TASK1

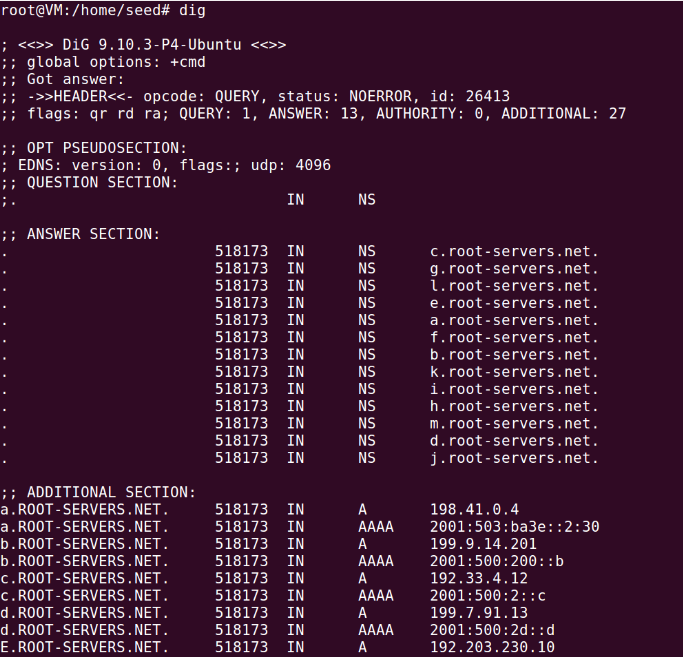
通常通过修改/etc/resolv.conf可以将自定义的localDNS服务器添加到本地环境，但是DHCP协议会动态分配localDNS服务器并覆盖自定义的local DNS服务器。但是我们可以通过修改/etc/resolvconf/resolv.conf.d/head来解决DHCP动态分配localDNS的问题。



执行sudo resolvconf -u命令使上述修改生效



执行dig获取localDNS的信息

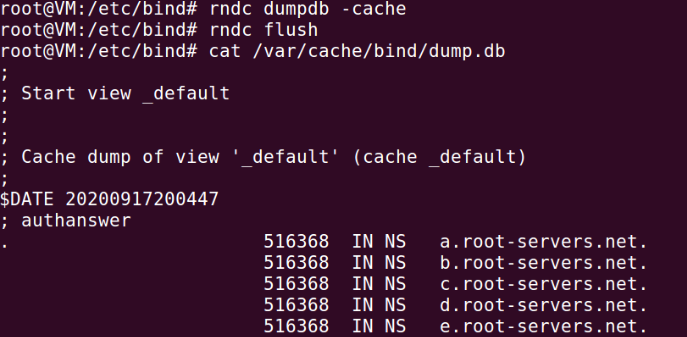


TASK2

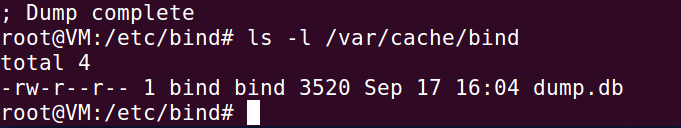
从/etc/bind/named.conf文件获取其配置信息。named.conf文件有很多”include”项，其中有一项是/etc/bind/named.conf.options，我们通常在这个文件中配置我们的自定义信息。往options文件中添加名为dump-file的项



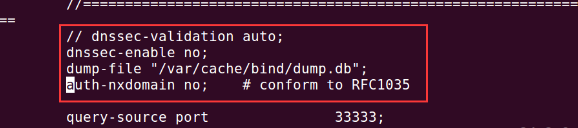
上述设置指明cache缓存应该被保存在哪个文件。通过执行rndc dumpdb -cache命令可以将cache保存到我们刚刚指定的文件中；通过rndc flush命令可以清除cache



