**Lab5实验报告**

57117138 吴伊杰

**Local DNS Attack Lab**

# Task 1: Configure the User Machine

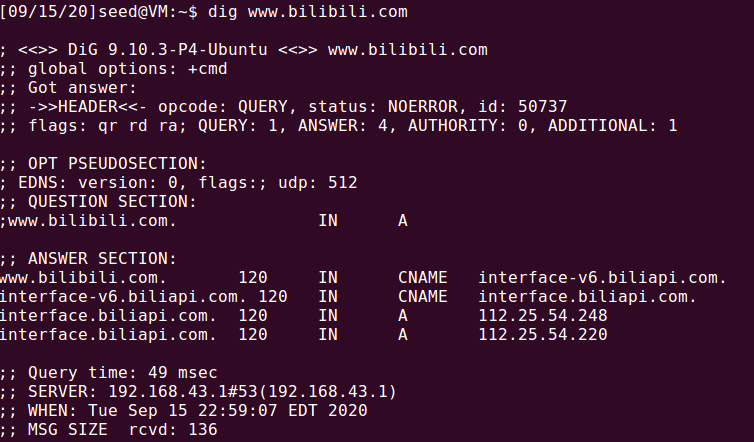
三台虚拟机的IP地址配置如下：

攻击者 192.168.43.115

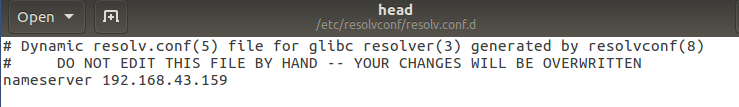
服务器 192.168.43.159

用户机 192.168.43.123

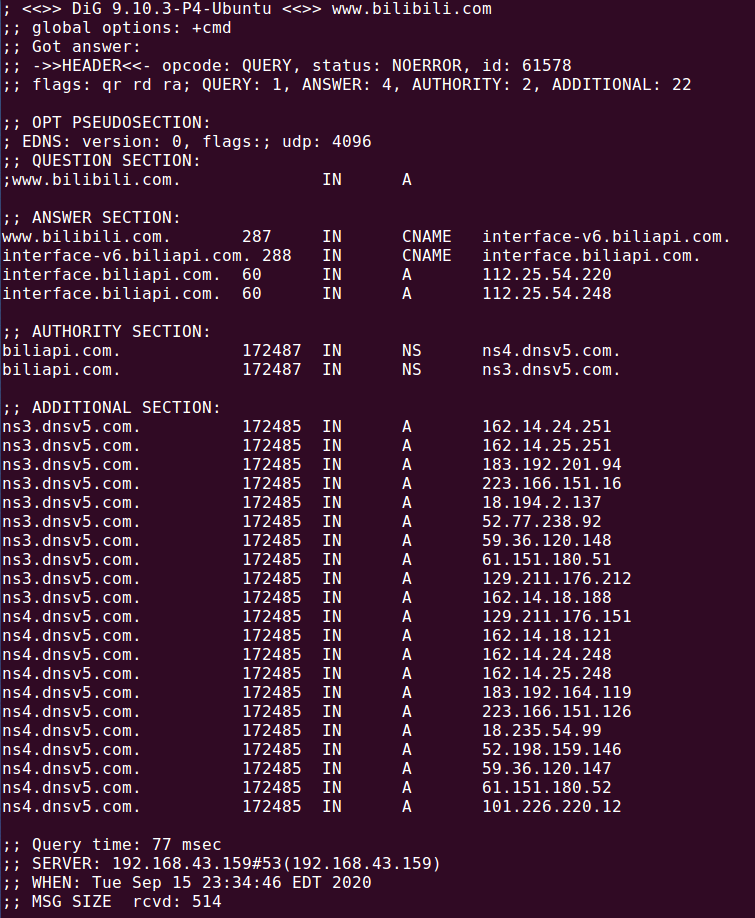
首先在未进行配置的用户机上尝试dig操作：



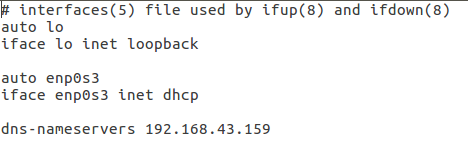
然后根据手册提供的路径去修改配置文件



再次执行dig指令，SERVER被修改为服务器的IP地址



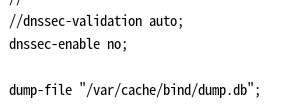
