网安综合课程设计

实验报告

（57117105 杨哲君）

***Local DNS Attack Lab***

实验环境：

DNS Server 192.168.80.137

user 192.168.80.138

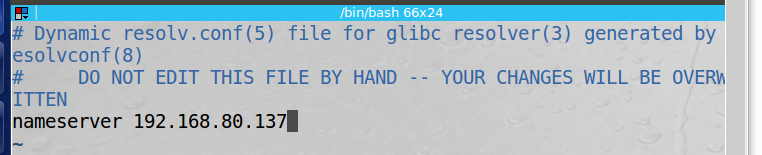
attacker 192.168.80.139

***Lab Tasks (Part I): Setting Up a Local DNS Server***

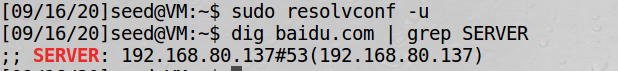
**Task 1: Configure the User Machine**

在user主机的/etc/resolvconf/resolv.conf.d/head文件中添加nameserver192。168.80.137，并使其起作用。





使用dig可以看到已经设置成功。

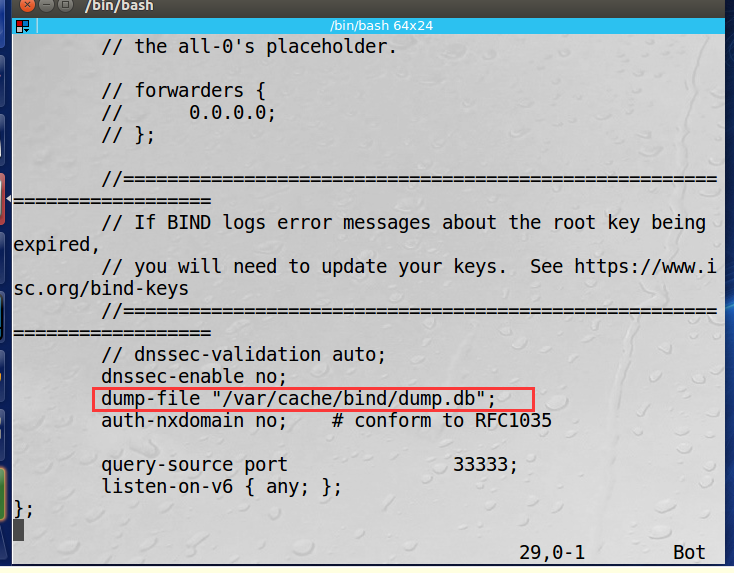


**Task 2: Set up a Local DNS Server**

**Step 1: Configure the BIND 9 server.**

在DNS server的主机中查看/etc/bind/named.conf.options，确认dump-file是存在的。





运行命令清理缓存。



**Step 2: Turn off DNSSEC**

在/etc/bind/named.conf.options中确认DNSSEC已经关闭。



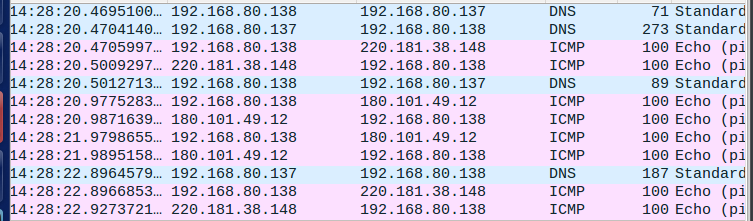
**Step 3: Start DNS server**

开启服务。



**Step 4: Use the DNS server**

在user机上ping [www.baidu.com](http://www.baidu.com)，



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

**Step 1: Create zones.**

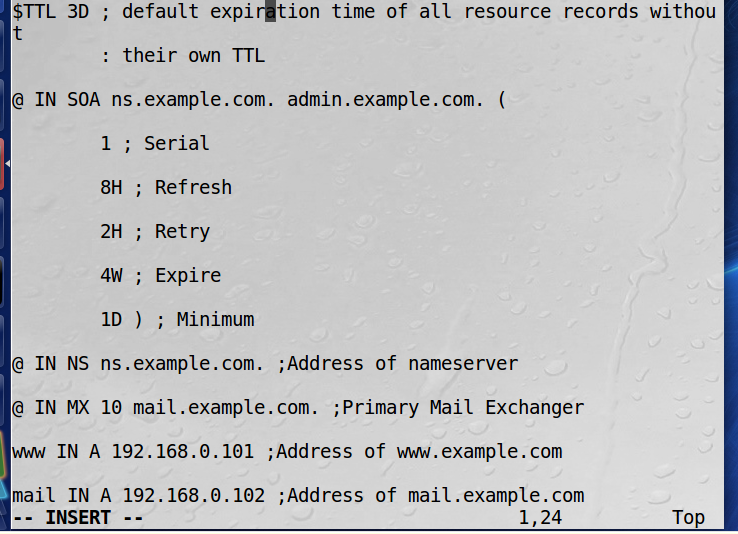
按实验手册规定，在DNS服务器中的/etc/bind/named.conf添加信息，分别是用于转发查找的zone和反向查找的zone。



