网络与信息安全课内实验报告

Host文件与DNS投毒

### 本次实验目的

1. 了解 host 文件和 DNS 系统的关系。

2. 使用 DNS 攻击工具进行 DNS 投毒，观察攻击情况，了解 DNS 攻击原理。

3. 了解资源记录并对MX资源记录类型进行观测；

4. 通过命令行直接向SMTP服务器投递邮件。

### 实验过程及分析

###### 了解Hosts文件

### Hosts是一个没有扩展名的系统文件，主要作用是定义IP地址和主机名的映射关系。当用户在浏览器中输入一个需要登录的网址时，系统会首先自动从Hosts文件中寻找对应的IP地址，一旦找到，浏览器会立即打开对应网页，如果没有找到，则浏览器会将网址提交DNS服务器进行IP地址解析。Hosts文件可以用文本打开，修改Hosts文件可以绕过DNS为域名指定IP地址。

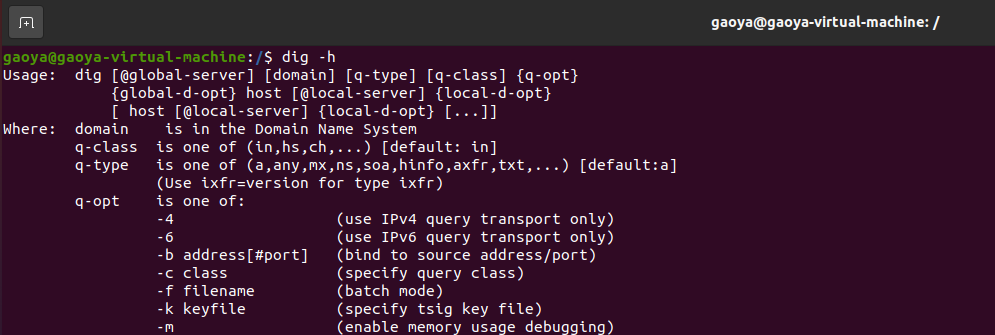
### 

www.google.com成功解析到了127.0.0.1

###### 使用 dig 工具查看网站域名解析过程

dig是一个在类Unix命令行模式下查询DNS包括NS记录，A记录，MX记录等信息的工具

查看 dig 命令用法：

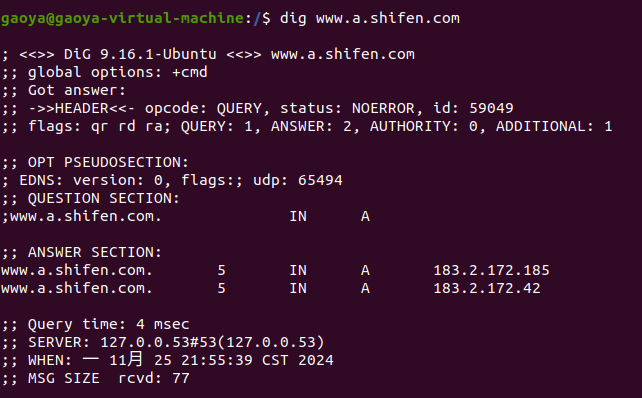


使用dig名称解析www.baidu.com：



结果显示，www.baidu.com有一个CNAME记录， CNAME 表示查询 www.baidu.com 的信息其实是 www.a.shifen.com 返回的 A 记录； 有两个A记录，即两个IP地址。

