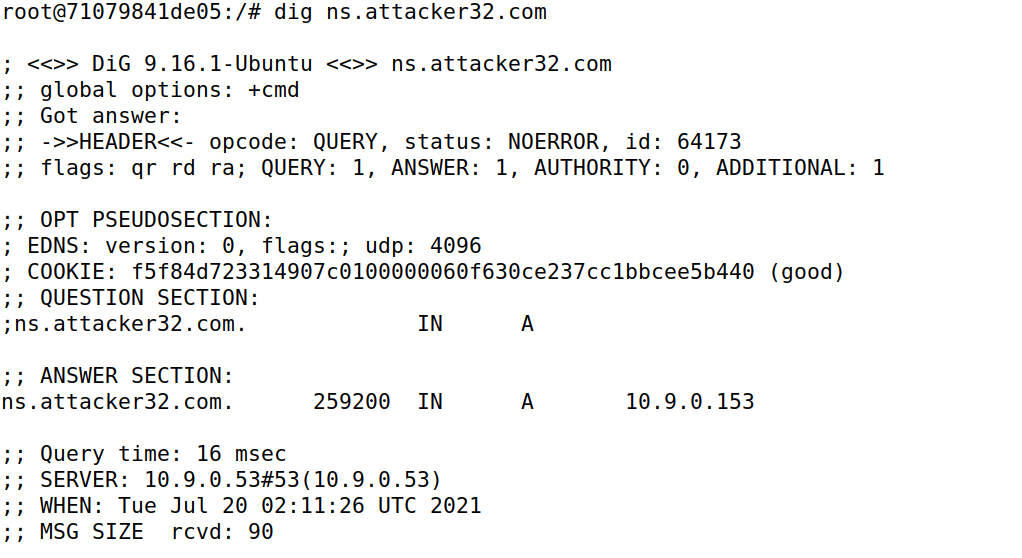
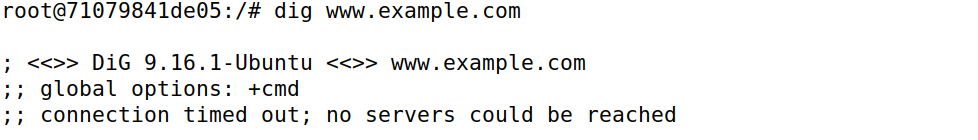
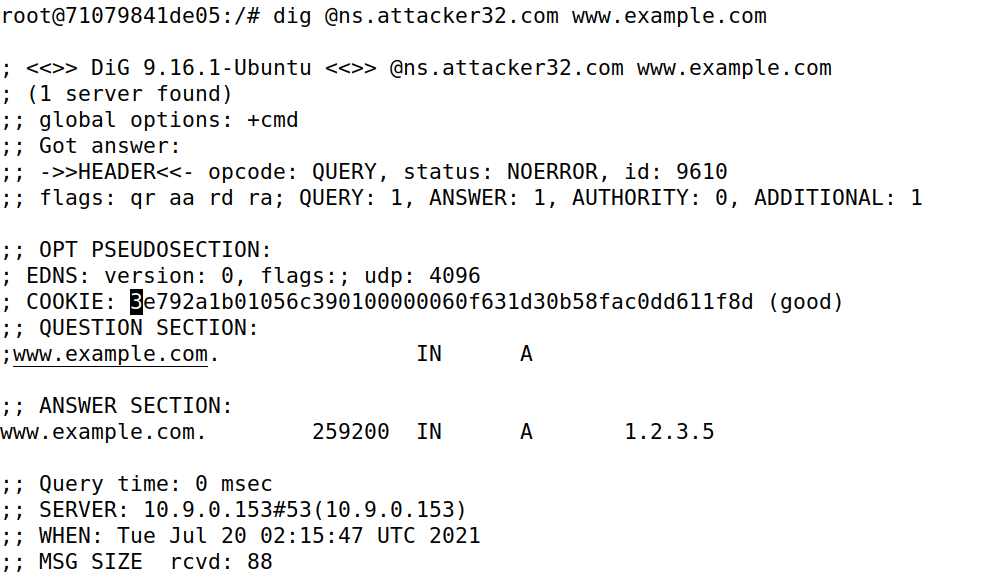
**第五次实验报告**

