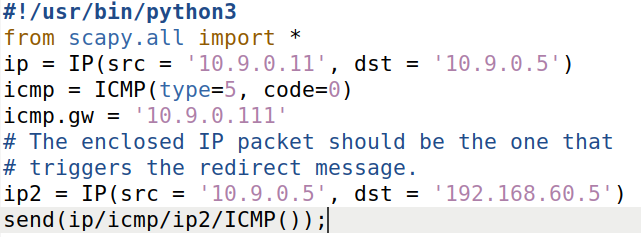
Lab3

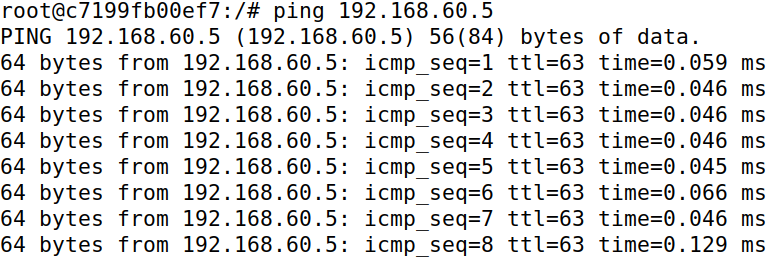
57118120黄逸飞

**Task1**

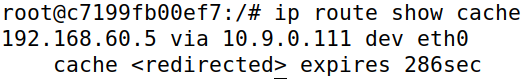
**代码**

****

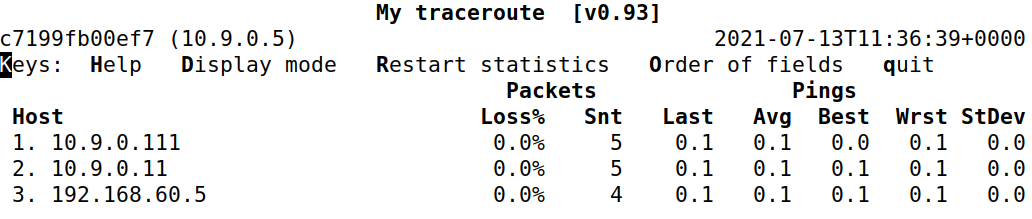
**Victim向192.168.60.5ping（后面不再展示）**

****

**Victim的Cache**

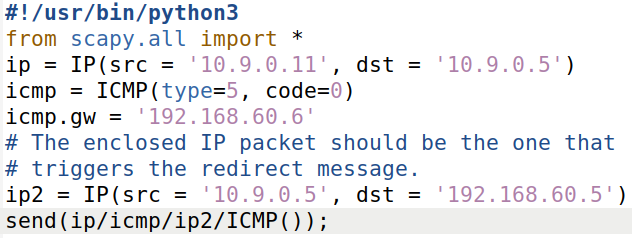
****

**Victim TraceRoute**

****

**Q1**

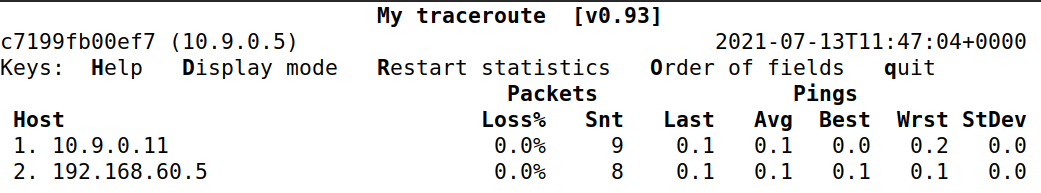
**代码**

****

**Cache中没有**

****

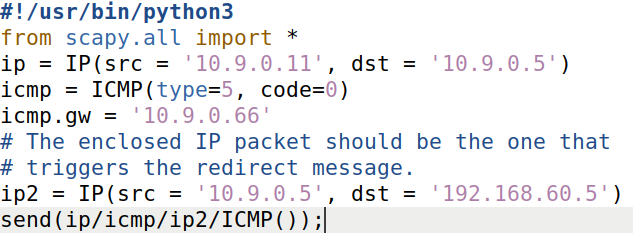
**TraceRoute也没有**

****

**不能向不在LAN的主机重定向**

**Q2**

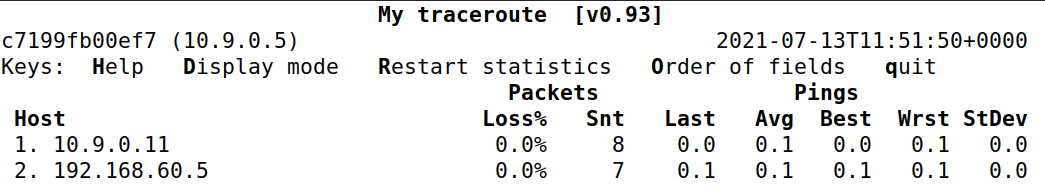
