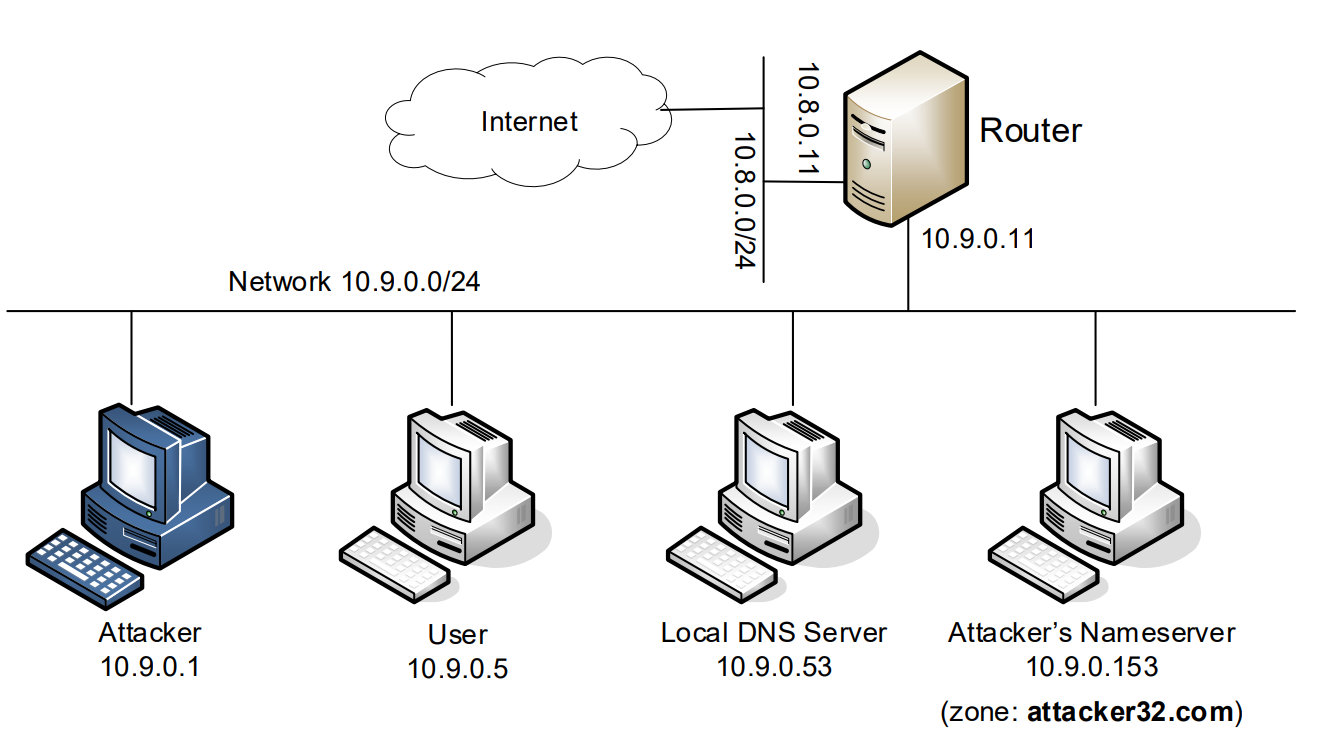
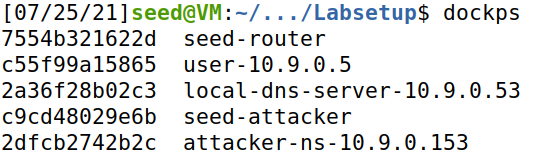
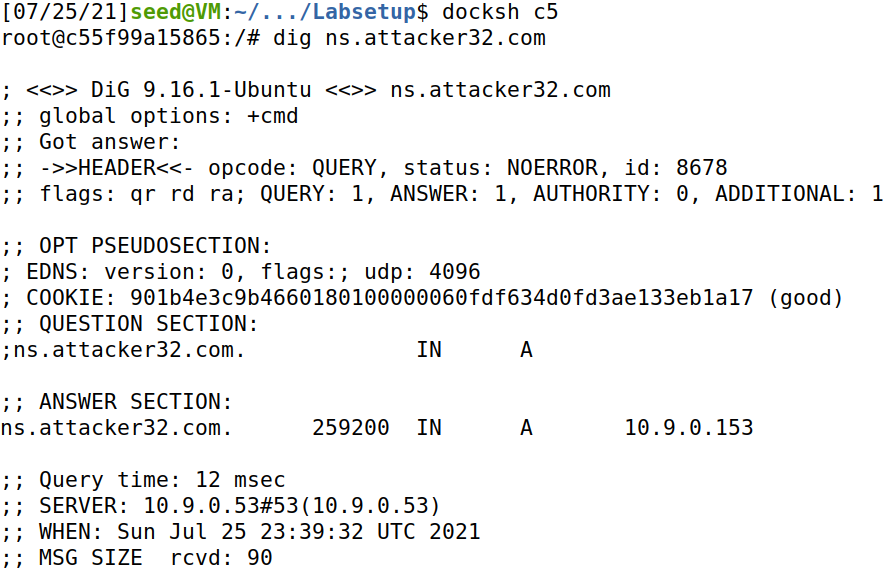
**第五次实验**

