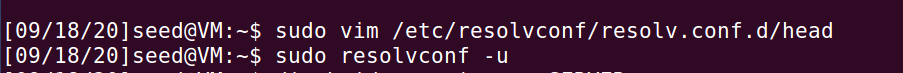
**Local DNS Attack Lab**

准备3台主机DNS server：172.20.10.7 user：172.20.10.6 attacker:172.20.10.8  
**Task1: Configure the User Machine**

首先在user上配置DNS服务器



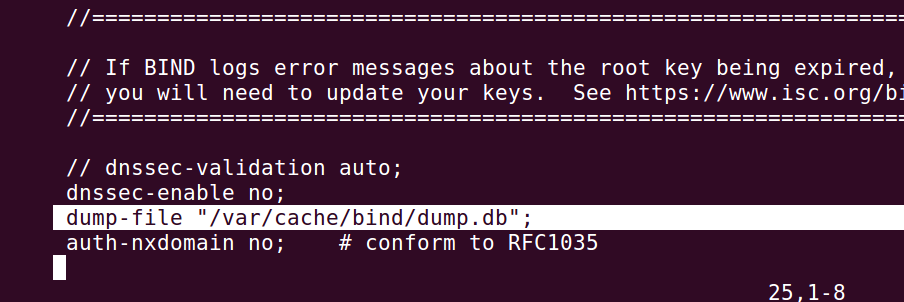
Dig 任意IP进行验证



设置成功

**Task2: Set up a Local DNS Server**

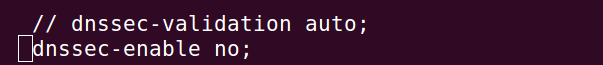
首先进入/etc/bind/named.conf.options文件查看该条目是否存在

****

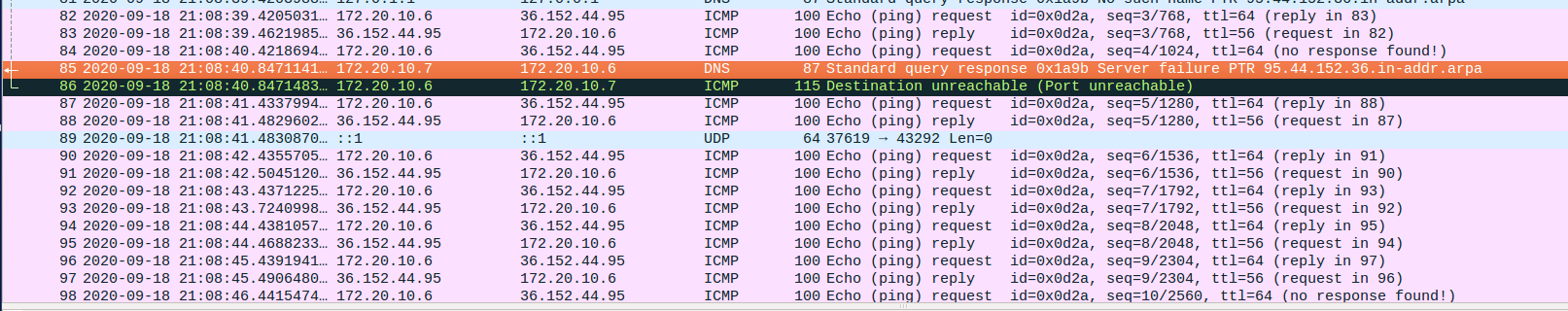
清除DNS服务器中的高速缓存

****

再次进入/etc/bind/named.conf.options，确认DNSSEC已经关闭

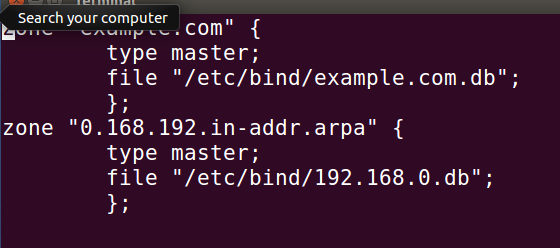
****

使用user主机ping 百度。可以发现是由user首先向本地DNS server 172.20.10.7 请求，然后再由DNS Server 通过递归查询获得[www.baidu.com](http://www.baidu.com) 获得对应IP后，最终发送给user主机，随后user开始于其目标主机通信。