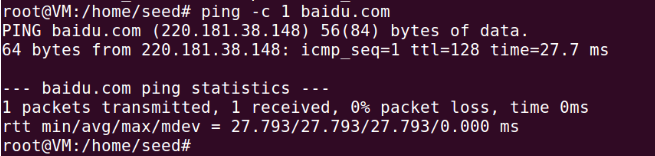
发现cache保存成功



关闭DNSSEC



Ping百度

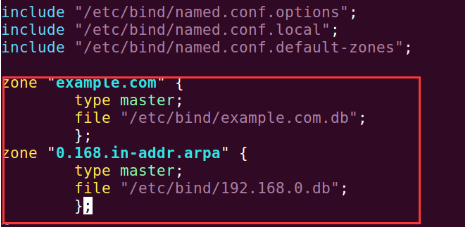




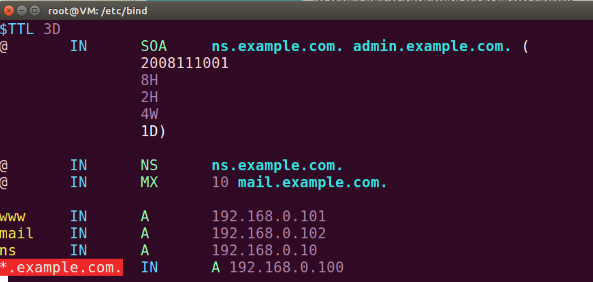
抓包发现配置成功

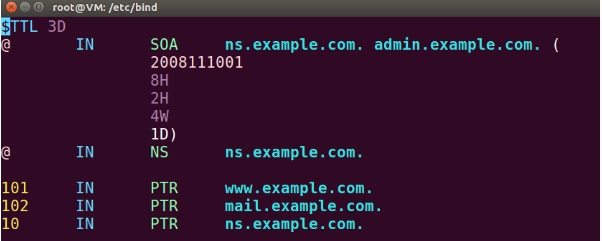
TASK3

修改/etc/bind/named.conf

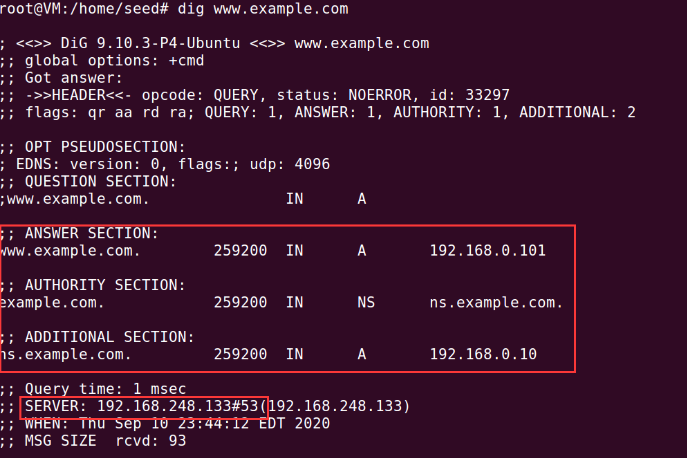


从官网下载example.com.db文件





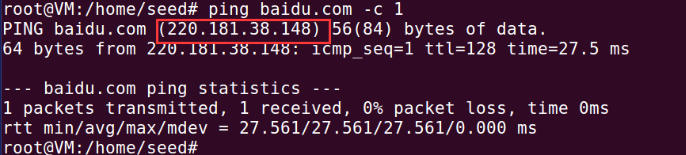
重启BIND，然后dig [www.example.com](http://www.example.com)