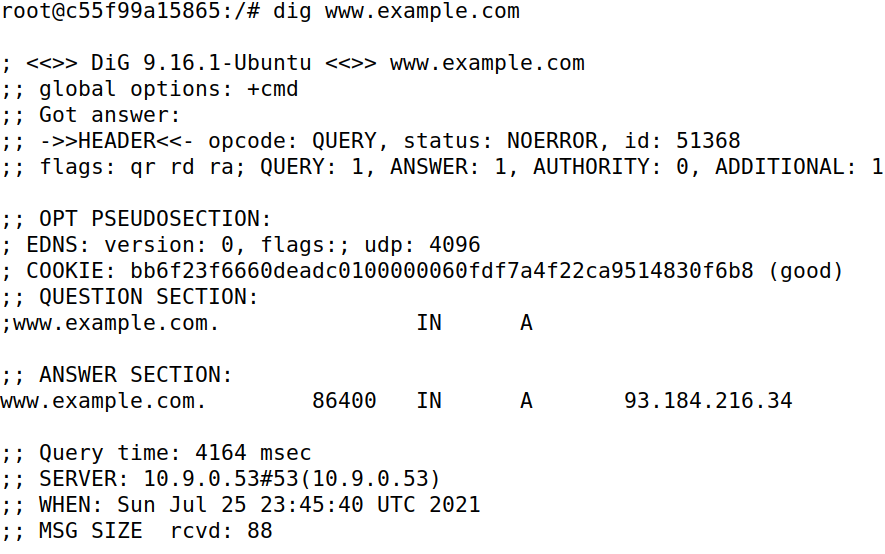
57118101 卞郡菁

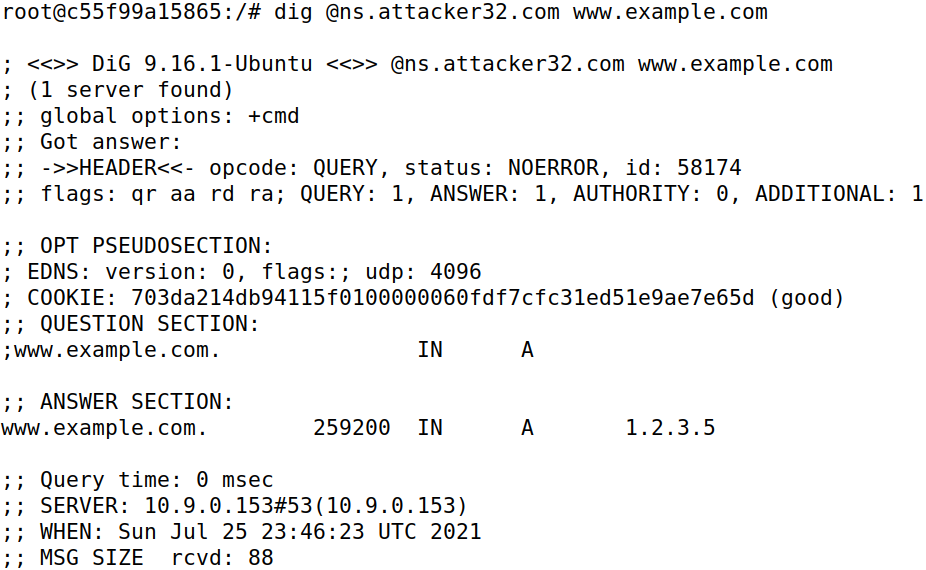
cd Desktop/Labs\_20.04/Network\ Security/Local\ DNS\ Attack\ Lab/Labsetup/



