**中国矿业大学计算机学院**

**2019级本科生计算机网络实验报告**

实验内容 协议报文分析

学生姓名 姚炜柏 学 号 02190567

专业班级 信安19-2班

学 院 计算机科学与技术学院

任课教师 顾 军

|  |  |
| --- | --- |
| **评语** |  |

综合成绩： 任课教师签字：

年 月 日

**实验编号：03**

**实验名称：协议报文分析**

**实验内容：**

1. 分别获取不同互联网访问情形下的本机网卡数据包；过滤捕获和过滤显示不同条件的数据包。
2. 获取ARP协议数据单元，进行报文格式解析。
3. 获取ping、tracert、nslookup命令对应的交互数据，进行报文格式解析。
4. 针对不同互联网应用的执行过程进行抓包，对DNS服务、WWW服务、Email服务、QQ通信、微信、迅雷文件下载等六种不同网络应用服务访问情形下的数据包进行逐层分析，给出各层协议的主要参数及意义。

**实验要求：**

（1）运用抓包工具，实时抓包，记录包状态变化；

（2）给出不同应用情境下的不同层次数据包的分析结果，对每种应用服务的协议数据需要从应用层、运输层、网络层、数据链路层四个层次对相关协议格式、字段取值进行解析。

（3）对基于TCP的应用层协议，需要获取TCP协议的工作过程，验证连接建立的三次握手过程、四次挥手过程以及滑动窗口工作机制。

（4）验证IP数据包、TCP报文段和UDP数据报的**校验和**。

（5）验证数据链路层的CRC**冗余校验**。

**预习要求：**

提前通过互联网或在实验室开始实验前登录实验管理服务器，点击预习链接，阅览或下载实验指导书——预习\网络协议\进阶-IP分组基本报文分析。

**操作与观察：**

正确按照实验指导书步骤操作，观察记录下操作结果。

**实验报告要求：**

1. 按照实验要求，完成全部实验内容
2. 在标准实验报告书上填写全部实验操作记录和观察结果
3. 登录实验管理服务器，提交实验报告电子档。
4. 提交纸质版实验报告。

**实验报告内容：**

ARP

Request

|  |
| --- |
| Reply |
|  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | Frame：物理层的数据帧概况 | | | Ethernet Ⅱ：数据链路层以太网帧头部信息 | | | 其中Destination表示目的地址，此处为广播 | | | Source表示源地址 | | | Type 表示上层时ARP协议 | | | ARP(请求) | | | Hardware type | 硬件类型，此处为1表示以太网 | | Protocol type | 协议类型，此处为IPv4 | | Hardware size | 硬件地址长度 | | Protocol size | 协议长度 | | Opcode | 操作码 | | Sender MAC address | 发送主机的MAC地址 | | Sender IP address | 发送主机的IP地址 | | Target MAC address | 目标主机的MAC地址 | | Target IP address | 目标主机的IP地址 |   ARP(应答)  将自己的MAC地址填入Sender IP address发送到IP地址为Request报文中Sender IP address的主机。 |

HTTP

|  |
| --- |
| 请求包 |
|  |
| 响应包 |
|  |
| |  | | --- | | Ethernet Ⅱ数据链路层以太网帧的头部信息： | | Destination：目标MAC地址 | | Source：源MAC地址 | | Internet Protocol Version 网络层IP包头部信息 | | Version：4 IPv4协议 | | Header Length：头部长度 | | Total Length：总长度 | | Identification：标志字段 | | Flags：标记字段 | | Fragment offset：分片的偏移量 | | Time to live：生存周期 | | Protocol：上层协议 | | Header checksum status：头部数据校验和 | | Source：源IP地址 | | Destination：目标IP地址 | | Transmission Control Protocol运输层数据包头部信息： | | Source Port：源端口 | | Destination Port：目标端口 | | Sequence number：序列号 | | Next sequence number：下一个序列号 | | Acknowledgment number：确认序列号 | | Header Length：头部长度 | | Flags：标记字段 | |
| Window size value：流量控制窗口大小 |
| Checksum：TCP数据段校验和 |
| 应用层分析(请求报文) |
| GET：请求方式，后面为请求内容 |
| Host：请求主机名 |
| Connection：相应有关选项 |
| User-Agent：发送请求操作的系统、浏览器等信息 |
| Referer：来源页面 |
| Accept-Encoding：客户端可识别的数据编码 |
| Accept-Language：浏览器支持的语言 |
| 响应报文 |
| 第一行为状态行 |
| Date：响应时间 |
| Server：服务器信息 |
| Content-Length：消息大小 |
| Connection：连接状态 |

