**lab5实验报告**

57117235 李娜

三个虚拟机在一个局域网中：

DNS服务器：10.0.2.4

攻击者主机：10.0.0.5

用户主机：10.0.2.6

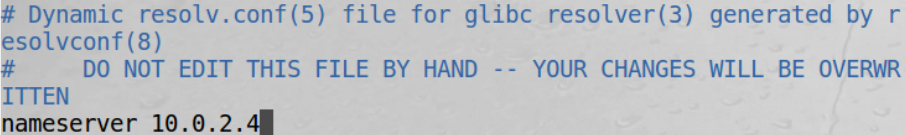
Local DNS Attack Lab

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

本实验内容是配置用户机和服务器；新建一个两个域，并配置域名和对应的IP地址，实现对该域名的DNS解析，增进学生对DNS服务和运行机制的了解。

一、Task1: Conﬁgure the User Machine

1、用vi打开/etc/resolvconf/resolv.conf.d/head后，把DNS服务器的IP地址添加进去，以防止DHCP自动覆盖我们设置的DNS服务器IP：

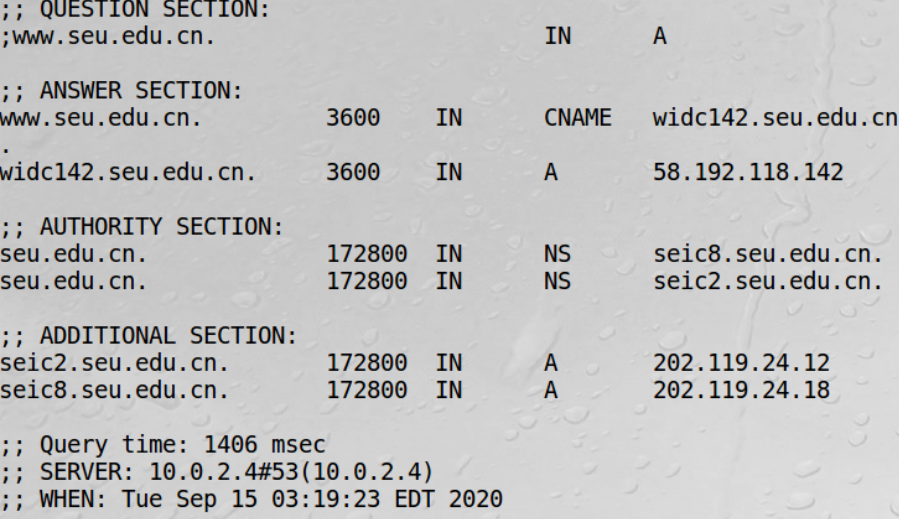


2、更新DNS服务器IP：



３、用dig命令测试域名系统是否工作正常：





收到响应，说明用户机设置完成。