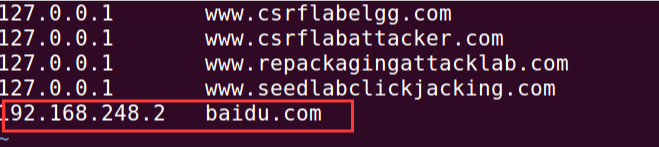
成功得到local DNS的返回结果。

TASK4

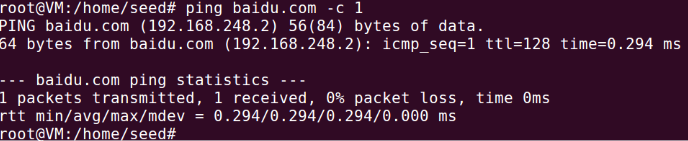
修改/etc/hosts文件之前



修改/etc/hosts



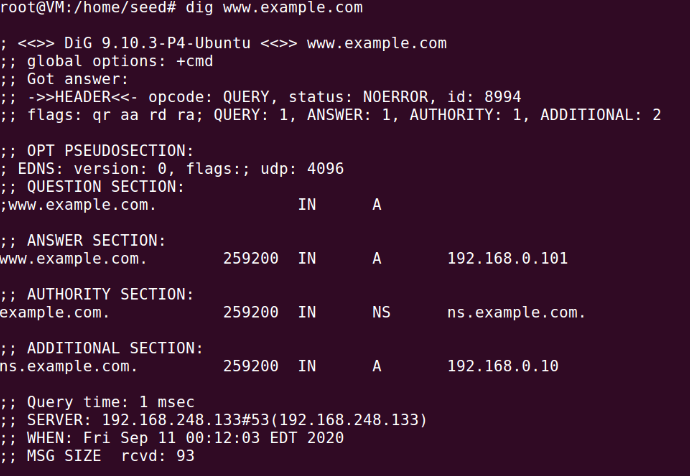
重新pingbaiduc.om



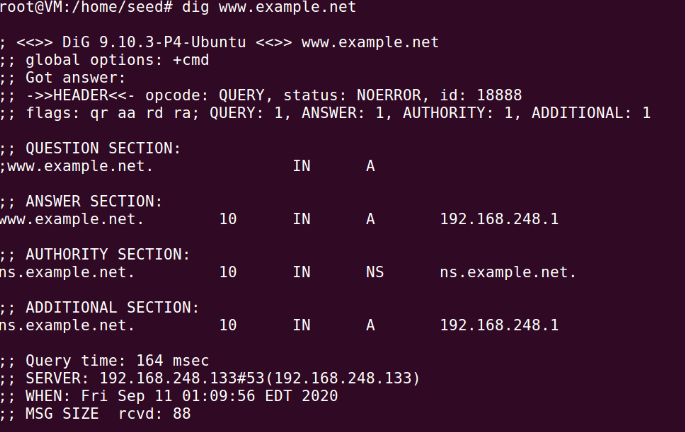
映射的ip被修改

TASK5

攻击者可以在受害者和localDNS所处的局域网中进行中间人攻击在未进行攻击之前，digwww.example.com



使用netwox进行监听和伪造数据包

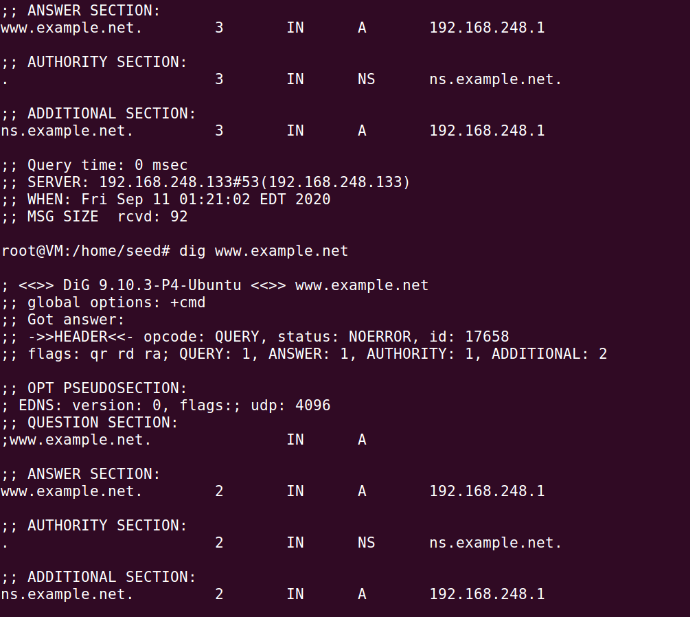


[www.example.com被映射到192.168.248.1](http://www.example.com被映射到192.168.248.1)

