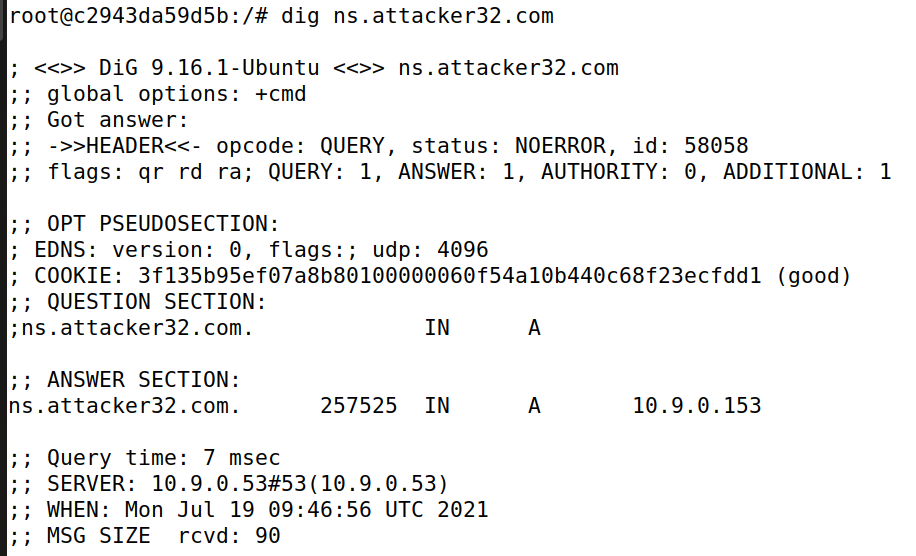
**57118126 苏恒 lab[5]-report**

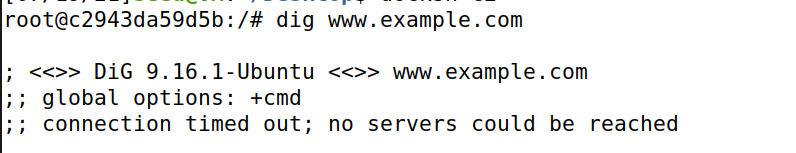
测试初始环境

获得ns.attacker32.com的IP

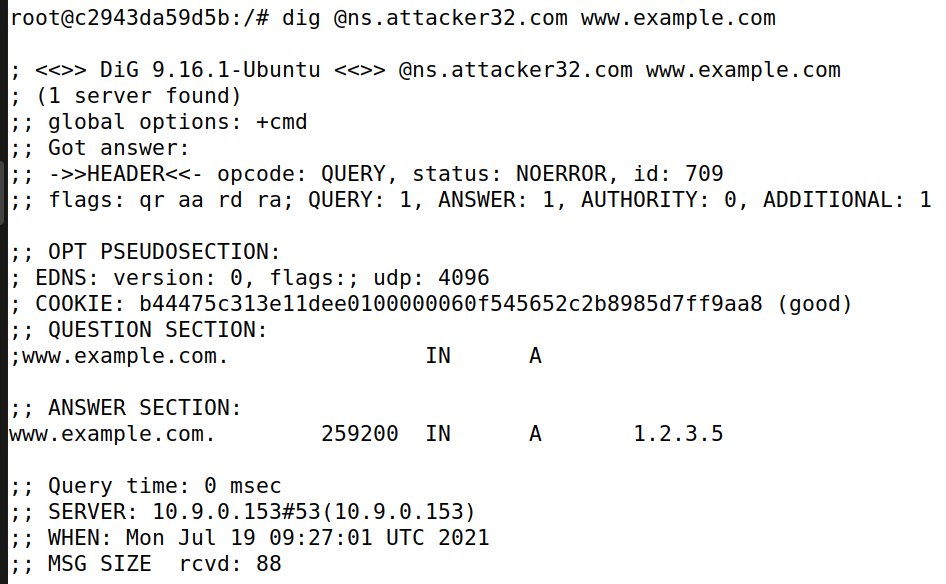


获得[www.example.com的IP](http://www.example.com的IP)

