**Local DNS Attack Lab 实验报告**

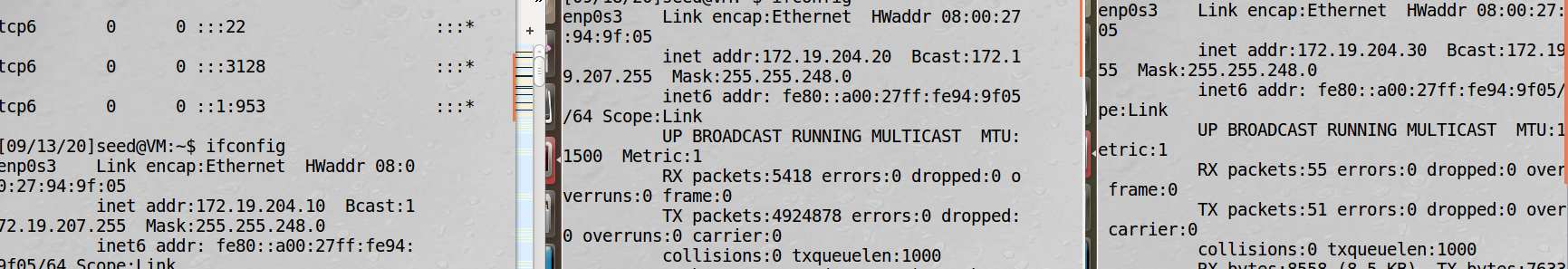
**57117207 高晓悦**

本实验需要三台主机，分别是——

主机A：172.19.204.10，作为用户机；

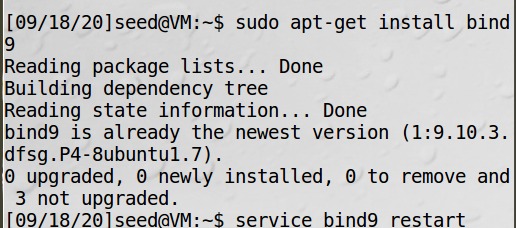
主机B：172.19.204.20，作为DNS服务器；

主机C：172.19.204.30，作为攻击机；



**Task 1: Confifigure the User Machine**

1. DNS服务器（主机B）上安装bind9并重启：



1. 更改用户机（主机A）的DNS配置：

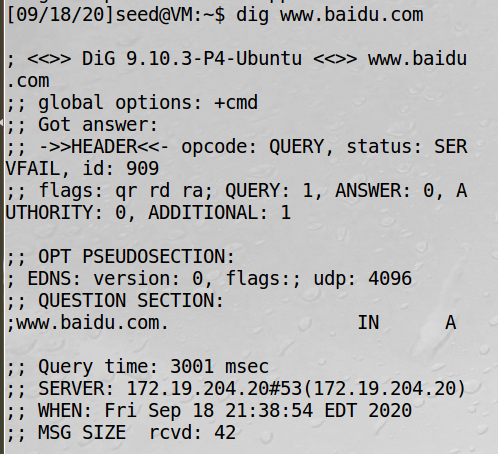
打开文件：

添加配置：

打开文件：

添加配置：

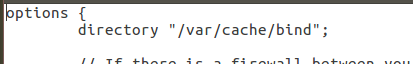
1. 用户机（主机A）执行dig www.baidu.com：

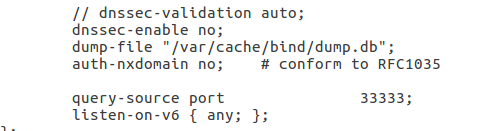


发现用户机的DNS服务器已变为主机B。

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

1. 修改文件，并关闭DNSSEC功能：





1. 执行命令：



1. 重启bind9：



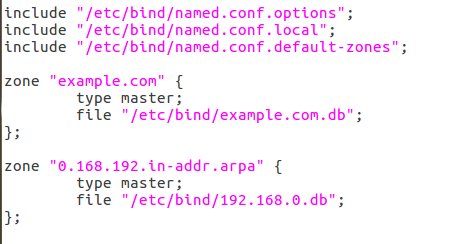
1. 用户机（主机A）上ping www.baidu.com，wireshark抓包发现用户机会先访问主机B：