但是这样修改的话，重启之后修改的文件就会被覆盖掉，解决此问题有很多办法，这里采取直接修改/etc/network/interfaces文件配置DNS的办法：



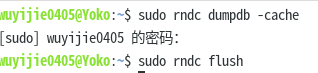
效果同上。

# Task 2: Set up a Local DNS Server

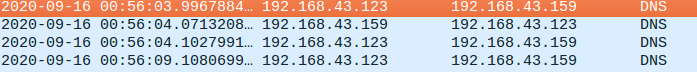
按照手册修改/etc/bind/named.conf.options文件



重启BIND 9服务器



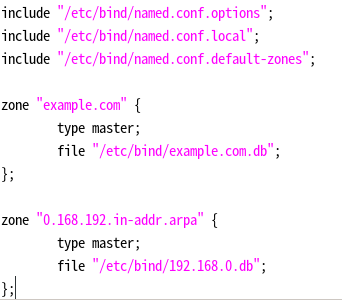
使用ping指令进行测试，用wireshark进行观察：



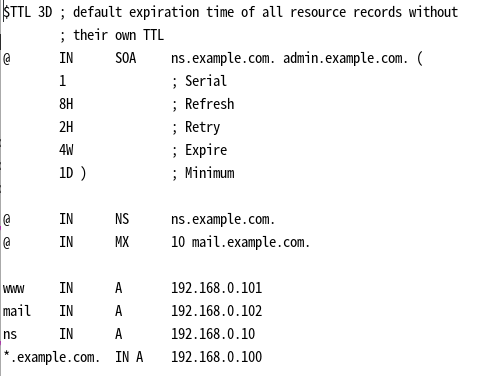
发现用户机会先向DNS服务器查询

# Task 3: Host a Zone in the Local DNS Server

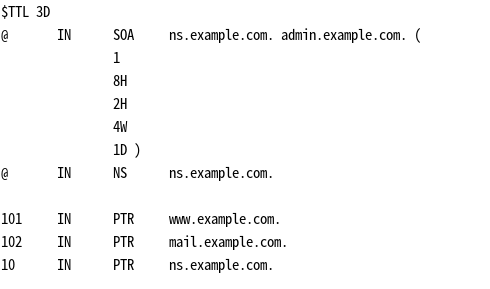
创建zones：在/etc/bind/named.conf文件中添加手册所给内容