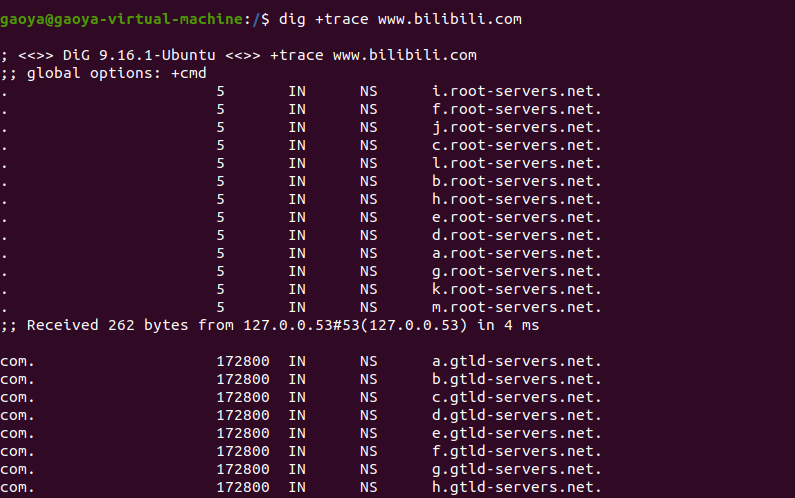
继续查询www.a.shifen.com，获取最后的IP地址：



使用 dig +trace 命令，查看www.bilibili.com完整的解析过程：

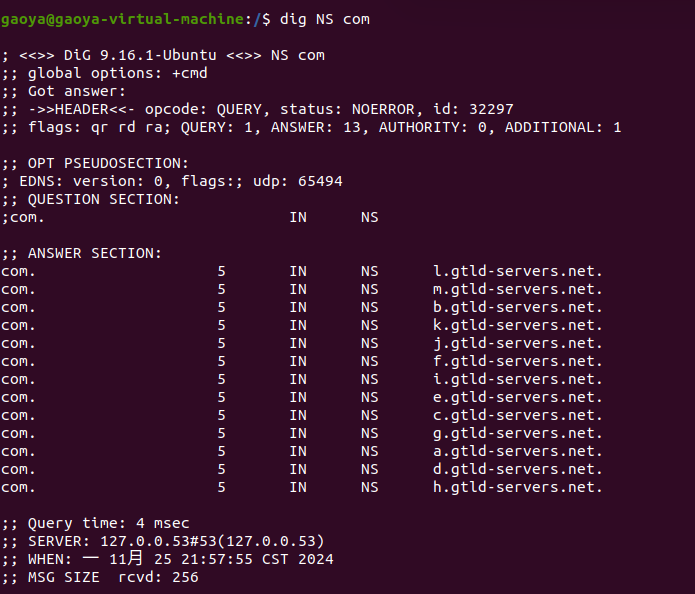
dig +trace命令返回的内容是DNS解析过程中所有经过的DNS服务器和域名路径，每个DNS服务器的IP地址、DNS记录类型、TTL、DNS记录值等信息都会被列出来。

第一步，查询 root 根服务器



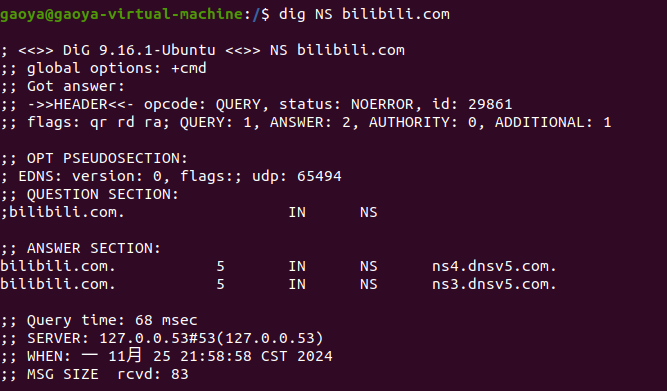
". IN NS"查询返回了根服务器的NS记录，告诉DNS客户端应该去.com服务器查询