**Step 2: Setup the forward lookup zone file**

创建第一个zone对应的文件，存放example.com下所以域名的记录。





**Step 3: Set up the reverse lookup zone file**

创建第二个zone对应的文件192.168.0.db。

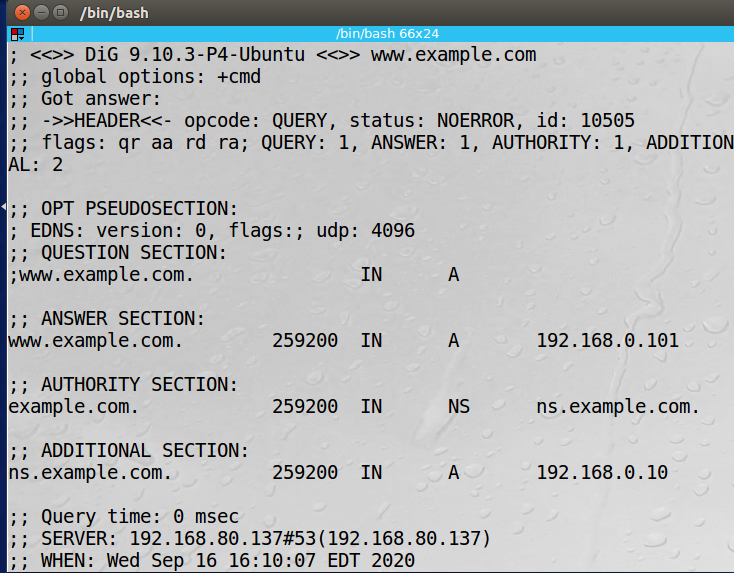




**Step 4: Restart the BIND server and test**

重新启动bind9服务器后，在user机上执行dig命令，解析域名，可以看到显示出了www.example.com 的IP地址。

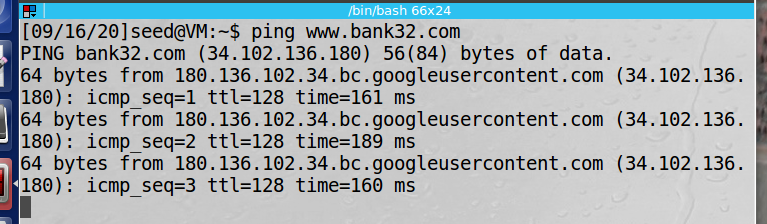




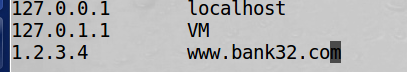
***Lab Tasks (Part II): Attacks on DNS***

**Task 4: Modifying the Host File**

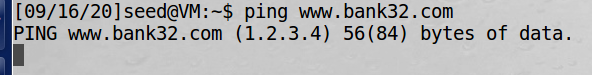
修改hosts文件前，ping [www.bank32.com](http://www.bank32.com)，发现经过DNS服务器解析之后的IP地址为180.136.102.34。



修改/etc/hosts文件，添加一条错误的映射关系使1.2.3.4映射到www,hosts.com。

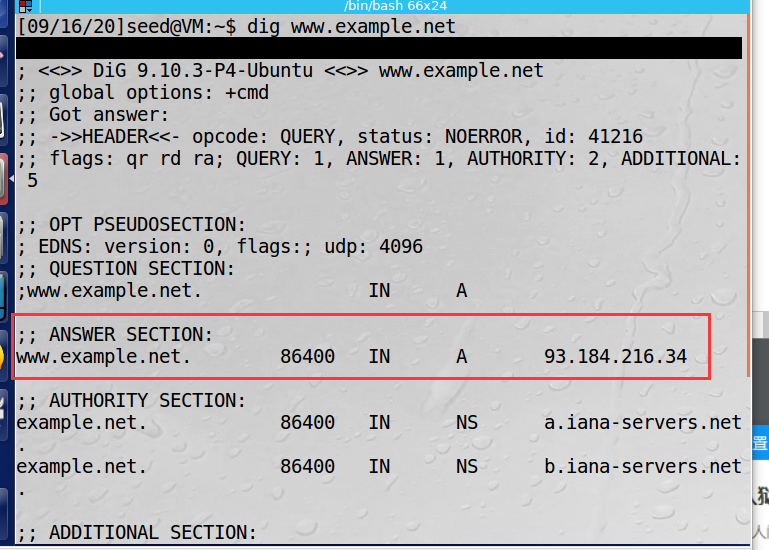


修改了hosts文件过后，[www.bank32.com经过DNS](http://www.bank32.com经过DNS)服务器解析之后，IP地址变成了1.2.3.4。