57118121 刘洪飞

测试设置，发现符合对于本地DNS解析和恶意解析服务器的设置

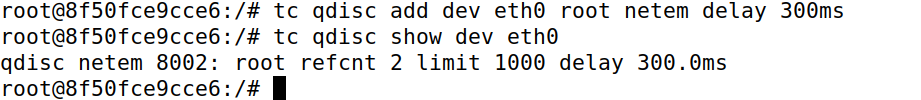




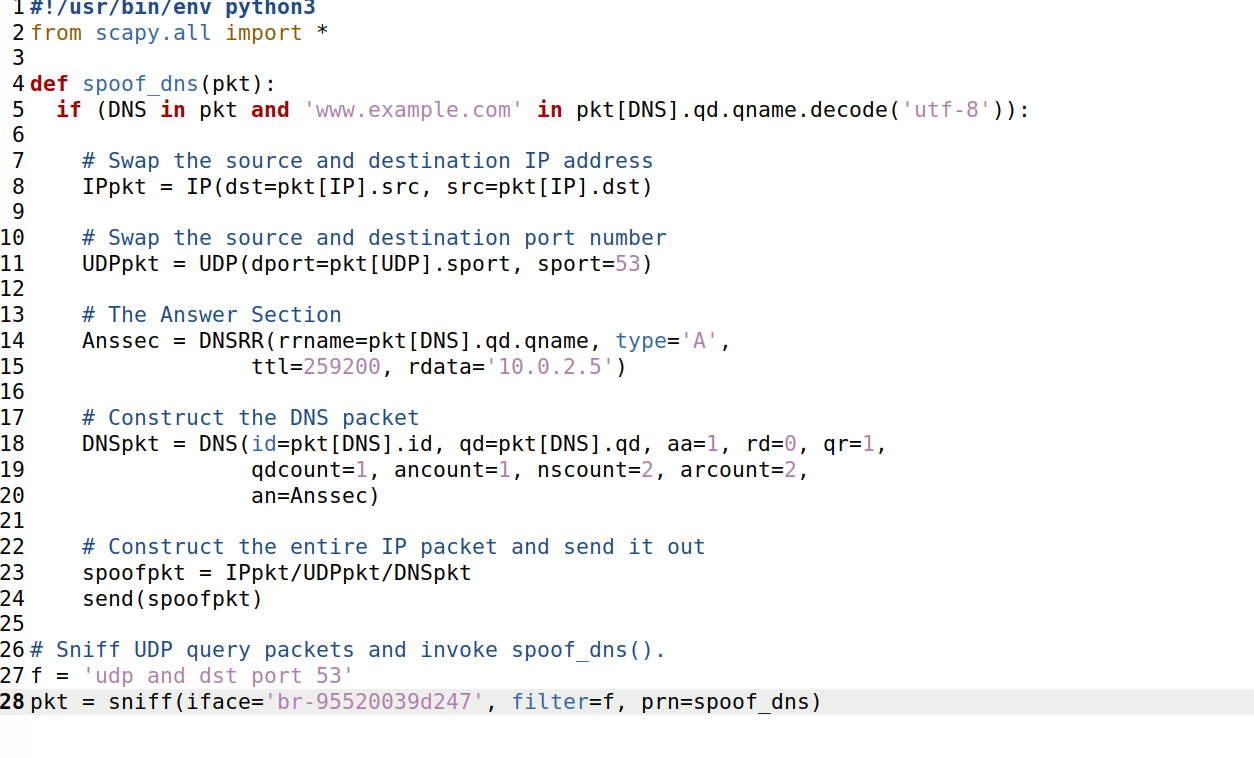


Task1

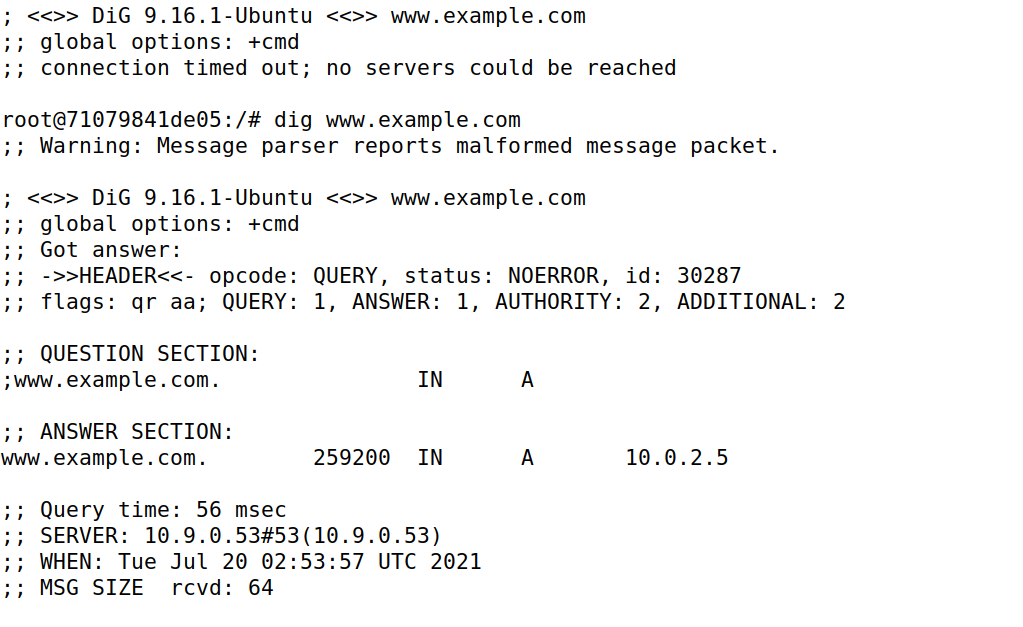
路由器设置延时



代码如下

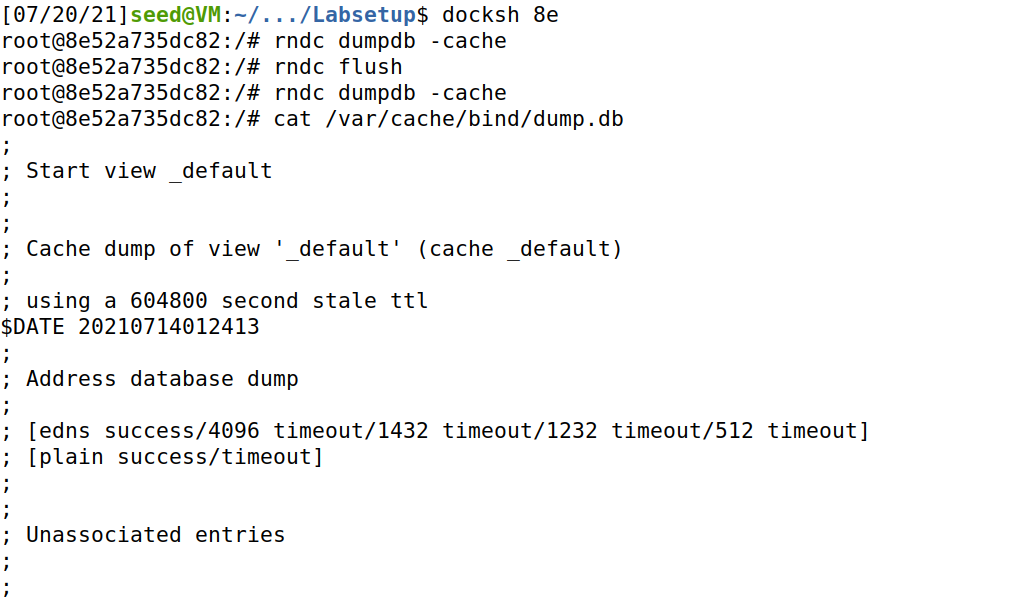