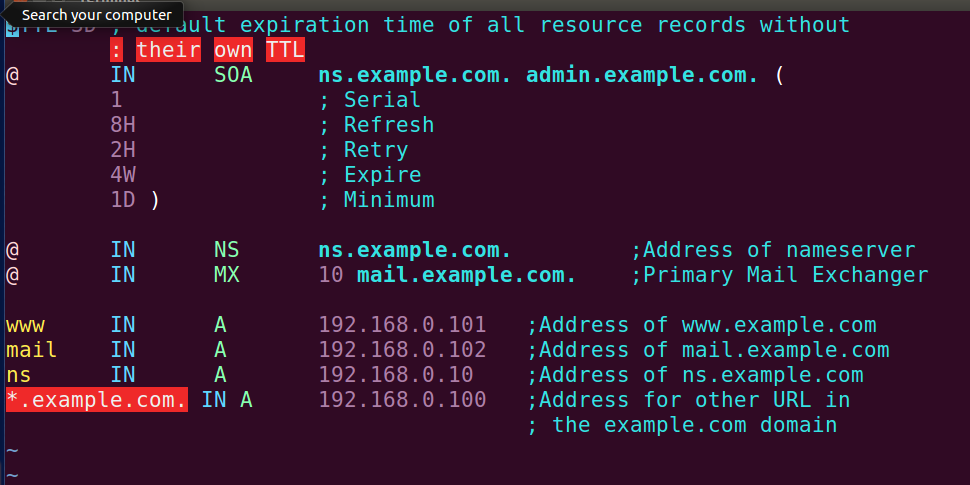
****

**Task3: Host a Zone in the Local DNS Server**

Step 1：Create zones



Step 2: Setup the forward lookup zone ﬁle.



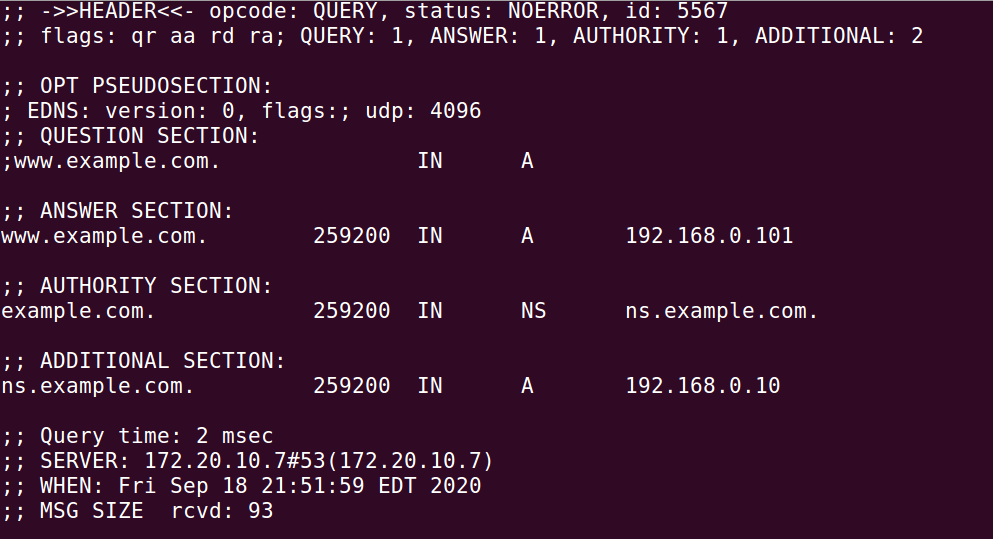
**Step 3: Set up the reverse lookup zone ﬁle.**



