|  |
| --- |
| 实验目的：  掌握使用Wireshark捕获及分析UDP协议  实验结果：   1. 从跟踪中选择一个 UDP 数据包。从此数据包中，确定 UDP 标头中有多少字段，并为这些字段命名。   屏幕截图 2023-03-27 150631  UDP 的标头有 4 个字段，各字段分别为：  Source Port：源端口号  Destination Port：目的端口号  Length：长度  Checksum：校验和   1. 通过查询 Wireshark 的数据包内容字段中显示的信息，确定每个 UDP 报头字段的长度   屏幕截图 2023-03-27 150737  屏幕截图 2023-03-27 150754  屏幕截图 2023-03-27 150823  屏幕截图 2023-03-27 150811  如上图所示，每个部分都是 2 byte，因此 UDP 头部长度为 8 byte = 64 bit。  3. 长度字段中的值是指的是什么？使用捕获的 UDP 数据包验证您的声明。  长度字段指示了在 UDP 报文段中的字节数(头部长度 + 数据长度)  79=71+8；  屏幕截图 2023-03-27 150844  4.UDP 有效负载中可包含的最大字节数是多少？  Length 字段占 2byte == 65536 bit，并且其中 8 byte 是 UDP 首部信息。  因此有效载荷 = 65536 - 8 = 65528 bit。  5. 最大可能的源端口号是多少？  两个 Port 字段占 2byte == 65536 bit，端口号从 0 开始算，  最大端口号 = 65536 - 1 = 65535。   1. UDP 的协议号是什么？ 以十六进制和十进制表示法给出答案。   屏幕截图 2023-03-27 151654  UDP 的协议号为 17，十六进制为 0x11。  7. 观察发送 UDP 数据包后接收响应的 UDP 数据包，这是对发送的 UDP 数据包的回复，请描述两个数据包中端口号之间的关系。(提示：对于响应 UDP 目的地应该为发送 UDP 包的地址。）  发送的 UDP 的源端口是响应 UDP 的目的端口，  发送的 UDP 的目的端口是响应 UDP 的源端口，  发送 UDP 数据包：  屏幕截图 2023-03-27 151000  接收UDP 数据包：  屏幕截图 2023-03-27 151013  打印数据包：    问题及收获：  如何捕获到udp协议？  多试几次，多等待一会，使用udp进行筛选；  什么是有效负载？  有效负载是被传输数据中的一部分，而这部分才是数据传输的最基本的目的，和有效负载一同被传送的数据还有：数据头或称作元数据，有时候也被称为开销数据，这些数据用来辅助数据传输。  长度字段指的是 UDP 报文中头部长度加数据长度 |