直接询问无法获取

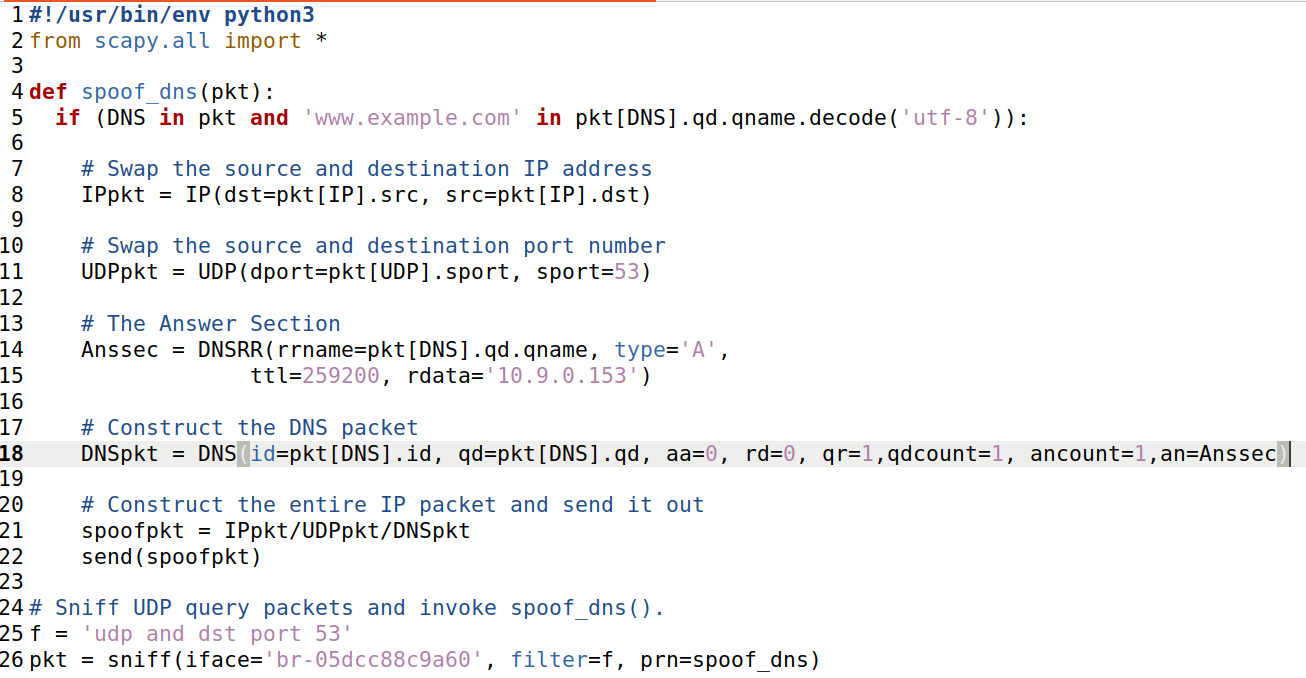


通过询问ns.attacker.com才能获取

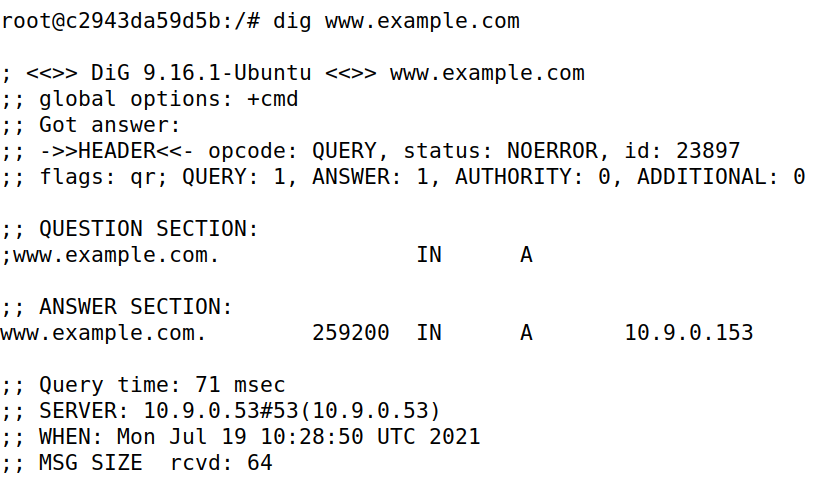


**Task1**

攻击代码如下



攻击结果如下，可以看到成功伪造了DNS响应

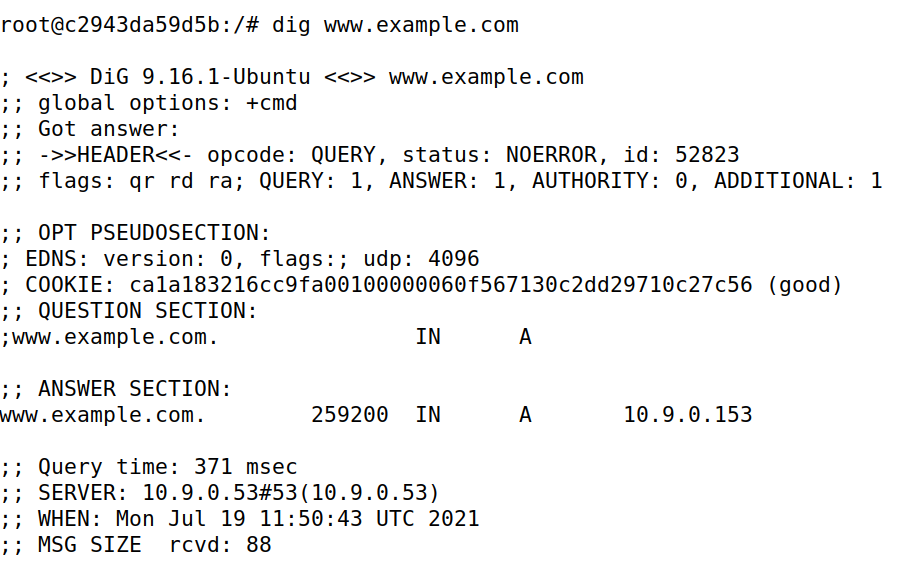


**Task2**

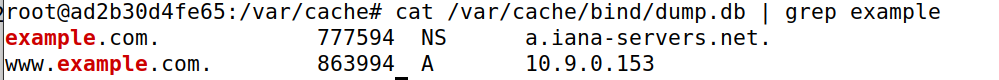
攻击代码



攻击效果如下，可以看到user主机得到的[www.example.com的IP](http://www.example.com的IP)是伪造的IP

