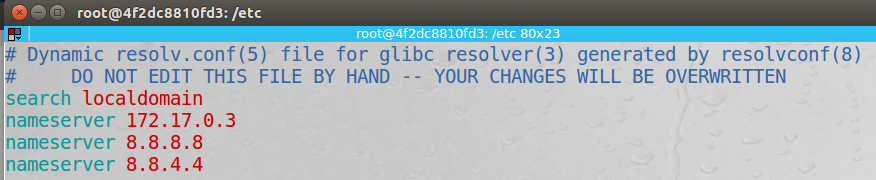
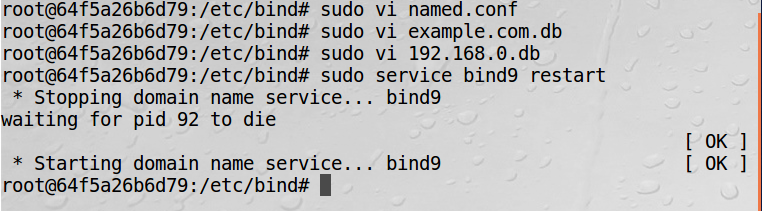
2

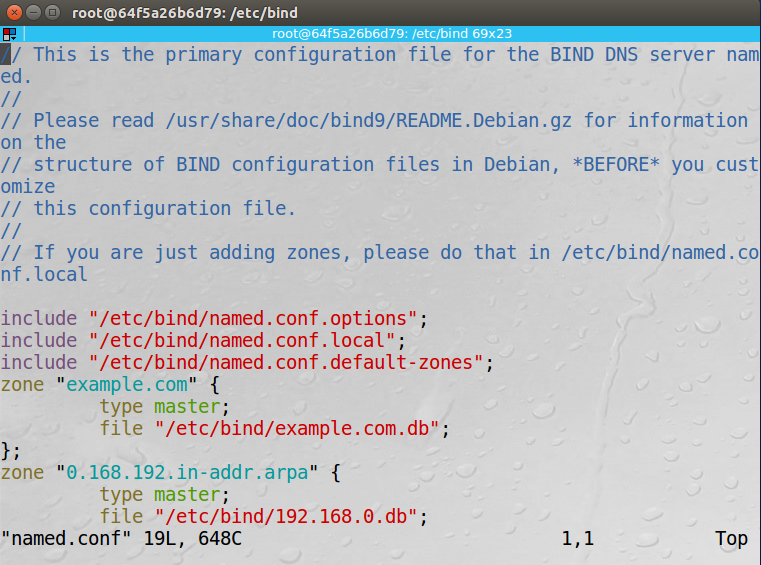
用户机编辑resolv.conf，修改默认DNS服务器为服务器ip

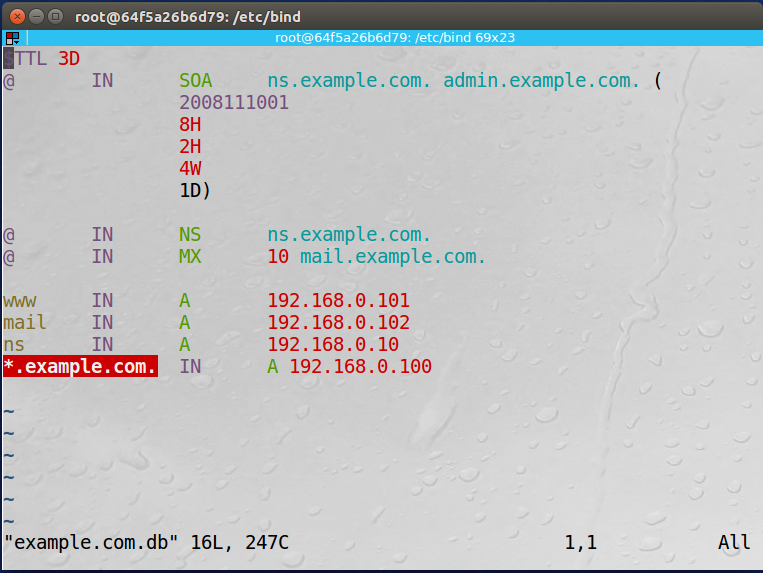
https://p.ananas.chaoxing.com/star3/origin/ea9d9b9a28adc7ee9efe4f606f238387.png