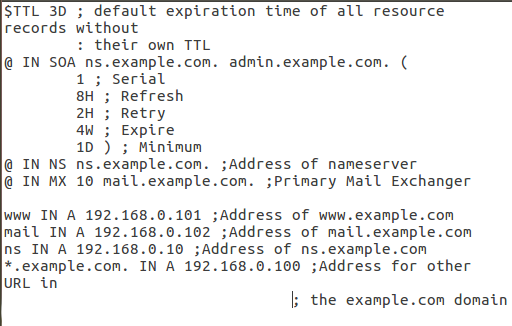
**Task 3: Host a Zone in the Local DNS Server**

1. 在本地DNS服务器（主机B）中的文件中添加两个zone：

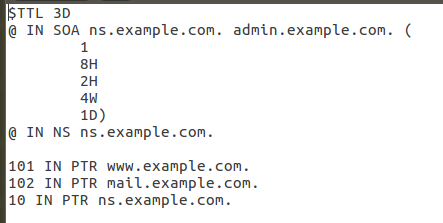




1. 在/etc/bind/文件夹下创建zone文件example.com.db：



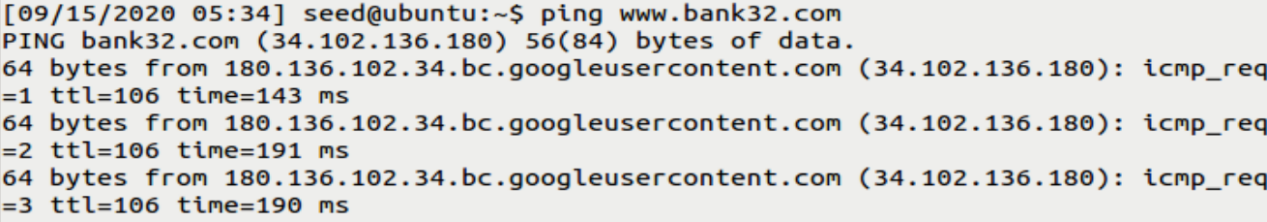
创建zone文件192.168.0.db：



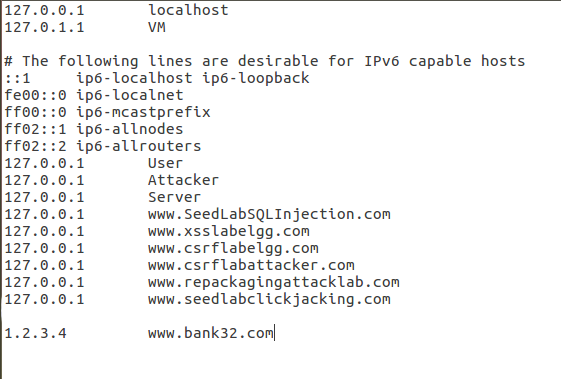
1. 重启bind9并在用户机上解析域名www.example.com。

**Task 4: Modifying the Host File**

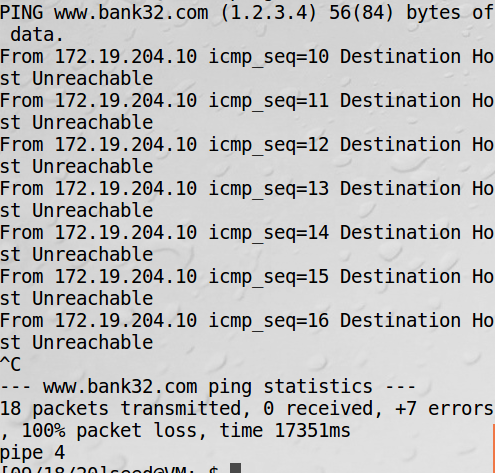