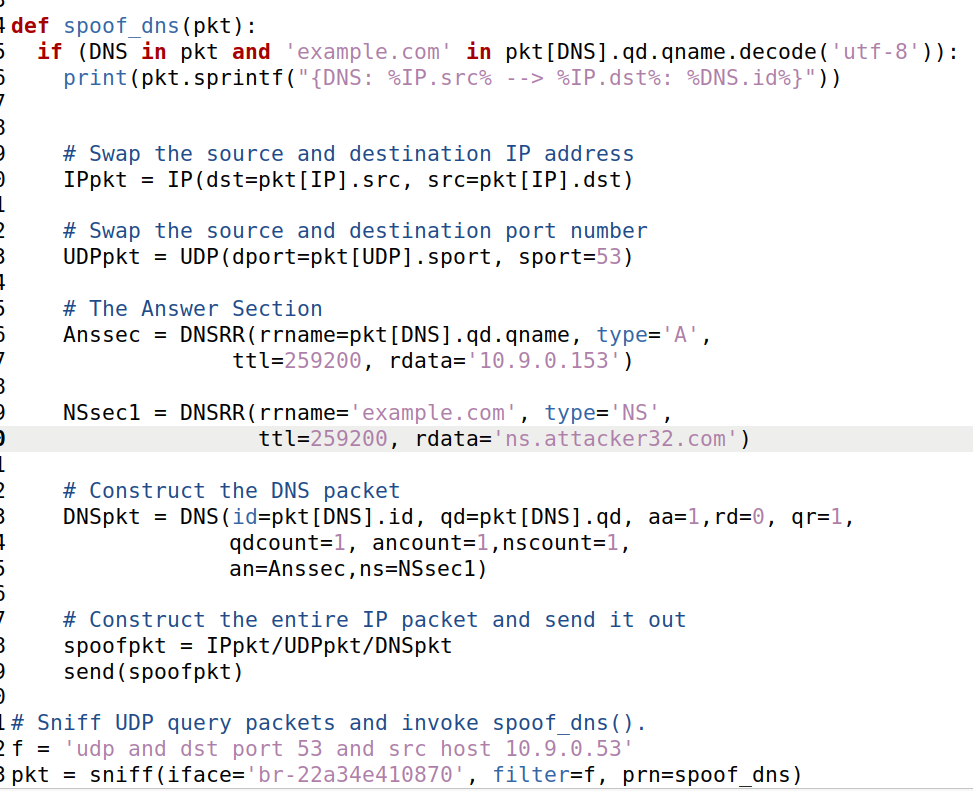


查看本地dns路由器的cache，如图，可以看到已经成功实现投毒

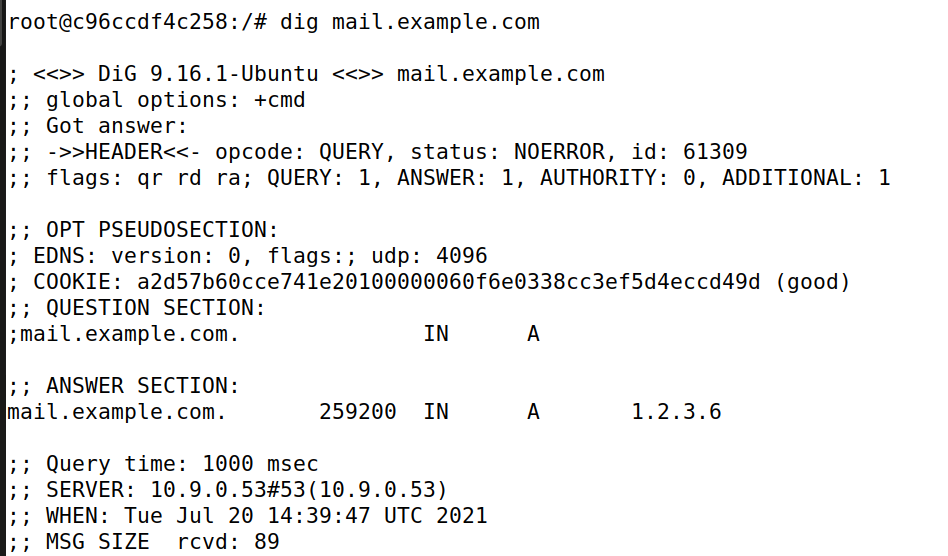


**Task3**

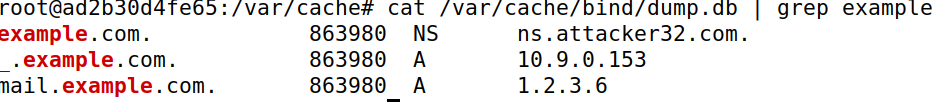
攻击代码



攻击效果如下，可以看到user主机得到了ns.attacker32.com伪造的mail.example.com的IP



查看本地dns路由器的cache，如图，可以看到有域名example.com的服务器的记录，由于之前有过一次对mail.example.com的DNS查询因此还有该地址的记录，攻击成功

