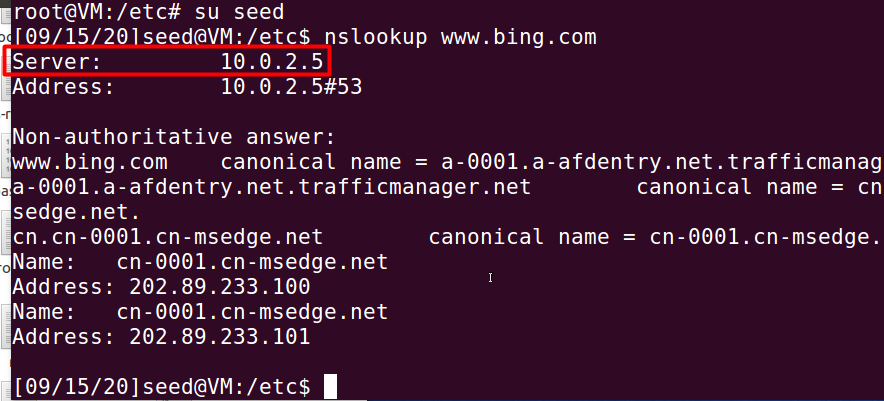
**lab5实验报告**

57117133 臧宇豪

**Task 1: Configure the User Machine**

DNS服务器的地址为10.0.2.5，按要求对测试机10.0.2.4进行配置后，查看测试机是否配置成功：



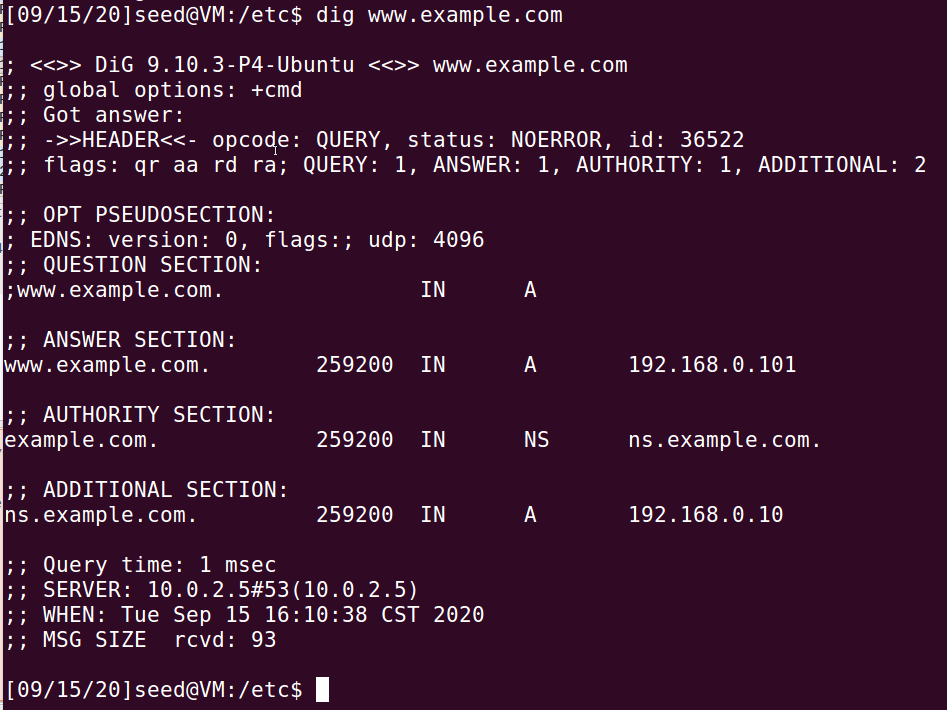
**Task 2: Set up a Local DNS Server**

Option配置：



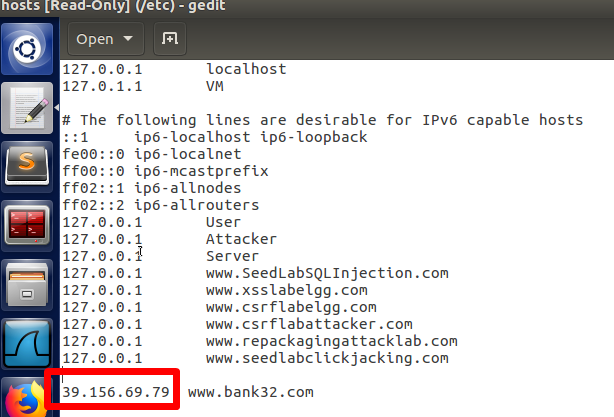
**Task 3: Host a Zone in the Local DNS Server**

