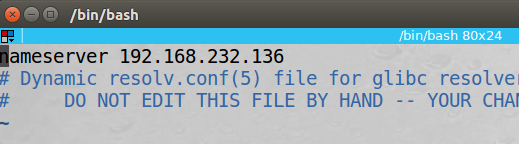
# Local DNS Attack Lab

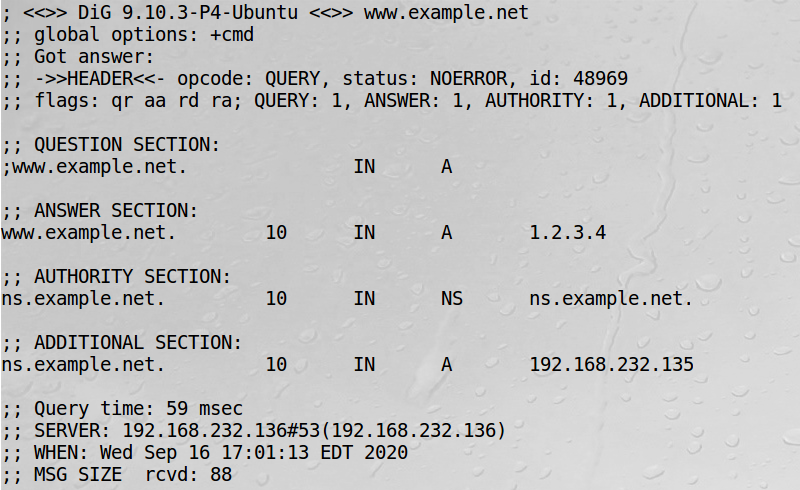
## Lab Tasks (Part I): Setting Up a Local DNS Server

## Task 1: Configure the User Machine

将网络改为NAT模式，为三个SEED虚拟机分配地址，将用户机的DNS地址改为虚拟机3的地址192.168.232.136

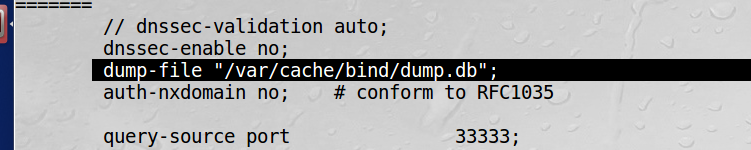


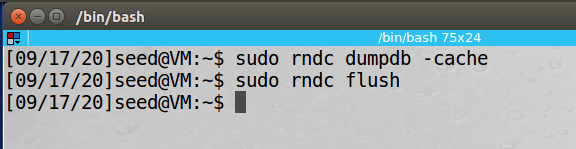
使用dig命令可以收到SERVER为192.168.232.136的信息，证明用户机中DNS设置成功



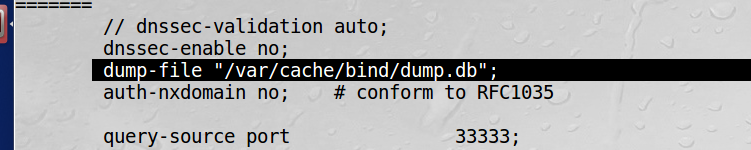
## Task 2: Set up a Local DNS Server

Step 1: Configure the BIND 9 server



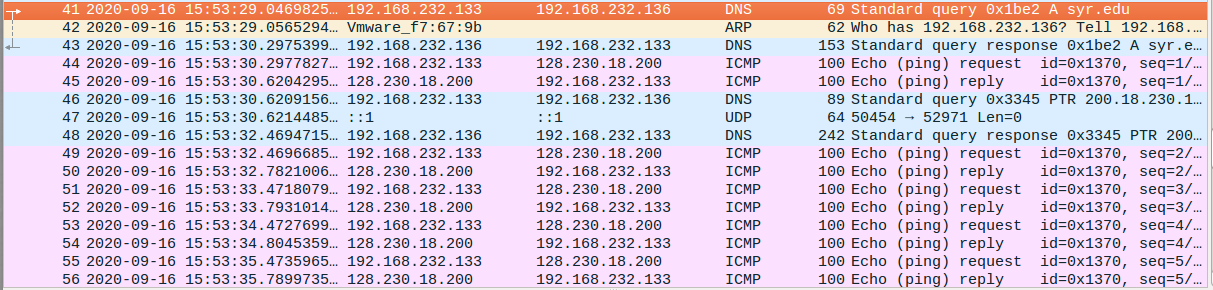


Step 2: Turn off DNSSEC



Step 3: Start DNS server.

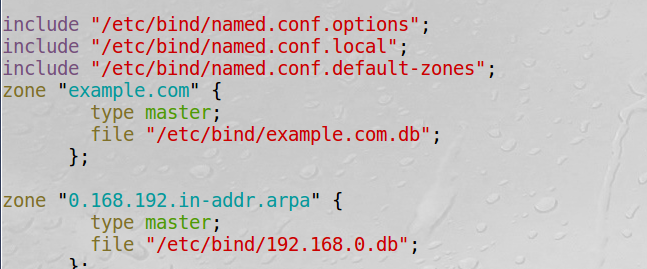
Step 4: Use the DNS server.