**代码**

****

**Cache没有**

****

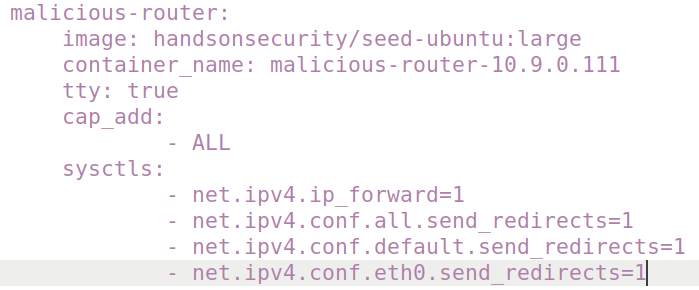
**TraceRoute没有**

****

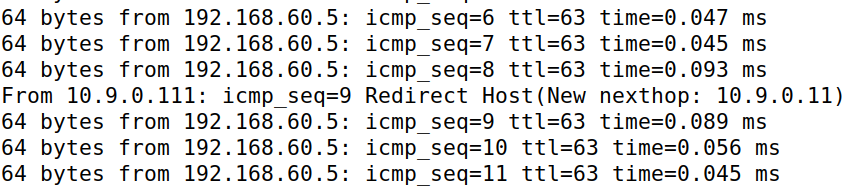
**不能向不存在的主机重定向**

**Q3**

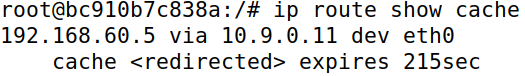
**在配置中设置**

****

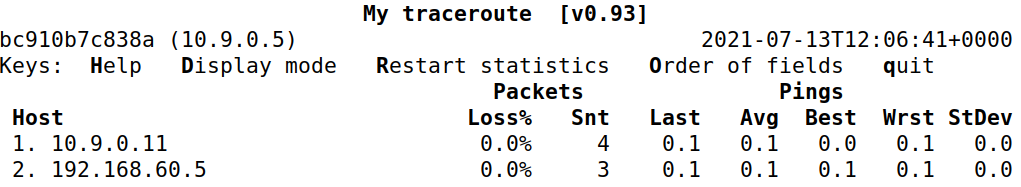
**运行代码可以在ping中看到重定向信息**

****

**可以在cache中看到正确的路由**

****

**TraceRoute也正常**

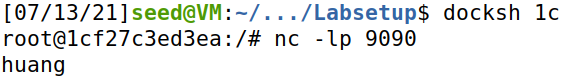
****

**应该是恶意主机的重定向设置打开，导致被定向到恶意主机后恶意主机为victim重新定向到了正确的主机。**

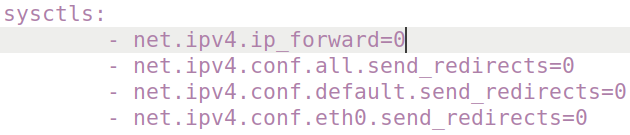
**Task2**

**测试NC功能，正常使用**

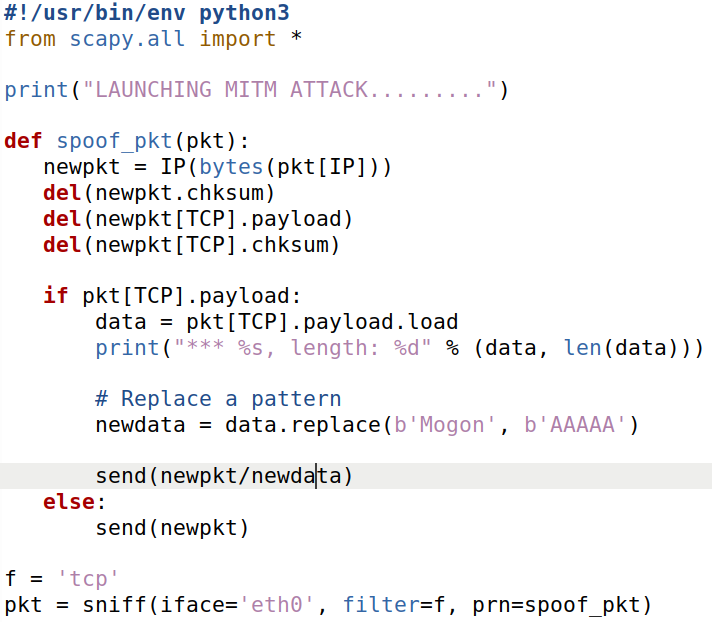
