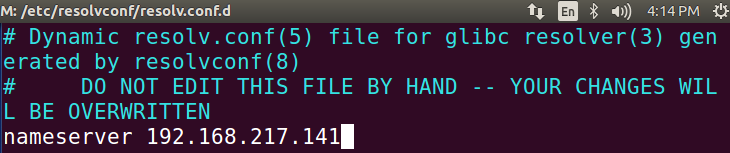
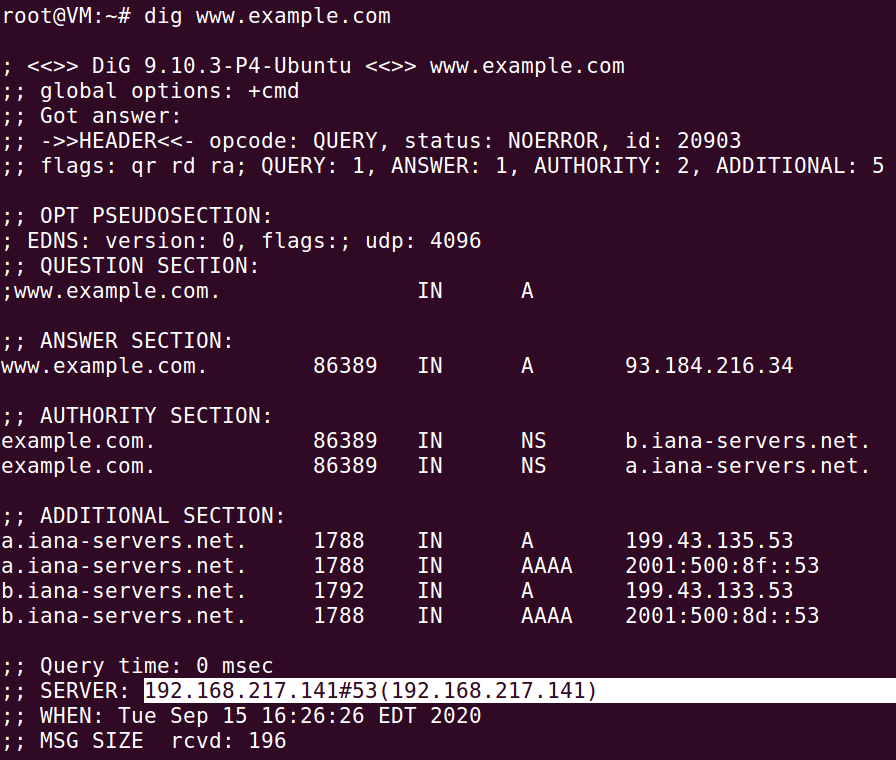
# Local DNS Attack Lab

**Setting Up a Local DNS Server**

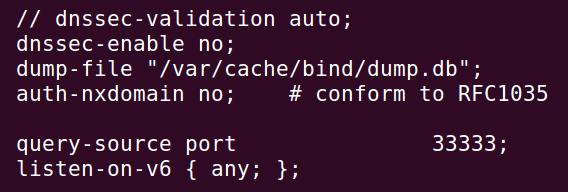
在本实验中，设置用户VM为192.168.217.140，服务器VM为192.168.217.141，攻击者VM为192.168.217.141。

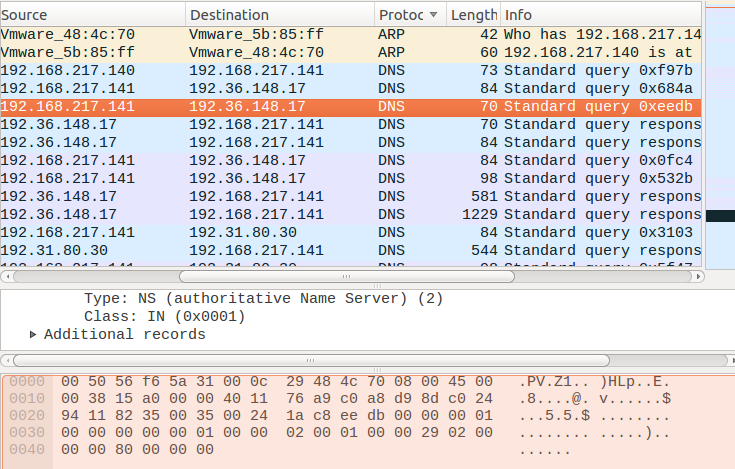
用户VM在/etc/resolvconf/resolv.conf.d/head文件中添加服务器VM的地址，可以看到DNS请求的服务器已经被设置为192.168.217.141。