按照要求对Zone进行配置，并在用户机上使用dig命令获取结果：

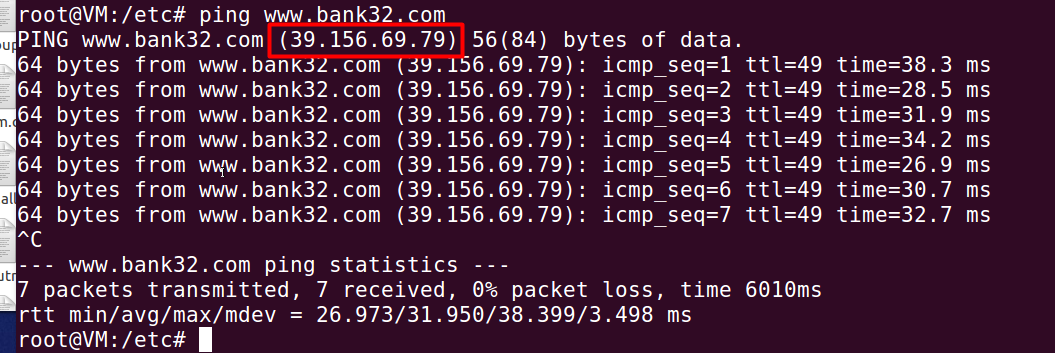


**Task 4: Modifying the Host File**

更改hosts文件：

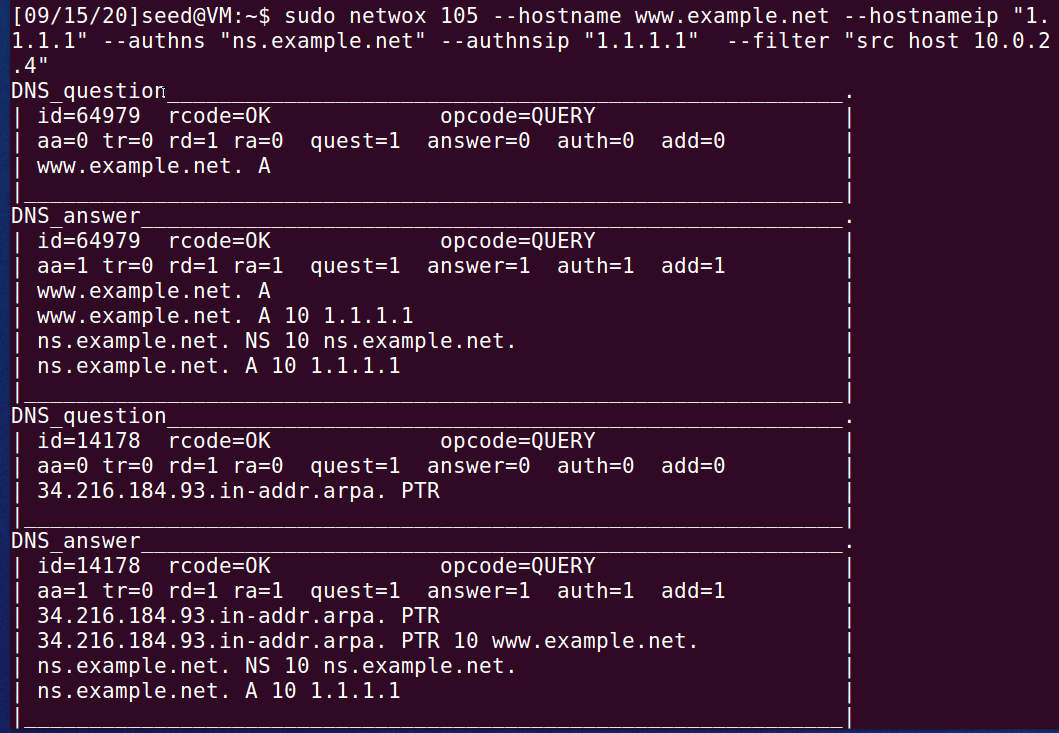


ping [www.bank32.com](http://www.bank32.com):



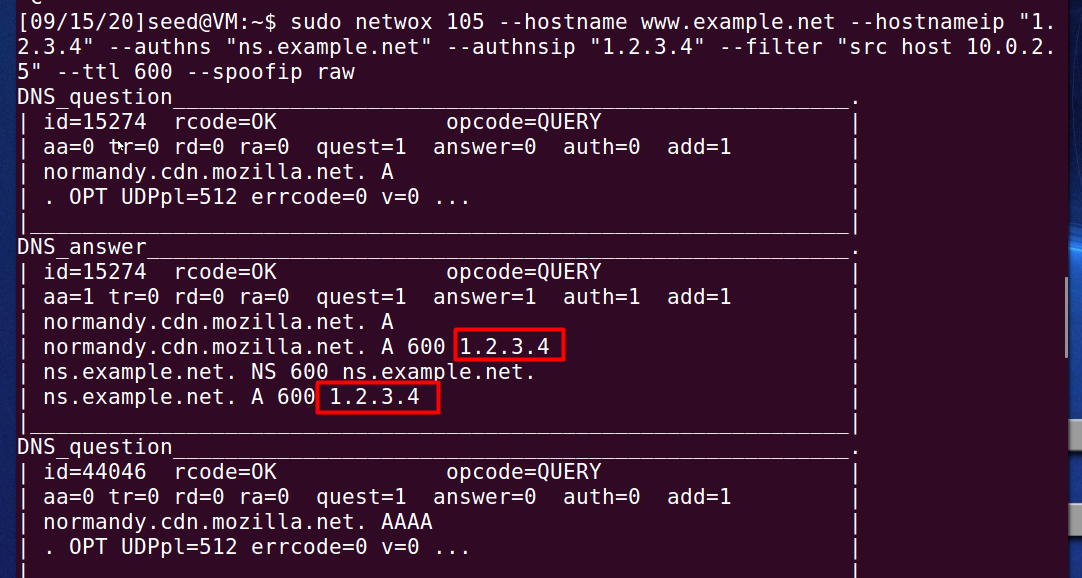
**Task 5: Directly Spoofing Response to User**