第二步，查询.com 服务器



"com. IN NS"行从根服务器获取了.com顶级域的NS记录

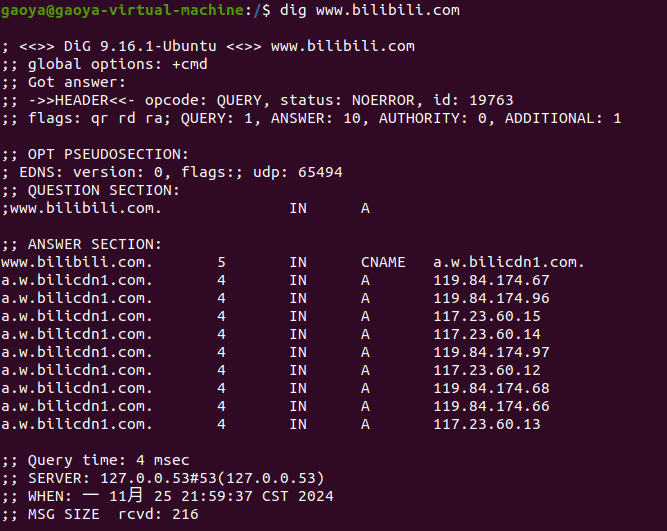
第三步，查询 bilibili.com 服务器



从.com服务器获取bilibili.com的NS记录

bibili.com一共有2个NS解析结果，分别是：ns4.dnsv5.com.，ns3.dnsv.com.

第四步，查询 www.bilibili.com 服务器地址



从bilibili.com的NS服务器获取www.bilibili.com的CNAME和A记录，最终解析出IP地址

###### DNS 投毒实验

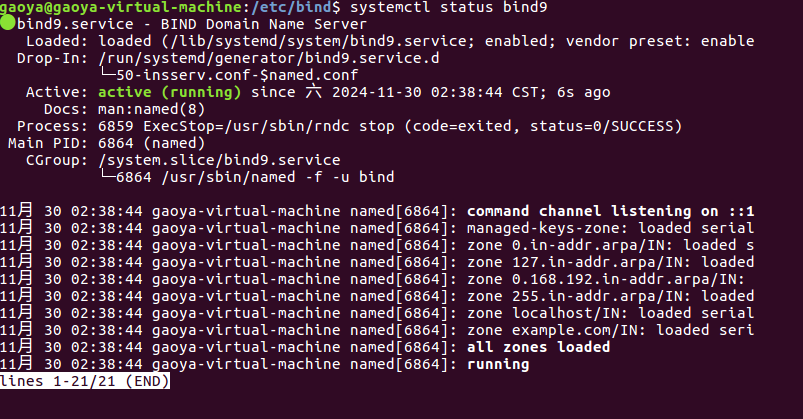
攻击原理：客户机在域名查询时, 若在本地缓存中未找到对应的IP地址, 便会向本地DNS服务器发送DNS请求报文(使用 dig 命令时不会检查本地缓存), 请求该域名对应的IP地址, 然后本地DNS服务器对该请求进行响应, 发送给客户机DNS响应报文。攻击机通过伪造本地DNS服务器给客户机的DNS响应报文, 以达到使用错误的IP地址欺骗客户机为查询域名的IP地址。由于需要伪装成本地DNS服务器的响应报文, 因此在客户机查询需要本地DNS服务器向DNS系统查询且等待时间较长的外网域名时, 更容易攻击成功。