TASK6

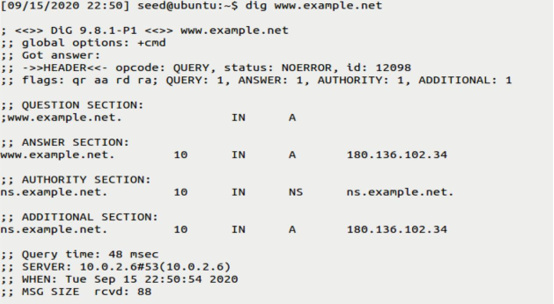


将污染对象设置为local DNS，并将spoofip字段设为raw

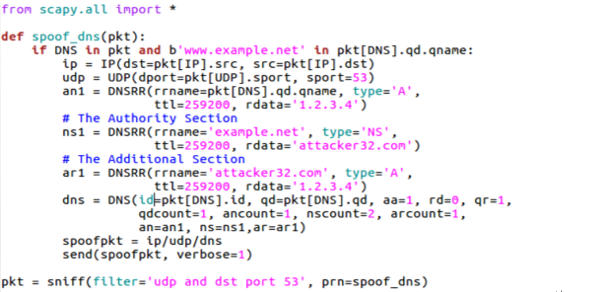


在ttl内多次dig www.example.net查询到的都是被污染后的信息。

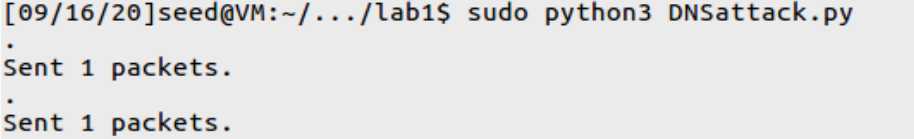
TASK7



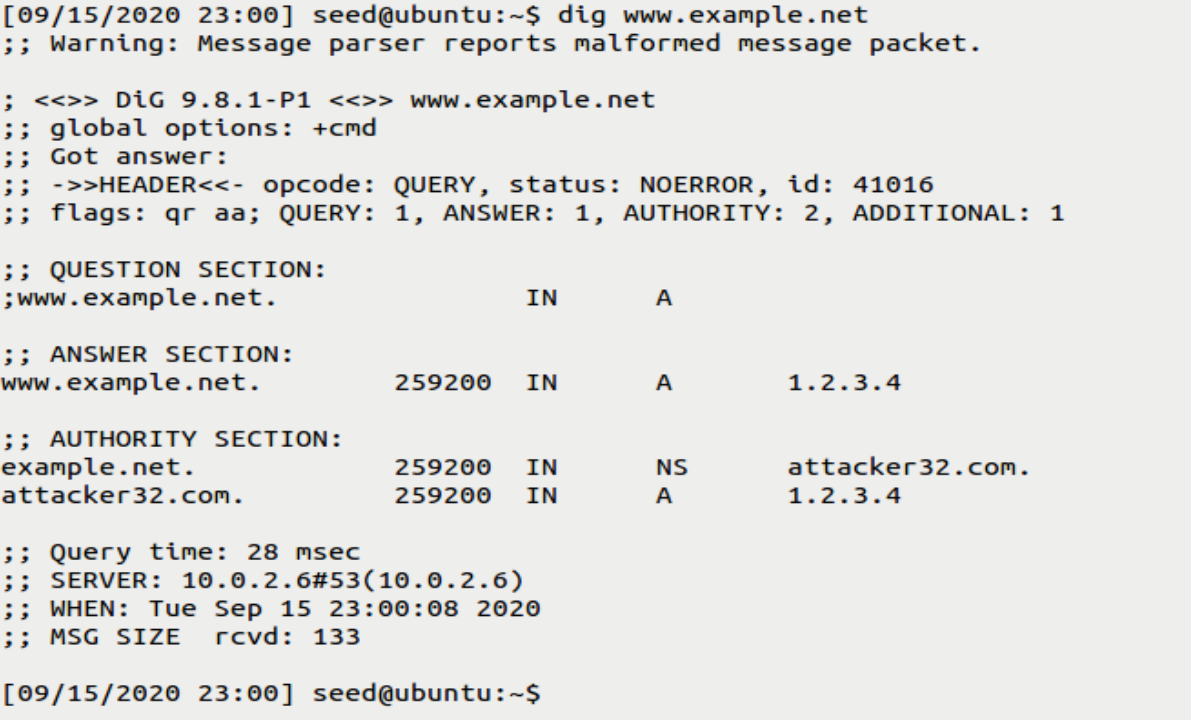