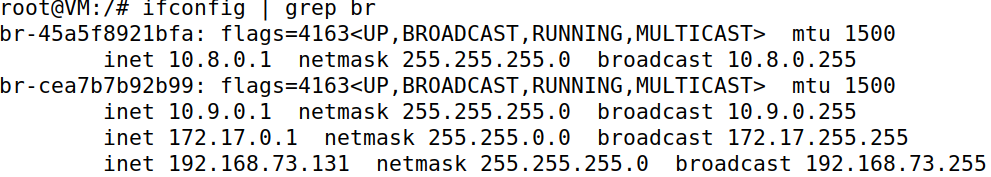


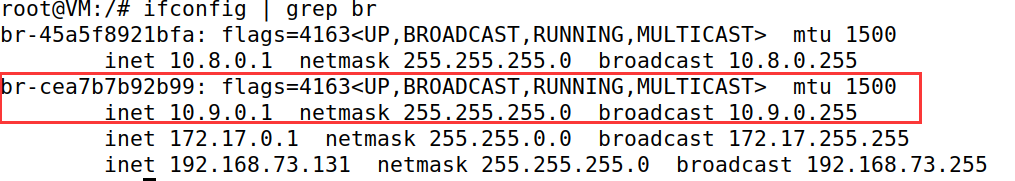




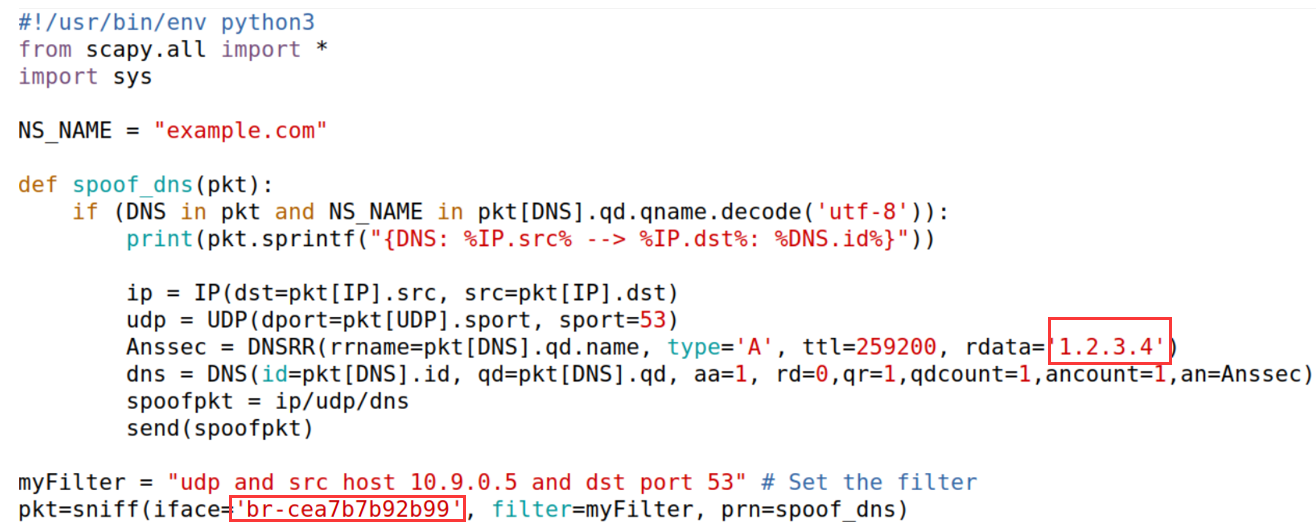


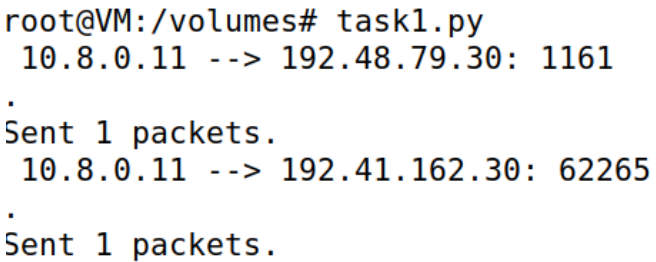
Task 1: Directly Spoofing Response to User