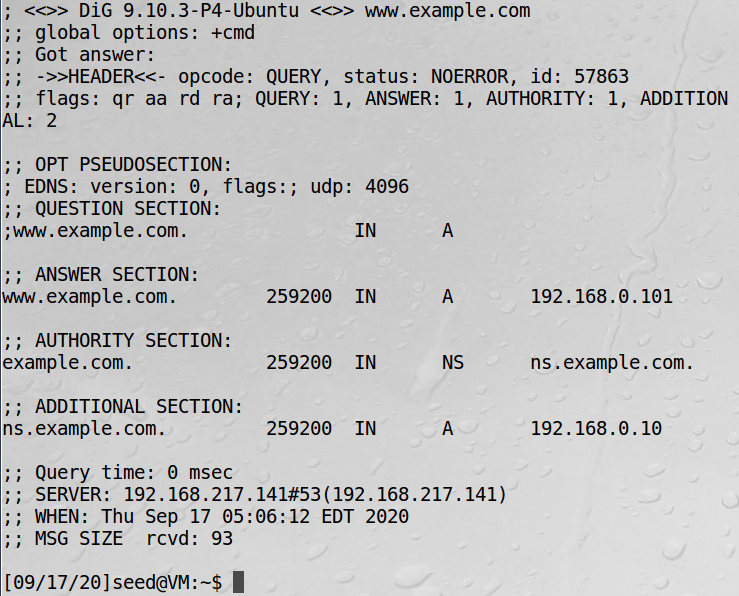


设置DNS服务器，使用ping命令并抓包，可以看到服务器VM正在承担DNS服务器的功能。



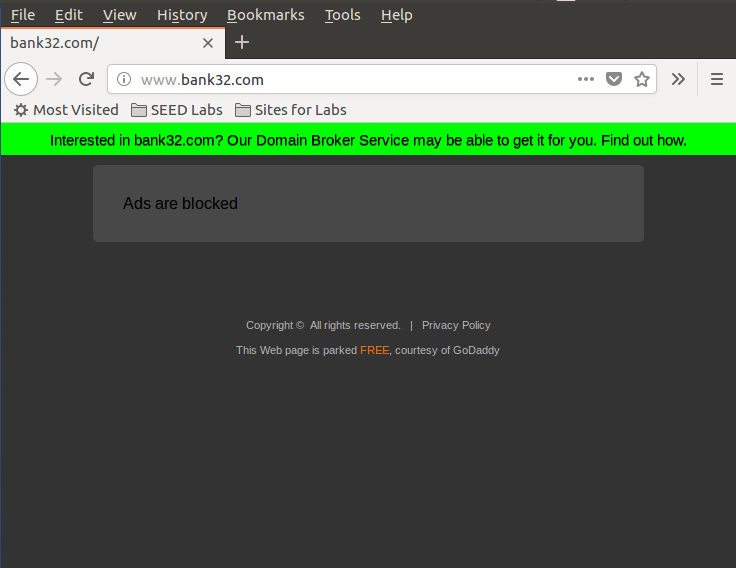


在DNS服务器上创建一个域，解析example.com，正常情况下用户解析的结果如下。

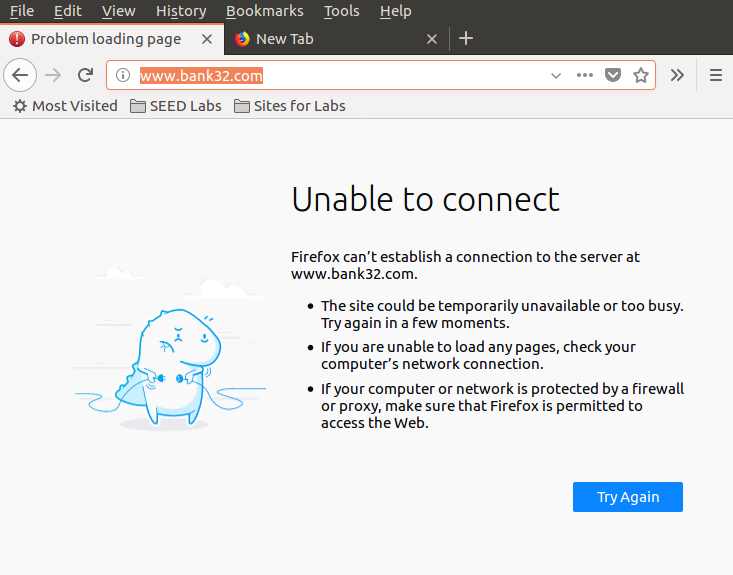


**Lab Tasks (Part II): Attacks on DNS**

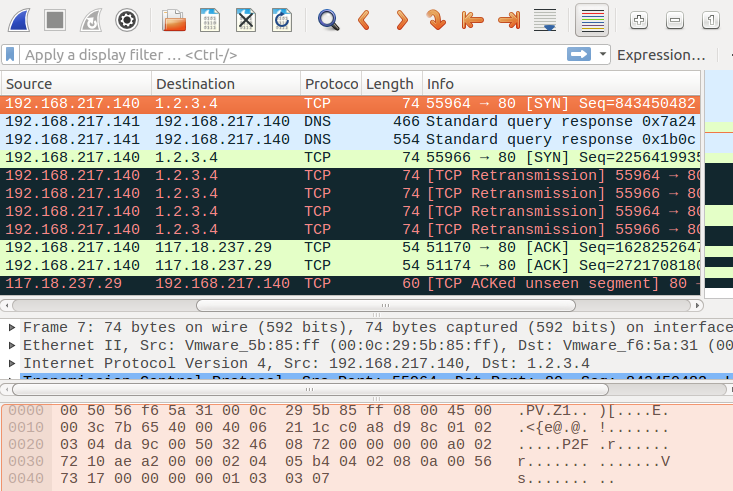
修改DNS服务器的HOSTS文件，使得[www.bank32.com](http://www.bank32.com)的解析地址更改为1.2.3.4，更改前后使用浏览器访问如下。