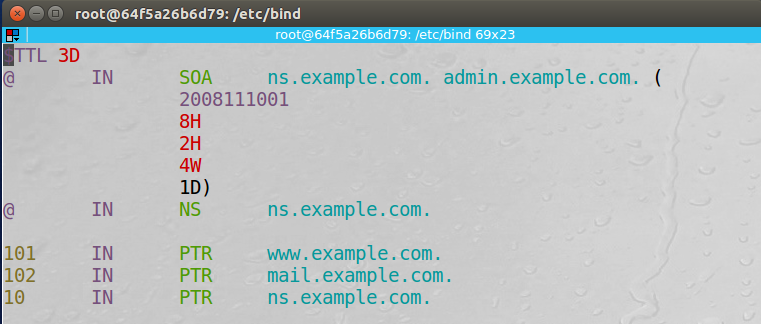


服务器配置如下：



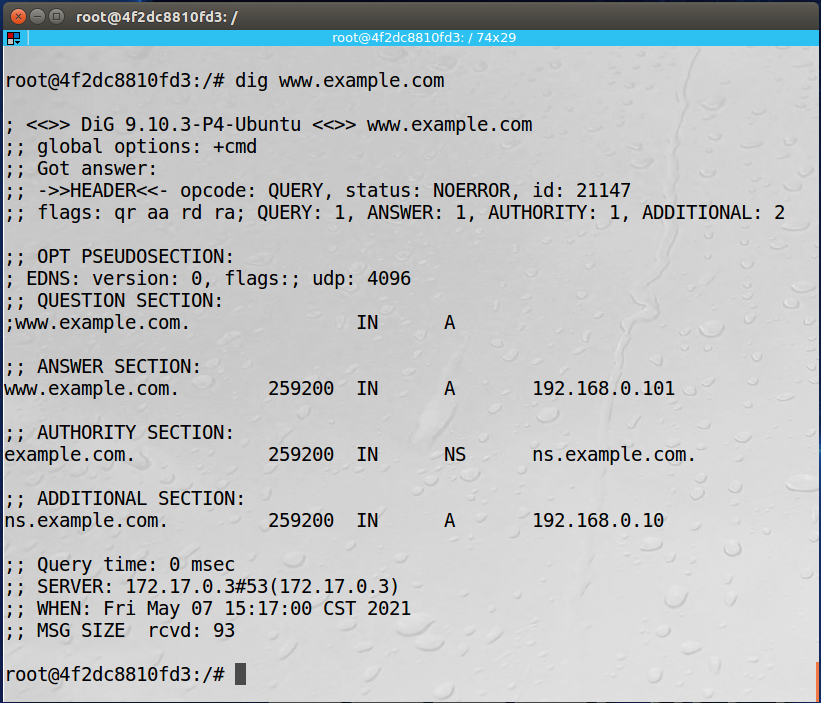






重启bind9服务

然后在用户机验证dig [www.example.com](http://www.example.com/)，看到向DNS服务器172.17.0.3查询该域名的ip地址，结果是我们设置的192.168.0.101

