Local DNS Attack Lab

Task1 Config user machine

首先，确定IP地址，

User: 10.0.2.18

Attacker: 10.0.2.17

DNS server: 10.0.2.16

配置固定IP地址，首先在/etc/network/interfaces中添加以下内容

auto enp0s3

iface enp0s3 inet static

address 10.0.2.xx

netmask 255.255.255.0

gateway 10.0.2.2

完成后执行以下命令

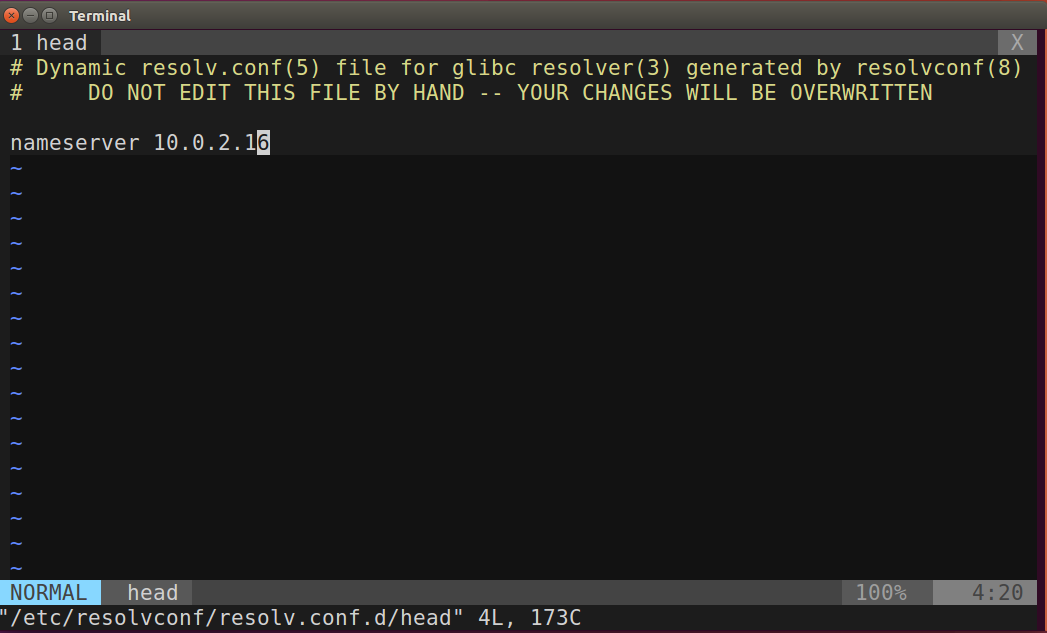
sudo /etc/init.d/networking restart

即可指定IP地址