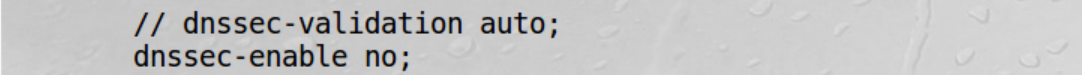
二、Task2: Set up a Local DNS Server

1、打开/etc/bind/named.conf.options，添加：



指定BIND缓存转储的位置。

2、打开/etc/bind/named.conf.options，修改：



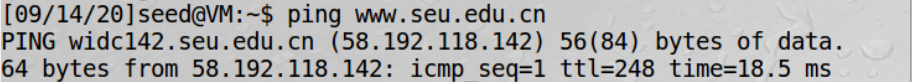
该步骤目的是关闭DNSSEC，展示没有这种保护机制时，攻击是如何产生的。

3、开启DNS服务：

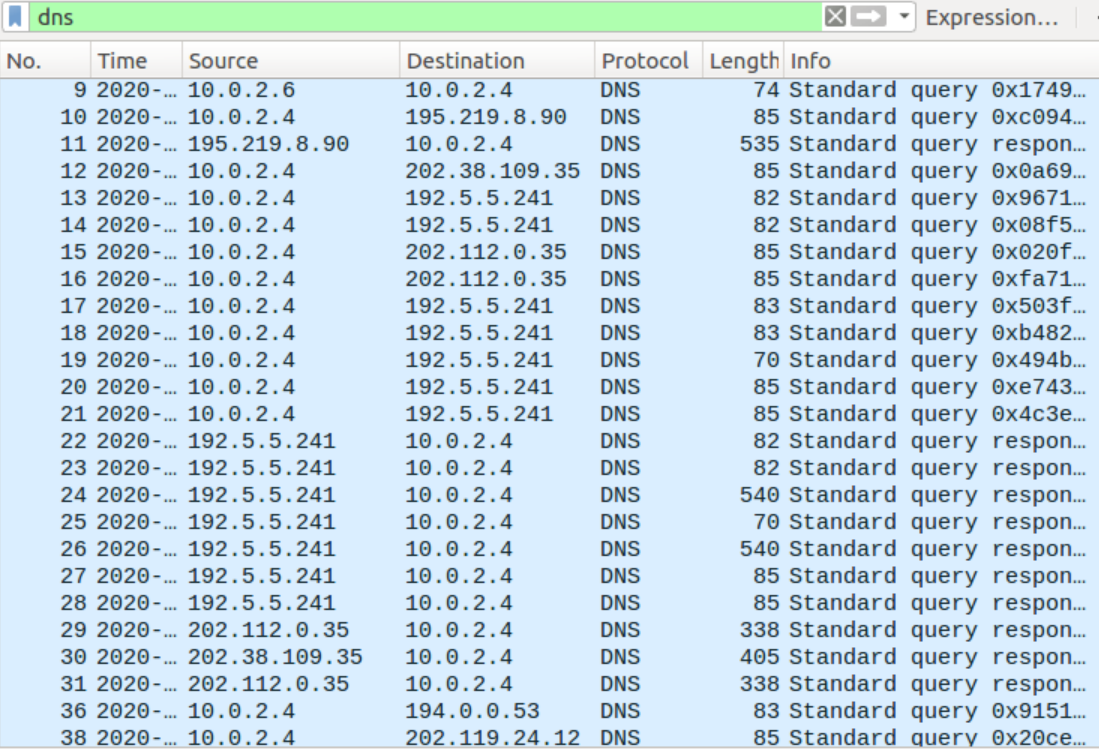


4、观察DNS服务器如何工作

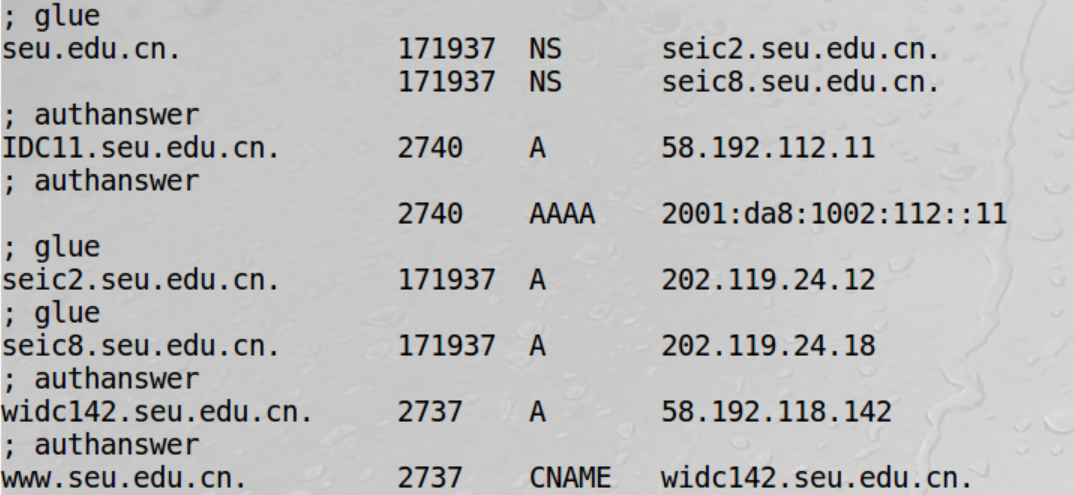
（1）用户主机向[www.seu.edu.cn发送ping](http://www.seu.edu.cn发送ping)请求：



（2）打开wireshark（在步骤（1）之前），可以看到在用户机向服务器查询[www.seu.edu.cn的IP](http://www.seu.edu.cn的IP)地址后（报文9），服务器向多个IP发起DNS查询：