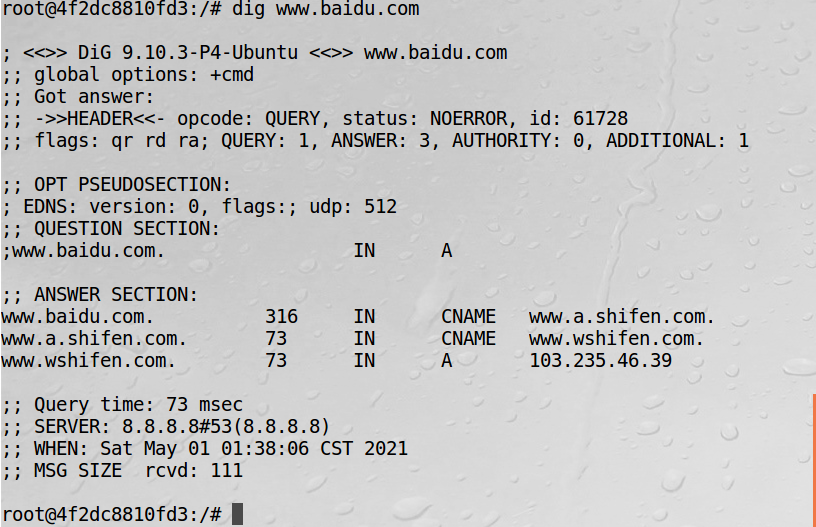


wireshark抓包看到由用户机发给DNS服务器的查询报文

https://p.ananas.chaoxing.com/star3/origin/b78460ca3e531d3fdfc3057e4f6ca888.png

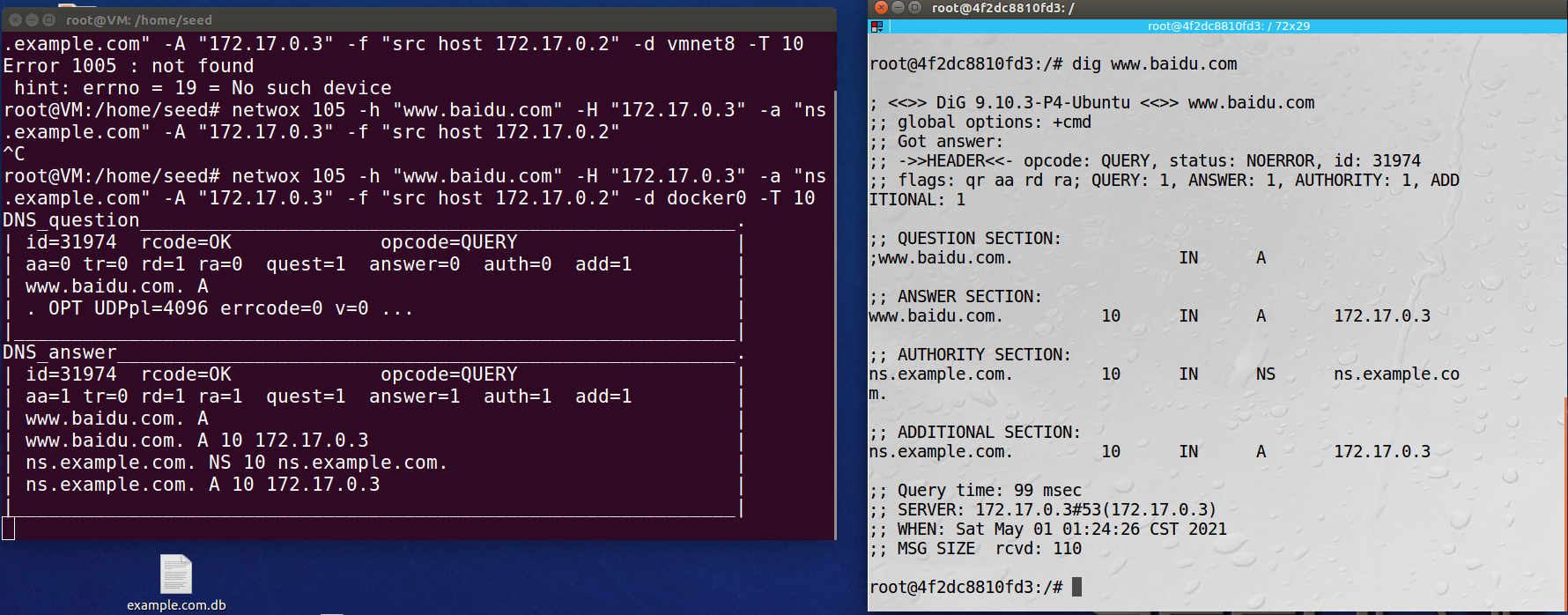
3

攻击前dig [www.baidu.com](http://www.baidu.com/)

  
显示其ip为103.235.46.39

攻击命令如下：

netwox 105 -h "www.baidu.com" -H "172.17.0.3" -a "ns.example.com" -A "172.17.0.3" -f "src host 172.17.0.2" -d docker0 -T 10