执行如下命令，使得对于[www.example.net的ping](http://www.example.net的ping)请求被重定向，攻击成功：



**Task 6: DNS Cache Poisoning Attack**

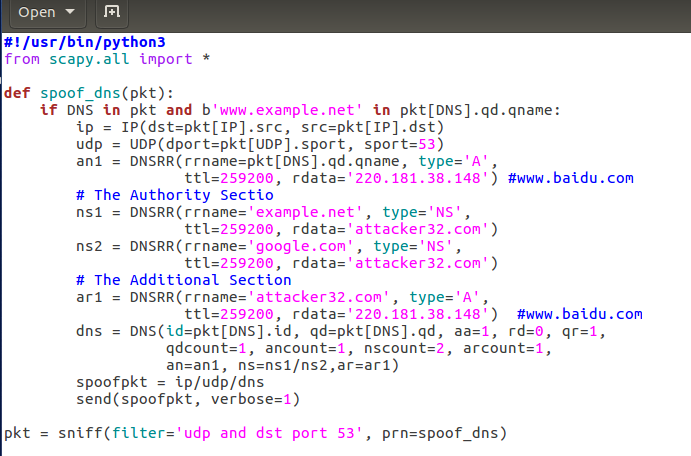
攻击机执行如下命令对DNS服务机进行攻击：

、

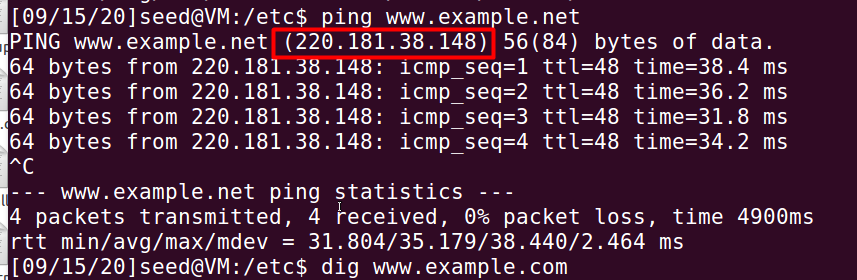
可以发现，攻击成功。

**Task 7: DNS Cache Poisoning: Targeting the Authority Section**

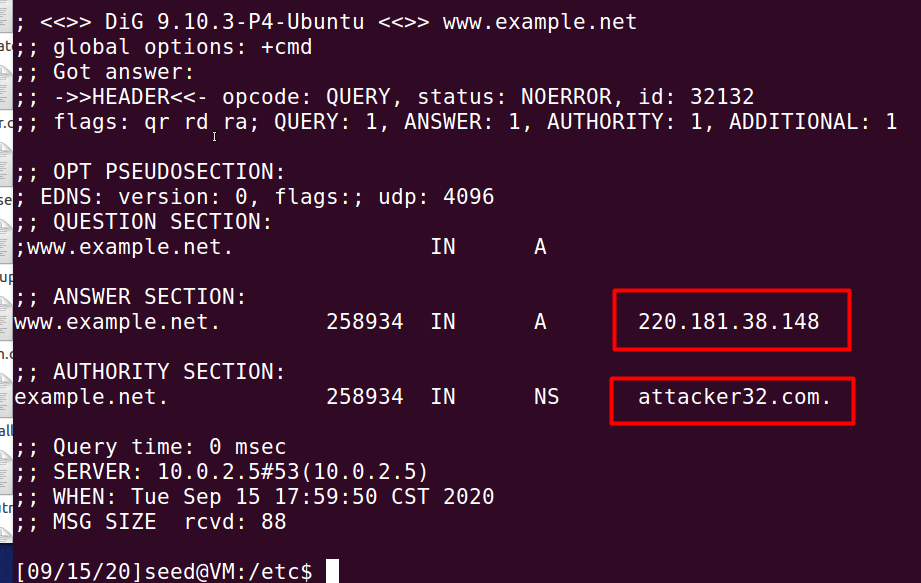
攻击机执行如下代码：



测试机ping [www.example.net](http://www.example.net):



测试机dig [www.example.net](http://www.example.net)



可以发现，攻击成功。