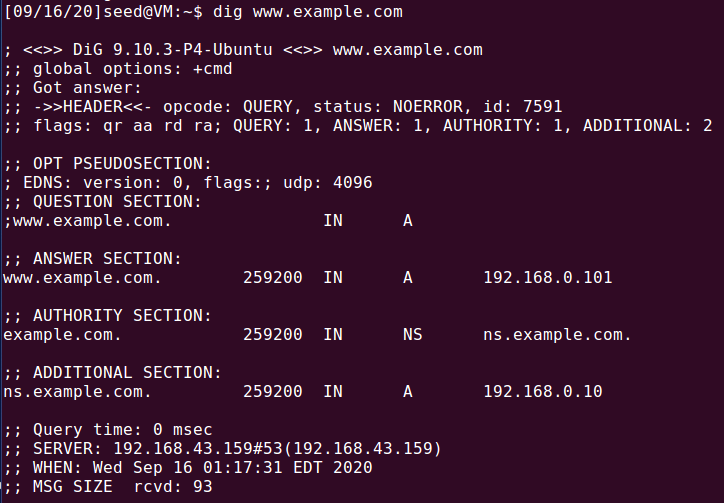
创建example.com.db文件：



创建192.168.0.db文件：



相关配置完成后，在用户机中用dig [www.example.com](http://www.example.com)命令测试，发现相关配置信息变化：



# Task 4: Modifying the Host File

先尝试ping [www.example.com](http://www.example.com)，注意到其IP地址为192.168.0.101



修改/etc/hosts文件，改变此网址的指向IP

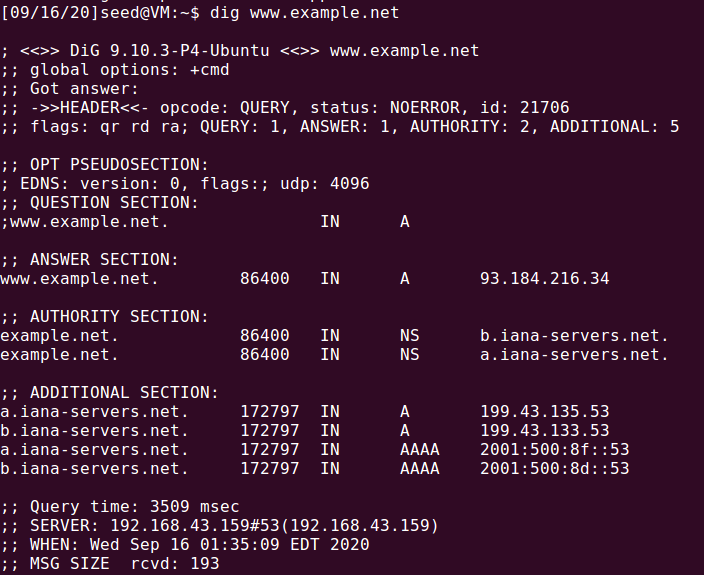


此时再次ping该网址，发现其IP变为1.2.3.4



# Task 5: Directly Spoofing Response to User

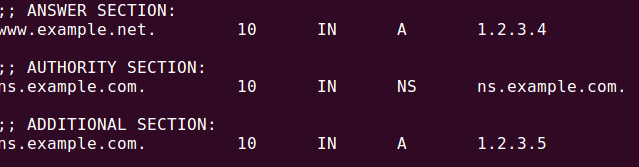
在攻击前dig [www.example.net](http://www.example.net)，其IP为93.184.216.34



然后构造指令



运行该攻击指令，再次令用户机dig www.example.net，其IP被改写为我们指定的地址

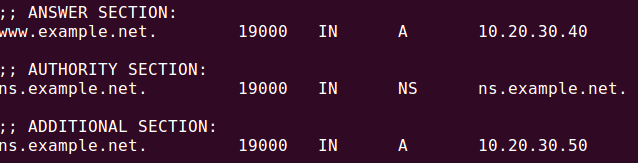


# Task 6: DNS Cache Poisoning Attack

构造指令如下：



攻击结果：

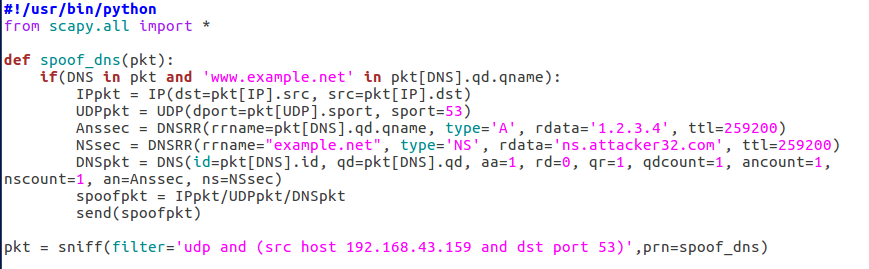


通过如下两个指令可以查看缓存



# Task 7: DNS Cache Poisoning: Targeting the Authority Section

利用scapy包按照如下脚本执行：



清除dns缓存，用户机dig [www.example.net](http://www.example.net)，此时会有如下信息：

;; AUTHORITY SECTION:

example.net. 259200 IN NS ns.attacker32.com.

表示攻击成功。