看到dig baidu的返回ip为我们的欺骗地址127.17.0.3，所以攻击成功。

4

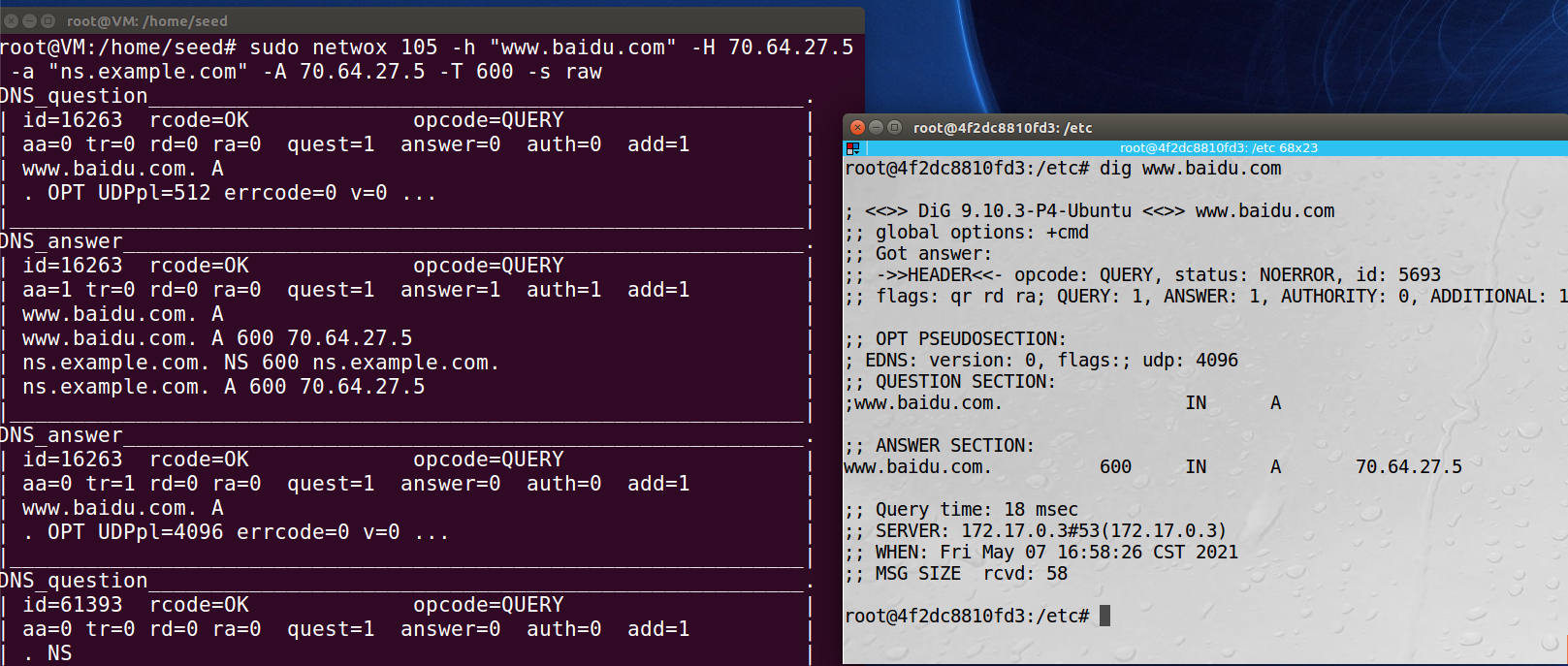
先在服务器命令行清空DNS缓存：

sudo rndc flush

攻击命令如下：

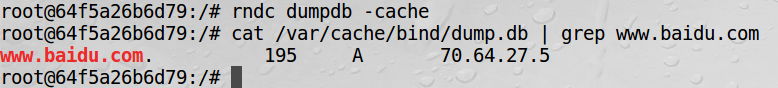
sudo netwox 105 -h "www.baidu.com" -H 70.64.27.5 -a "ns.example.com" -A 70.64.27.5 -T 600 -s raw