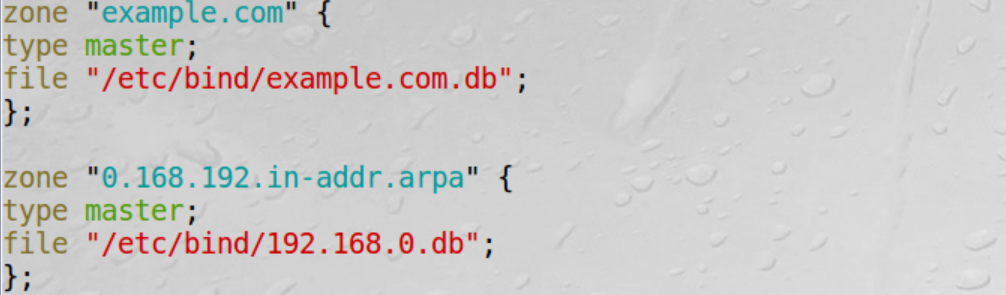
（3）查看服务器的DNS缓存：



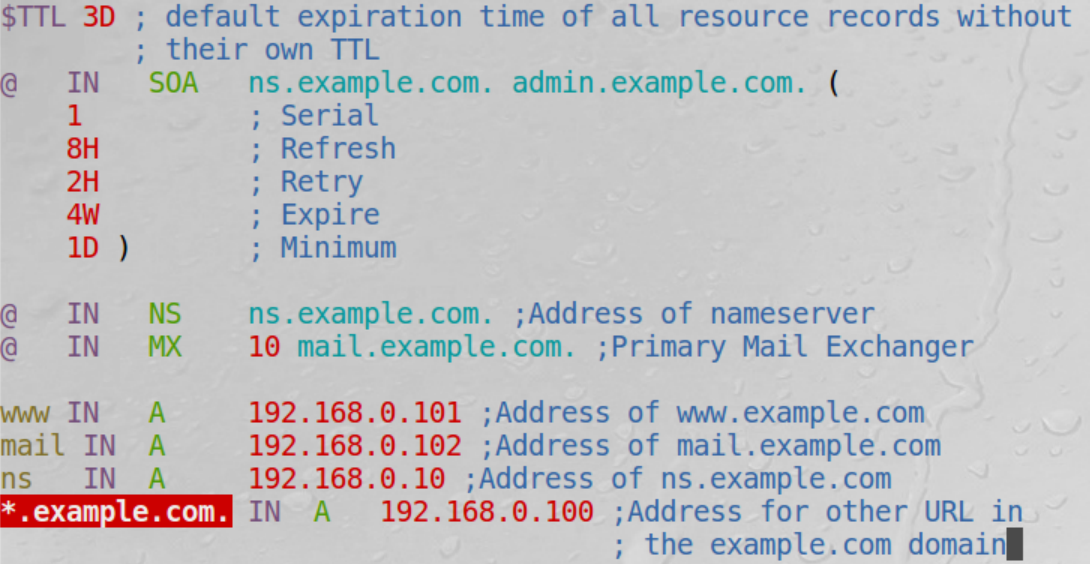
可以看到，DNS服务器最终查询的结果为——[www.seu.edu.cn的IP](http://www.seu.edu.cn的IP)地址是58.192.118.42。

三、Task3: Host a Zone in the Local DNS Server

1、在/etc/bind/named.conf文件中添加如下内容，配置两个区域：



2、在/etc/bind/目录中，创建以下example.com.db区域文件，实现从域名到IP的映射：



3、在/etc/bind/目录中，创建以下192.168.0.db文件，实现IP到域名的映射：

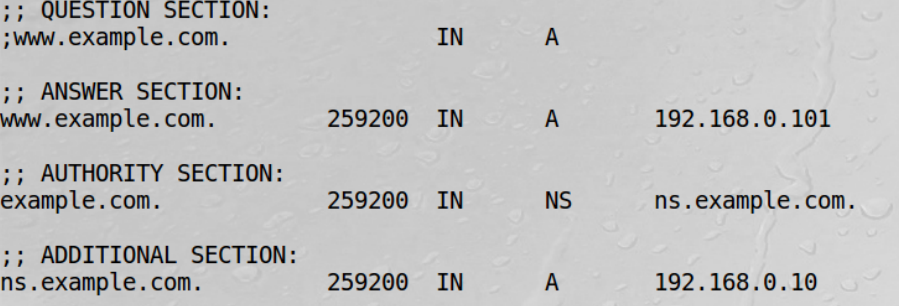


4、重启DNS服务：



用dig命令查询域名[www.example.com](http://www.example.com)：





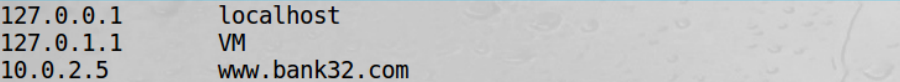
可以看到，用户机查询到[www.example.com的IP](http://www.example.com的IP)地址为192.168.0.101，和前面配置的地址一致。其中也显示了前面配置的一个权威服务器ns.example.com及其IP地址192.168.0.10。

