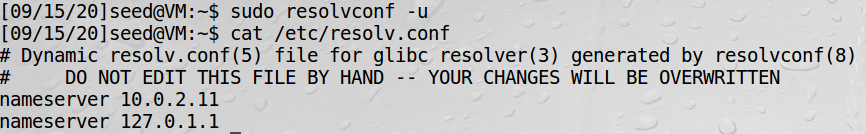
**实验五：**

**Local DNS Attack Lab**

**57117101 焦典**

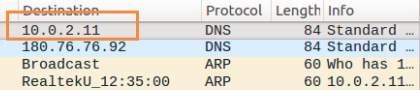
## **Task 1: Conﬁgure the User Machine**

1.定义DNS服务器，执行命令后，刚刚定义的信息出现



2.验证是否设置成功，设置成功





## **Task 2: Setup a Local DNS Server**

1.配置服务器信息





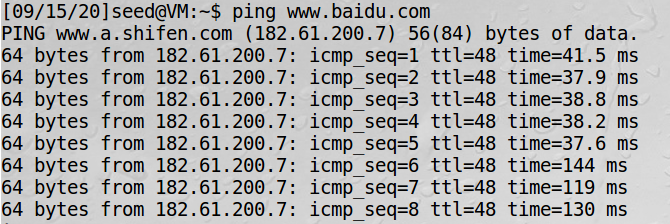
2.更新cache的内容



3.关闭DNSSEC



4.打开并使用DNS服务器

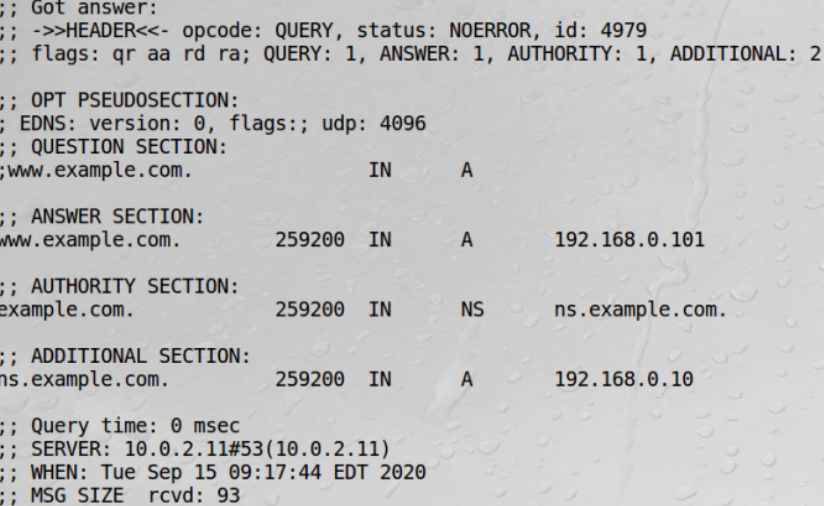


## **Task 3: Host a Zone in the Local DNS Server**

1.创建zones



2.移动文件至bind目录下，重启BIND服务器并测试，有效



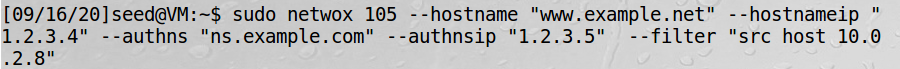
## **Task 4: Modifying the Host File**

1.添加在被攻击的主机，发现可以解析

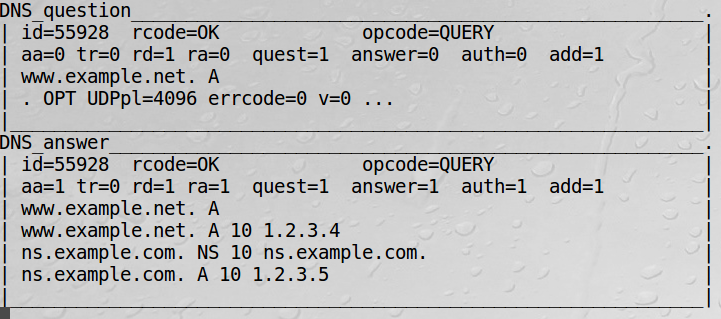


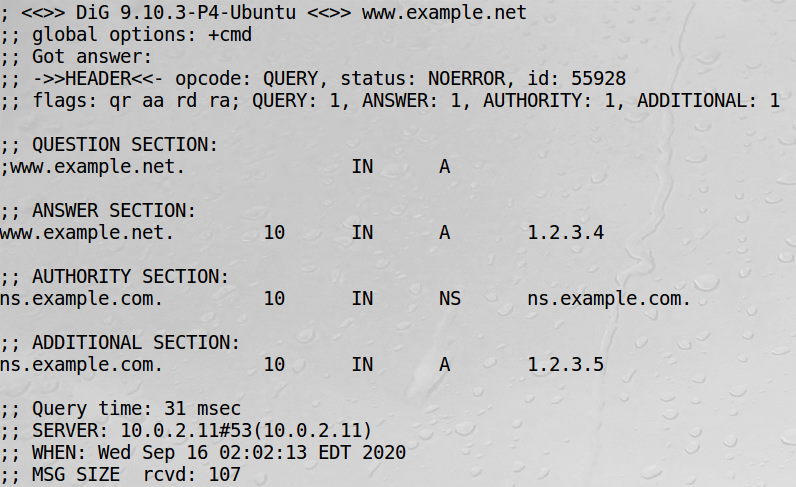
## **Task 5: Directly Spooﬁng Response to User**

1.执行命令进行攻击



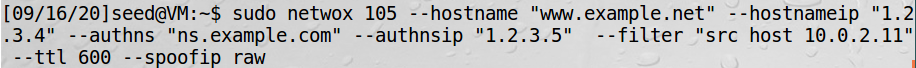
2.攻击后得到伪造的响应



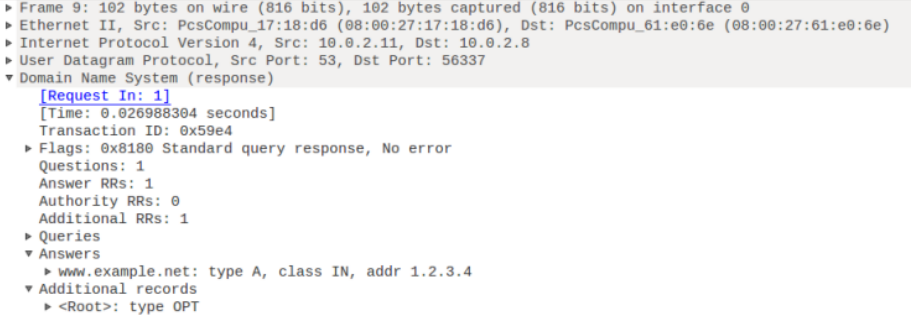


## **Task 6: DNS Cache Poisoning Attack**

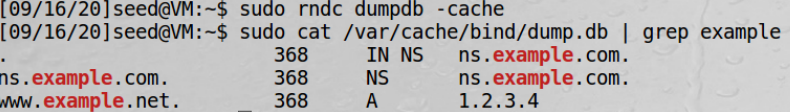
1.在攻击者处执行命令



2.用wireshark抓包



3.查看域名服务器的缓存信息，可见已成功污染



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

1.运行攻击代码，发现伪造信息已经存在于缓存

