|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **计算机网络与通信实验报告（三）** | | | | | | |
| 学 号 | 姓 名 | | 班 级 | | 报告日期 | |
| 2022211939 | 杨涛 | | 2211106 | | 2024.11.5 | |
| 实验内容 | **利用分组嗅探器分析传输层与网络层协议** | | | | | |
| 实验目的 | 1、了解传输层TCP/UDP协议构造；  2、了解网络层IP协议构造； | | | | | |
| 实验预备知识 | TCP/UDP协议、IP协议、ICMP协议等 | | | | | |
| 实验过程描述 | 1. **对传输层协议TCP/UDP进行捕包分析**   (1)启动浏览器，打开http://gaia.cs.umass.edu/ethereal- labs/alice.txt 网页，得到ALICE'S ADVENTURES IN WONDERLAND文本，将该文件保存到主机上。  (2)打开http://gaia.cs.umass.edu/ethereal-labs/TCP -ethe real-file1.html，在Browse按钮旁的文本框中输入保存在主机上的文件ALICE'S ADVENTURES IN WONDERLAND的全名（含路径），此时不要按“Upload alice.txt file”按钮。  (3)启动分组捕获软件，开始分组俘获。  (4)在浏览器中，单击“Upload alice.txt file”按钮，将文件上传到gaia.cs.umass.edu服务器，一旦文件上传完毕，一个简短的贺词信息将显示在你的浏览器窗口中。  (5)停止俘获。  (6)在显示筛选规则中输入“tcp”。  **2、对网络层协议IP进行捕包分析**  (1)打开捕包软件开始捕包；  (2)开启pingplotter，然后在“Address to Trace”窗口输入目的地目标的名字：在“#of times to Trace”区域输入3。然后选择Edit-> Options-> Packet，确认在packet size字段的值为56，点OK。然后按下Trace按钮。  (3)接下来，发送一组具有较长长度的数据包，通过Edit->Options-> Packet在包大小区域输入值为2000，点OK。接着按下Resume按钮；  (4)再发送一组具有更长长度的数据包，通过Edit->Options->Packet在包大小区域输入值为3500，点OK。接着按下Resume按钮；  (5)停止捕包。 | | | | | |
| 实验结果 | **一、 对传输层协议TCP/UDP进行捕包分析**  (1) 向gaia.cs.umass.edu服务器传送文件的客户端主机的IP地址和TCP端口号是多少？  客户端主机的IP为**192.168.128.63**，TCP端口号为**13968**      (2) Gaia.cs.umass.edu服务器的IP地址是多少？对这一连接，它用来发送和接收TCP报文段的端口号是多少？      Gaia.cs.umass.edu服务器的IP地址为**128.119.245.12**  其用来发送和接收TCP报文段的端口号为**80**  (3) 客户服务器之间用于初始化TCP连接的TCP SYN报文段的序号（sequence number）是多少？在该报文段中，是用什么来标示该报文段是SYN报文段的？    客户服务器之间用于初始化TCP连接的TCP SYN报文段的序号（sequence number）是**0 (3621733455)**，使用**Flags:0x002**来标示该段报文段是SYN报文段。  (4) 服务器向客户端发送的SYNACK报文段序号是多少？该报文段中，ACKnowledgement字段的值是多少？Gaia.cs.umass.edu服务器是如何决定此值的？在该报文段中，是用什么来标示该报文段是SYNACK报文段的？    服务器向客户端发送的SYNACK报文段序号是**0 (1569077778)**，ACKnowledgement字段的值是**1 (3621733455)**，由客户服务器传递的SequenceNumber值加1得到，**Flags=0x012**标示该报文段是SYNACK报文段。  (5) 包含HTTP POST命令的TCP报文段的序号是多少？  TCP报文段的序号是3621885824。    (6) 考虑在TCP连接中含有HTTP POST并把它作为第一个片段的TCP片段。在TCP连接（包括含有HTTP POST的片段）中最先的六个片段的序列号是多少？每一个片段是什么时候发送的？每一个片段接收到ACK是什么时候？请给出每一个TCP片段发送和确认被收到时的间隔，即六个片段中的每一个RTT值是多少？当接收到每一个ACK时的EstimatedRTT值是多少？假设对于第一个片段来说，EstimatedRTT值和标准的RTT值相同。  EstimatedRTT=(1-α)\*EstimatedRTT+α\*SampleRTT （假设α＝0.125）可以知道如何计算即可。         |  |  |  |  |  | | --- | --- | --- | --- | --- | | 序号 | 发送时间 | 接收时间 | RTT | EstimatedRTT | | 3621733456 | 1.880582 | 2.217722 | 0.337140 | 0.337140 | | 3621734160 | 1.880582 | 2.217722 | 0.337140 | 0.337140 | | 3621735520 | 1.880582 | 2.218618 | 0.338036 | 0.337194 | | 3621736880 | 1.880582 | 2.218618 | 0.338036 | 0.337247 | | 3621738240 | 1.880582 | 2.218618 | 0.338036 | 0.337301 | | 3621739600 | 1.880582 | 2.218618 | 0.338036 | 0.337354 |     (7) 前六个TCP报文段的长度各是多少？    **704bytes、1360bytes、1360bytes、1360bytes、1360bytes、1360bytes**  (8) 在整个跟踪过程中，接收端公示的最小的可用缓存空间是多少？限制发送端的传输以后，接收端的缓存是否仍然不够用？  