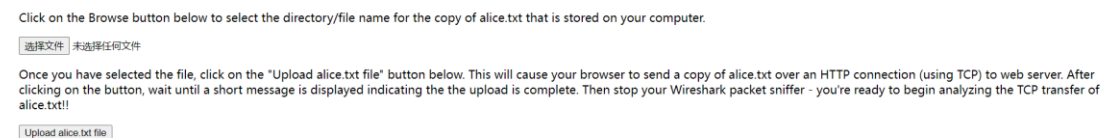


截图+说明

1. 批量捕获 TCP 传输

- 在 elearnning 实验 5 有关文件中下载 alice.txt
- 然后登录 <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html> 将会看到如下页面：



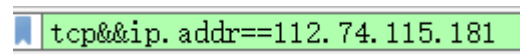
- 使用“选择”按钮来选择 alice.txt。不要点击“上传 alice.txt 文件”按钮。
- 接下来使用 wireshark 开始抓包。
- 返回浏览器，按“上传 alice.txt 文件”按钮将文件上传到服务器。
- 停止 Wireshark 数据包捕获。

2. 查看捕获结果

(1) 将文件传输到服务器的源 IP 地址和源 TCP 端口号是什么？筛选出对应 HTTP 消息并查看用于携带此 HTTP 消息的 TCP 数据包的详细信息。

(2) 服务器的 IP 地址是什么？端口号是哪个？

接着根据本地 ip 地址或源 ip 地址，以及 tcp 条件进行筛选。

 (语法示例)

3. TCP 基础

根据 TCP 段的内容回答以下问题：

(3) 用于启动客户端计算机与服务器之间 TCP 连接的 TCP SYN 段的 sequence number 是多少？是什么字段将该段标识为 SYN 段？

(4) 服务器发送给客户端计算机来回复 SYN 的 SYNACK 段的 sequence number 是多少？SYNACK 段中的 Acknowledgment 字段的值是多少？服务器是如何确定该值的？是什么字段将该段标识为 SYN ACK 段？

(5) 包含 HTTP POST 命令的 TCP 段的 sequence number 是多少？（提示：为了找到 POST 命令，需要查看 Wireshark 窗口底部的“16 进制数据查看面板”中带有“POST”）

(6) 将包含 HTTP POST 的 TCP 段视为 TCP 连接中的第一个段。TCP 连接的前三个段（包括包含 HTTP POST 的段）的 sequence number 分别是多少？

(7) 包含 HTTP POST 的 TCP 段之后的那个 TCP 段的长度 (TCP Segment Len) 是多少？

(8) 可用缓冲区大小（看包含 HTTP POST 的 TCP 段的 Win 字段，即 calculated window size）是多少？