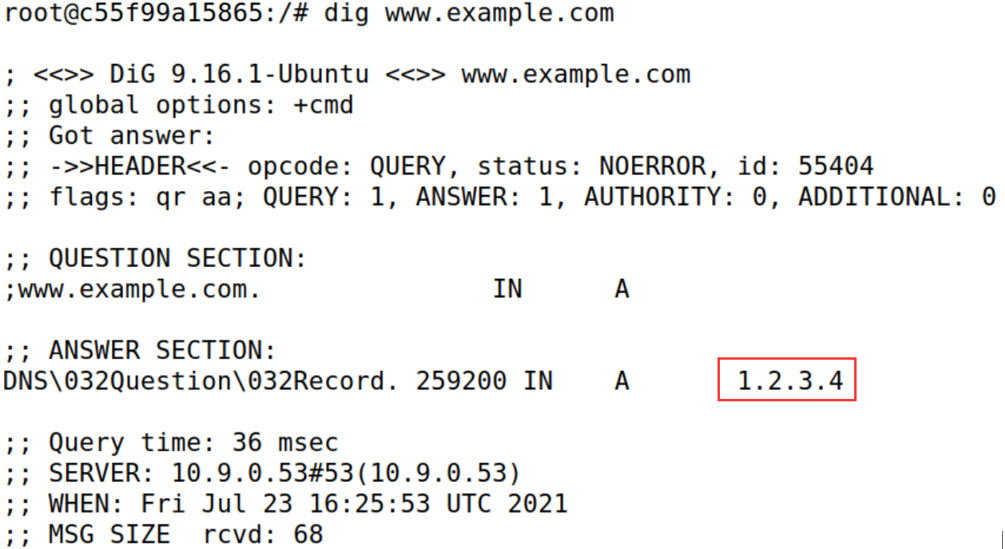




cea7b7b92b99

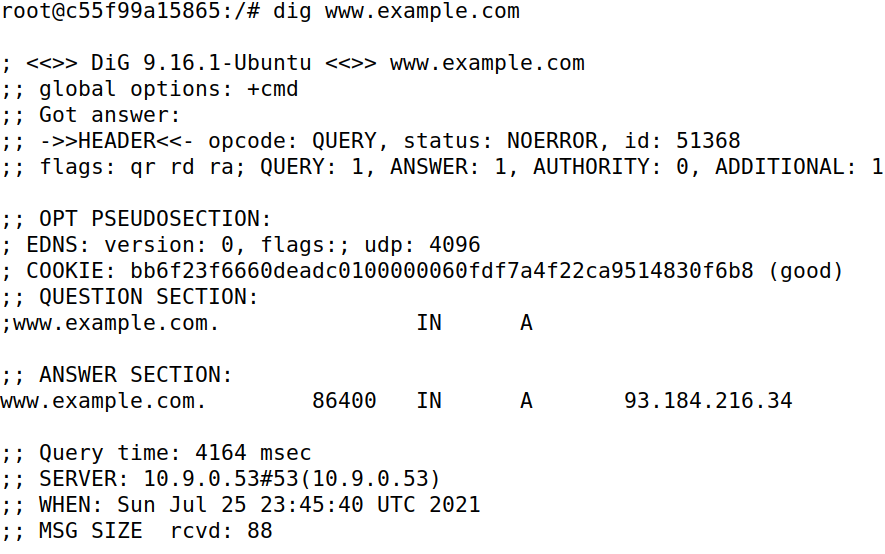




Task 2 DNS Cache Poisoning Attack-Spoofing Answers

在本地 DNS 服务器 10.9.0.53 上输入命令 rndc flush 刷新缓存

在受害者机器上 dig [www.example.com](http://www.example.com)