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

****

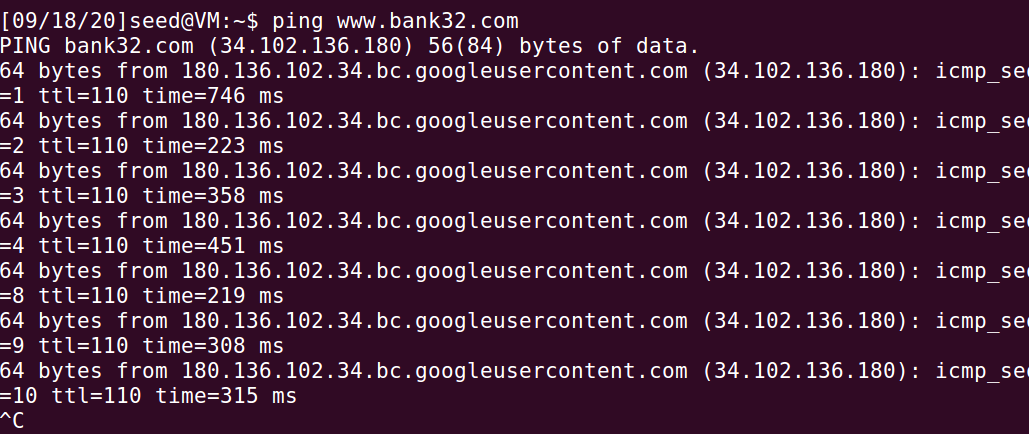
重启DNS服务并测试example.com



可以看到user已经可以成功找到[www.example.com](http://www.example.com)

**Task4: Modifying the Host File**

更改hosts文件前，可以ping通[www.bank32.com](http://www.bank32.com)

****

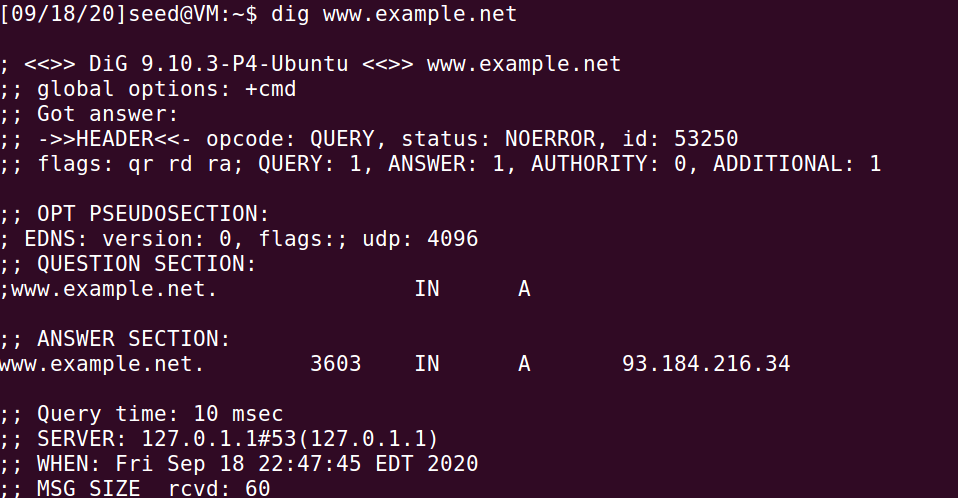
在/etc/hosts文件里加上1.2.3.4 [www.bank32.com](http://www.bank32.com)