（二）、Lab Tasks (Part II):Attacks on DNS

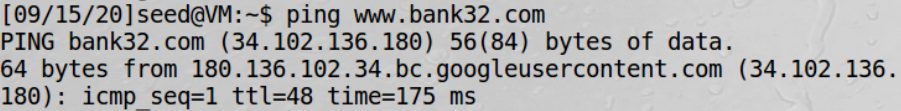
本实验的目的在于实现DNS攻击，通过对用户的DNS查询返回伪造的IP地址，将用户对域名的访问导向特定IP地址，这可能是攻击者精心设计的网页，以获取用户隐私数据。

一、Task4: Modifying the Host File

1、修改用户机上的/etc/hosts文件，把域名www.bank32.com和IP地址10.0.2.5（为局域网内另一台虚拟机的IP地址） 的对应关系添加进去：

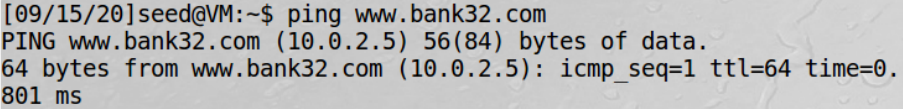


2、修改前在用户机上ping该域名：



收到来自IP地址34.102.136.180的回复。

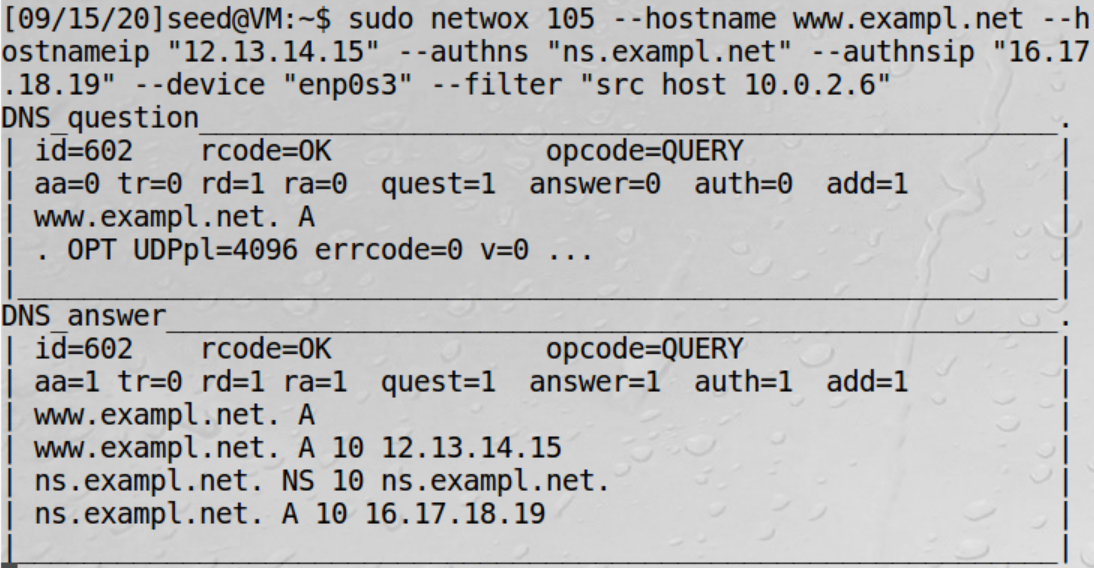
修改后在用户机上ping该域名：



收到IP地址10.0.2.5的回复。用户机在发送DNS查询时，首先会查询自己的/etc/hosts文件，查询其中是否有该域名和IP地址的映射，如果有，就直接把该域名解析成对应的IP地址。所以当攻击者修改hosts文件时，用户机会使用攻击者指定的IP地址，容易造成信息泄露。