1. 配置DNS服务端：

按照实验步骤配置完成后，执行dig [www.example.com](http://www.example.com)查看



刷新DNS缓存，然后重启DNS服务器，将DNS数据导出并查看初始状态

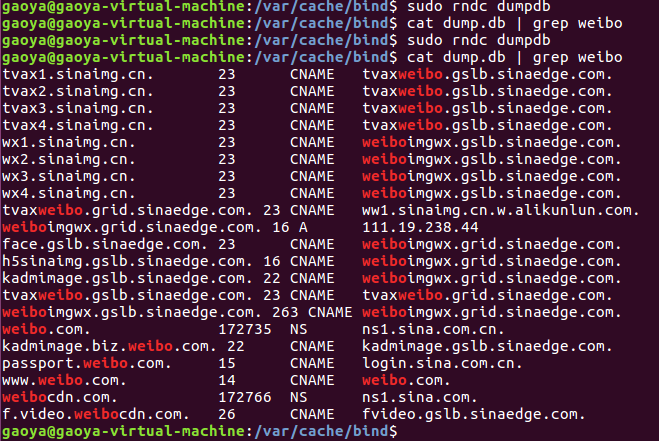


1. 配置Ubuntu攻击端

在Ubuntu服务端进行IP地址查询 192.168.217.133

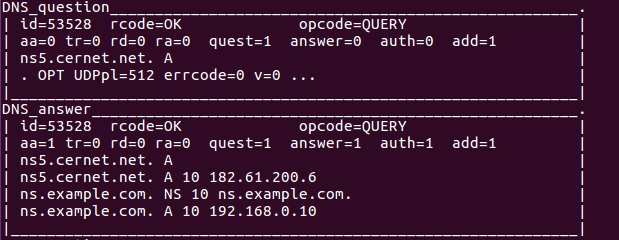


用浏览器访问[www.weibo.com](http://www.weibo.com)，再回到Ubuntu服务端，重新使用rndc生成日志记录

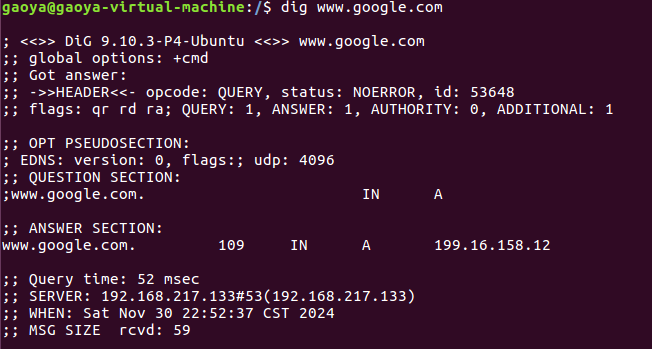


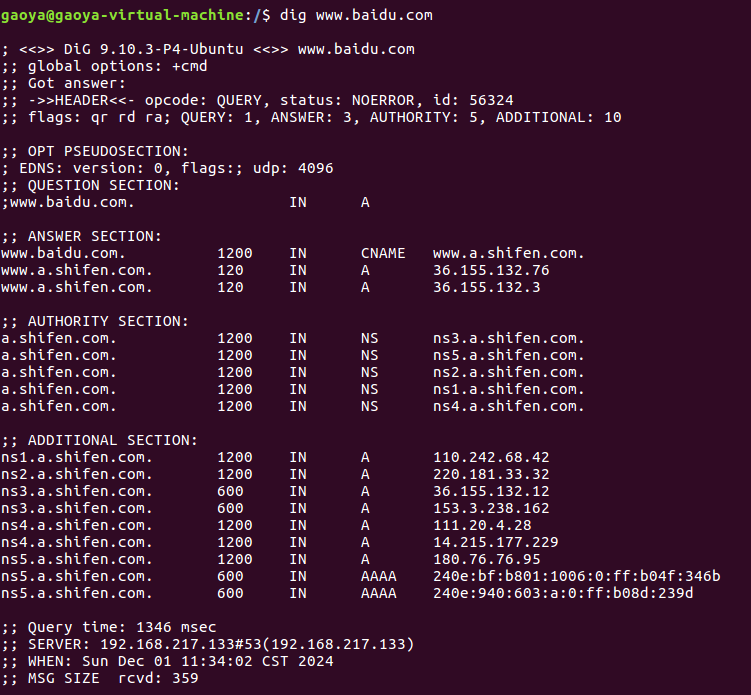
执行sudo netwox 105 --hostname "www.baidu.com" --hostnameip 182.61.200.6 --authns "ns.example.com" --authnsip 192.168.0.10 --filter "src host 192.168.217.133"