编写的攻击代码



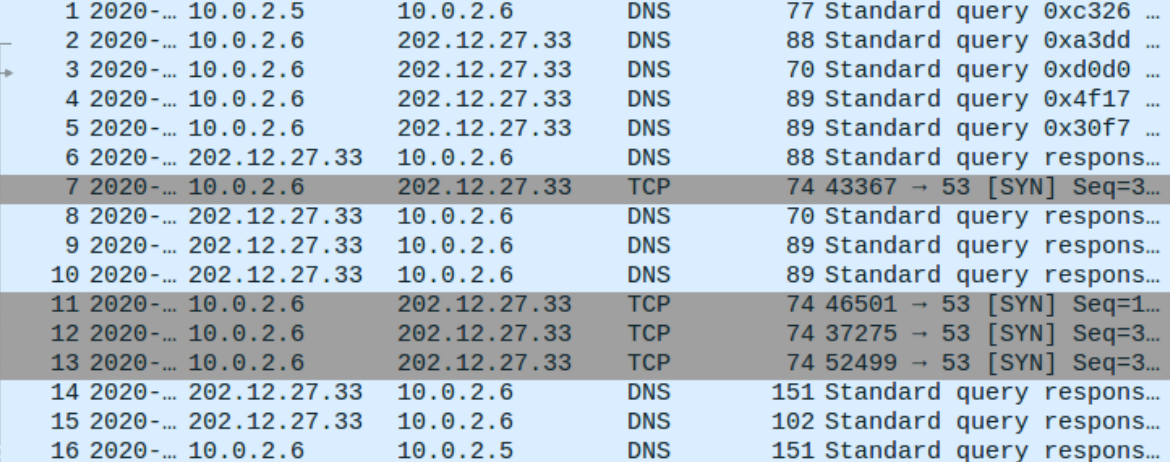
攻击者运行攻击代码



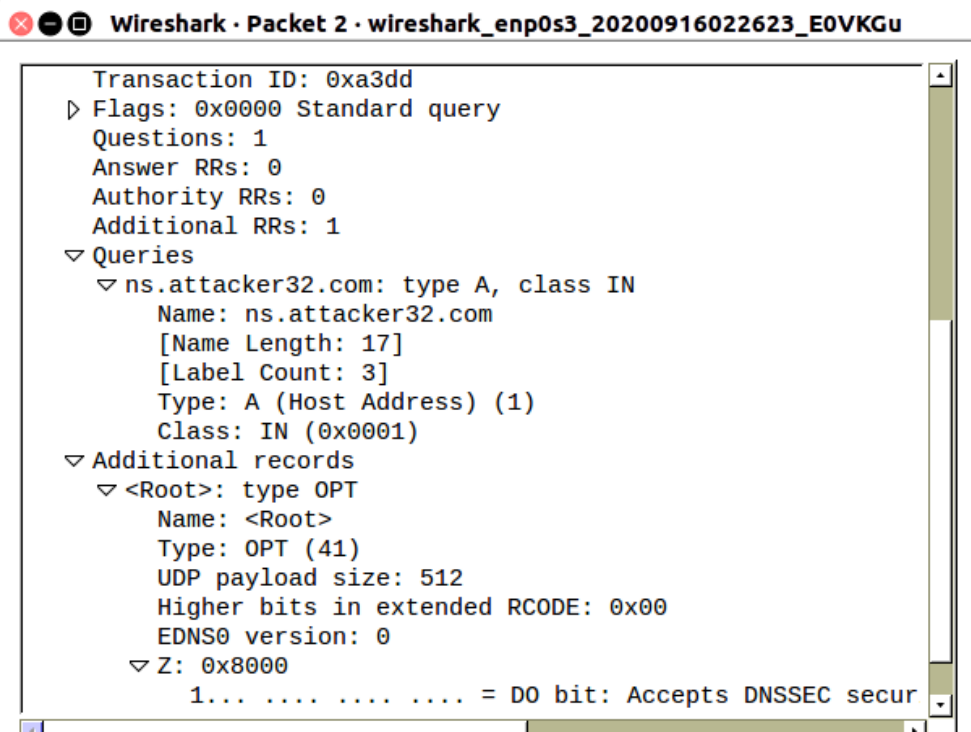
同时，在VM B处查询www.example.net的IP地址，可以看到此时在AUTHORITY SECTION中，对于所有example.net下的域名，都需要查询attacker32.com这个域名服务器。www.example.net最终返回的查询结果为攻击者自定义的IP地址1.2.3.4。