然后指定DNS服务器

在/etc/resolvconf/resolv.conf.d/head中添加以下内容

nameserver 10.0.2.16

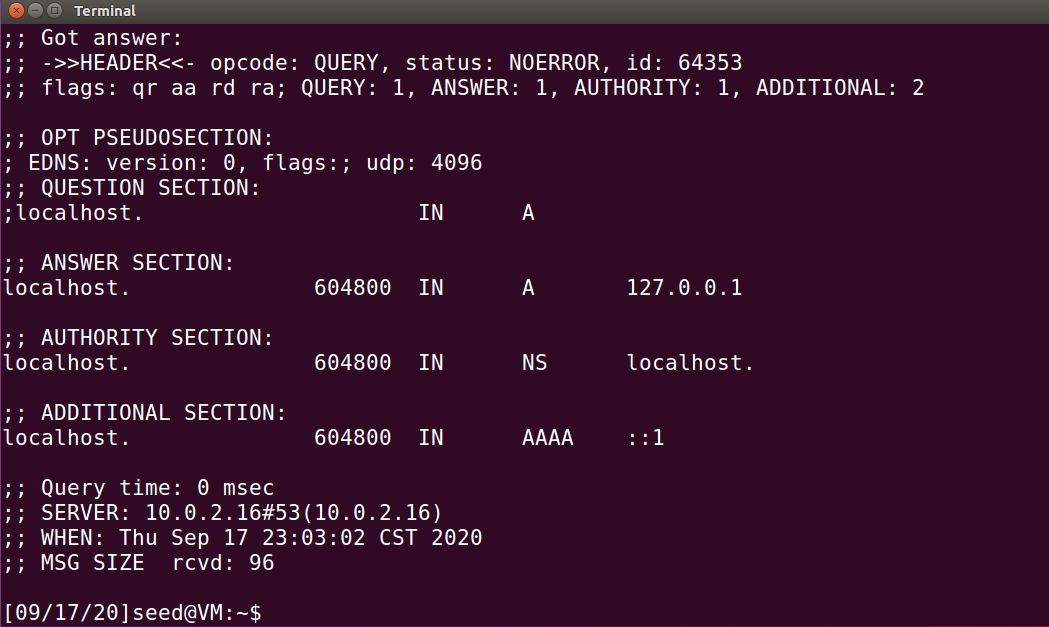


保存后执行以下命令

sudo resolvconf -u

完成指定DNS服务器

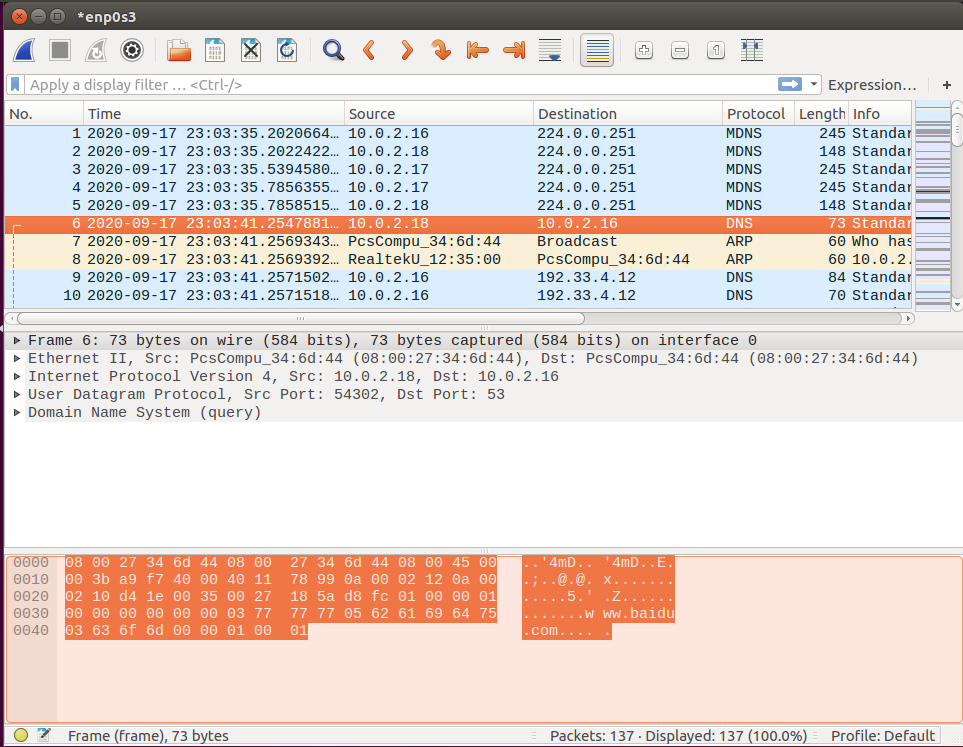
此时用dig可以发现，DNS、服务器已经改成了10.0.2.16



Task2 Set up a local DNS server

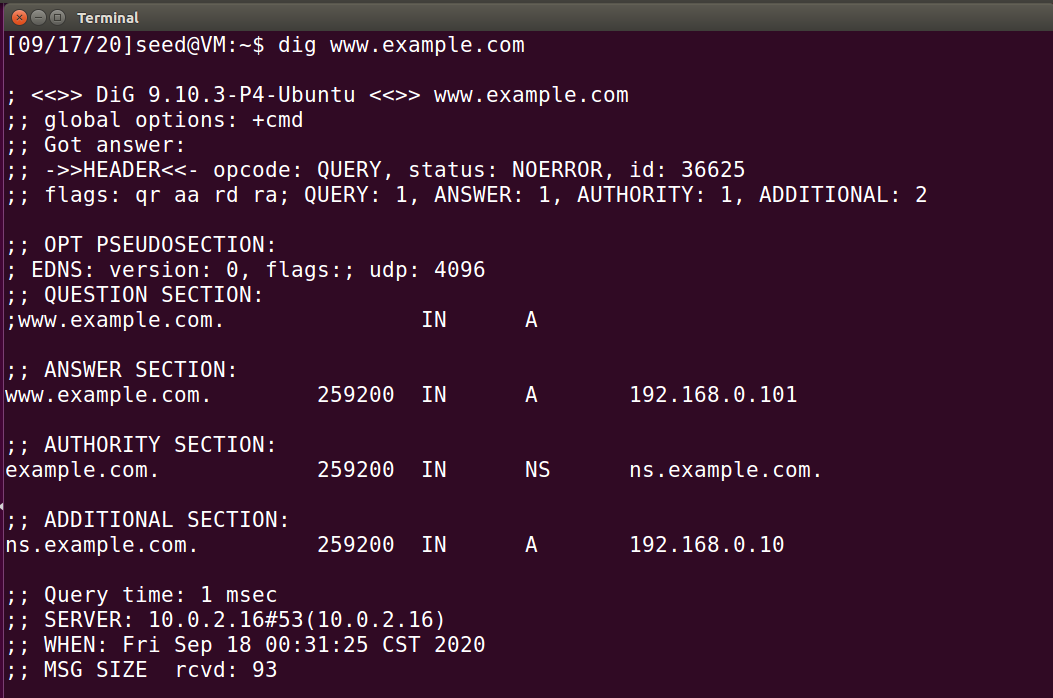
打开/etc/bind/named.conf.options发现配置已经符合要求，直接重启服务即可

