Lab5

张镇57117126

实验环境：

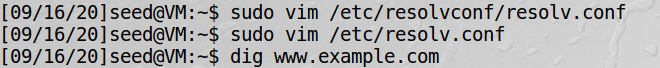
DNS server：192.168.52.136

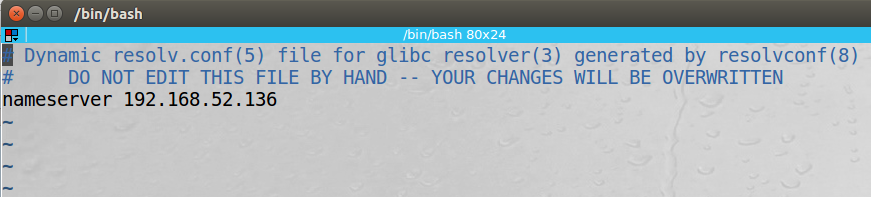
Victim：192.168.52.133

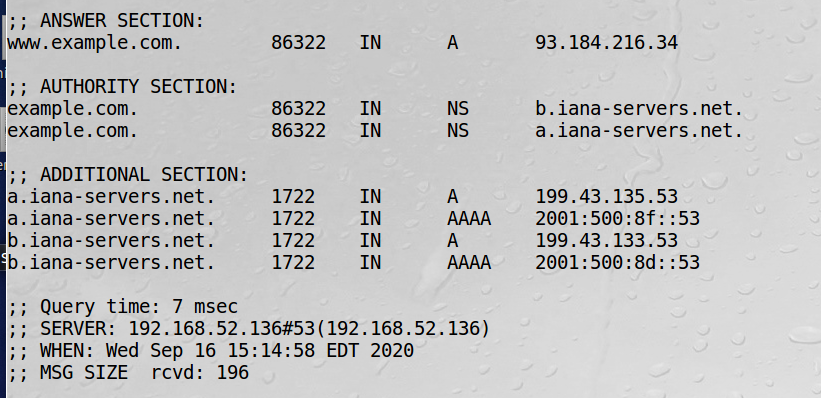
Attacker：192.168.52.137

Task1.Conﬁgure the User Machine

首先打开三台虚拟机，在被攻击的虚拟机上进行配置：



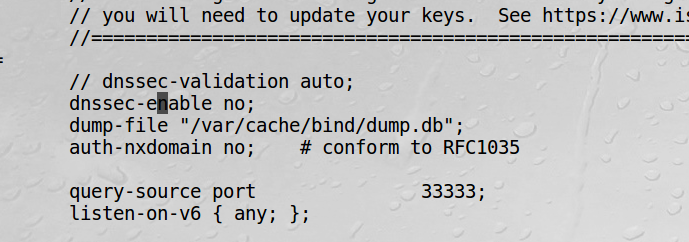




通过dig之后我们可以看到server为我们配置的DNS服务器的IP地址。

Task2. Set up a Local DNS Server

首先确认该条目的存在：



然后运行命令清理缓存：

C:\Users\lenovo\AppData\Roaming\Tencent\Users\345312414\QQ\WinTemp\RichOle\H60I2ATA@3KA3HZ%S4WQLFW.png

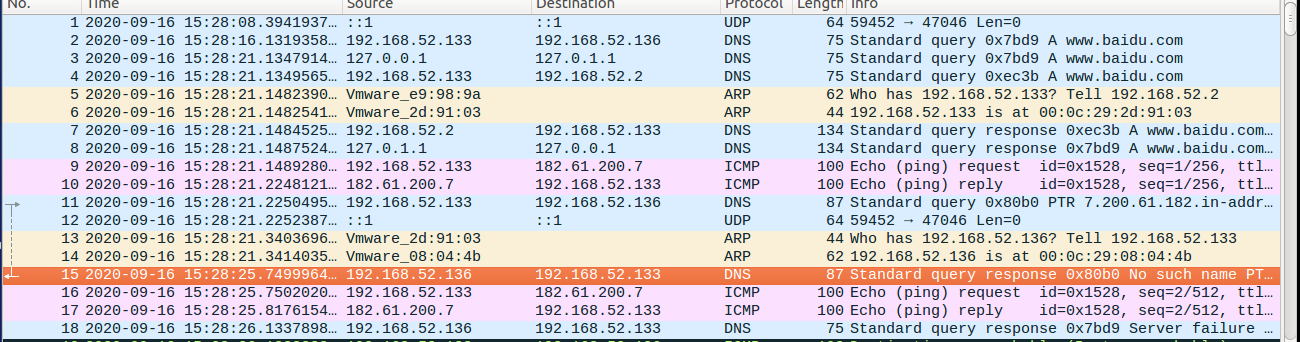
确认DNSSEC已经关闭：

C:\Users\lenovo\AppData\Roaming\Tencent\Users\345312414\QQ\WinTemp\RichOle\R2@389ZR7K2C)(@EUEAL7@M.png

启动服务器：

C:\Users\lenovo\AppData\Roaming\Tencent\Users\345312414\QQ\WinTemp\RichOle\(05X}L7D6C}`(UTV3$DW$O8.png

