**Lab18-1: Local DNS Attack Lab**

**实验环境：**

攻击者192.168.43.166；

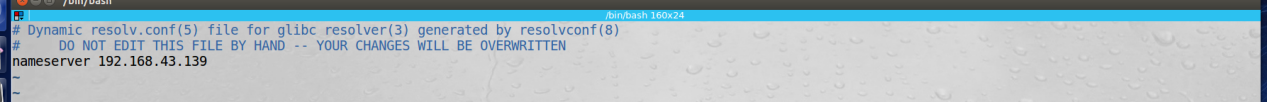
被攻击者192.168.43.139；

主机A 192.168.43.85。

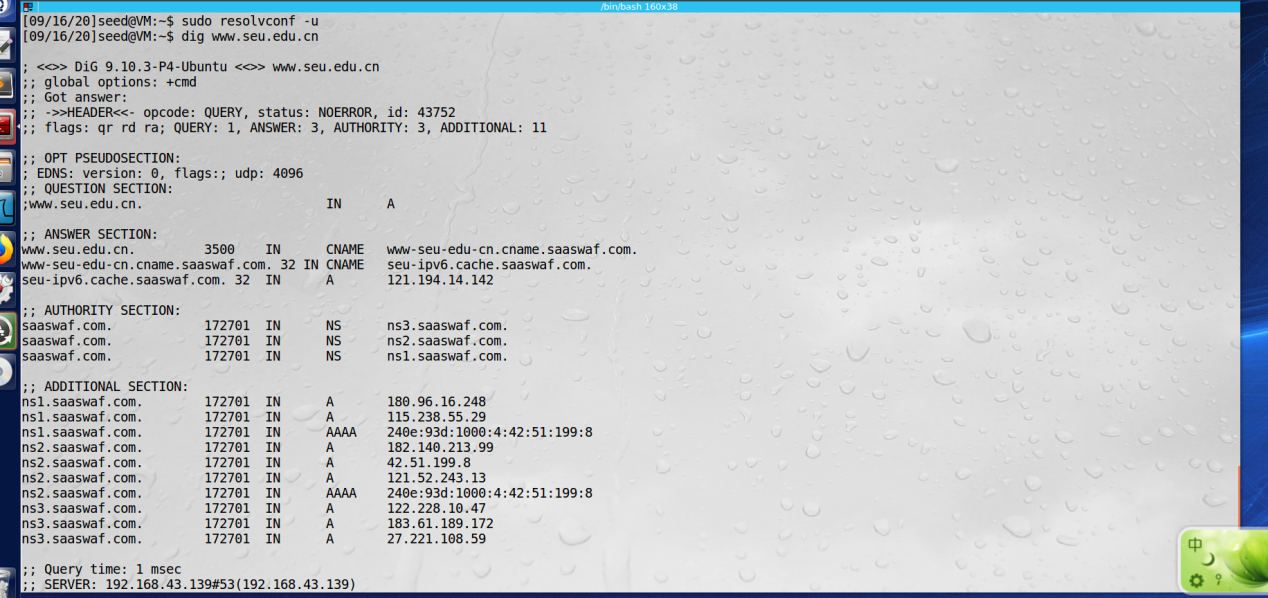
**Task 1: Configure the User Machine**

将A配置为被攻击者的主DNS服务器：





令配置生效；使用dig命令检验，发现配置成功（见最后一行）：



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

**Step 1: Configure the BIND 9 server**

设置DNS缓存的存储地址：





**Step 2: Turn off DNSSEC**

关闭DNSSEC保护机制：



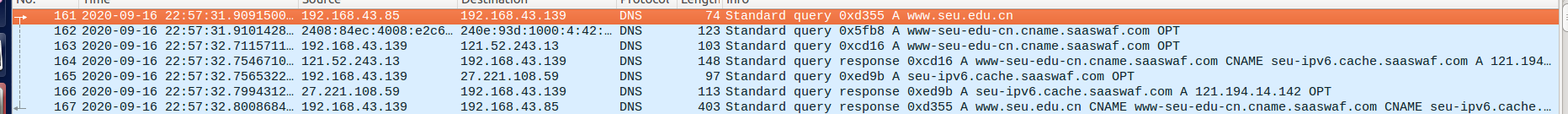
**Step 3: Start DNS server**

重启DNS服务器，使配置生效：