在User机器上执行ping www.baidu.com时候发现向本地DNS服务器进行了查询



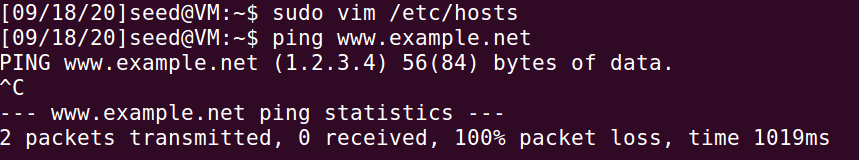
Task3 Host a Zone in the Local DNS Server

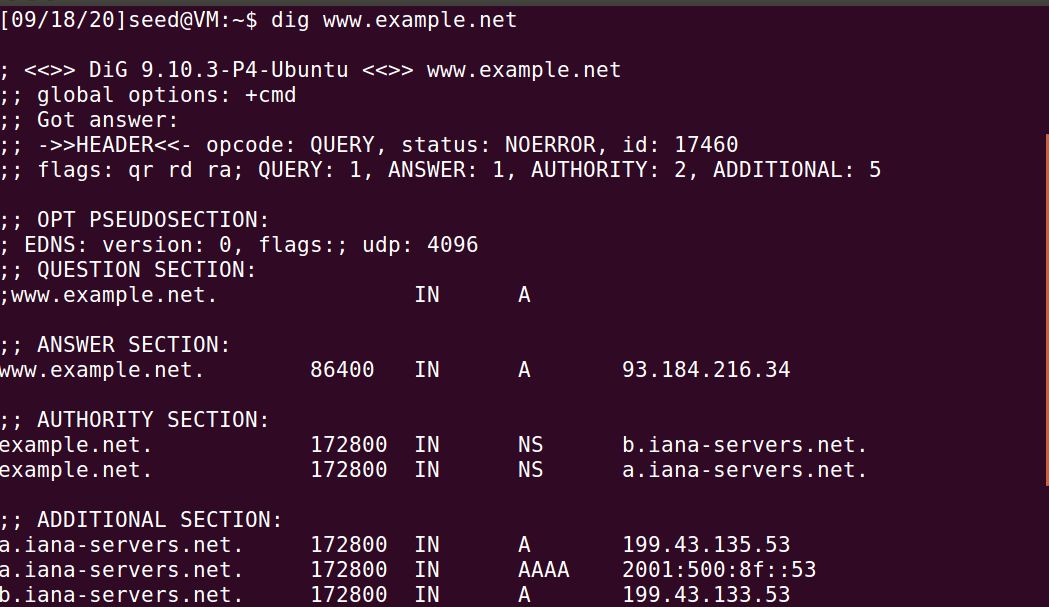
按照任务中提示完成配置并执行，发现DNS解析的结果成为了设定的结果



Task4 Modifying Host file

在/etc/hosts文件中添加一句1.2.3.4 www.example.net

