小实验 3 实验指导书

1、实验要求

本次小实验由 3 个抓包观察实验(第二部分)和 3 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。

2、实验题目及指导

抓包实验 1：观察 ICMPv4 超时消息:

依次执行以下操作：

- 开启 Wireshark 捕获数据帧
- 运行 ping -i 3 www.baidu.com

注 1：Linux 环境限制 TTL 选项为 ping -t

注 2：macOS 环境限制 TTL 选项为 ping -m

注 3：如果没有收到超时回显，尝试调整 TTL 的跳数

观察 Wireshark 中捕获的数据包，并回答以下问题。

（1）收到的 ICMP 包头中，Type 字段和 Code 字段分别是多少？**[截图展示 ICMP 超时数据包包头]**

参考答案：Type 字段为 11，Code 字段为 0。

抓包实验 2：观察 ICMPv4 回显请求及应答消息

依次执行以下操作：

- 开启 Wireshark 捕获数据帧
- 运行 ping www.baidu.com

观察 Wireshark 中捕获的数据包，并回答以下问题。

（1）ICMP 请求分组中，Type 字段和 Code 字段分别是多少？**[截图展示 ICMP 请求数据包包头]**

参考答案：Type 字段为 8，Code 字段为 0。

（2）ICMP 回显分组中，Type 字段和 Code 字段分别是多少？ **[截图展示 ICMP 回显数据包包头]**

参考答案：Type 字段为 0，Code 字段为 0。

（3）一对请求和回复分组中的标识符，序号和数据是否相等？**[截图展示 ICMP 一对请求和回显数据包包头]**

参考答案：对应分组对的标识符，序号和数据字段均相等。

抓包实验 3：观察 ARP 分组各式

依次执行以下操作：

- 开启 Wireshark 捕获数据帧
- 运行 arp -d 命令删除主机所有 ARP 表项（只删除网关亦可）
- 用浏览器浏览网页

注 1：windows 用户注意用管理员权限打开 CMD

注 2：macOS 用户删除主机所有 ARP 表项的命令是 sudo arp -a -d

观察 Wireshark 中捕获的数据包，并回答以下问题。

（1）ARP 协议在以太网帧头中载荷类型的编号是？**[截图展示 ARP 包以太网头]**

参考答案：0x0806

（2）ARP 分组头中，以太网硬件类型编号和 IP 协议类型编号分别是？**[截图展示 ARP 包包头]**

参考答案：硬件类型以太网：1，协议类型 IPv4：0x0800

（3）ARP 请求分组中，操作码（Opcode）值是？源 IP 地址及 MAC 地址，目的 IP 地址及 MAC 地址是多少？**[截图展示 ARP 请求包包头]**

参考答案：Opcode 值是 1，(Sender)源 IP 和 MAC 是本机，(Target)目的 IP 和 MAC 是请求的 IP 地址和广播地址

（4）ARP 回复分组中，操作码（Opcode）值是？源 IP 地址及 MAC 地址，目的 IP 地址及 MAC 地址是多少？**[截图展示 ARP 回复包包头]**

参考答案：Opcode 值是 2，(Sender)源 IP 和 MAC 是请求的 IP 地址和回复的 MAC，(Target)目的 IP 和 MAC 是本机

3、简述题

（1）上网查找资料，看看 ICMPv4 消息的隐患，以及黑客是如何利用它发起攻击的，由此思考为什么很多系统不发送 ICMPv4 消息。

（2）ping 同一局域网内的主机和局域网外的主机，都会产生 ARP 报文么？所产生的 ARP 报文有何不同，为什么？

（3）ARP 请求数据包是支撑 TCP/IP 协议正常运作的广播包。如果滥发或错发 ARP 广播包会产生那些不良影响？如何发现和应对？

4、参考资料

RFC 792(ICMPv4 报文格式)： https://www.rfc-editor.org/rfc/rfc792

RFC 826 (ARP 报文格式)： https://www.rfc-editor.org/rfc/rfc826