最小可用缓存空间为30720；    限制发送后，缓存基本够用，接受窗口变大了    (9) 在跟踪文件中是否有重传的报文段？进行判断的依据是什么？  存在重传的报文段，依据：TCP Analysis Flags is a retransmission  **二、对网络层协议IP进行捕包分析**  (10) 选择你的电脑所发送的第一个ICMP请求消息，在包详细信息窗口扩展包的Internet协议部分。你的电脑的IP地址是多少？  10.236.248.40    (11) 在IP包头部，上层协议区域的值是多少？    上层协议区域的值是1(ICMP)  (12) IP头部有多少字节？IP数据包的有效载荷是多少字节？解释你是怎样确定有效载荷的数量的？  IP头部有**20字节**，通过4\*HeaderLength得出；  IP数据包的有效载荷是36字节，通过数据包大小减去IP头部大小得出。    (13) 这个IP数据包被分割了吗？解释你是怎样确定这个数据包是否被分割？    没有被分割，IP头部的Flags以及FragmentOffset分别为0x0，0，表示没有分割标志被设置以及包偏移量为0，所以得出数据包没有被分割。  (14) 接下来单击列名按IP源地址排序数据包，选择你的电脑发送的第一个ICMP请求消息，扩展显示IP协议的数据。    (15) 在包捕获列表窗口，你能看到在第一个ICMP下的所有并发的ICMP消息吗？    可以  (16) 往同一IP的数据包哪些字段在改变，而且必须改变？为什么？哪些字段是保持不变的，而且必须保持不变？      标识符Identification、Time to live TTL、校验和checksum必须改变。  如果同一个分组存在分段现象，那么Identification字段就用于标识段的归属，便于接收方重组包。所以不同分组的Identification字段不同。对于不同分组，TTL值每次加1，以此来实现路由跟踪。从而每次计算得的checksum不同。  版本号version、首部长度header length、服务类型differentiated services field、数据报总长度total length、标志flags、段偏移 fragment offset、协议protocol、源IP source、目的IP destination 保持不变。  版本号version、首部长度header length、服务类型differentiated services field、协议protocol必须保持不变。  (17) 描述一下在IP数据包的Identification字段的值是什么样的？    IP数据包的Identification字段，也称为标识字段（Identification），是一个16位的字段，用于标识和唯一标识IP数据包。每个IP数据包在传输过程中都会分配一个不同的标识号，以便接收端能够将数据包进行正确重组，并确保数据包在目标系统上以正确的顺序被重新组装。  (18) Identification字段和TTL字段的值是多少？  Identification：0x5245；TTL：4    (19) 所有的通过最近的路由器发送到你的电脑去的ICMP的TTL溢出回复是不是值都保持不变呢？为什么？  是，保持不变。  TTL初始值由发送方生成，此值多数情况下是不会改变的，而TTL会在经过路由器时自减一，最近的路由器发到本机的ICMP的TTL只会减1。      (20)那个消息是否传送多于一个IP数据包的分片？看第一个被分割的IP数据包的片段，在IP头部有什么信息指出数据包已经被分割？在IP头部有什么信息指出这是否是第一个与后面片段相对的片段？这个IP数据包的长度是多少？    Pingplotter传送了多于一个IP数据包的分片。More fragments标志位被置1，说明该包之后还有相同消息对应的包，指示数据包已经被分割。    第一个片段与之后的相同分组对应的片段的identification值相同，且第一个片段的段偏移Fragment offset为0。   1. 看被分割的IP数据包的第二个片段。在IP头部有什么信息指出这不是第一个数据包片段？有更多的片段吗？你是怎么知道的？和上一个分片的长度加起来是2000吗？     段偏移Fragment offset不为0，说明这不是第一个数据包片段。More Fragments为0，说明已经没有更多的片段了。  和上一分片相加，IP数据包的总长度为1500+520=2020，不为2000。这是因为，在不分片的情况下，头部长度为20字节，有效载荷1980字节，而现在相同identification对应的分组被分片了，对于每一个片段都需要一个20字节的头部，故第一个IP数据包的头部长度为20字节，有效载荷1480字节，总长度1500字节；第二个IP数据包的头部长度为20字节，有效载荷500字节，总长度520字节。  (22) 哪个字段在第一个和第二个片段之间的IP头部改变了？Identification变了吗？  TotalLength、FragmentOffset和Identification也变了。  (23) 再找出在pingplotter中把包的大小改成3500后，你的电脑所发送的第一个ICMP请求消息。    (24) 从原始的数据包中产生了多少片段？片偏移分别为多少？    3个包，偏移量分别为0、1480、2960  (25) 在片段之中IP头部哪些字段改变了？Identification变了吗？  IP数据包总长度Total length，标志位Flags，段偏移Fragment offset，头部校验和Header checksum发生了变化。 | | | | | |
| 实验当中问题  及解决方法 | 1. pingplotter新版不可以提前预设count值。   解决方法：运行时看着count，当count基本为3时，暂停跟踪。  2、用pingplotter路由跟踪时，当分组大小增加为2000和3500时，仅用icmp的条件进行筛选会存在分片遗漏。  解决方法：因为非末尾的分片仅有IP协议，没有ICMP协议，所以将筛选条件放宽为icmp 或者 ip即可。  3、在分析理应被分割的数据报时，发现分割标记未被设置。  解决：Ethereal在对应位置显示的是此次数据传输的最后一个数据报，因此标记为必然为0.可以在展开信息中追踪到本次传输发送的第一个数据报进行分析。这样便得到正确结果。 | | | | | |
| 成绩（教师打分） | 优秀 | 良好 | | 及格 | | 不及格 |