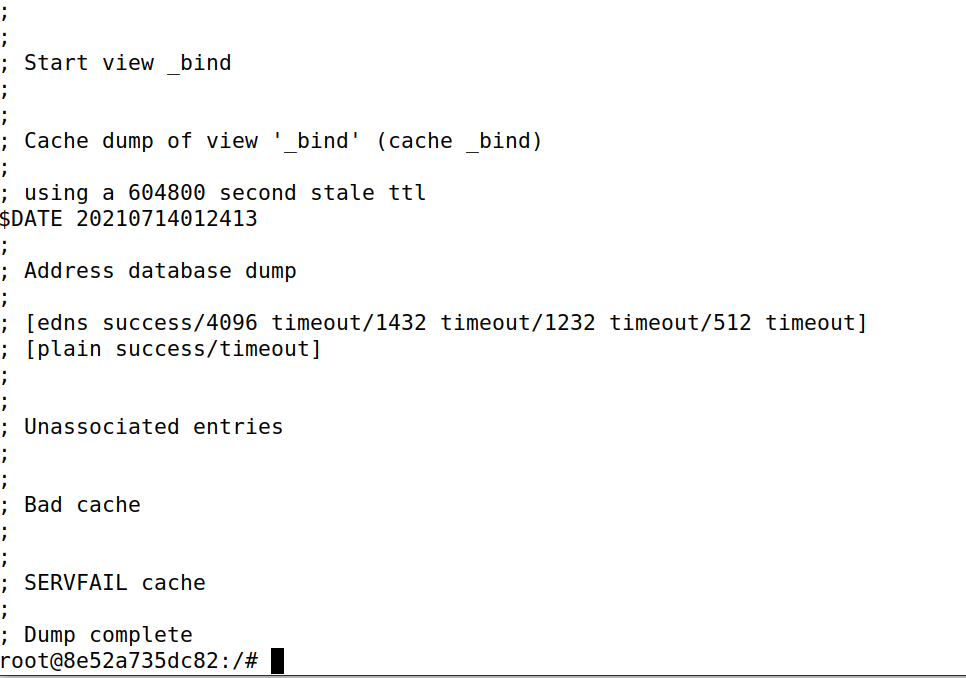
运行代码，发现攻击成功



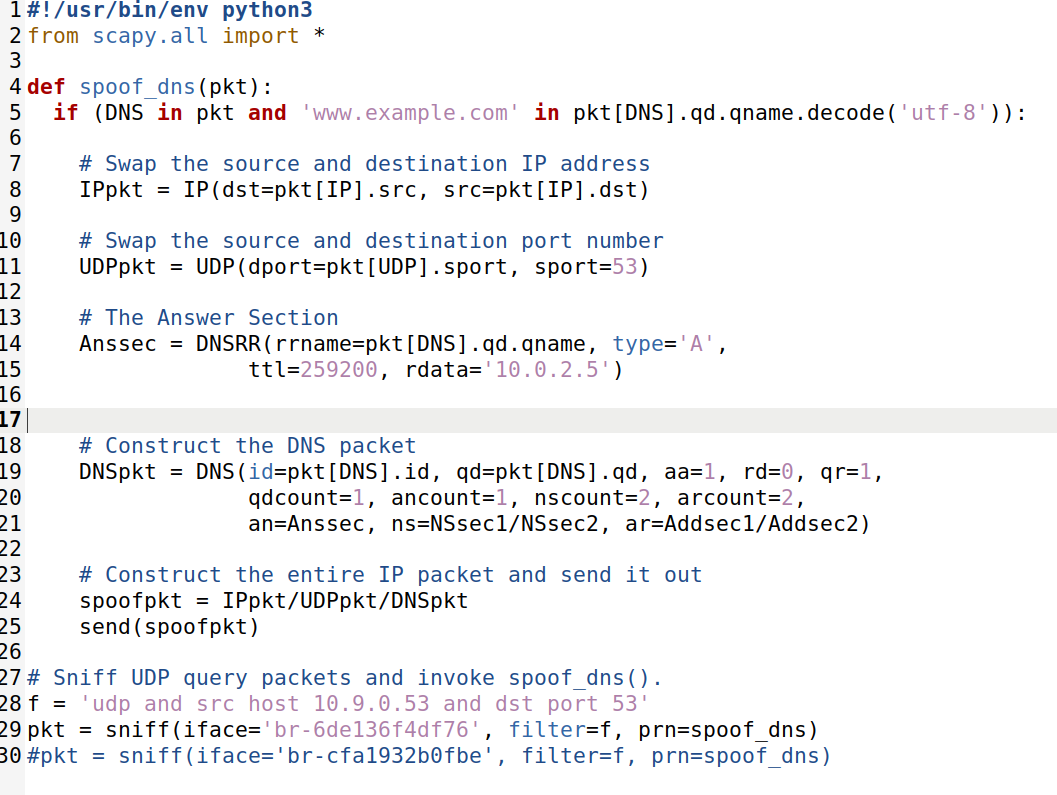
Task2

清空缓存

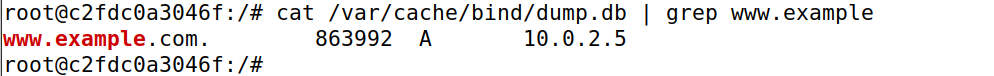




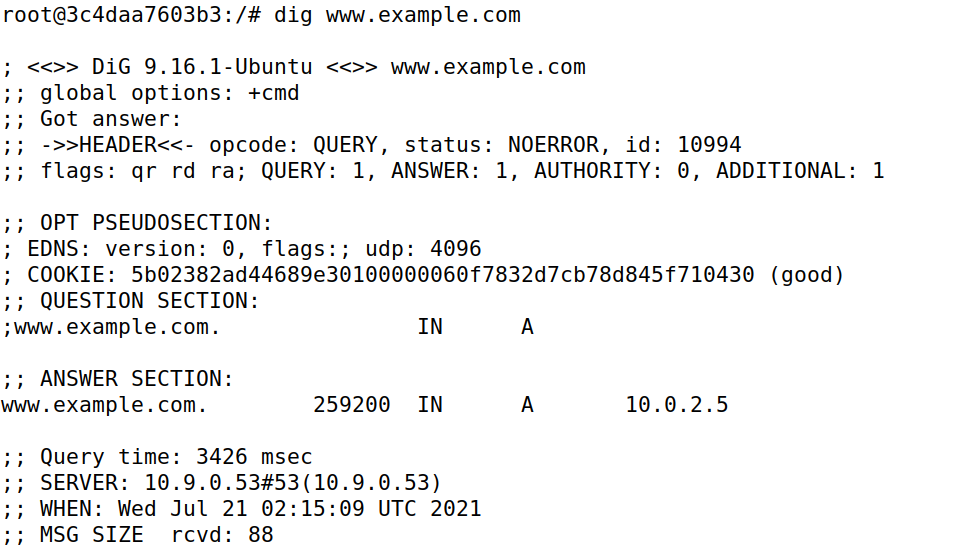
代码如下



被解析成功，缓存被污染