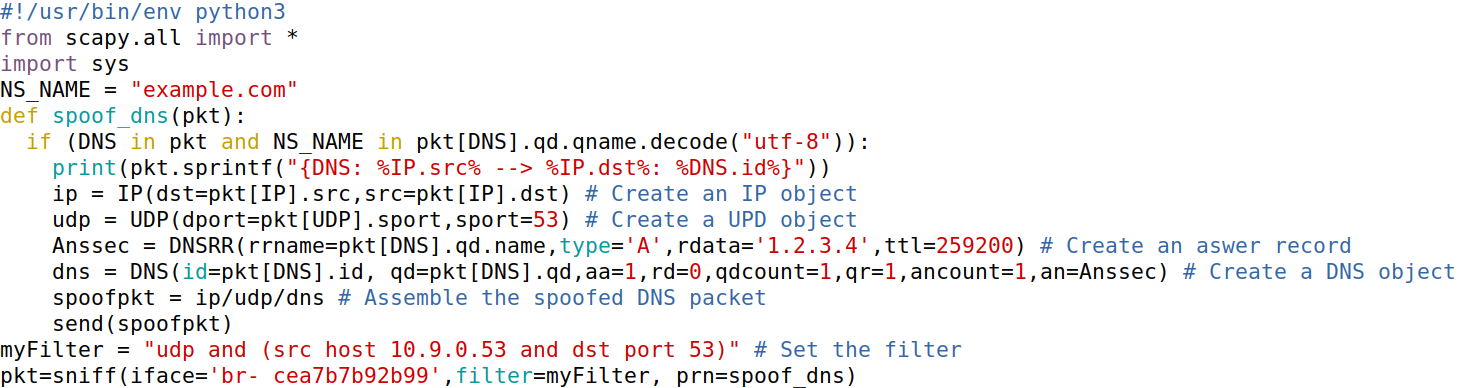


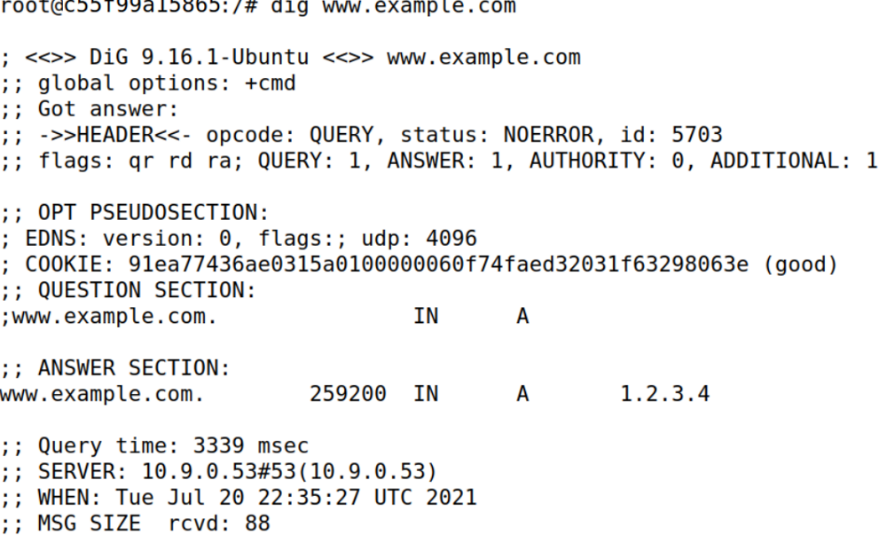
在 10.9.0.53，输入 rndc dumpdb -cache，输入 cat /var/cache/bind/dump.db 查看