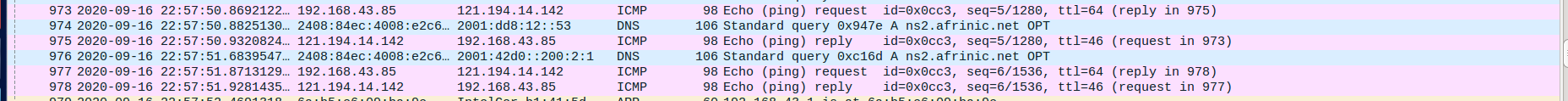


**Step 4: Use the DNS server**

在被攻击者主机上使用ping命令，并查看ping命令触发的DNS查询；被攻击者向它的本地DNS服务器（即主机A）发起查询，而该服务器继续向上查询后，将得到的结果反馈给被攻击者：



对同一域名后面的ping使用到了DNS的缓存功能：



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

**Step 1: Create zones**

在DNS服务器中创建两个区域条目内容（分别用于正向查找和反向查找）：



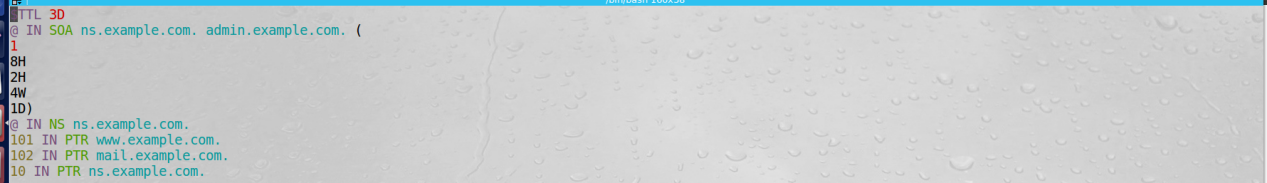
**Step 2: Setup the forward lookup zone file**

设置正向查找区域文件：



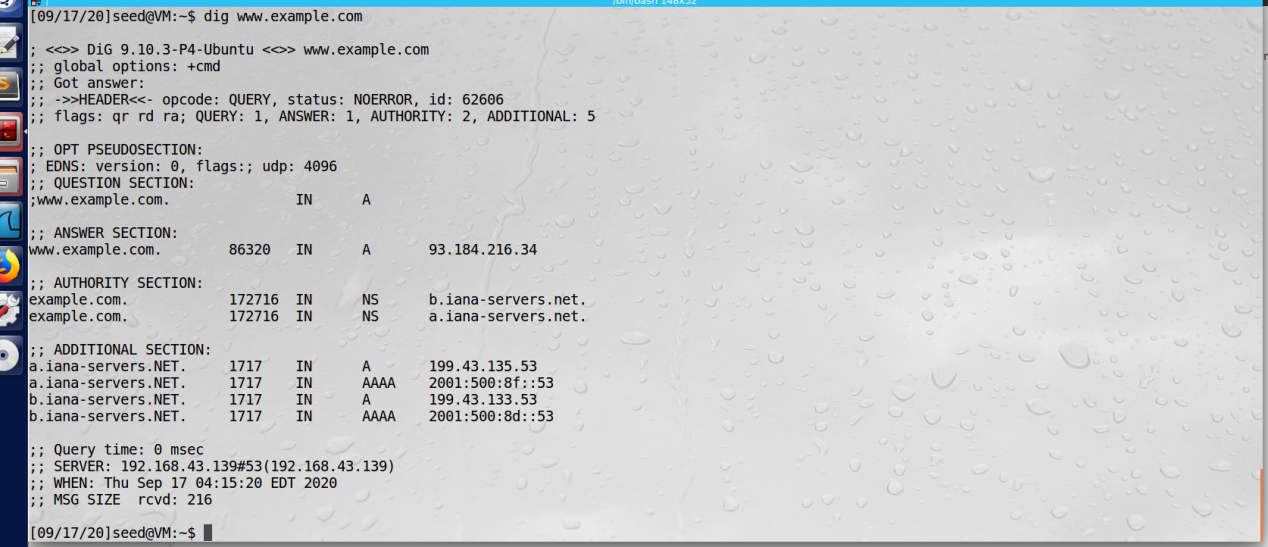
**Step 3: Set up the reverse lookup zone file**