客户机dig [www.baidu.com](http://www.baidu.com/)，结果如下：



可以看到用户机dig百度从DNS服务器获取的结果正是我们设置的ip 70.64.27.5，攻击成功。

查看DNS服务器缓存：

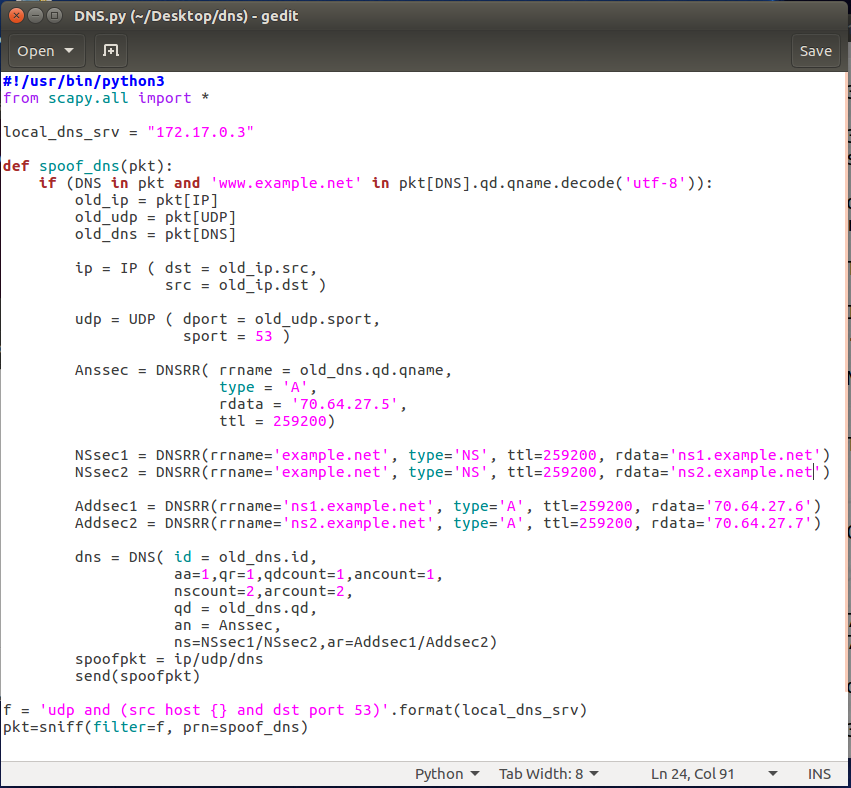


说明DNS服务器已经中毒

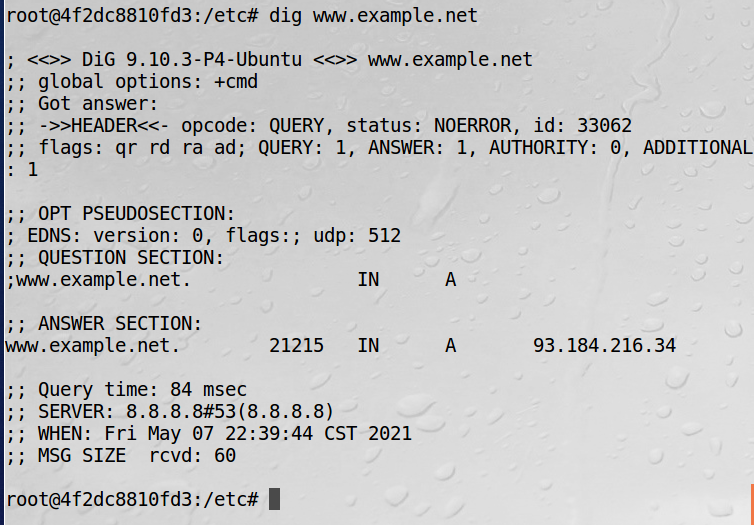
5

scapy脚本如下：



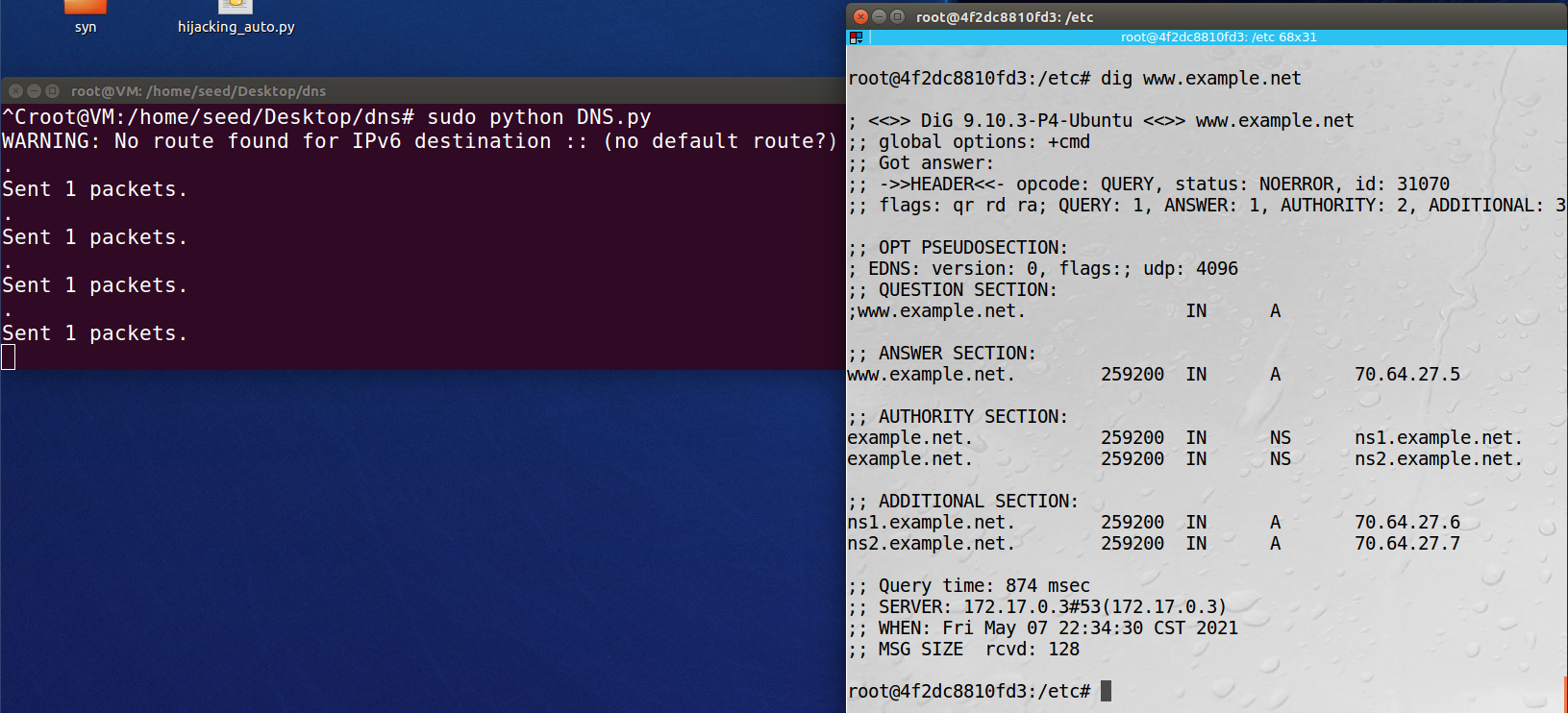


攻击前dig [www.example.net结果如下:](http://www.example.xn--net-128d473c33tue1b/)



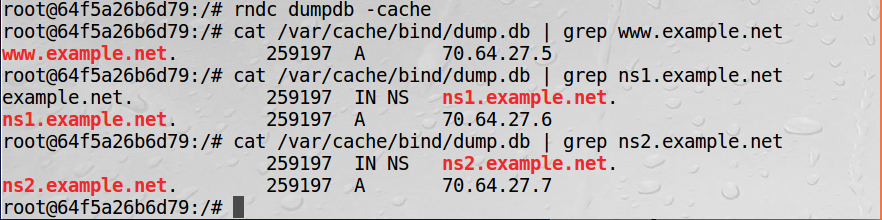
其dns服务器8.8.8.8查询到其ip为93.184.216.34

先清空dns服务器的缓存，然后在攻击机上运行脚本，在客户机上dig www.example.net



可以看到攻击成功，dig www.example.net的结果为我们脚本中设置的70.64.27.5，授权域ns1和ns2，其附加域对应ip为70.64.27.6和70.64.27.7