再次ping，效果如下，可以看到IP地址被恶意修改

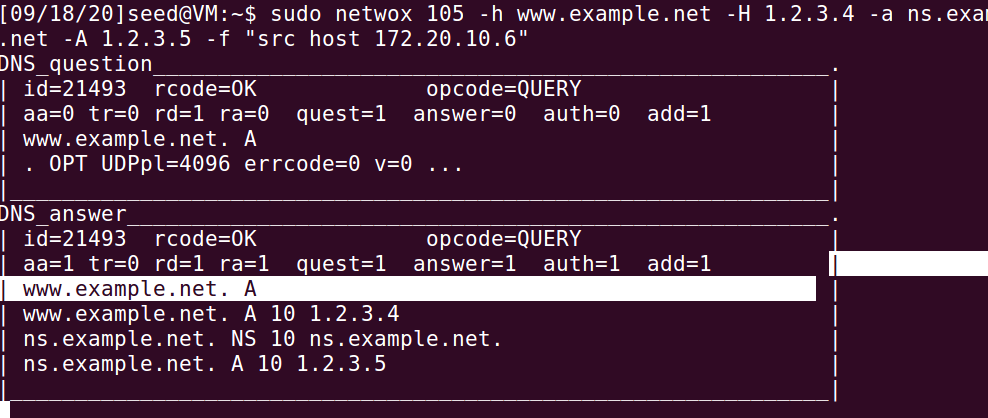


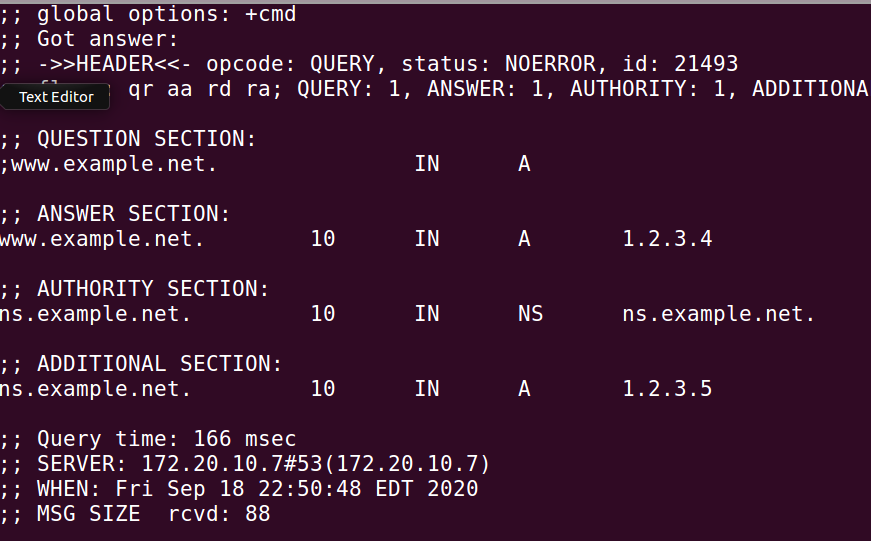
**Task5: Directly Spooﬁng Response to User**

攻击前，dig www.example.net的结果如下图所示



在atttacker中执行该命令，并在user中再次dig [www.example.net可以发现ip](http://www.example.net可以发现ip)地址已经发生更改。并且在attacker端显示了拦截的数据包和发送的伪造数据包。attacker伪造报文成功。