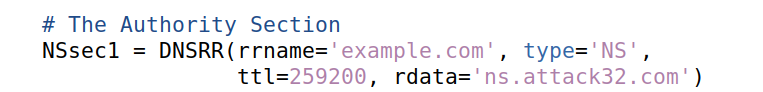


解析更改成功

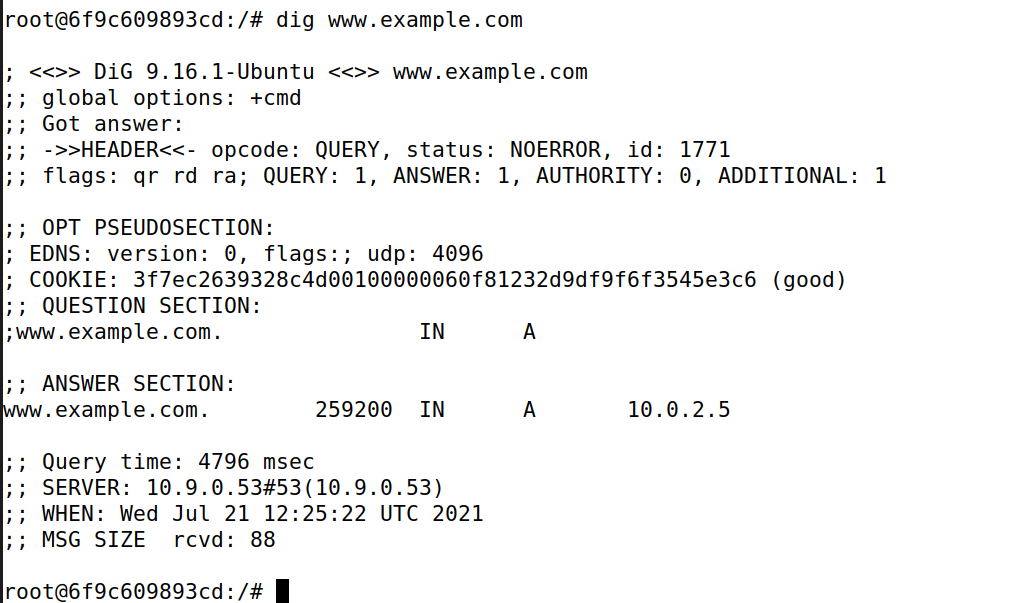


Task3

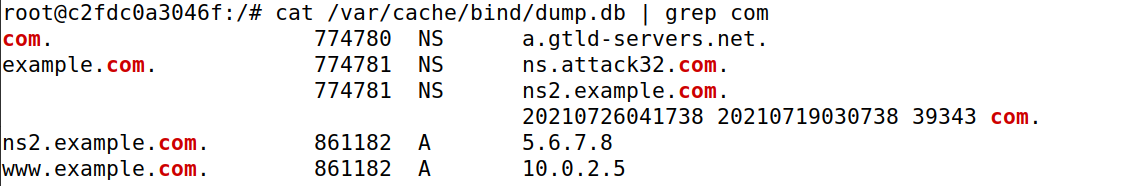
修改代码如下



dig 得到如下结果，www.example.com 被解析到了 10.0.2.5

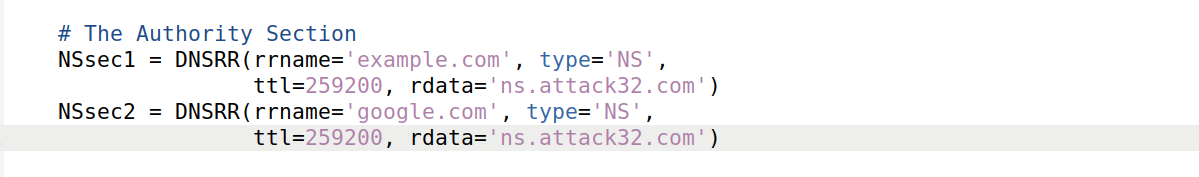