此时可以查看 DNS 缓存正常。

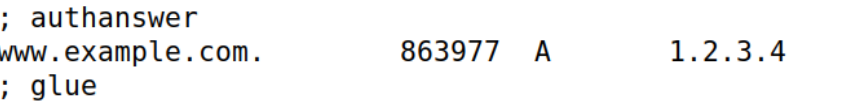


在攻击者主机 10.9.0.1 上运行脚本如下：

得到结果

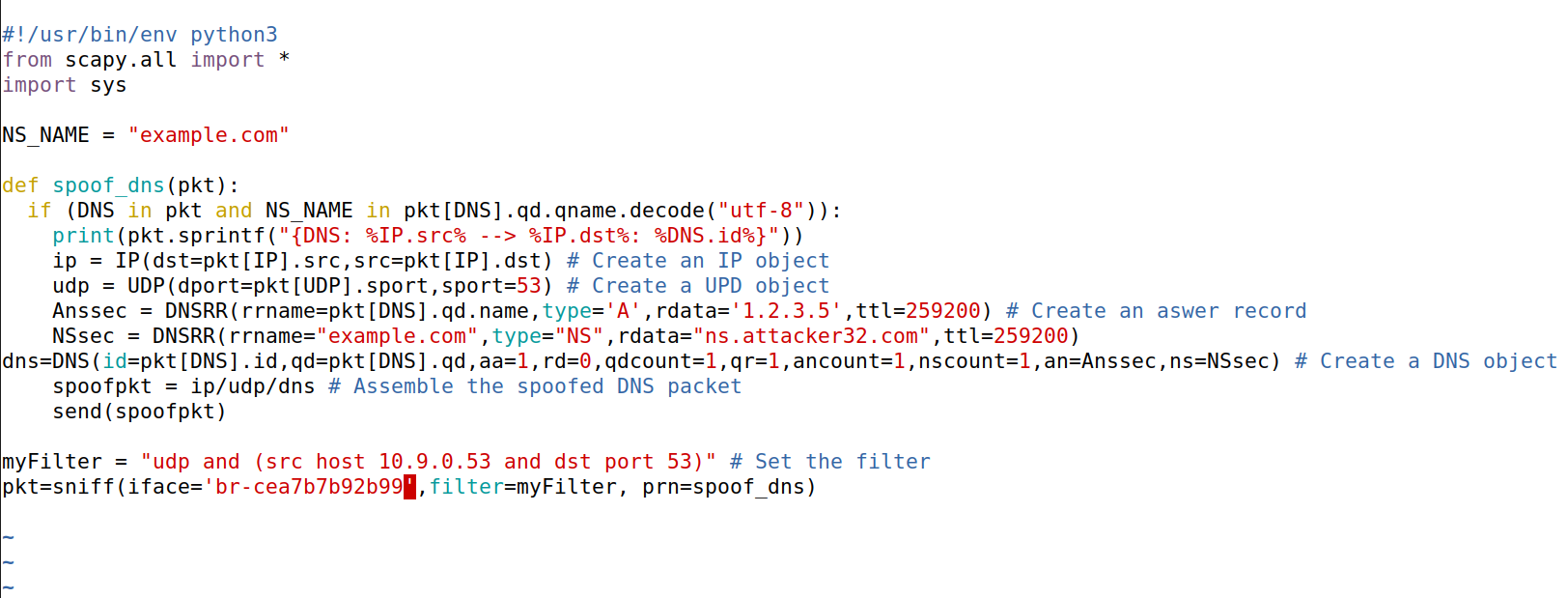


在 DNS 服务器上输入 rndc flush，rndc dumpdb -cache，cat /var/cache/bind/dump.db 查看

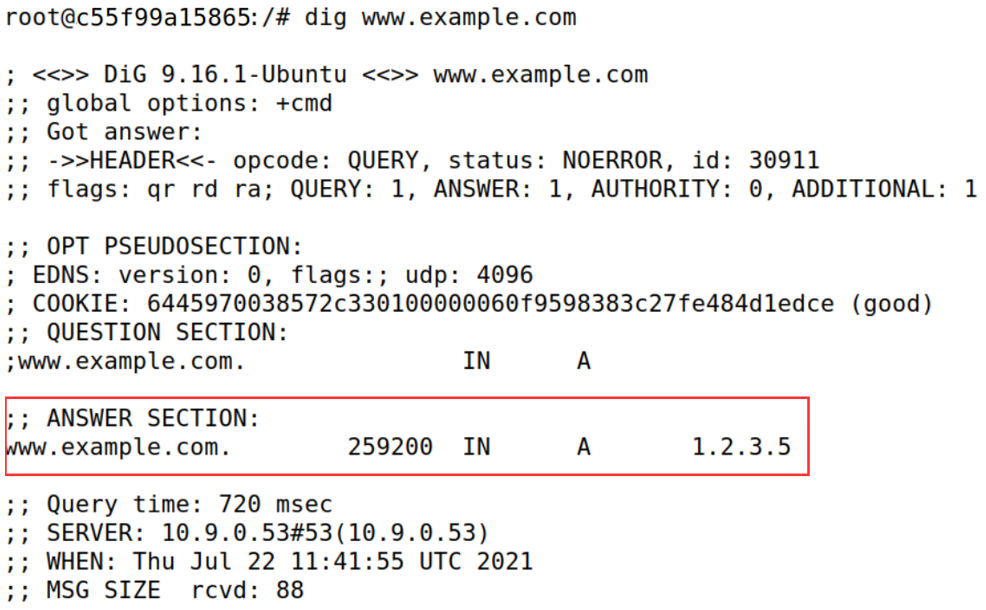