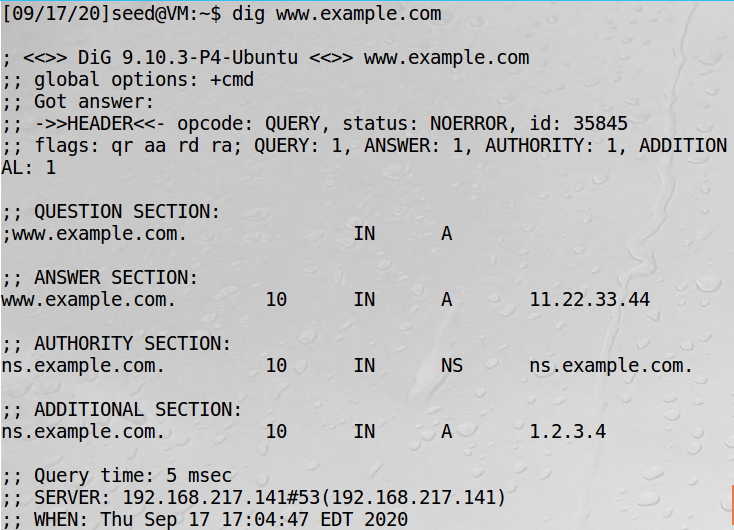


可以看到服务器正尝试向[www.bank32.com的IP](http://www.bank32.com的IP)地址，即缓存中记录的地址1.2.3.4发送请求。

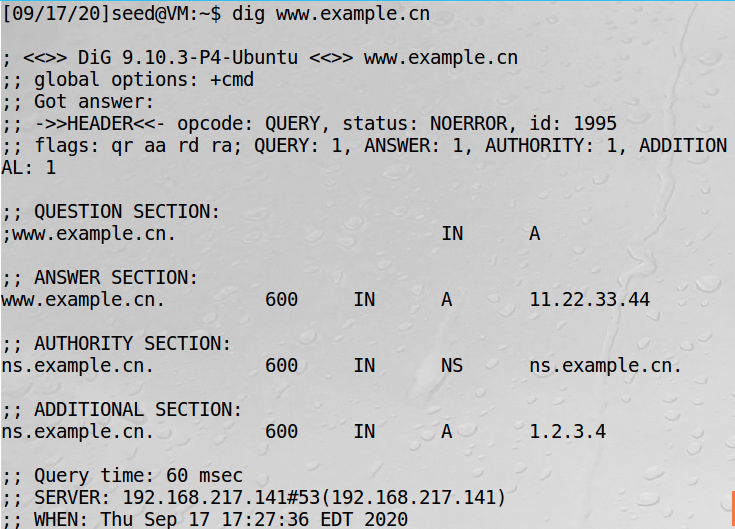
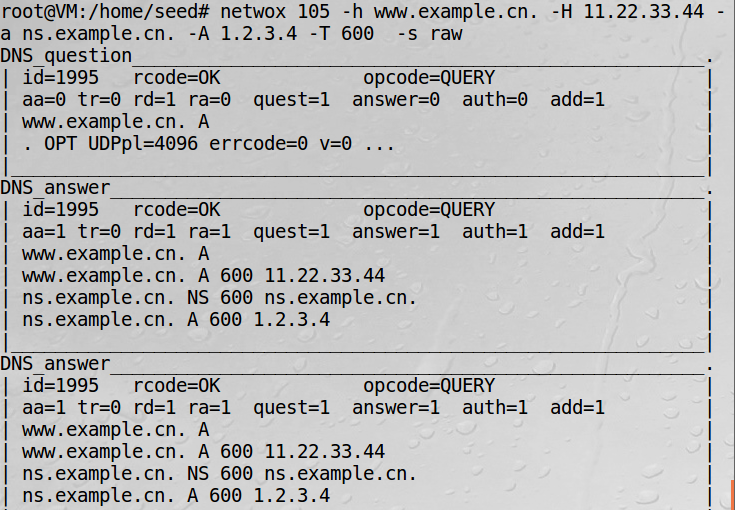


在攻击者VM中使用netwox 105对用户进行DNS回应欺骗，使得用户的解析结果如图所示。





攻击者对DNS服务器进行欺骗，伪造了[www.example.cn](http://www.example.cn)的回复。用户解析结果如图所示。



使用SCAPY构造DNS报文实现Authority Section的欺骗，可以看到映射已经被改为attack32.com。