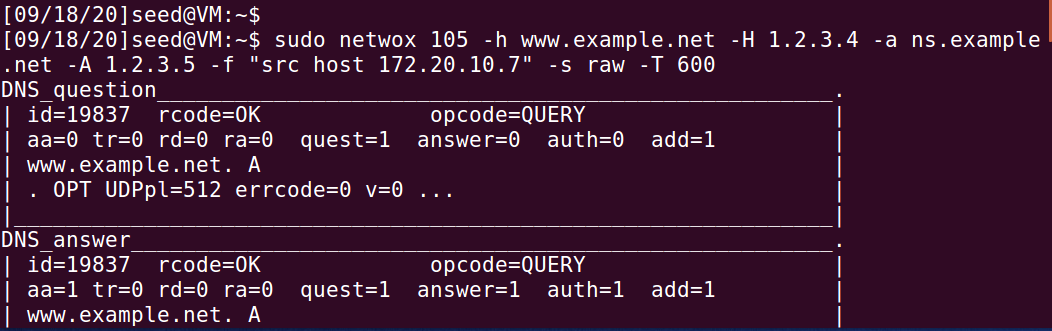


**Task6: DNS Cache Poisoning Attack**

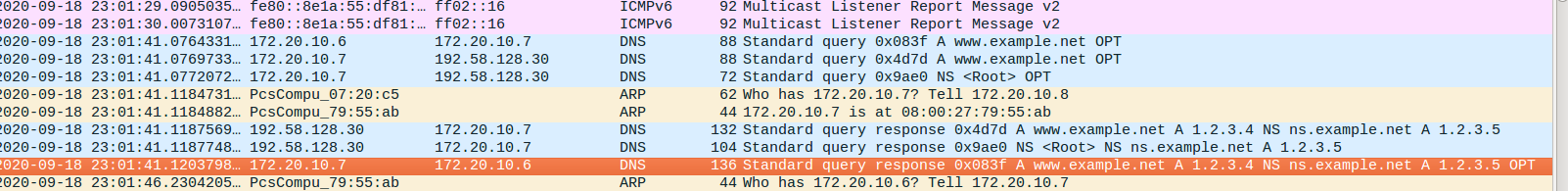
在DNS Server 中清空DNS缓存



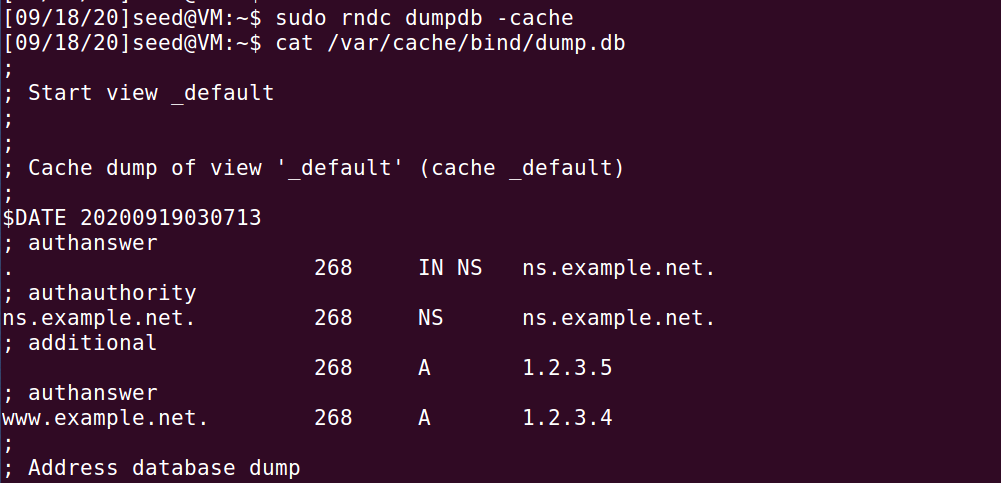
在attacker中运行上述命令，嗅探来源为本地DNS Server的IP地址数据包



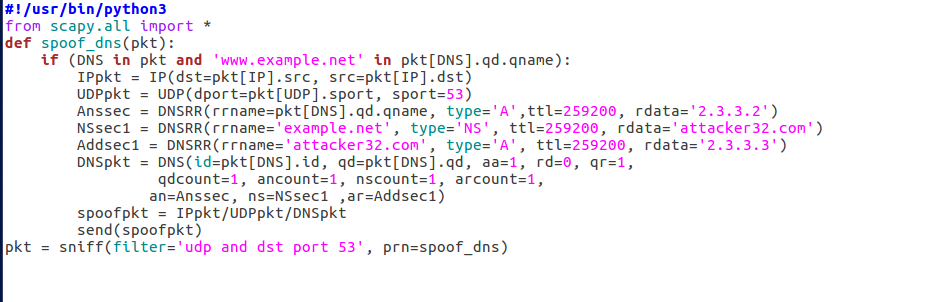
在user中重新ping ，wireshark中可以看到伪造的数据包成功回复。



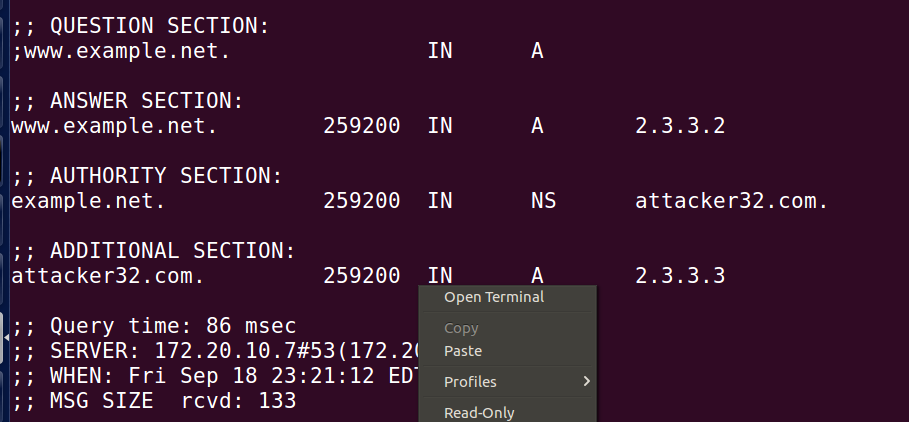
运行指定命令，可以看到本地DNS缓存，可以看到[www.example.net对应的IP](http://www.example.net对应的IP)地址为1.2.3.4。攻击成功

**Task7: DNS Cache Poisoning: Targeting the Authority Section**

在attacker中编写并运行下图的python脚本

****

User中dig example.net 可以发现ip地址已经发生更改



在本地DNS Server缓存中也可以看到。说明攻击成功