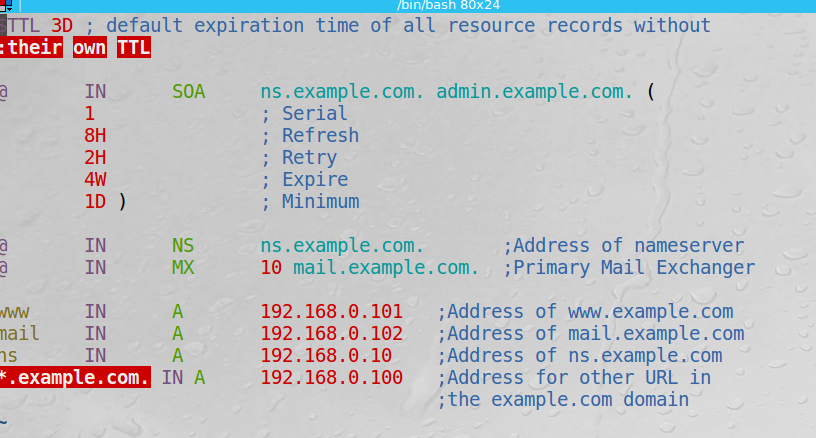
在 用户主机中ping syr.edu，用Wireshark 抓包，user先向本地DNS服务器请求域名解析服务，再由DNS服务器递归查询获得syr.edu对应的IP地址，最终发送给 user，随后user开始ping的过程。

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

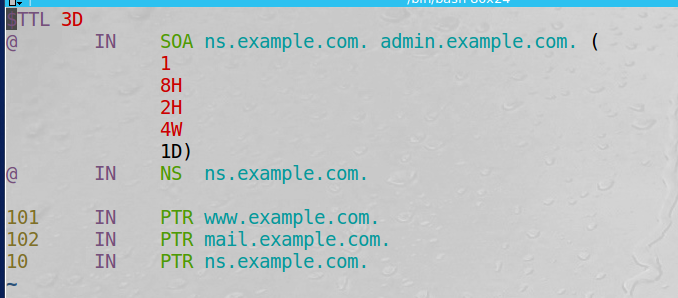
Step 1: Create zones



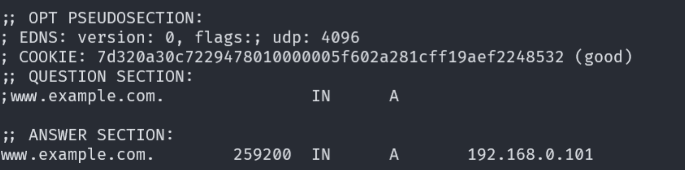
Step 2: Setup the forward lookup zone file.



Step 3: Set up the reverse lookup zone file

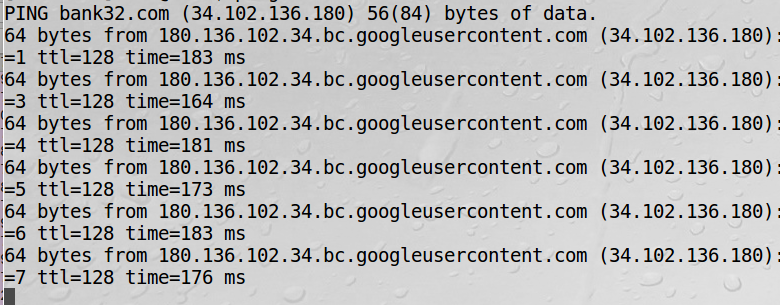


Step 4: Restart the BIND server and test.