服务器已经把 ns.attack32.com 作为了 example.com 的 DNS

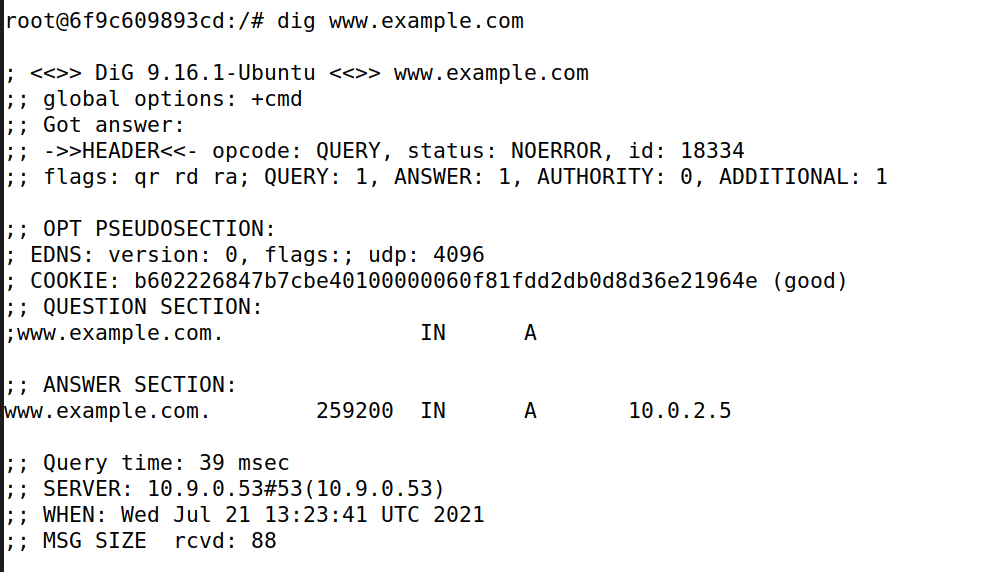


Task4

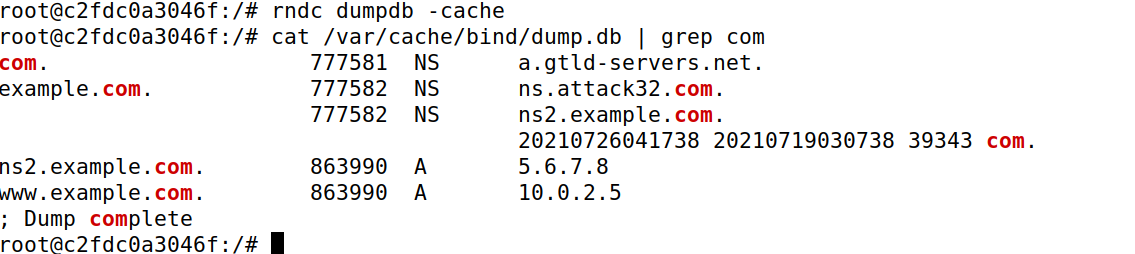
修改代码



dig 得到如下结果，www.example.com 被解析到了 10.0.2.5

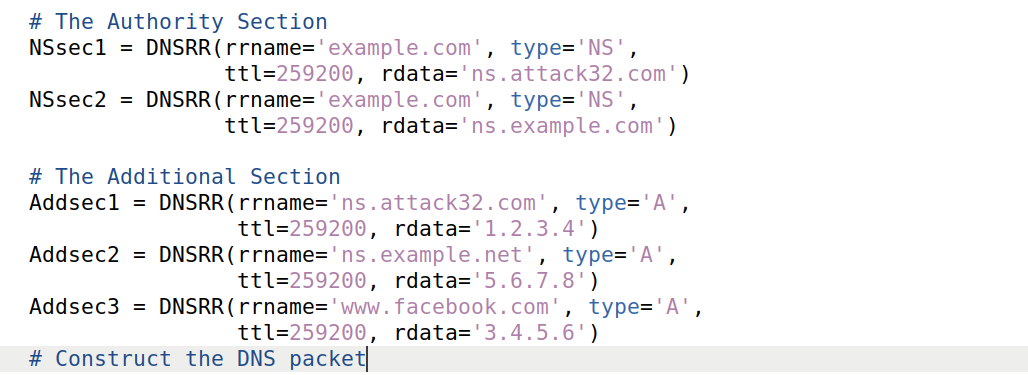