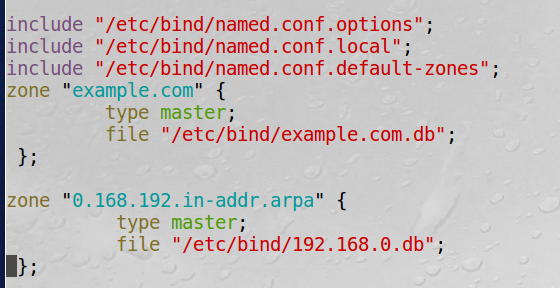
我们在用户虚拟机上ping [www.baidu.com](http://www.baidu.com)，并用wireshark进行抓包：



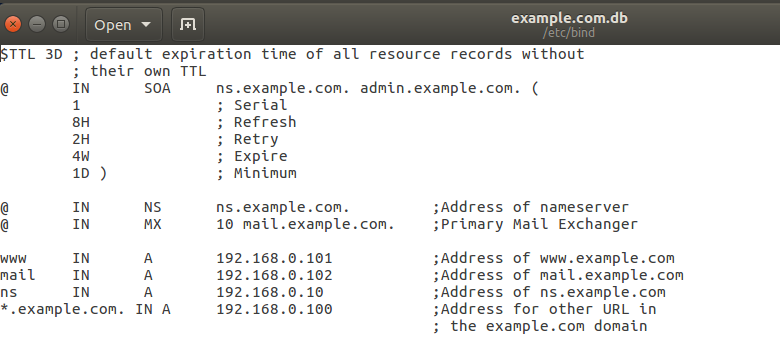
可以看到 user 首先向本地 DNS Server请求域名解析服务，再由DNS Server通过递归查询获得www.baidu.com对应的IP地址， 最终发送给 user，随后 user 开始 ping 的过程。

Task3. Host a Zone in the Local DNS Server

首先创建zone：



创建建/etc/bind/example.com.db，并添加下图声音：

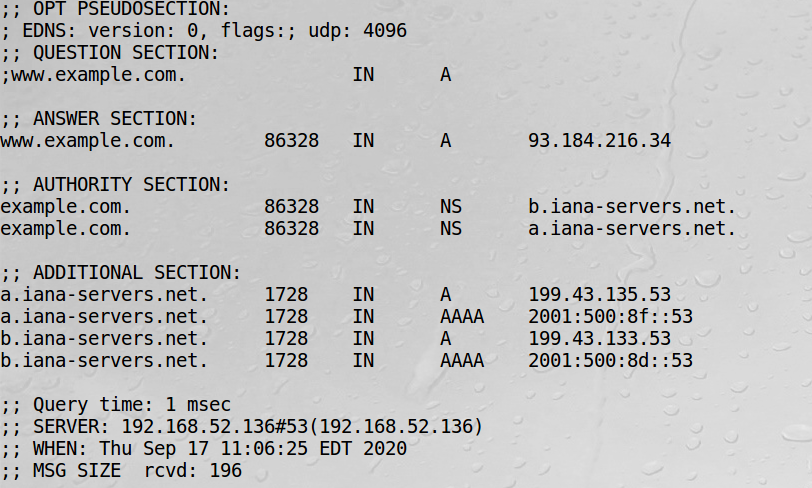


创建/etc/bind/192.168.0.db 文件并添加上图信息



重启服务器：

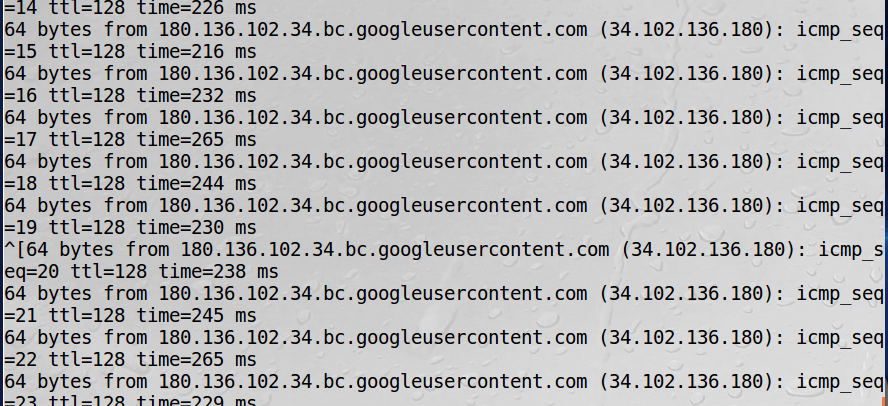
C:\Users\lenovo\AppData\Roaming\Tencent\Users\345312414\QQ\WinTemp\RichOle\L3W}0VJ@{U@JTW$BQXY7IEX.png



dig [www.example.com之后可以看到返回了他的IP](http://www.example.com之后可以看到返回了他的IP)地址。

Task4. Modifying the HostFile

首先ping通[www.bank32.com](http://www.bank32.com)