地址被成功解析

## Task 4: Modifying the Host File

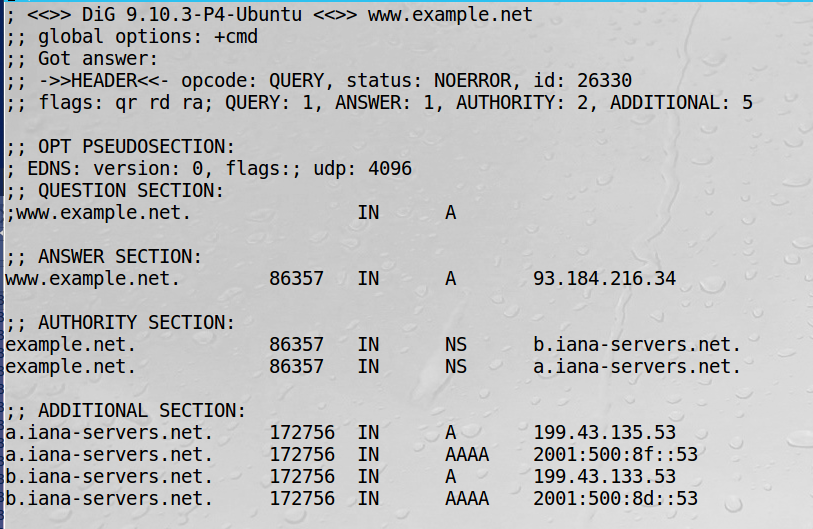


先ping bank32.com, 得到真实的外部IP，修改host地址后再Ping，发现地址已经改变



## Task 5: Directly Spoofing Response to User

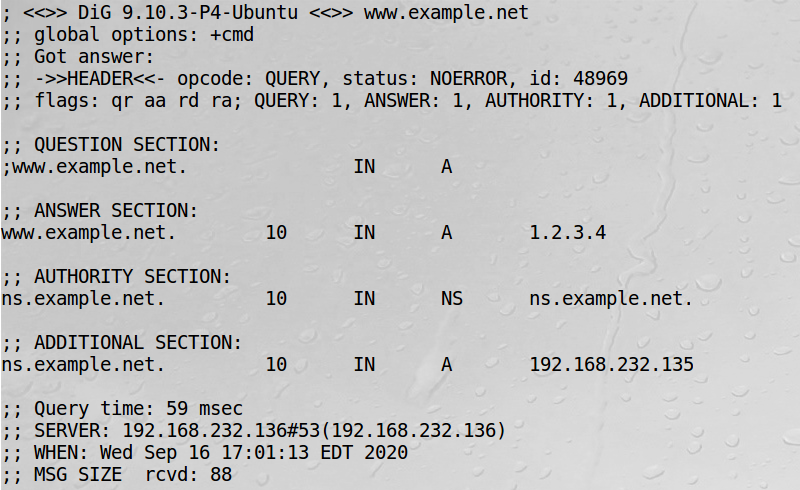
攻击前dig得到真实的外部IP



发起攻击



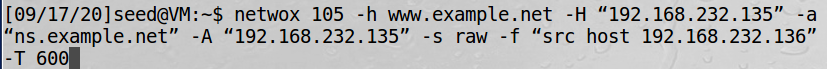
再次dig，地址改变

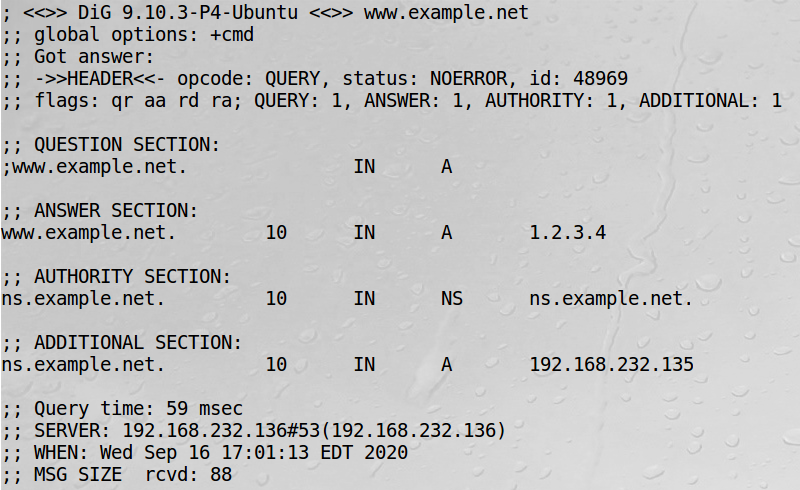


攻击者的shell中也能看到对应变化

## Task 6: DNS Cache Poisoning Attack

发起攻击后请求解析



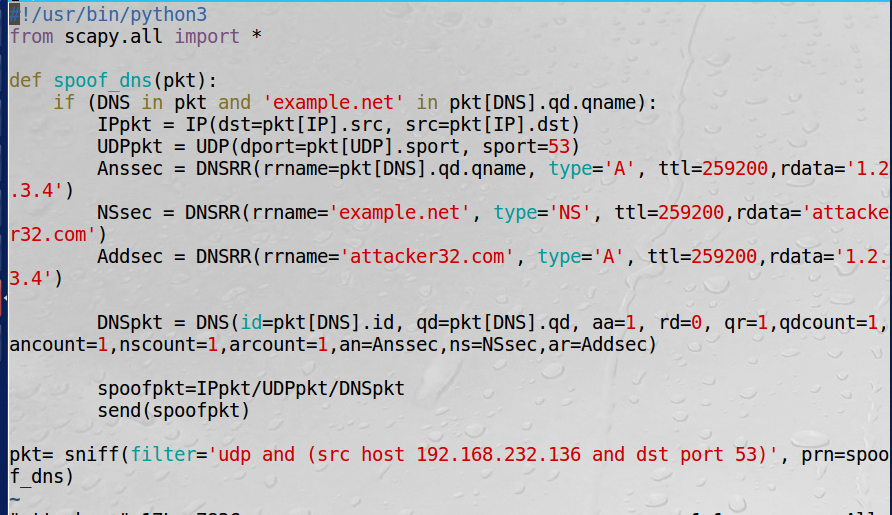


在DNS服务器中使用rndc dumpdb -cache之后查看缓存：



攻击成功

## Task 7: DNS Cache Poisoning: Target the Authority Section



在DNS服务器上可以观察到DNS服务器向attacker32.com发起了DNS请求