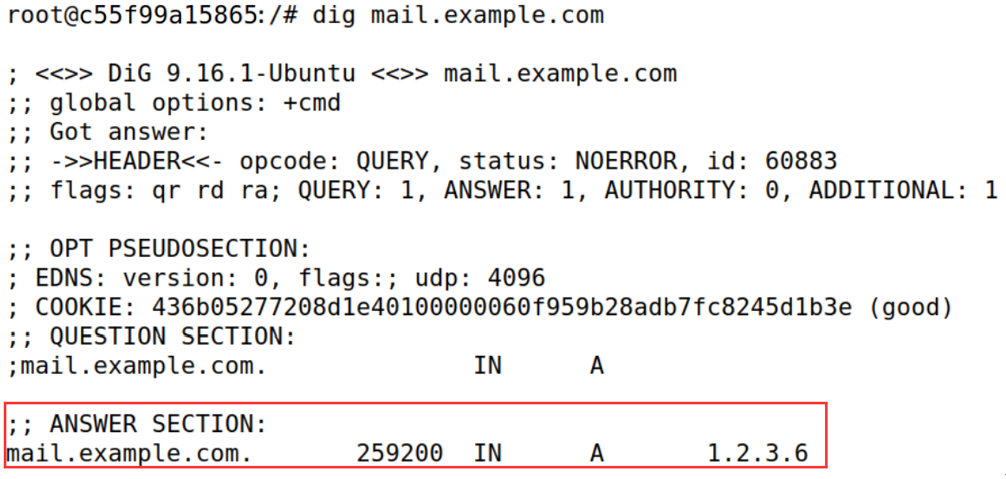
**Task3**

用以下程序进行攻击

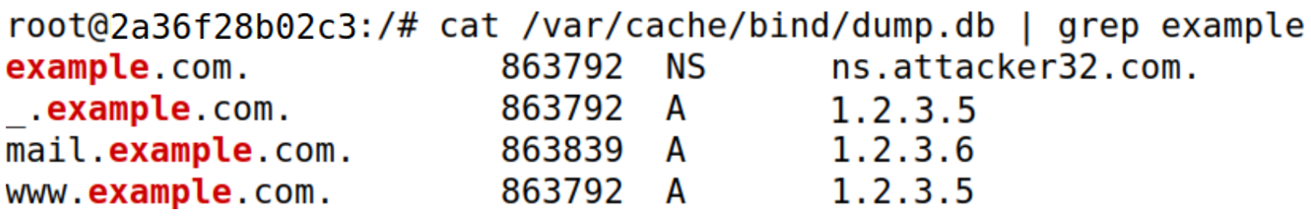


在 user 上查看





在本地 DNS 服务器上查看缓存，可以看到欺骗 NS 记录。



在恶意 DNS 路由器上 cat /etc/bind/zone\_example.com 的文件中，也可看到不同的子域名对应不同的 IP。

攻击成功。

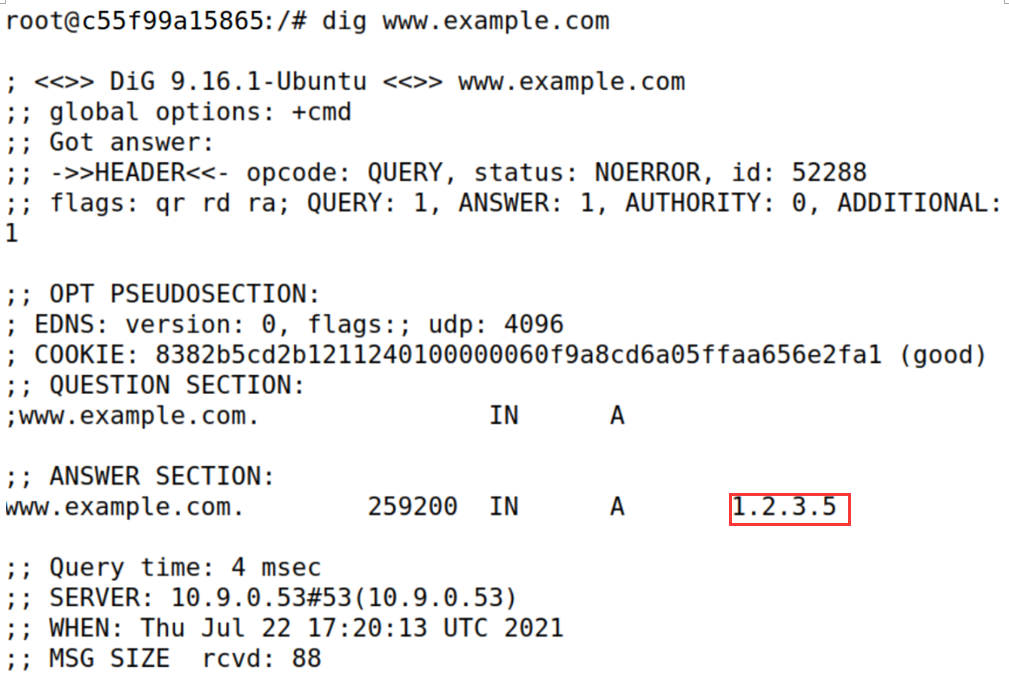
**Task4**

用以下程序进行攻击