ICMP

|  |
| --- |
|  |
|  |

ICMP报文分析,此为ICMP询问报文

|  |
| --- |
| Type：8代表请求，0代表应答 |
| Code：为0代表回显应答 |
| Checksum：检验和 |
| Identifier：标识符 |
| Sequence number：序列号 |

UDP

|  |
| --- |
|  |

|  |
| --- |
| Source Port：源端口号 |
| Destination Port：目标端口号 |
| Length：数据包长度 |
| Checksum：校验和 |
| Date：填充数据，此处有71bytes数据 |

TCP三次握手四次挥手

第一次握手

|  |
| --- |
| SYN为1，seq=0 |

第二次握手

|  |
| --- |
| SYN=1，ACK=1，seq=0，ack=1 |

第三次握手

|  |
| --- |
| ACK=1，seq=1，ack=1 |

四次挥手

|  |
| --- |
|  |

第一次挥手

|  |
| --- |
| FIN=1，ACK=1，发送序列号seq=78，ack=1 |

第二次挥手

|  |
| --- |
| ACK=1，ack=seq+1=79，seq=1 |

第三次挥手

|  |
| --- |
| FIN=1，ACK=1，ack=79，seq=1 |

第四次挥手

|  |
| --- |
| ACK=1，seq=79,ack=2 |

验证握手

|  |  |  |  |
| --- | --- | --- | --- |
|  | SYN与ACK | seq | ack |
| 第一次握手 | 10 | x=0 | 0 |
| 第二次握手 | 11 | y=0 | x+1=1 |
| 第三次握手 | 01 | x+1=1 | y+1=1 |

验证挥手

|  |  |  |  |
| --- | --- | --- | --- |
|  | FIN与ACK | seq | ack |
| 第一次挥手 | 10 | u=78 | 1 |
| 第二次挥手 | 01 | v=1 | u+1=79 |
| 第三次挥手 | 11 | w=1 | u+1=79 |
| 第四次挥手 | 01 | u+1=79 | w+1=2 |

滑动窗口

在报文交互过程中，主动方将Window size value发送给被动方（如第一次挥手时，Window size value的值为303），在被动方发送确认时也将自己得Window size value发送给主动方（如第二次挥手时，Window size value的值为509），这样双方就知道了对方得窗口大小。此后发送数据时连续发送数据大小不能超过对方窗口大小。发送窗口满之后只有当收到确认时才可能继续发送数据。

PING

|  |
| --- |
|  |

总共ping了五次，对象为39.156.69.79，共有5个request和replyICMP包

|  |
| --- |
|  |

Ethernet Ⅱ数据帧内容

|  |
| --- |
|  |
| Destination：目的MAC地址 |
| Source：源MAC地址 |
| Type：数据包类型 |

IP数据包内容

|  |
| --- |
|  |

|  |
| --- |
| Version：4表示IPv4 |
| Header Length：5首部长度为5\*4bytes |
| Flags：标志位 |
| Flagment offset：分片偏移位 |
| Time to live：生存时间 |
| Protocol：1表示ICMP |
| Header checksum：首部检验和 |
| Source：源IP地址 |
| Destination：目的IP地址 |

ICMP数据包

|  |
| --- |
|  |
| Type：指定ICMP报文类型 |
| Code：0表示回显请求 |
| Checksum：校验和 |
| Identifier：匹配Reque和Reply的标识符 |
| Sequence number：匹配Reque和Reply的序列号 |
| Date：数据 |

**Tracert**

|  |
| --- |
|  |

|  |
| --- |
|  |

ttl=1、2、3各有三个，得知每一跳发送三个包，包被路由器丢弃后发送超时通知，可以解析出该路由器IP地址，第一跳路由IP地址为10.4.255.254，第二条路由IP地址为10.2.1.1。

|  |
| --- |
| 发送Type为11的ICMP报文，Time to live即为跳数。 |

nslookup

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

UDP数据帧分析

|  |
| --- |
| Source Port：源端口号 |
| Destination Port：目的端口号 |
| Length：长度字段 |
| Checksum：校验和 |