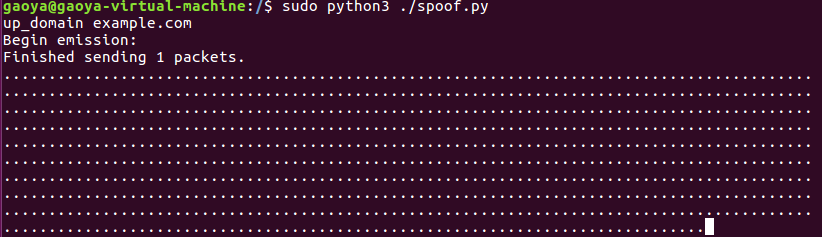
Ubuntu攻击端显示如下

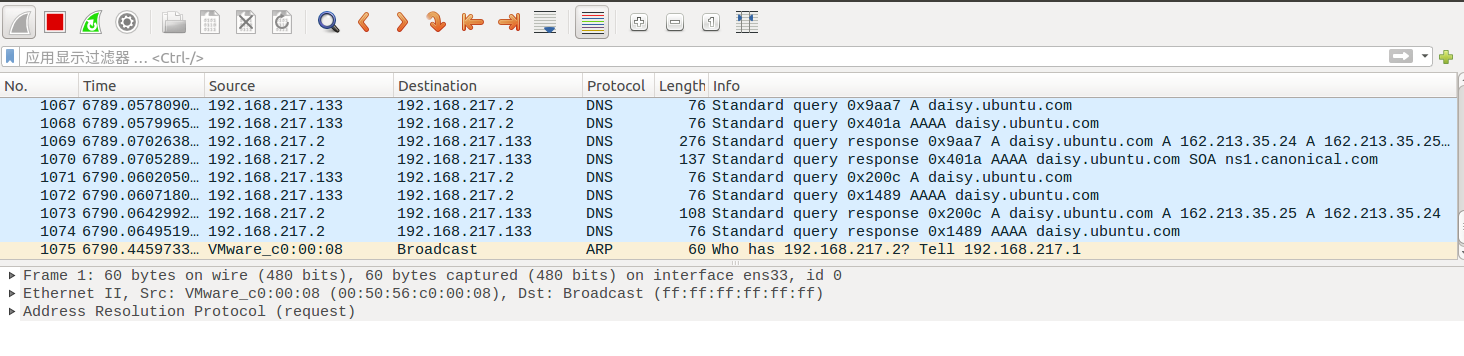


在**Ubuntu测试机**上分别先后执行dig [www.google.com](http://www.google.com) 和dig [www.baidu.com](http://www.baidu.com)