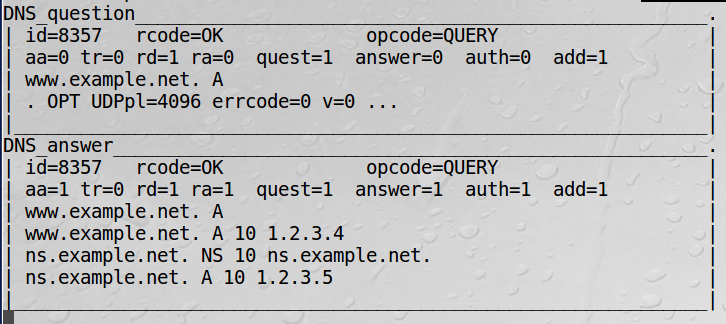
Task 5: Directly Spoofing Response to User

攻击前，user机使用dig命令发送请求报文，可以看到域名[www.example.net的DNS](http://www.example.net的DNS)查询结果为93.184.216.34。

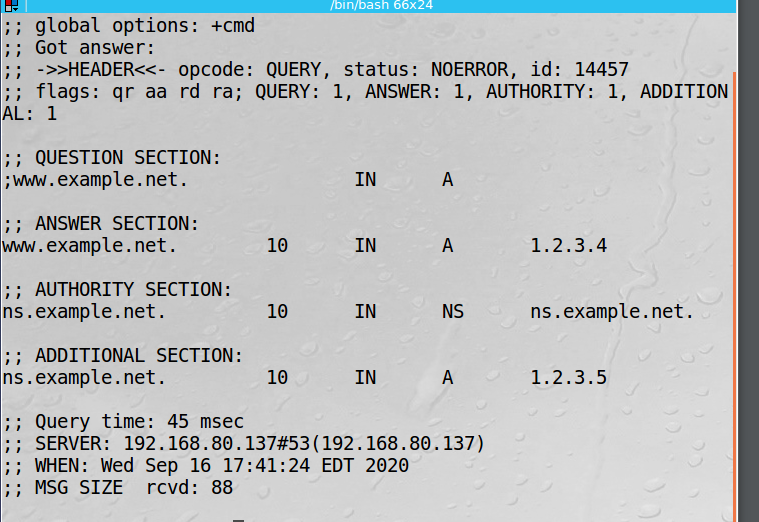


在攻击者机中运行下面的命令，通过netwox伪造DNS回复。并且嗅探到了来自DNS服务器的DNS请求报文和伪造的DNS响应报文。





在user机再次使用dig命令，可以看到攻击生效，[www.example.net的IP](http://www.example.net的IP)被映射为1.2.3.4。

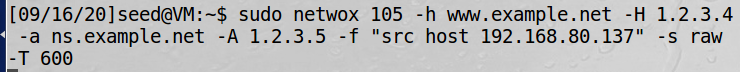


**Task 6: DNS Cache Poisoning Attack**

先在DNS服务器中清空DNS缓存。

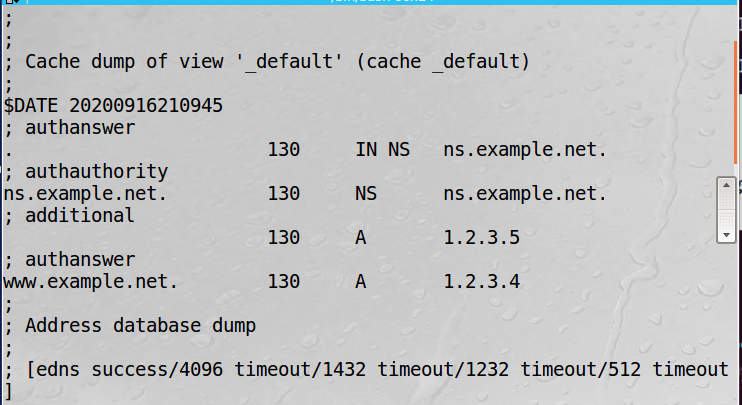


在攻击者主机中运行下面的命令，嗅探来自于DNS服务器的IP地址的数据包。



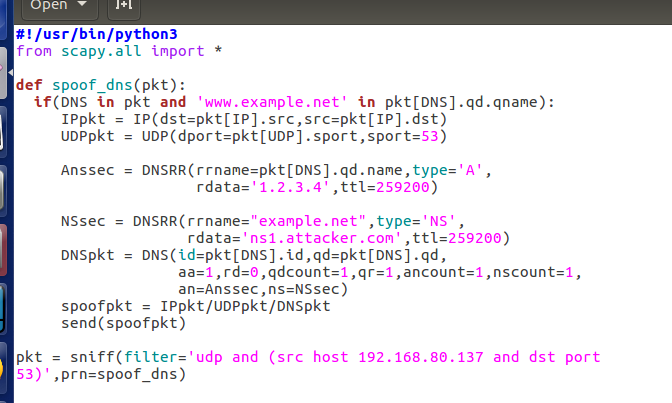
将本地DNS缓存转储，然后通过cat命令打印，可以看到[www.example.net对应的IP](http://www.example.net对应的IP)地址为1.2.3.4，DNS缓存成功被污染。





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

编写并运行脚本。



在DNS服务器主机清空缓存。



查看DNS缓存，可以看到攻击成功。