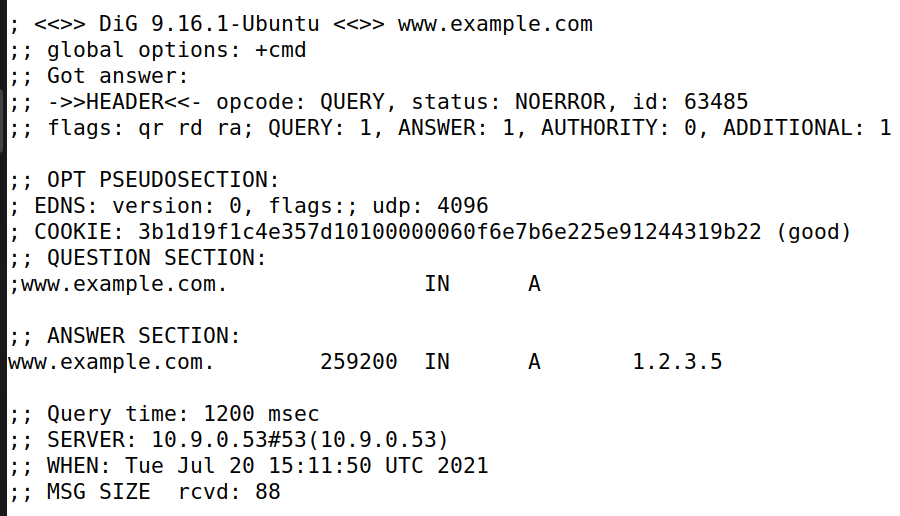


Task4

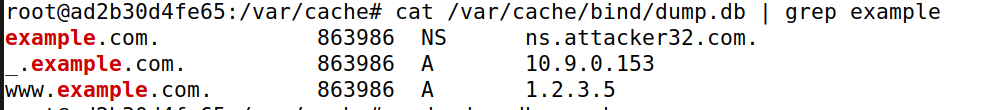
攻击代码



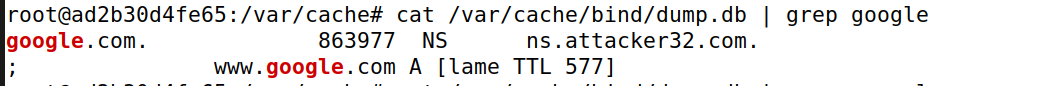
攻击效果，得到了由ns.attacker32.com伪造的IP



查看本地路由器的缓存，发现只有example.com域名的NS项，没有google.com的项



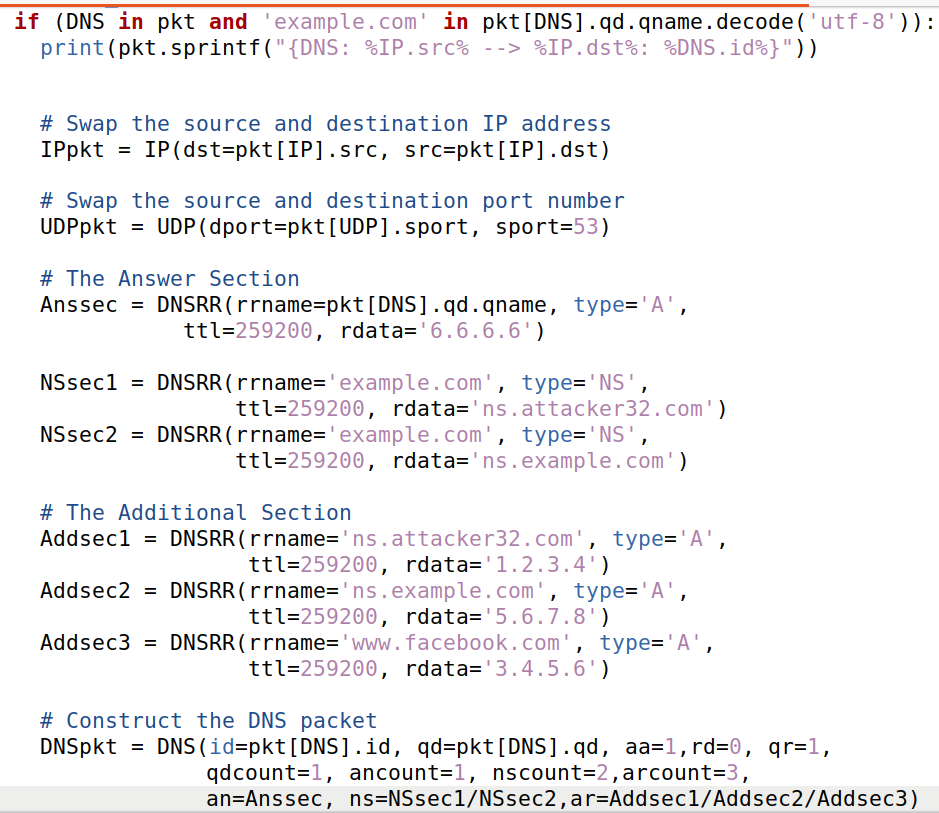