服务器已经把 ns.attack32.com 作为example.com 的 DNS。但并不接受把 ns.attack32.com 作为了 google.com 的 DNS，有可能原因是询问的是example.com而不是 google.com。

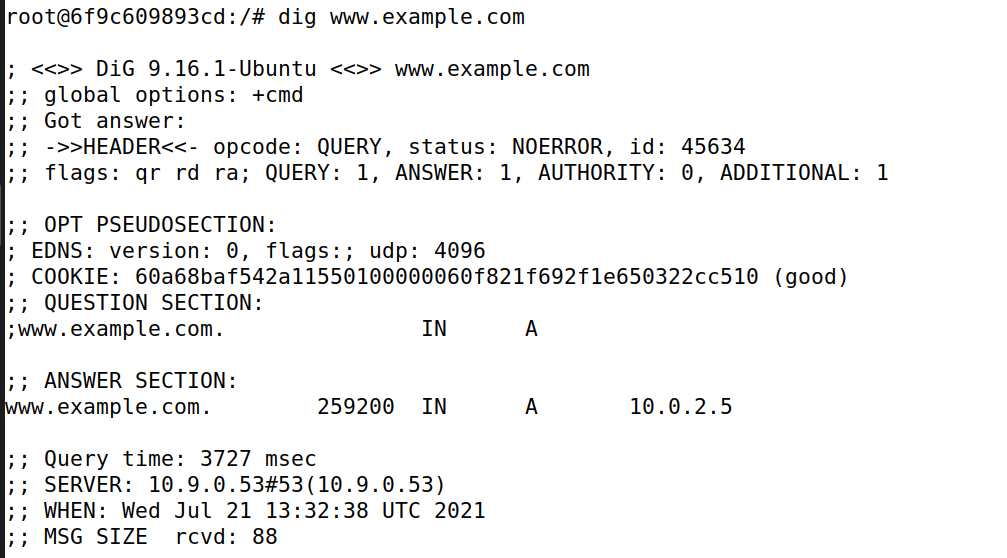


Task5

代码修改如下

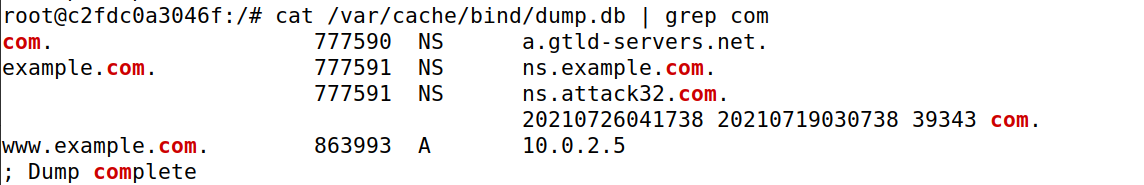


运行代码，dig结果如下



本地缓存如下

Addtional 部分没有缓存，由于与 dig询问的www.example.com 无关，所以不会存储，这可能是设计的一种安全机制，防止转入恶意的DNS解析，只与询问相关，可以很大程度防止攻击



，另外由于中间一段additional选项要求是[www.example.net](http://www.example.net)，从后向前解析，与com不匹配，也是无关，也不会存储