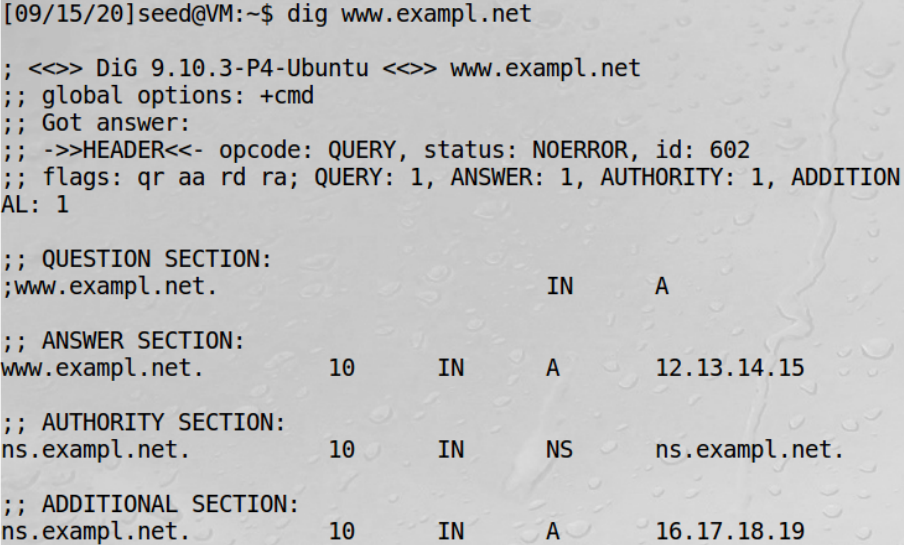
二、Task 5: Directly Spooﬁng Response to User

1、在攻击者主机上运行以下命令：



攻击者监听用户机发送的报文，当用户机发送了一个DNS查询报文，要查询域名www..exampl.net的IP地址时，攻击者主机就立刻伪造一个DNS响应报文，将该域名导向虚假的IP地址12.13.14.15。攻击者还在DNS回应中伪造了权威DNS服务器的域名和IP地址。

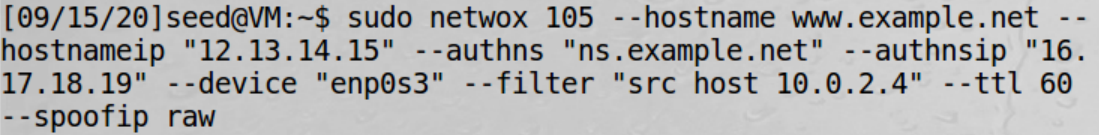
2、用户机使用dig命令，查询[www.exampl.net的IP](http://www.exampl.net的IP)地址：



可以看到，用户机收到的IP地址是12.13.14.15，为攻击者伪造的DNS响应报文中的IP地址，用户机还收到了伪造的权威DNS服务器的域名和IP地址，说明用户接受了伪造的DNS响应报文，攻击者成功实现攻击。