将攻击代码中检测条件改为google.com，user主机dig [www.google.com](http://www.google.com)，发现本地路由器中的缓存如下



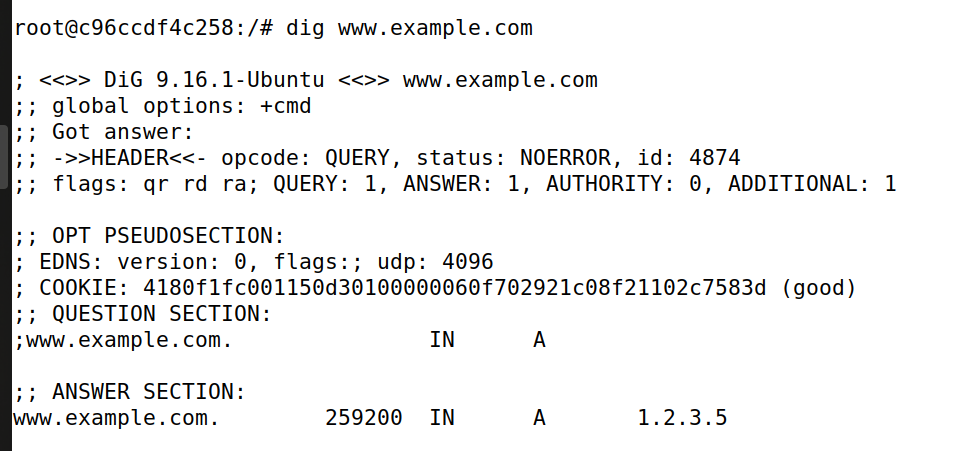
说明只能实现对DNS查询的域名对应域进行NS伪造攻击

Task5

攻击代码



攻击效果，得到的是ns.attacker32.com伪造的IP而非程序伪造的IP。既然这个伪造报文已经影响了本地服务器对应域的ns，那其answer部分应该不可能比本地域名服务器再向ns询问更慢，因此原因不明。



本地路由器缓存如图，没有facebook项