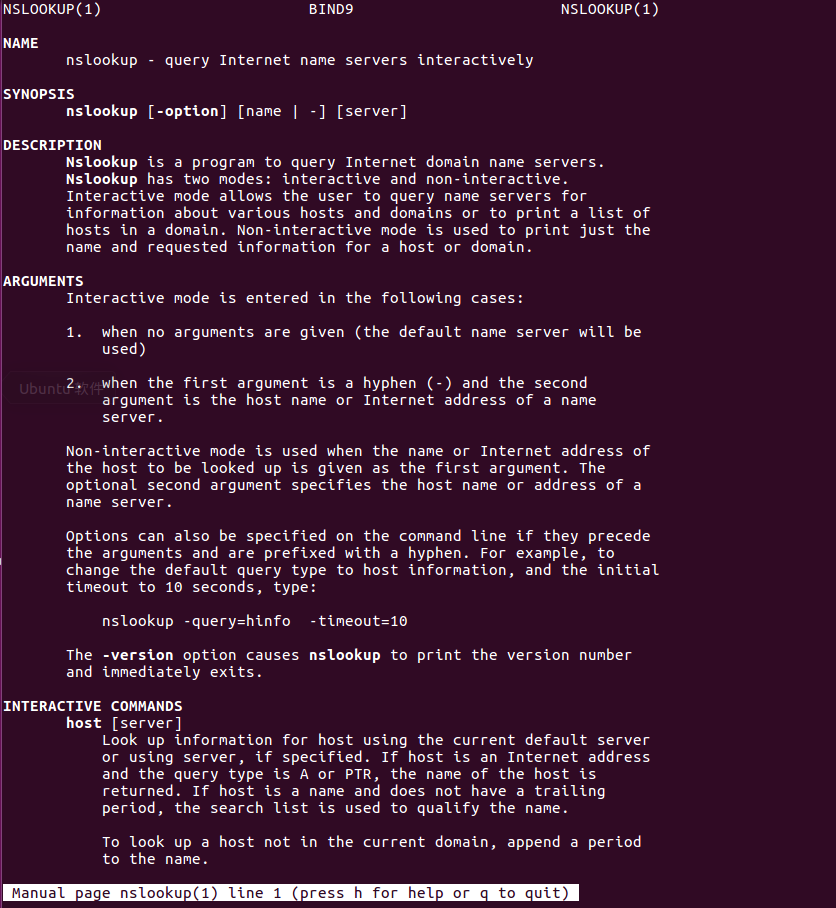


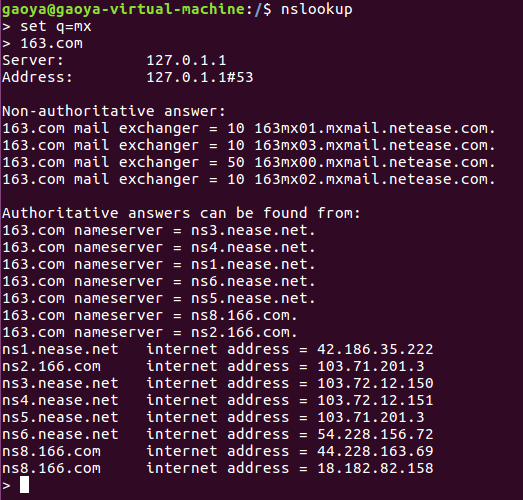


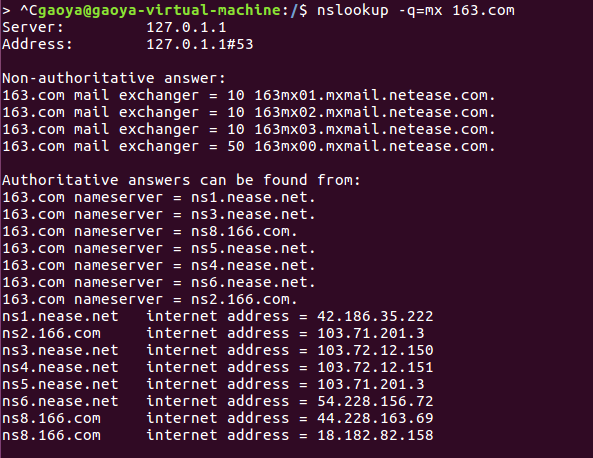
###### 使用nslookup工具对MX记录进行观测

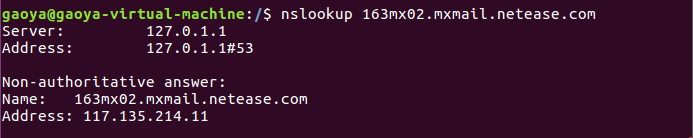
查看nslookup命令使用方法

man nslookup









###### 向SMTP服务器投递邮件实验





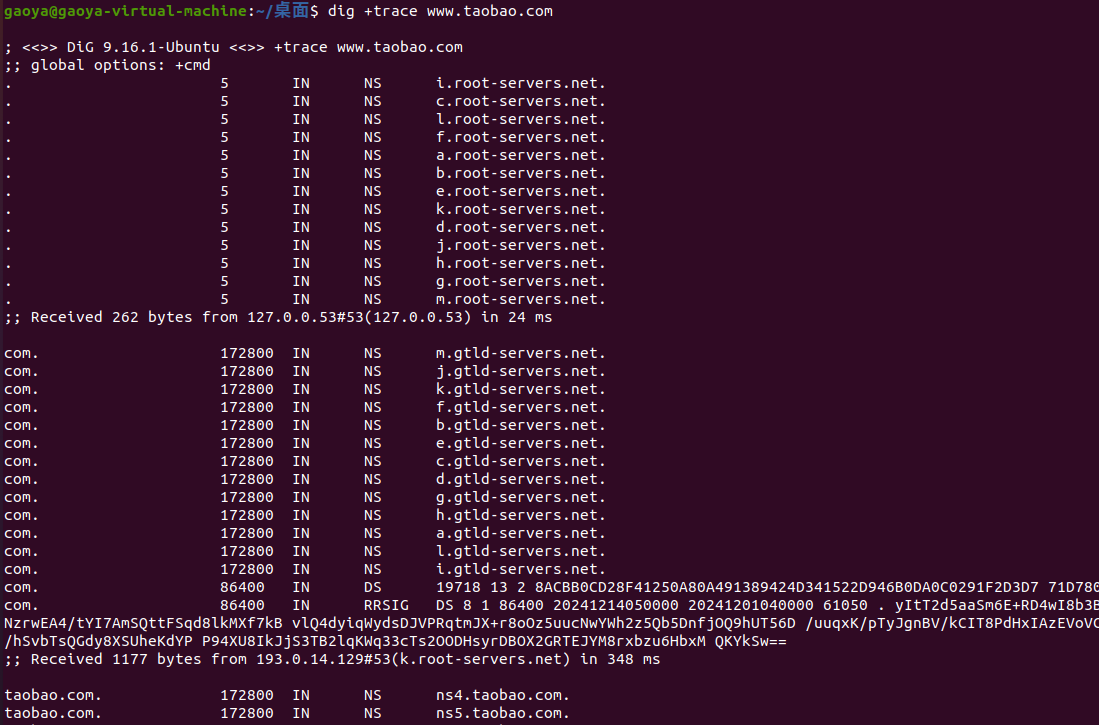




### 使用dig+trace解析另一个域名

域名：www.taobao.com

使用dig +trace www.taobao.com进行解析。

过程解释：

根服务器查询：首先查询根服务器，获取.com域的顶级域名服务器地址。

顶级域名服务器查询：查询.com域服务器，获取taobao.com的权威域名服务器地址。

权威域名服务器查询：查询taobao.com的权威服务器，获取www.taobao.com的IP地址。

结果：成功解析出www.taobao.com的IP地址。

### 遇到的困难及解决方式

1.困难：

sudo apt install apache2安装时显示网络不可达，无法发起与 mirrors.tuna.tsinghua.edu.cn:80 (2402:f000:1:400::2) 的连接

解决方式：

ubuntu16 自带的源有问题，编辑/etc/apt/sources.list文件，文件开头添加其他源

2.困难：

sudo netwox 105 -h "www.baidu.com" -H "182.61.200.6" -a "ns.example.com" -A "192.168.0.10" -f "src host 192.168.217.133" -d ens33命令无响应

解决方式：

修改为sudo netwox 105 --hostname "www.baidu.com" --hostnameip 182.61.200.6 --authns "ns.example.com" --authnsip 192.168.0.10 --filter "src host 192.168.217.133"

3.困难：

执行程序时显示ERROR: Loading module scapy.layers.mspac

解决方式：

Ubuntu16.04默认使用Python 2.7，而安装的scapy可能不再支持Python 2

安装Python3.5和pip3，再安装scapy

4.困难：

在应用程序启动wireshark抓包无权限，但在终端使用sudo启动后，终端被wireshark占用，无法再输入命令执行投毒程序

解决方式：

添加用户组，给与普通用户权限