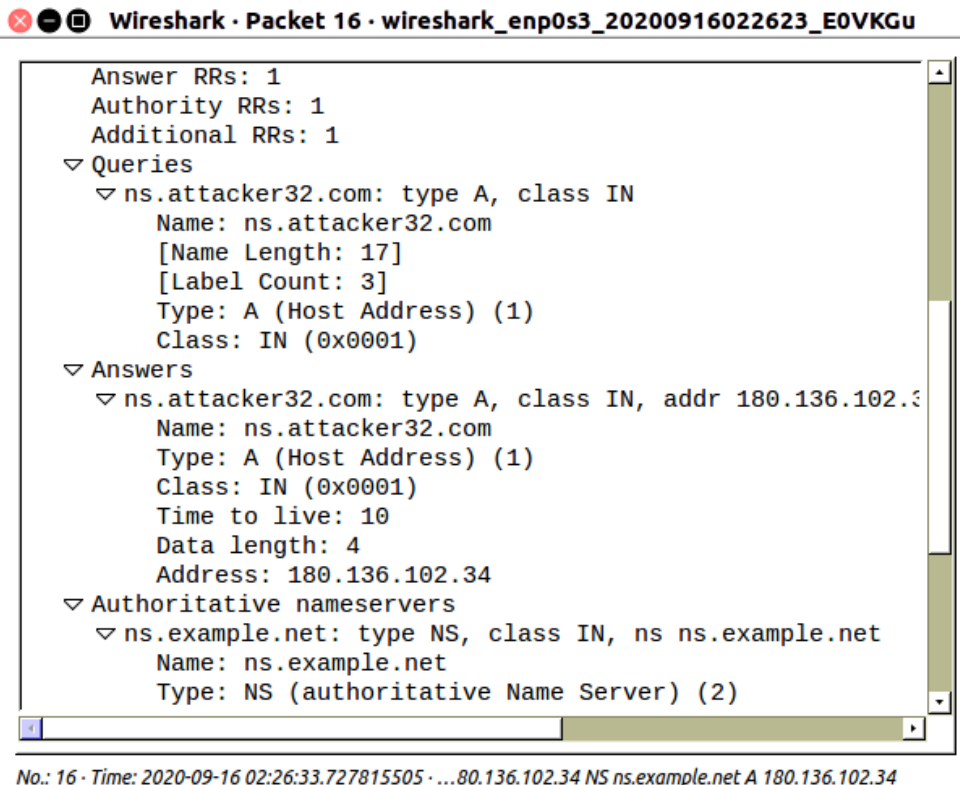
在用户主机VM B上用wireshark抓包，结果如下图所示：



可以看到，用户VM B（10.0.2.5）首先向本地DNS服务器（10.0.2.6）发送一个DNS查询报文（报文1），但是本地DNS服务器无法解析，所以DNS服务器向IP地址为202.12.27.33的DNS服务器发送一个DNS查询报文（报文2），在报文中询问ns.attacker32.com的IP地址。



在检测到报文2来自于本地DNS服务器时，攻击者立马伪装一个DNS响应报文（报文6），本地DNS服务器将响应结果返回给用户主机10.0.2.5（报文16）。报文16的内容如下图所示：



从以上抓包结果可知，对于所有example.net下的域名，都需要查询attacker32.com这个域名服务器。攻击成功。