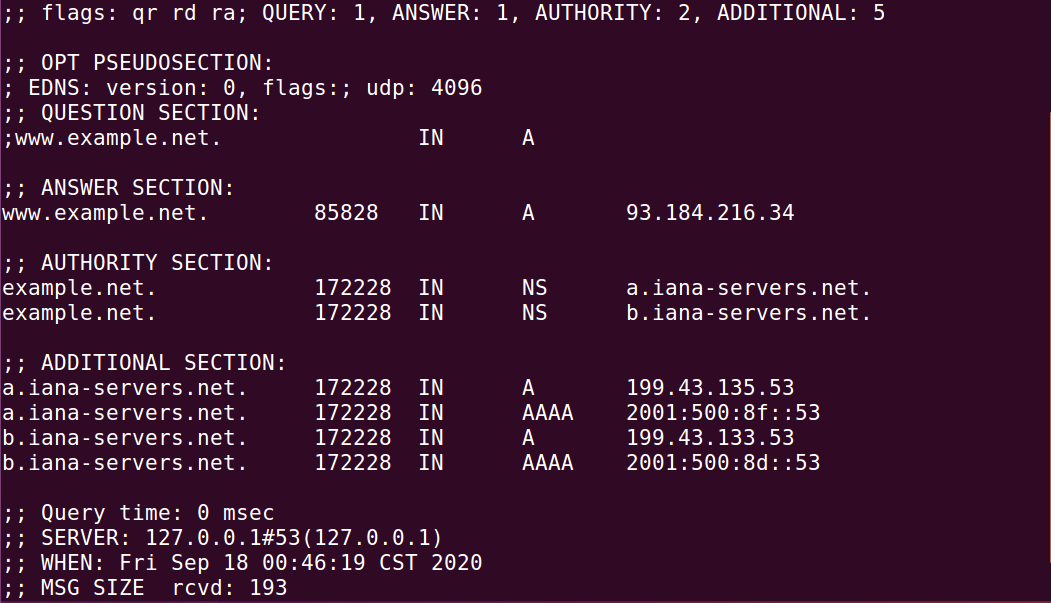




可以发现ping命令解析到了地址1.2.3.4上，但是dig命令正常解析

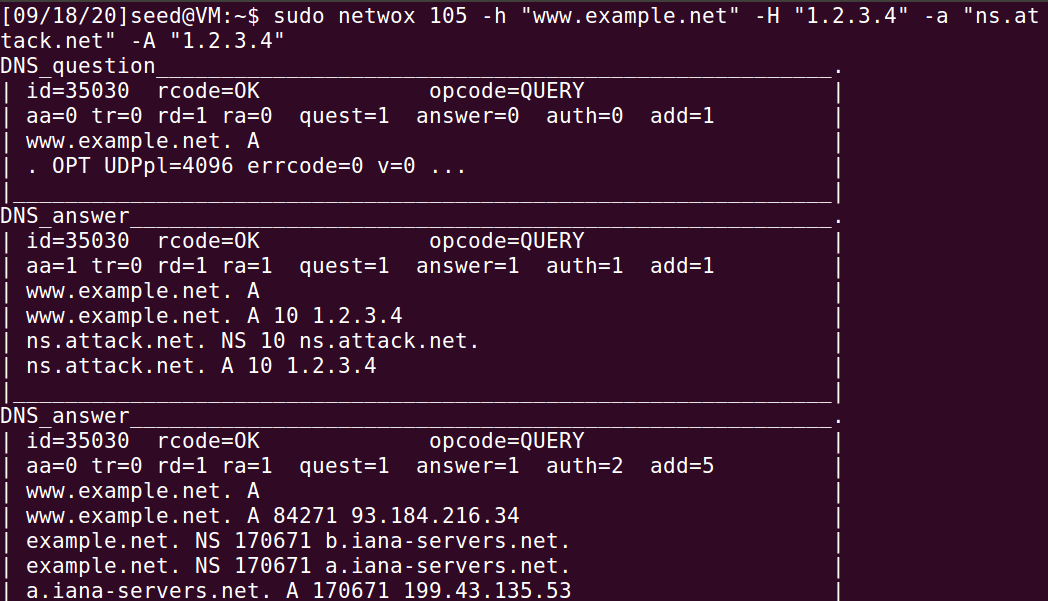
Task5 Directly Spoofing Response to Use

按照任务中的提示，直接执行命令

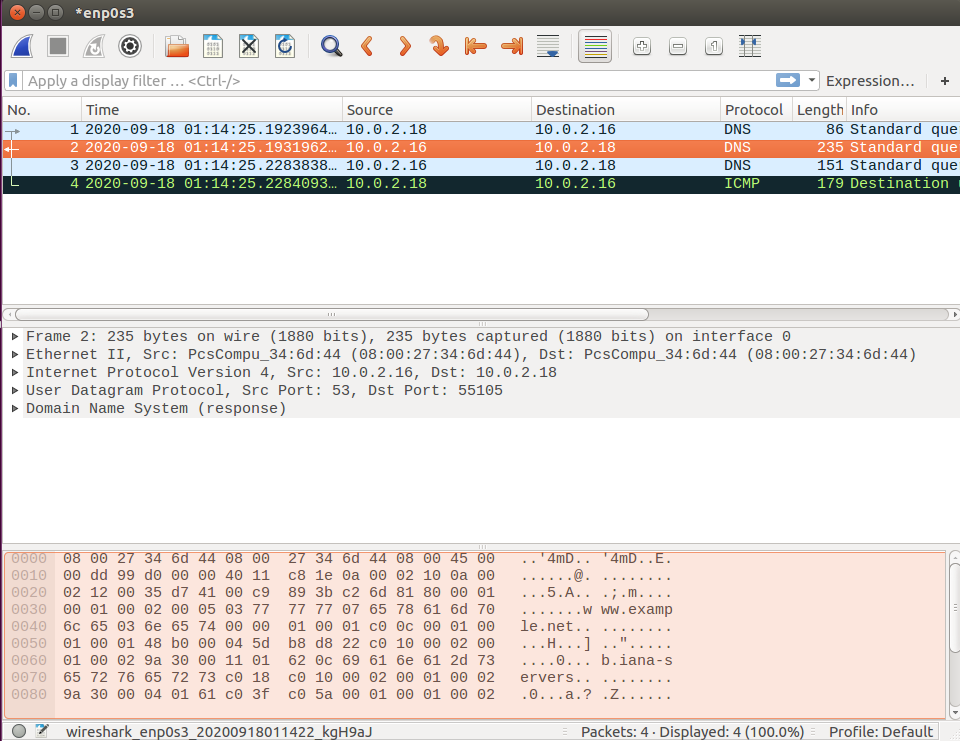


发现并没有完成伪造

执行netwox命令的一端输出如下



发现一个DNS询问回答了两次，再抓包



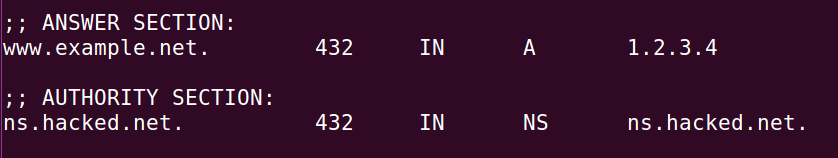