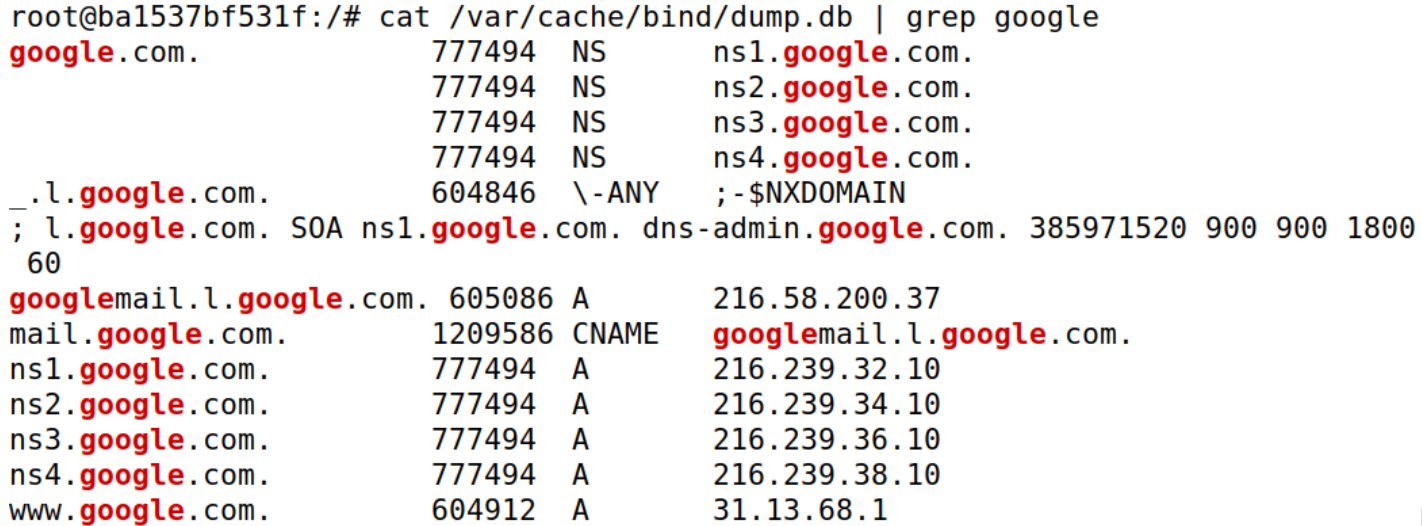
攻击后查看缓存，dig 得到如下结果：

对于www.example.com ，dig之后发现其接受ns.attack32.com作为其DNS，www.example.com被解析到了 1.2.3.5。



对于google.com：dig之后发现其未接受ns.attack32.com作为其DNS 。

查询本地DNS缓存：



**Task 5: Spoofing Records in the Additional Section**