设置反向查找区域文件：



**Step 4: Restart the BIND server and test**

重启服务器并检测上述配置：

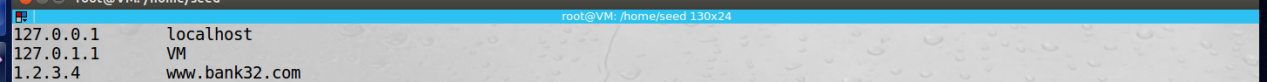


**Task 4: Modifying the Host File**

进行攻击前的正常ip：



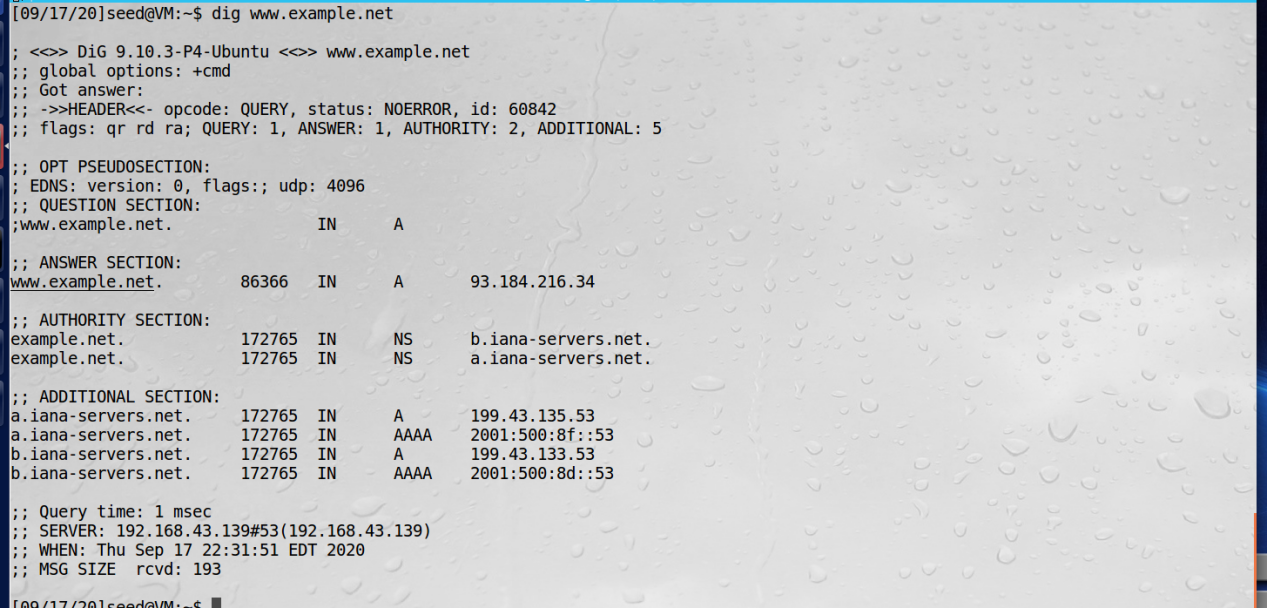
被攻击后，执行ping命令时该域名的ip发生了改变：



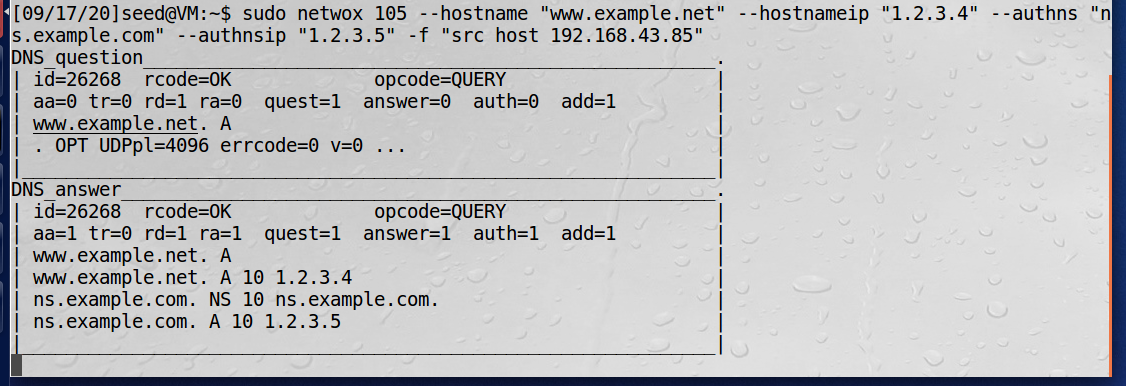