DNS报文分析

|  |
| --- |
| Transacti ID：标识字段 |
| Flags：标志字段 |
| Question：问题数 |
| Answer RRs：回答资源记录数 |
| Authority RRs：授权资源记录数 |
| Additional RRs：附加资源记录数 |

**WWW服务**

|  |
| --- |
|  |

|  |
| --- |
|  |
| |  | | --- | | Ethernet Ⅱ数据链路层以太网帧的头部信息： | | Destination：目标MAC地址 | | Source：源MAC地址 | | Internet Protocol Version 网络层IP包头部信息 | | Version：4 IPv4协议 | | Header Length：头部长度 | | Total Length：总长度 | | Identification：标志字段 | | Flags：标记字段 | | Fragment offset：分片的偏移量 | | Time to live：生存周期 | | Protocol：上层协议 | | Header checksum status：头部数据校验和 | | Source：源IP地址 | | Destination：目标IP地址 | | Transmission Control Protocol运输层数据包头部信息： | | Source Port：源端口 | | Destination Port：目标端口 | | Sequence number：序列号 | | Next sequence number：下一个序列号 | | Acknowledgment number：确认序列号 | | Header Length：头部长度 | | Flags：标记字段 | |
| Window size value：流量控制窗口大小 |
| Checksum：TCP数据段校验和 |
| 应用层分析(请求报文) |
| GET：请求方式，后面为请求内容 |
| Host：请求主机名 |
| Connection：相应有关选项 |
| User-Agent：发送请求操作的系统、浏览器等信息 |
| Referer：来源页面 |
| Accept-Encoding：客户端可识别的数据编码 |
| Accept-Language：浏览器支持的语言 |
| 响应报文 |
| 第一行为状态行 |
| Date：响应时间 |
| Server：服务器信息 |
| Content-Length：消息大小 |
| Connection：连接状态 |

**DNS服务**

|  |
| --- |
|  |

抓到的DNS包

|  |
| --- |
|  |

请求包

|  |
| --- |
|  |

|  |
| --- |
| Transaction ID：对应请求报文和应答报文 |
| Flags：标志字段 |
| Question：问题数 |
| Answer RRs：回答资源记录数 |
| Authority RRs：授权资源记录数 |
| Additional RRs：附加资源记录数 |

应答包

|  |
| --- |
| Transaction ID为0x0001与请求包对应 |

QQ服务

|  |
| --- |
|  |

|  |  |
| --- | --- |
| 图中OICQ中Data即为qq号，标蓝部分为qq号的十六进制  **微信服务**   |  | | --- | | 发送微信消息，成功抓到3个TCP包和三个SSL包 |   **Email服务** |

|  |
| --- |
| 使用foxmail给自己发邮件，[1685962487@qq.com](mailto:1685962487@qq.com)为邮箱账号 |

校验和验证：

IP数据报：

|  |
| --- |
|  |

|  |
| --- |
| 根据循环加法，最后结果为E106，取反为1EF9，与报文中校验和字段一致 |

UDP数据报

UDP校验和为伪首部加上首部加上数据部分然后取反得到

伪首部

|  |  |  |  |
| --- | --- | --- | --- |
| 源IP地址 | 目的IP地址 | 协议类型 | UDP长度 |

首部

|  |  |  |  |
| --- | --- | --- | --- |
| 源端口 | 目的端口 | 长度 | 校验和 |

|  |
| --- |
|  |

此处

|  |
| --- |
| 源IP地址：dfa6 9726 |
| 目的IP地址：0a04 d405 |
| 协议类型：0011 |
| UDP长度：003f |
| 源端口：1f40 |
| 目的端口：0fa0 |
| 长度：0076 |

循环加和为0FBE5，取反结果为0x041a

TCP数据报

TCP校验和和UDP校验和计算相似，伪首部加首部加数据然后取反

|  |
| --- |
| 源IP地址：3104 20c4 |
| 目的IP地址：0a04 d405 |
| 协议类型：0006 |
| TCP长度：0020 |
| 源端口：0050 |
| 目的端口：d147 |

|  |
| --- |
| 循环加和为取反结果为0xfeb3 |

**实验体会：**

以前有稍微使用过wireshark和burpsuite，但实验仍做得不是很顺利，问题主要在知识不牢固，不知道该抓什么类型的包。