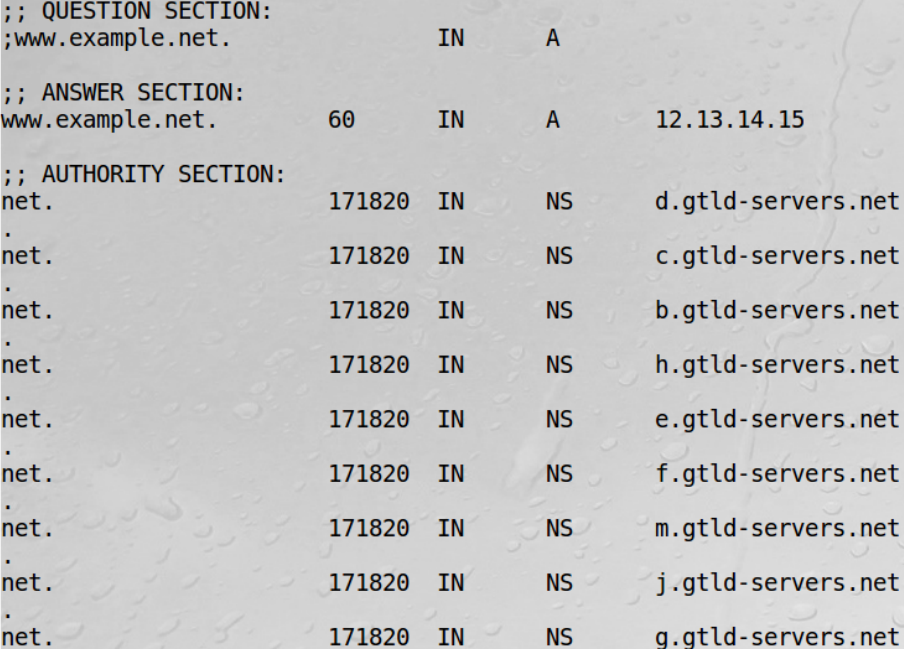
三、Task 6: DNS Cache Poisoning Attack

1、在攻击者的主机上运行以下命令：



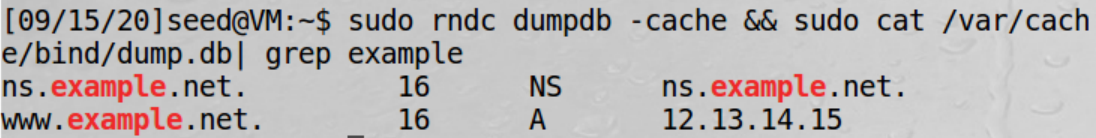
攻击者主机监听DNS服务器发送的报文，若服务器查询域名[www.example.net](http://www.example.net)，则返回伪造的DNS响应，并设置该域名对应的IP地址是12.13.14.15。

2、用户机使用dig命令，查询[www.example.net的IP](http://www.example.net的IP)地址：



可以看到，用户机受到攻击者的欺骗，返回的IP地址是攻击者设置的虚假IP地址12.13.14.15。

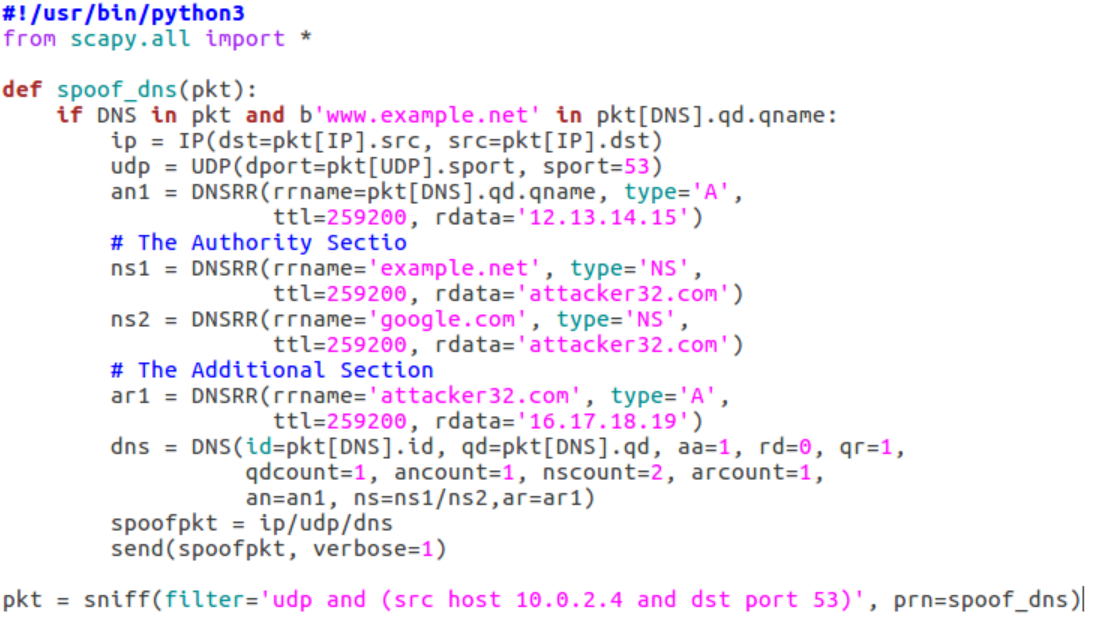
3、查看服务器的DNS缓存：



可以看到，服务器中缓存的是攻击者设置的虚假IP地址，说明服务器收到了攻击者伪造的DNS响应报文，并把它放在缓存中，即攻击者实现了DNS缓存中毒攻击。服务器在ttl内再解析该域名时都不会询问别的DNS服务器，而是直接返回缓存中的IP地址，这样攻击者可以在一段时间不再实施攻击。

