通过下载一个非常简单的HTML文件（该文件非常短，并且不嵌入任何对象）。   1. 启动Web browser。 2. 启动Ethereal分组嗅探器。在窗口的显示过滤说明处输入“http”，分组列表子窗口中将只显示所俘获到的HTTP报文。 3. 一分钟以后，开始Ethereal分组俘获。 4. 在打开的Web browser窗口中输入一下地址（浏览器中将显示一个只有一行文字的非常简单的HTML文件）：   http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html   1. 停止分组俘获。   **2、HTTP 条件GET/response交互**   1. 启动浏览器，清空浏览器的缓存（在浏览器中，选择“工具”菜单中的“Internet选项”命令，在出现的对话框中，选择“删除文件”）。 2. 启动Ethereal分组俘获器。开始Ethereal分组俘获。 3. 在浏览器的地址栏中输入以下URL: http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file2.html,你的浏览器中将显示一个具有五行的非常简单的HTML文件。 4. 在你的浏览器中重新输入相同的URL或单击浏览器中的“刷新”按钮。 5. 停止Ethereal分组俘获，在显示过滤筛选说明处输入“http”,分组列表子窗口中将只显示所俘获到的HTTP报文。   **3.获取长文件**   1. 启动浏览器，将浏览器的缓存清空。 2. 启动Ethereal分组俘获器。开始Ethereal分组俘获。 3. 在浏览器的地址栏中输入以下URL: http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file3.html，浏览器将显示一个相当大的美国权力法案。 4. 停止Ethereal分组俘获，在显示过滤筛选说明处输入“http”,分组列表子窗口中将只显示所俘获到的HTTP报文。   **4.嵌有对象的HTML文档**   1. 启动浏览器，将浏览器的缓存清空。 2. 启动Ethereal分组俘获器。开始Ethereal分组俘获。 3. 在浏览器的地址栏中输入以下URL: http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file4.html，浏览器将显示一个具有两个图片的短HTTP文件 4. 停止Ethereal分组俘获，在显示过滤筛选说明处输入“http”,分组列表子窗口中将只显示所俘获到的HTTP报文。   **5.HTTP认证**   1. 启动浏览器，将浏览器的缓存清空。 2. 启动Ethereal分组俘获器。开始Ethereal分组俘获。 3. 在浏览器的地址栏中输入以下URL: https://gaia.cs.umass.edu/ethereal-labs/protected\_pages/HTTP-ethereal-file5.html，浏览器将显示一个HTTP文件，输入所需要的用户名和密码(用户名：eth-students,密码:network)。 4. 停止Ethereal分组俘获，在显示过滤筛选说明处输入“http”,分组列表子窗口中将只显示所俘获到的HTTP报文。   **6.跟踪DNS**   1. 利用ipconfig命令清空你的主机上的DNS缓存。 2. 启动浏览器，将浏览器的缓存清空。 3. 启动Ethereal分组俘获器，在显示过滤筛选说明处输入“ip.addr==your\_IP\_address”(如：ip.addr==10.17.7.23)，过滤器将会删除所有目的地址和源地址都与指定IP地址不同的分组。 4. 开始Ethereal分组俘获。 5. 在浏览器的地址栏中输入：<http://www.ietf.org> 6. 停止分组俘获。 7. 开始Ethereal分组俘获。 8. 在www.mit.edu上进行nslookup（即执行命令：nslookup www.mit.edu）。 9. 停止分组俘获。 10. 重复上面的实验，只是将命令替换为：nslookup –type=NS mit.edu | | | | | |
|  | * **利用ethereal分别对TCP套接字的实现及UDP套接字的实现捕分析**   安装java虚拟机。熟悉捕包软件的使用，进行相应的捕包。具体程序上课时拷贝。  Tcp抓包      端口为9999    Udp抓包      端口为9876     * **利用ethereal分析协议HTTP、FTP和DNS**      1. 你的浏览器运行的是HTTP1.0，还是HTTP1.1？你所访问的服务器所运行的HTTP版本号是多少？   我的浏览运行的是HTTP1.1，服务器也是1.1  （2）你的浏览器向服务器指出它能接收何种语言版本的对象？    （3）你的计算机的IP地址是多少？服务器gaia.cs.umass.edu的IP地址是多少？  我的计算机IP:10.241.24.140,服务器是128.119.245.12  （4）从服务器向你的浏览器返回的状态代码是多少？  200  （5）你从服务器上所获取的HTML文件的最后修改时间是多少？    2024/10/23 5:59:01   1. 返回到你的浏览器的内容一共多少字节？     126     1. 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？   没有   1. 分析服务器响应报文的内容，服务器是否明确返回了文件的内容？如何获知？     明确了是(text/html)   1. 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？     最后的修改的时间  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。    304并没有 因为之前访问过，浏览器缓存了访问记录，因此可以直接调取缓存内的内容   1. 你的浏览器一共发出了多少个HTTP GET请求？     2个  （12）承载这一个HTTP响应报文一共需要多少个data-containing TCP报文段？  4个    （13）与这个HTTP GET请求相对应的响应报文的状态代码和状态短语是什么？  200 OK   1. 你的浏览器一共发出了多少个HTTP GET请求？这些请求被发送到的目的地的IP地址是多少？     4个:128.119.245.12 ,52.51.131.59  （15）浏览器在下载这两个图片时，是串行下载还是并行下载？请解释。  串行下载，可以通过时间判断，是下载完第一个图片，才开始下载第二个图片的   1. 对于浏览器发出的最初的HTTP GET请求，服务器的响应是什么(状态代码和状态短语)?     401 Unauthorized  6.跟踪DNS      执行命令：nslookup www.mit.edu，如下：  1730116258406  1730116342186 | | | | | |
| 实验当中问题  及解决方法 | 1、在使用ethereal抓取报文时，发现发过来的报文绝大部分标记为异常报文(开启IPv4和TCP checksum)    IMG_256  目前很多网卡已经支持IP片以及IP/TCP/UDP等协议的校验和计算，用来减少内核层面的运算(减少CPU负载)，当协议层发现网卡支持相应的特性时，会将相应的处理交给网卡操作。如上面提到的校验和，正常情况下，校验和由对应的协议层处理，但在网卡使能情况下会将其推迟到网卡层面处理，网卡处理结束后直接发送，这就是为什么wireshark抓到的报文里面的校验和会提示不正确的原因，同样地，TCP会选择不大于滑动窗口的报文(该报文可能大于MSS)，交由网卡去分片处理。使用ethtool -k 命令可以查看网卡支持的特性。  理论上的解决方式：关闭网卡的Checksum功能，但是本人没有找到，故解决不了 | | | | | |
| 成绩（教师打分） | 优秀 | 良好 | | 及格 | | 不及格 |