**ICMP隧道通讯实验报告**

|  |  |  |
| --- | --- | --- |
|  |  | **实验时间**：2021/8/11 |

**一、实验目的**

实践学习ICMP隧道通讯原理

**二、实验内容与实验步骤**

1，发送端对消息文件进行Base64编码

2，接收端抓取ICMP包

3，发送端使用ICMP隧道发送编码后的消息

4，接收端将抓取到的内容进行Base64解码

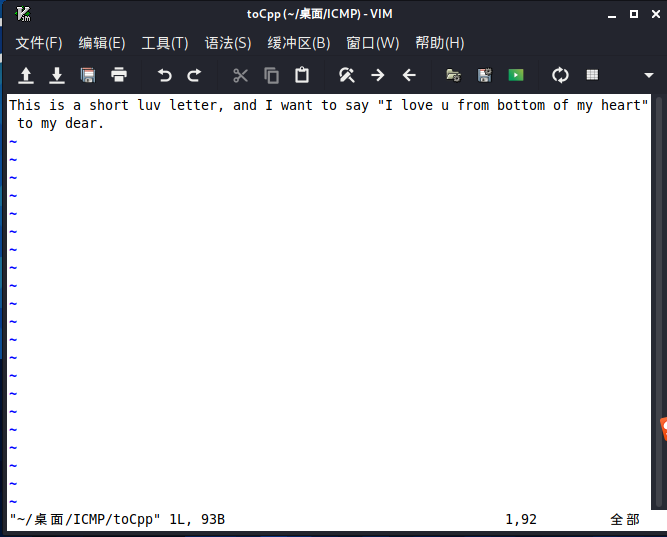
**三、实验环境**

Linux version 5.10.0-kali3-amd64

SMP Debian 5.10.13-1kali1

Microsoft Windows 10 家庭中文版10.0.19042

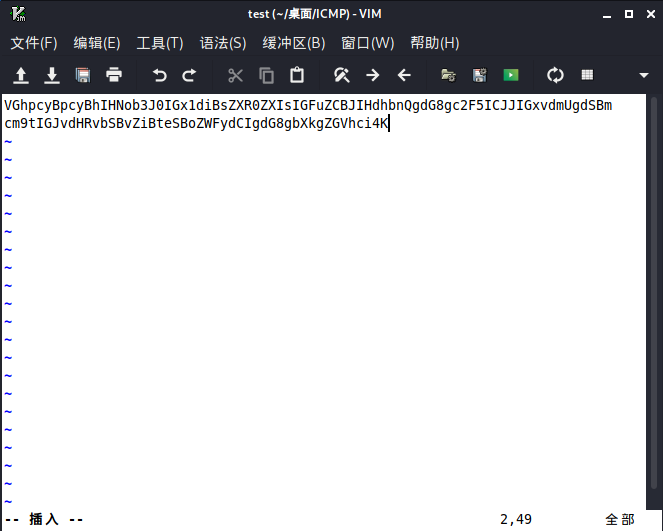
**四、实验过程分析** 1，新建消息文件



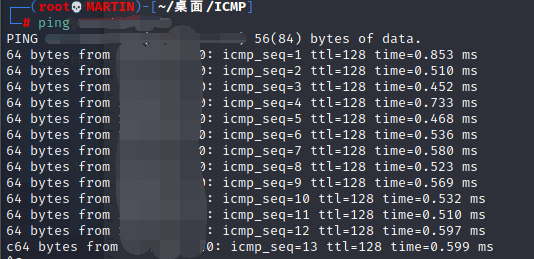
2，使用base64对文件进行编码



编码结果



3，ping接收方ip地址，测试是否存在通路



4，在icmp包载荷中放入编码后的消息



Hping3 xx.xx.xx.xx –icmp -d 1024 –sign Martin –file test -u

xx.xx.xx.xx:目标ip地址

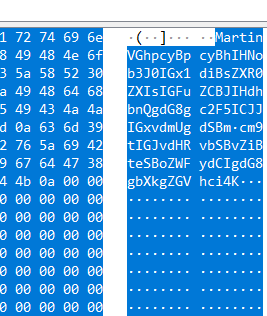
-icmp:选择的通讯协议

-d:载荷大小

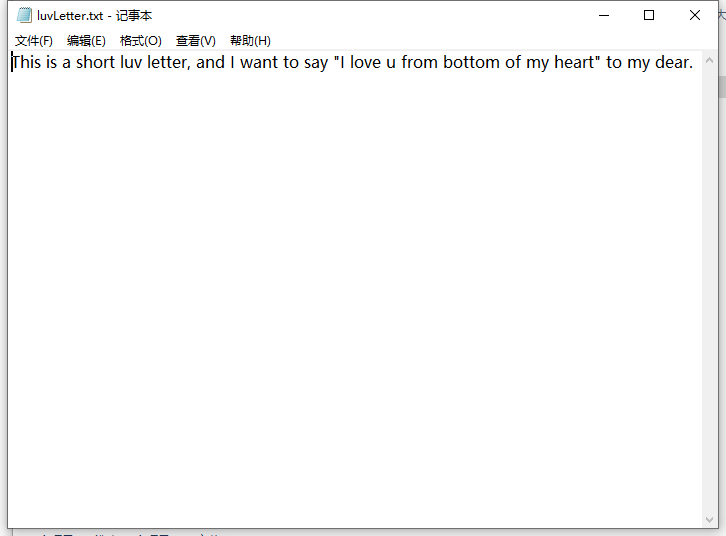
--sign:标志，会在载荷中加入标志，标志后的内容就是我们的消息载荷

--file:选择文件

5，接收方使用wireShark进行抓包，过滤器使用icmp



6，使用certutil -decode进行解码，恢复原始信息



**五、实验结果总结**

1，ICMP隧道技术操作比较便捷，而且逻辑也很简单，非常容易上手

2，在wireShark进行抓包的时候切记选择好抓包使用的网卡，否则会出现抓不到包的尴尬情况

3，在设置载荷的时候不可大于1472，为ICMP报文最大载荷

**六、附录**