四、Task 7: DNS Cache Poisoning: Targeting the Authority Section

1、在攻击者主机上运行以下代码：

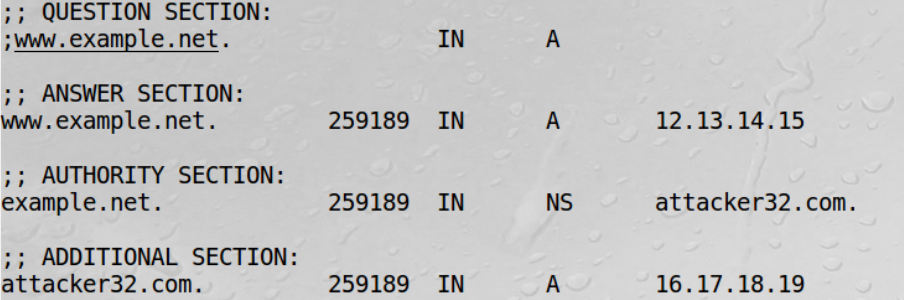


攻击者监听DNS服务器和端口53，当服务器发送一个DNS查询报文且查询的域名为[www.example.net](http://www.example.net)时，就伪造一个DNS响应发送给服务器，设定该域名对应的IP地址为12.13.14.15。同时还在Authority部分填入域名attacker32.com及对应IP地址，该响应报文被DNS服务器缓存后，DNS服务器再查询域名\*.example.net（\*代表任意前缀）时，都会询问主机attacker32.com ，只要攻击者掌握了这个域名，就可以控制用户对\*.example.net的访问。

2、清理DNS服务器的缓存：

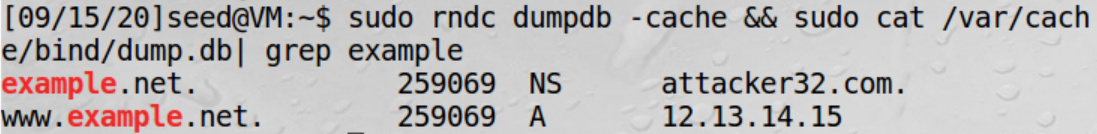


3、在用户机上先ping [www.example.net](http://www.example.net)，再使用dig [www.example.net](http://www.example.net)命令：



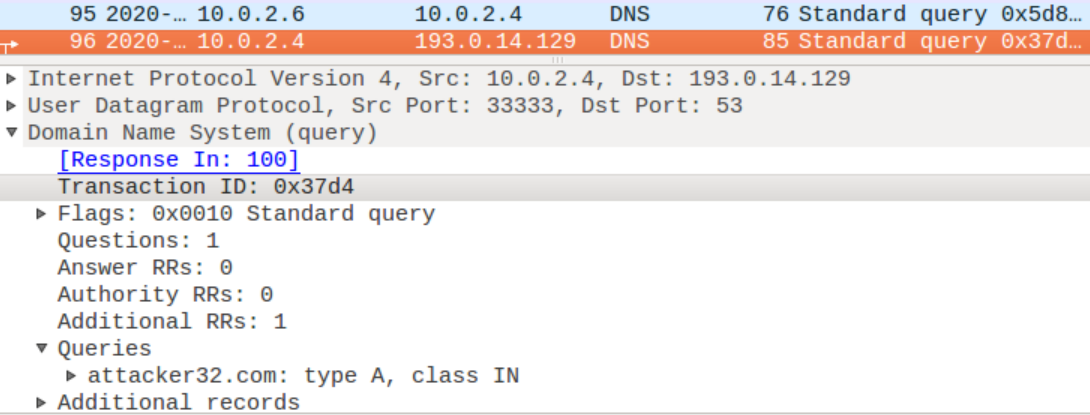
可以看到，用户机收到的回应不仅Answer部分被修改为攻击者伪造的IP地址，Authority部分也被成功伪造，即要查询\*.example.net域名，会转向服务器attacker32.com。

在服务器上查看DNS缓存：



缓存中不仅存放了[www.example.net对应的IP](http://www.example.net对应的IP)地址，还存放了域名example.net可查询的服务器。

4、打开wireshark，在用户机上执行命令ping mail.example.net：



报文95是用户机向服务器查询域名mail.example.net的IP地址。报文96是DNS服务器查询域名attacker32.com的IP地址，即服务器按照DNS缓存里的内容想要解析attacker.com的IP地址。如果攻击者控制了域名attacker32.com，就可以将用户对\*.example.net的访问导向特定主机，从而获取用户隐私。