|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名： | | 学号： | 专业年级： | 班级： |
| 分组： | | 实验室： | 指导教师：郭念 | 实验日期： |
| **实验的准备阶段**  **(指导教师填写)** | **课程名称** | **网络协议分析与攻防技术** | | |
| **实验名称** | 实验三 应用层协议 | | |
| **实验目的** | 1. 理解HTTP协议的工作原理 2. 理解DNS协议的工作原理 | | |
| **实验内容** | 应用层协议工作流程  1 ) 地址解析：如用客户端浏览器请求这个页面，会调用DNS协议域名，得服务器的IP地址。  2）DNS会向本地的DNS服务器发送DNS 请求报文，并收到服务器的解析报文，获得访问主机的IP地址。  3）封装HTTP请求数据包，请求部分结合本机自己的信息，封装成一个HTTP请求数据包  4）封装成TCP包，建立TCP连接（TCP的三次握手）  5）客户机发送请求命令  6）服务器响应  7）服务器关闭TCP连接 | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 □设计性 □综合性 | | |
| **实验的重点、难点** | DNS的工作流程和报文格式  HTTP的工作流程和报文格式 | | |
| **实验环境** | 本次实验根据本地主机和访问的服务器的真实网络地址进行。 | | |
| **实验的实施阶段** | **实验步骤及实验结果** | **一、利用网络协议分析软件抓取DNS协议数据包**  1.1  在打开本地主机上的“网络协议分析软件”，设置本地活动接口为捕获接口。然后单击”开始捕获分组“按钮，捕捉数据包。**实验过程截图如下：**    1.2  打开浏览器，在地址栏输入[www.qq.com](http://www.qq.com),按下回车，并在[www.qq.com](http://www.qq.com)主页搜索框输入河南大学进行搜索，选择查看一个搜索结果后。**实验过程截图如下：**    1.3  在网络协议分析软件单击“停止捕获分组”，在过滤器栏输入DNS。**实验过程截图如下：**    1.4  在分组列表查找第一个DNS请求报文“www.qq.com”。**实验过程截图如下：**      依次回答下图中各个字段的取值和含义    问题数：1  回答数：0  管理机构数：0  附加信息数：0  问题区：  回答区：无  管理机构区：无  附加信息区：无  在分组列表中分组编号为：  13749  1.5  在分组列表查找Standard query response报文[www.qq.com](http://www.qq.com)，。**实验过程截图如下：**    依次回答下图中各个字段的取值和含义    问题数：1  回答数：3  管理机构数：3  附加信息数：14  问题区：  回答区：  管理机构区：  附加信息区：  在分组列表中分组编号为：  13748  回答在DNS服务中，  本地主机IP地址是：109.244.211.100  DNS服务器地址是：218.68.91.163  **二、利用网络协议分析软件抓取TCP连接数据包**  2.1 在过滤器栏输入tcp，在分组列表查找1.5中DNS响应报文后的第一个TCP握手报文（SYN）。**实验过程截图如下：**    回答TCP报文首部各个字段的值和含义：    源端口：51792  目的端口：443  序号：0  确认号：0  检验和：0x3546  紧急指针：0  选项：  在分组列表中分组编号为：  6668  2.2  在分组列表查找第二次握手报文【SYN ACK】。**实验过程截图如下：**    回答TCP报文首部各个字段的值和含义：    源端口：443  目的端口：51792  序号：0  确认号：1  检验和：0x59da  紧急指针：0  选项：    在分组列表中分组编号为：  6674  2.3  在分组列表查找第三次握手报文【ACK】。**实验过程截图如下：**    回答TCP报文首部各个字段的值和含义：    源端口：51792  目的端口：443  序号：1  确认号：1  检验和：0x353a  紧急指针：0  选项：无  回答下面的问题：   1. [www.qq.com的IP](http://www.qq.com的IP)地址有哪些？为什么   有203.208.43.98 因为本地主机和[www.qq.com进行tcp](http://www.qq.com进行tcp)连接的时候，向这个ip发送tcp报文。   1. 本地主机访问的Web服务器IP地址是什么？   10.12.51.225  **三、分析HTTP报文**  3.1 在网络协议分析软件的分组列表中，查找TCP连接建立后的第一个HTTP报文。**实验过程截图如下：**    回答开始行各个字段的值和含义。  回答TCP报文首部各个字段的值和含义：   |  |  | | --- | --- | | **首部名称** | **含义** | | Content-Length | 内容长度 | | Content-Type | 内容类型 | | Content-Encoding | 内容编码 | | Content-Language | 内容语言 | | Host | 主机 | | Connection | 连接 | | Accept | 接受 | | Accept-Encoding | 接受编码 | | Accept-Charset | 接受字符设置 | | Accept-Language | 接受语言 | | If-Modified-Since | 请求头标签 | | Max-Forwards | 最大前缀 | | Location | 位置 |   回答实体主体是否有内容？如有，是什么？  有，tcp报文长度  3.2 在网络协议分析软件的分组列表中，查找3.1中HTTP请求报文的响应报文。**实验过程截图如下：**    回答开始行各个字段的值和含义。  回答TCP报文首部各个字段的值和含义：   |  |  | | --- | --- | | **首部名称** | **含义** | | Content-Length | 内容长度 | | Content-Type | 内容类型 | | Content-Encoding | 内容编码 | | Content-Language | 内容语言 | | Host | 主机 | | Connection | 连接 | | Accept | 接受 | | Accept-Encoding | 接受编码 | | Accept-Charset | 接受字符设置 | | Accept-Language | 接受语言 | | If-Modified-Since | 请求头标签 | | Max-Forwards | 最大前缀 | | Location | 位置 |   回答实体主体是否有内容？如有，是什么？  有，tcp报文长度 | | |
| **实验结果的处理阶段** | **实验结果的分析与总结** | **【实验思考】**  1．在浏览器输入境外域名,分析其域名解析过程。  首先，浏览器将检查域名是否存在于浏览器的DNS缓存中。如果缓存中存在该域名的DNS解析结果，则浏览器将直接使用缓存中的解析结果，跳过后续步骤。  如果缓存中不存在该域名的DNS解析结果，浏览器将向本地DNS服务器发送DNS查询请求。本地DNS服务器是由Internet服务提供商（ISP）提供的，通常位于用户所在的城市或区域。  如果本地DNS服务器缓存中存在该域名的DNS解析结果，则本地DNS服务器将返回缓存中的解析结果给浏览器。否则，本地DNS服务器将执行以下步骤：  本地DNS服务器将向根域名服务器发起DNS查询请求，询问根域名服务器关于该域名的授权域名服务器的信息。  根域名服务器将返回一个包含该域名授权域名服务器的IP地址的DNS响应报文给本地DNS服务器。  本地DNS服务器将向授权域名服务器发送DNS查询请求，询问关于该域名的IP地址信息。  授权域名服务器将返回一个包含该域名对应的IP地址的DNS响应报文给本地DNS服务器。  最后，本地DNS服务器将把该域名的IP地址返回给浏览器。  浏览器使用该IP地址来与该域名所对应的服务器建立TCP连接，并发送HTTP请求。  服务器接收到HTTP请求后，将返回HTTP响应报文给浏览器。  浏览器接收到HTTP响应报文后，将解析报文内容，并将内容渲染到用户的屏幕上 | | |