在DNS服务器查询缓存：

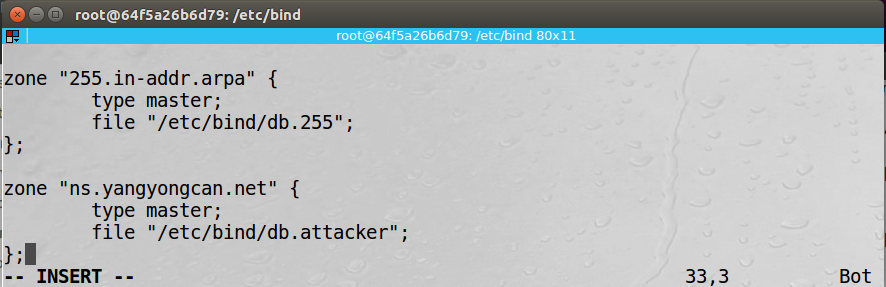


www.example.net及其授权域ip均被毒化，验证攻击成功。

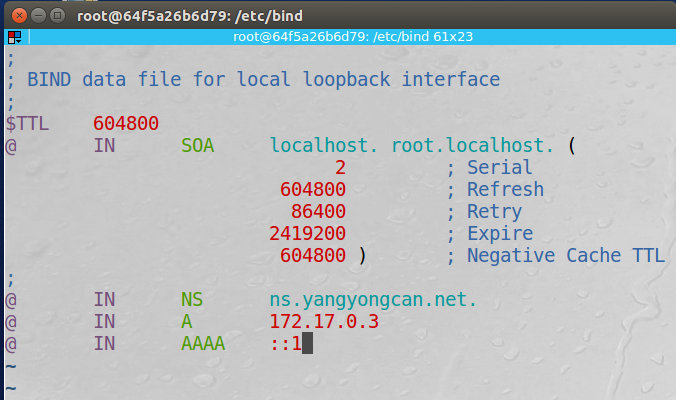
6

注释掉之前DNS服务器关于www.example.com的配置：

配置服务机的/etc/bind/named.conf.default-zones文件

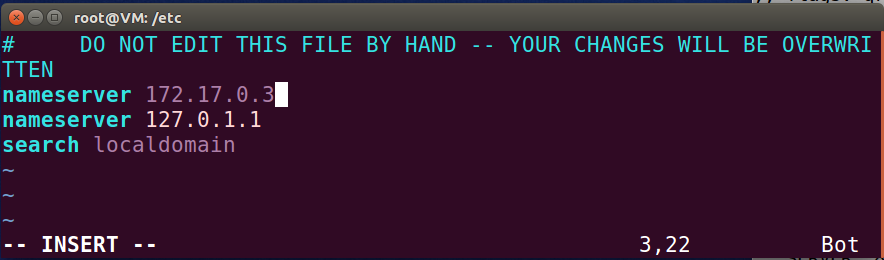


创建db.attacker



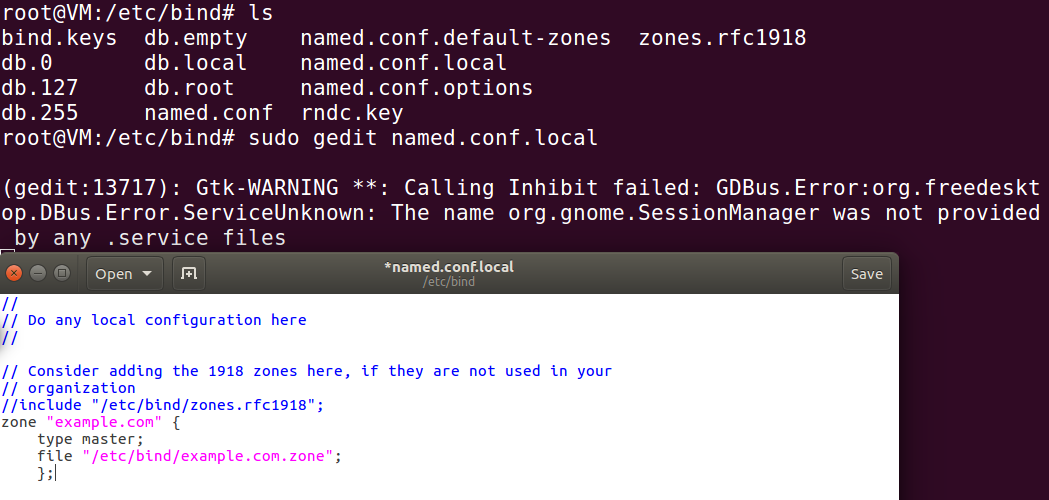
将攻击机的默认DNS服务器设置为服务机:



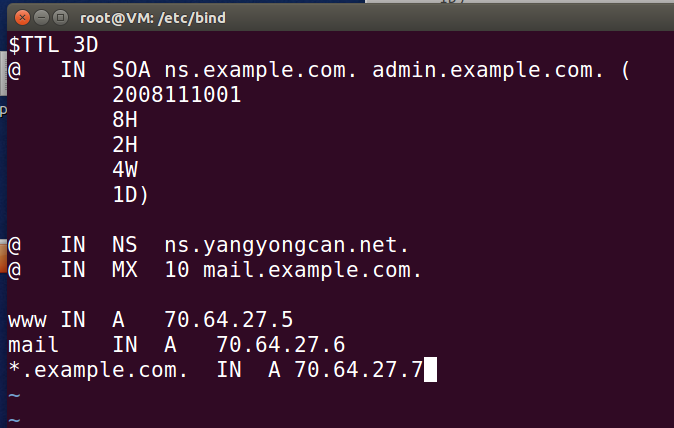


攻击机安装bind9

编辑etc/bind/named.conf.default-zones，添加example.com的定义



添加/etc/bind/example.com.db文件：

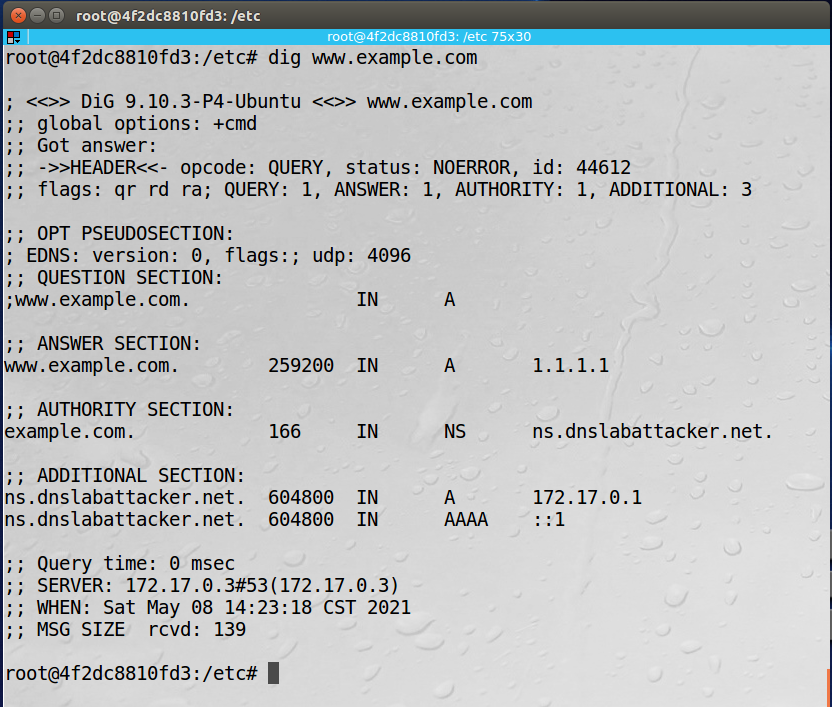


清空缓存并重启攻击机和服务机的bind9

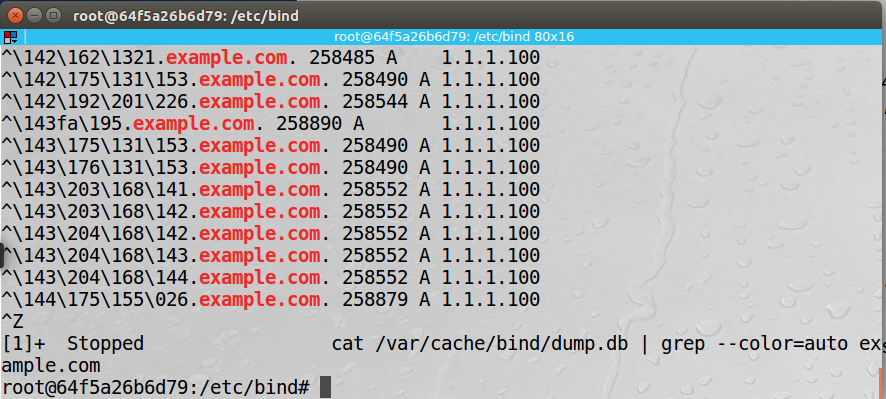
7

  
udp.c

编译运行udp.c，在客户机dig www.example.com如下，在未修改域名为姓名时攻击成功一次，截图如下:



查看DNS服务器，可以看到缓存中毒，验证攻击成功



但是修改域名为自己姓名后多次尝试攻击未能成功