发现正确的DNS解析比伪造的DNS解析来得早，因此解析正确

Task6 DNS Cache Poisoning Attack

按照任务中的要求执行netwox命令

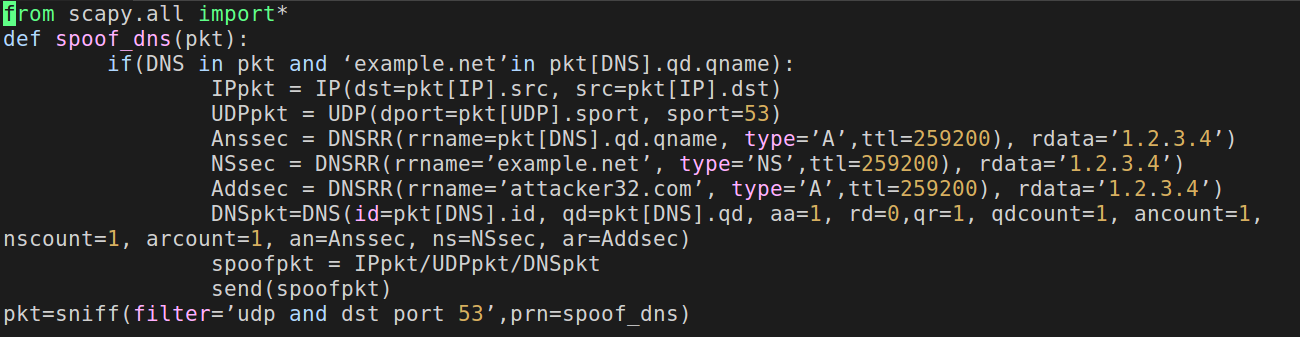


执行dig命令后结果如下，发现已经被修改



Task7 DNS Cache Poisoning: Targeting the Authority Section

按照Guideline中的提示完成Python程序



执行后发现Authority Section中解析的地址已经改为attacker32.com了