**Task 5: Directly Spoofing Response to User**

被攻击者在被攻击前的相应信息：



进行攻击，生成了伪造的应答：



**Task 6: DNS Cache Poisoning Attack**

进行攻击：

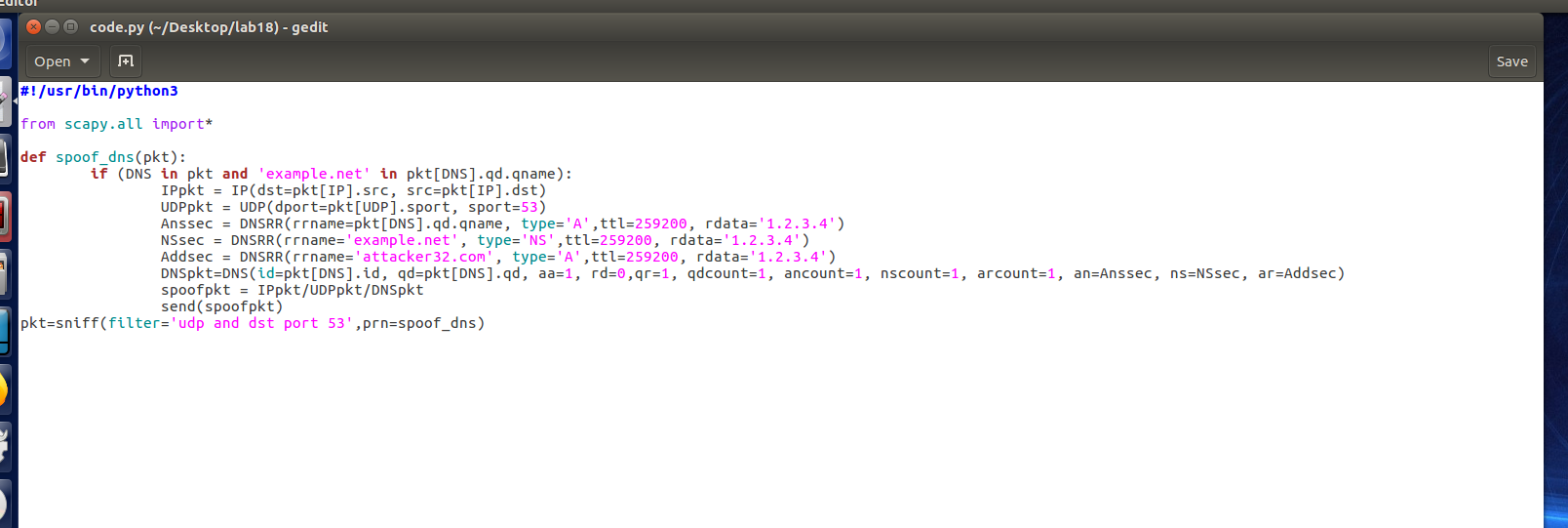


结果：



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

进行攻击：



结果：

