|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名：崔文帅 | | 学号：2025060163 | 专业年级： 20网工 | 班级： 网三 |
| 分组： | | 实验室：402 | 指导教师：郭念 | 实验日期：2023/3/3 |
| **实验的准备阶段**  **(指导教师填写)** | **课程名称** | **网络协议分析与攻防技术** | | |
| **实验名称** | 实验二 ICMP控制报文协议 | | |
| **实验目的** | 1) 掌握ICMP协议的报文格式。 | | |
| **实验内容** | 目的不可达: 当路由器收到一个无法传递下去的IP报文时，会发送ICMP目的不可达报文（Type为3）给IP报文的源发送方,报文中的“代码”就表示发送失败的原因。 | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 □设计性 □综合性 | | |
| **实验的重点、难点** | ARP工作流程和报文格式 | | |
| **实验环境** | vimage.png  本次实验根据虚拟机的真实MAC地址进行实 | | |
| **实验的实施阶段** | **实验步骤及实验结果** | **一、查看主机IP信息**  1.1  在主机A上,单击”开始”->”运行”-〉输入“cmd”->”ipconfig /all”,显示主机A的IP设置。**实验结果截图如下：**    **二、设置网络协议分析软件参数**  2.1  在主机A上，打开“网络协议分析软件”单击“过滤器”->“添加”->”类型过滤器”->”icmp协议”->”接受”->”设置参数”-〉“确定”，软件只抓取icmp协议的数据包。单击“开始”按钮，捕捉数据包。**实验结果截图如下：**    2.2  在命令行下输入“ping 20.0.0.2 ”对server主机发送icmp数据包。**实验结果截图如下：**    2.3  在数据包分类列表中，单击第一个发送报文，源地址为192.168.1.2，目的地址为20.0.0.2，主机A发送给server的ICMP回显请求报文,其中生存时间TTL=128。**实验结果截图如下：**    l  类型：8，表示此报文为ICMP回显请求报文。  l  代码：0，ICMP回显请求和应答报文类型均为0。  l  校验和：校验和部分为ICMP报头及数据部分的校验数据。  l  标识符：512，对此请求的应答报文中的标识符也为512。  l  序列号：256，确认ICMP应答报文。  l  数据： abcdefghijklmnopqrstuvwabcdefghi 。  2.4  在数据包分类列表中，单击第一个接收报文，源IP地址为20.0.0.2，目的IP地址为192.168.1.2，主机server发送给主机A的ICMP回显应答报文,其中生存时间TTL=127。**实验结果截图如下：**    l  类型：0，ICMP回显应答报文类型为0。  l  代码：0，ICMP回显报文代码均为0。  l  校验和：由软件自动计算。  l  标识符：512，与主机A发送ICMP回显请求报文的标识符相同。  l  序列号：256，与主机A发送的ICMP回显请求报文的标识符相同。  l  数据：abcdefghijklmnopqrstuvwabcdefghi。  2.5  单击清空按钮，清空捕捉的数据包。**实验结果截图如下：**    2.6  在命令行下输入“ping 20.0.0.3 ”主机发送icmp数据包。**实验结果截图如下：**    2.7  单击ICMP回显下的192.168.1.2<=>20.0.0.3，可以看到ICMP回显请求数据包中类型为8，目标IP地址为 20.0.0.3。**实验结果截图如下：**  2.8  单击ICMP不可达中192.168.1.2<=>192.168.1.200，可以看到ICMP不可达数据包中类型为3，代码1表示主机不可达，只能由路由器产生。**实验结果截图如下：**    **三、利数据包发送器编辑ICMP不可达数据包**  3.1  单击清空按钮，清空捕捉的数据包。**实验结果截图如下：**    3.2  启动主机A上的数据包发送器,单击菜单栏”添加”按钮,在协议模板中选择”ICMP回显协议模板”，单击“确定”按钮，软件自动添加一个ICMP数据包。**实验结果截图如下：**    3.3  在数据包编辑区，目的物理地址为网关192.168.1.200的实际MAC地址（具体方法为：单击地址本-->更新地址本-->选择更新后的IP或者MAC-->单击确定，或者手动进行输入，下同）、源物理地址填为主机A的MAC地址、总长度填入60、发送IP地址填入192.168.1.2、目标IP地址20.0.0.3、类型填入8，标识符填入512（此值可指定范围内的任意值）、序列号填入4352（此值可指定范围内的任意值）、ICMP回显数据部分填入91 92 93 94 95 96 97 98 91 92 93 94 95 96 97 98 91 92 93 94 95 96 97 98 91 92 93 94 95 96 97 98。ICMP回显数据部分填入内容数量32个即可。**实验结果截图如下：**    3.4  在数据包列表区选中数据包，单击工具栏“校验和”按钮，软件自动计算数据包的校验和。**实验结果截图如下：**    3.5  单击工具栏“发送”按钮，在发送数据包中，选中循环发送、发送次数填入1，单击“开始”按钮。发送编辑好的数据包。**实验结果截图如下：**    3.6  在网络协议分析软件中，单击会话树中的发送数据包，在右侧的协议结构树中显示发送数据包的详细信息，显示类型8，表示回显请求报文，标识符为512、序列号为4352。**实验结果截图如下：**    3.7  单击会话树中的接收数据包，在右侧的协议结构树中，显示接收数据包的详细信息，类型为3表示为不可达报文，代码为1表示由路由器发送。**实验结果截图如下：** | | |
| **实验结果的处理阶段** | **实验结果的分析与总结** | **【实验思考】**  ICMP协议就是ping服务吗？  Ping基于ICMP协议工作，ICMP中的echo请求和echo回应消息通常用于执行ping网络工具的功能。Ping工具向目标主机发送echo请求消息，等待目标主机返回echo回应消息来检测可达性和网络延迟。因此，可以说ICMP协议提供了ping服务。但是icmp协议并不只用于ping服务，还用于诊断和排除网络故障，以及支持其他网络协议的正常运行。 | | |