小实验 4 实验指导书

1、实验要求

本次小实验由 2 个抓包观察实验(第二部分)和 2 个简述题(第三部分)构成。所有抓包实验都需要给出简短的实验报告，内容包括：

(1)文字回答：回答指导书中提出的问题。要求简短，每个实验回答总计不宜超过 100 字。有参考答案的题目可不做文字回答。

(2)过程截图：展示关键实验过程，也可作为文字回答的补充。若无特别要求，则每个实验至少一张截图，展示实验过程。若有具体截图要求([]为要求)，则按照[]中要求给出对应截图。

注意 1：本次小实验中，抓包实验 2(5)，2(6)为选做实验。不完成不扣分，完成也没有额外的加分

2、实验题目及指导

抓包实验 1：观察 UDP 消息

依次执行以下操作：

- 开启 Wireshark 捕获数据帧
- 任意浏览网页，构造 UDP 数据包

观察 Wireshark 中捕获的数据包，并回答以下问题。

（1）UDP 数据包在 IP 层的类型编号是？**[截图展示 UDP 数据包 IP 头类型编号]**

参考答案：17

（2）UDP 数据包头字段依次是？[**截图展示 UDP 数据包头信息**]

参考答案：源端口号(16bit)，目的端口号(16bit)，UDP 包总长(16bit)，校验和(16bit)

抓包实验 2：观察 TCP 消息

依次执行以下操作：

- 访问 http://test.ustc.edu.cn/
- 开启 Wireshark 捕获数据帧
- 使用网站测速功能，观察测速时的 TCP 流量

注 1：为了观察到完整 TCP 流，请在测速结束后等待一段时间再停止 Wireshark 捕获

注 2：选择数据包->右键->对话过滤器->TCP；可以很方便的提取单流过滤条件(ip 对 + port 对)

观察 Wireshark 中捕获的数据包，并回答以下问题。

（1）TCP 数据包在 IP 层的类型编号是？[**截图展示 TCP 数据包 IP 头类型编号**]

参考答案：6

（2）TCP 数据包头字段依次是？[**截图展示 TCP 数据包头**]

参考答案：源端口号(16bit)，目的端口号(16bit)，报文序列号(32bit)，报文确认序列号(32bit)，包头长度(4bit)，保留位和标记位(12bit)，窗口大小(16bit)，校验和(16bit)，紧急指针

(16bit)，选项

（3）TCP 三次握手过程使用三个数据包，他们的标记位，序列号，确认序列号有什么特点？TCP 握手时使用选项协商链接参数，举出一个例子？[**截图展示 TCP 三次握手数据包包头**]

参考答案：(流向，标记位，序列号，确认序列号)依次为：

(A->B,SYN,SEQ=X,ACK=0)

(B->A,SYN||ACK,SEQ=Y,ACK=X+1)

(A->B,ACK,SEQ=X+1,ACK=Y+1)

通过选项协商的例子：MTU 大小，对 SACK 的支持与否等等

（4）TCP 传输过程中利用序列号和确认序列号实现数据的可靠传输。序列号增长和包长关系是什么？确认包确认序列号和原包序列号的关系是什么？[**截图展示序列号和确认号变化规律**]

参考答案：TCP 序列号的增长差值与前一个包的 TCP 段长度(TCP 数据字段)相等；数据包对应确认包中，确认序列号与(原包序列号+段长)相等。

（5）TCP 四次挥手过程使用四个数据包，他们的标记位，序列号，确认序列号有什么特点？（选做）

注 1：关闭链接数据包可能因为丢包而不完整(不足四个)，或因为使用了 RST 报文而不完整，实验中可以多次重复实验以观察现象

参考答案：四个数据包分两组，分别代表链接双方的关闭操作，特点类似。以 A 主动关闭与 B 的链接为例，(流向，标记位，序列号，确认序列号)依次为：

(A->B,FIN,SEQ=X,ACK=Y)

(B->A,ACK,SEQ=Y,ACK=X+1)

（6）使用 Wireshark 工具栏的统计->TCP 流图形功能，观察 TCP 拥塞控制算法的行为。（选做）

参考答案：略（考虑到大部分同学使用无线网络，拥塞控制机制受丢包影响较大，故设为选做）

Wireshark 过滤语句参考

（1）ip 地址过滤(ip.addr == <your_ip>)

（2）限定 TCP 特定流((ip.addr == <ip_a> and ip.addr == <ip_b>) and (tcp.port == <port_a> and tcp.port == <port_b>))

（3）限定 TCP 标记位(tcp.flags.syn，tcp.flags.fin 等等)

3、简述题

（1）TCP 建立连接时使用选项协商 MTU 信息。上网查资料，TCP 选项还支持什么特殊的功能？

（2）反射 DoS 攻击中，攻击者将数据包源地址改为受害者 IP 向公共服务(DNS，NTP 等等)发送请求，公共服务回复数据包至受害者 IP，使受害者带宽耗尽。为什么此类攻击大多使用基于 UDP 的公共服务，而不是基于 TCP 呢？

4、参考资料

RFC 768(UDP 报文格式)： https://www.rfc-editor.org/rfc/rfc768

RFC 793(TCP 报文格式)： https://www.rfc-editor.org/rfc/rfc793