****

****

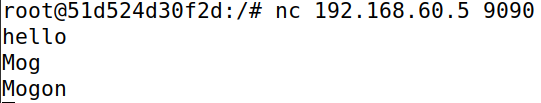
**对恶意主机的设置**

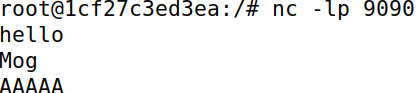
****

**代码，将Mogon改为AAAAA**

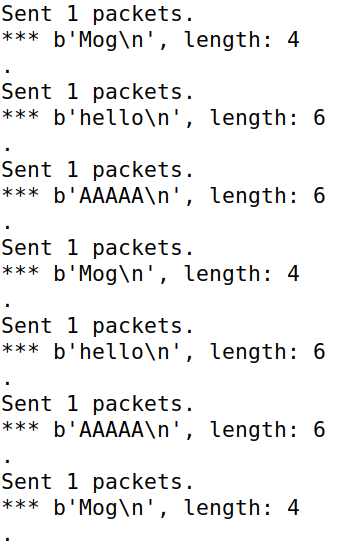
****

**重定向成功后，打开程序测试**

****

****

**但这时会不停捕获到重复包**

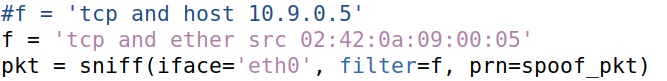
****

**Q4**

**只需要过滤捕获从Victim到Host的包，因为本次实验只需要对victim到host的单向攻击，并且host到victim的路由没有被修改，想要达到host对victim的中间人攻击条件不够。**

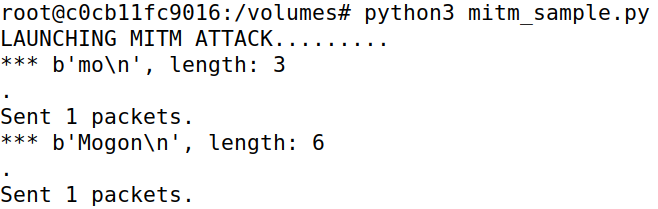
**Q5**

**修改代码的两种方法**

****

**其中第一种没有效果，因为伪造的包的源地址还是10.9.0.5，没有过滤的作用。**

**第二种Mac地址的过滤可以成功：**

****