添加地址映射：

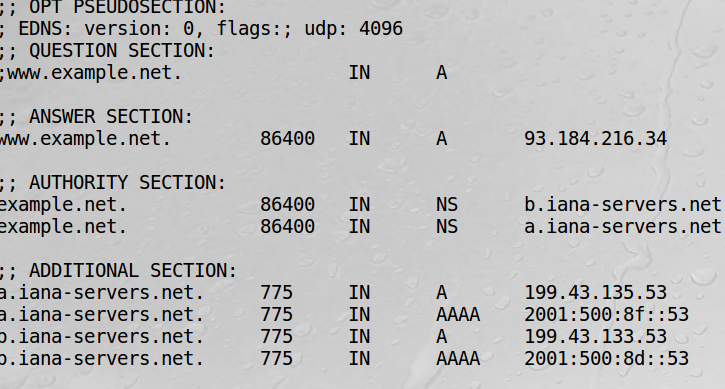


再次ping [www.bank32.com](http://www.bank32.com)，发现发生了变化

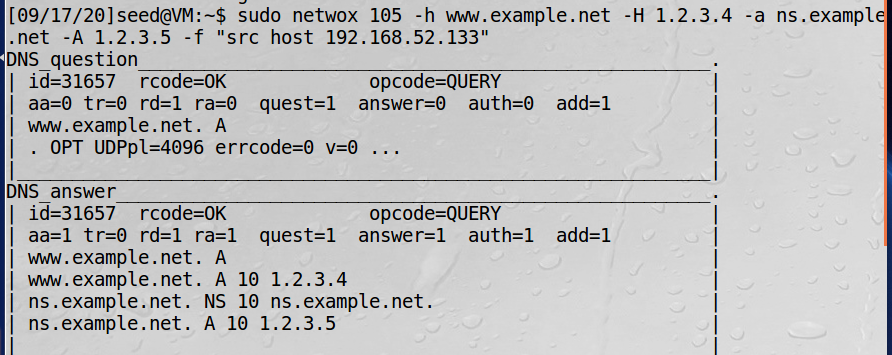
C:\Users\lenovo\AppData\Roaming\Tencent\Users\345312414\QQ\WinTemp\RichOle\%_`~FO14QKS]SQF6@~SFJZO.png

Task5. Directly Spooﬁng Response to User

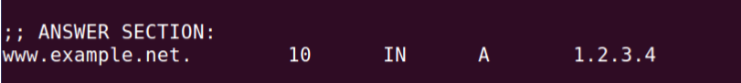
首先在用户上dig [www.example.net，DNS](http://www.example.net，DNS)查询结果为93.184.216.34



在攻击者虚拟机上运行如下命令：

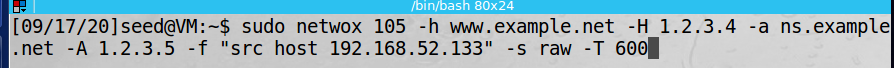


然后在主机上继续dig，发现结果如下：

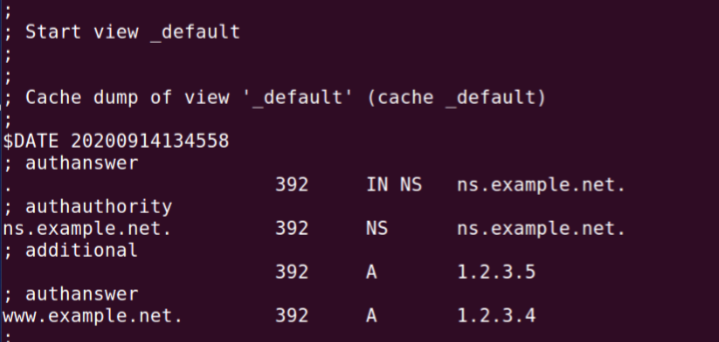


Task6.

首先在DNS服务器上清理缓存，并在attacker上运行以下命令：

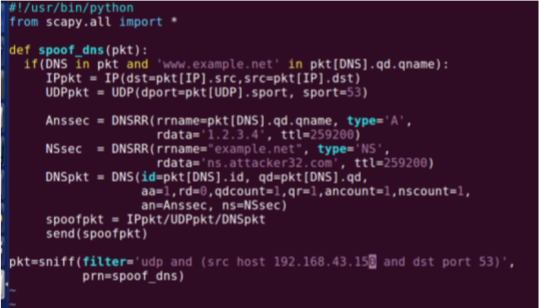


依次运行sudo rndc dumpdb –cache，sudo cat /var/cache/bind/dump.db，可打印DNS缓存存储：

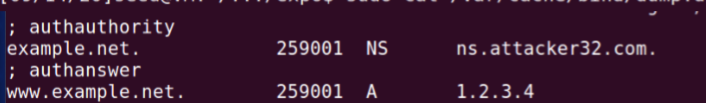


Task7

首先在attack上编译并运行如下代码：



在DNS上清理缓存，并依次输入在Task6中的俩个命令，查看如下结果：



在user主机上dig [www.example.net](http://www.example.net)也能证实：