1. 攻击前用户机（主机A）ping www.bank32.com：



1. 修改/etc/hosts文件，将www.bank32.com指向1.2.3.4：



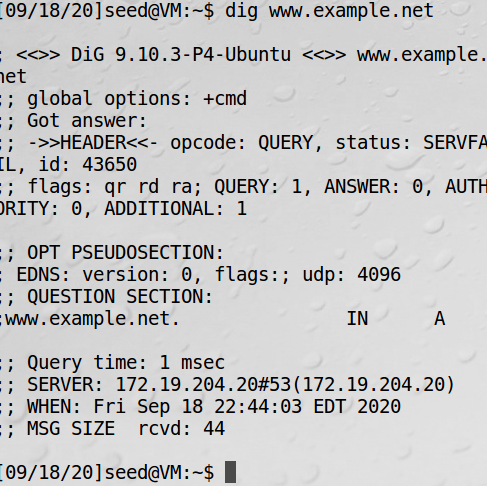
1. 攻击后用户机（主机A）再ping www.bank32.com：



发现攻击后对应的IP改变了。

**Task 5: Directly Spoofifing Response to User**

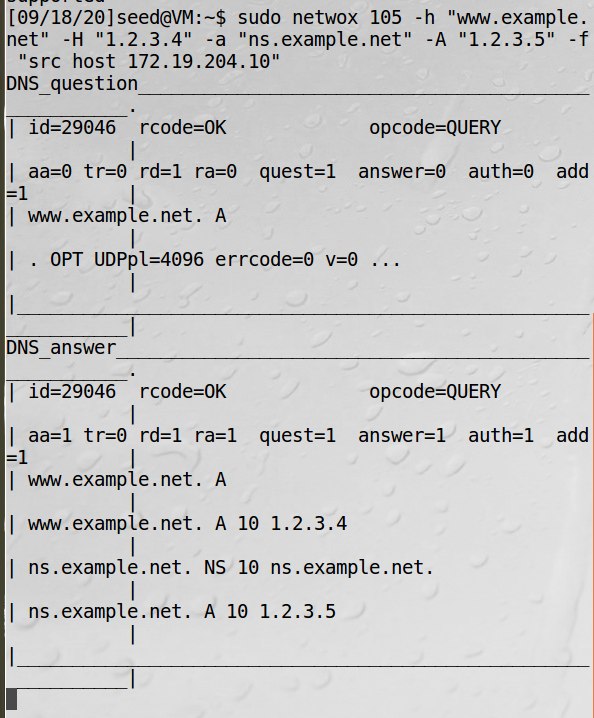
1、攻击前dig www.example.net：



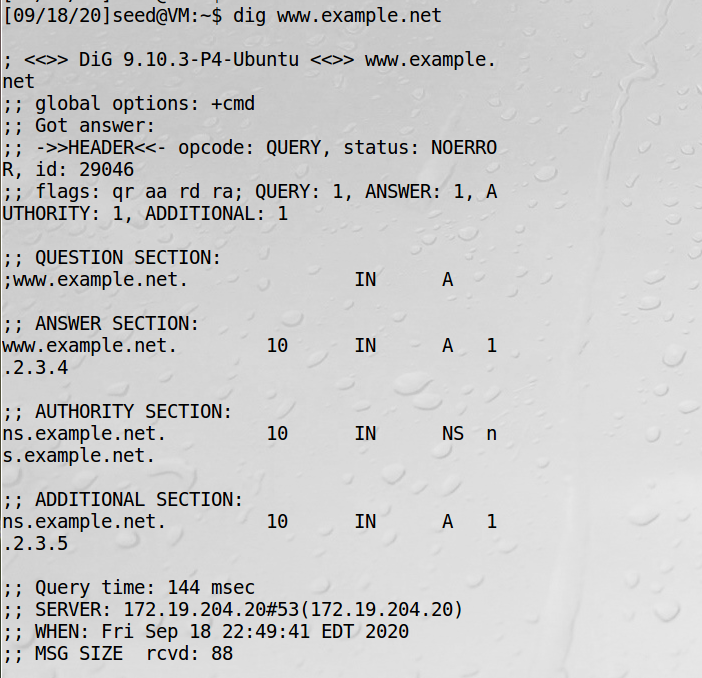
1. 清楚本地DNS服务器缓存：



3、在攻击机（主机C）中实施攻击：



4、在用户机（主机A）上再次dig www.example.net：



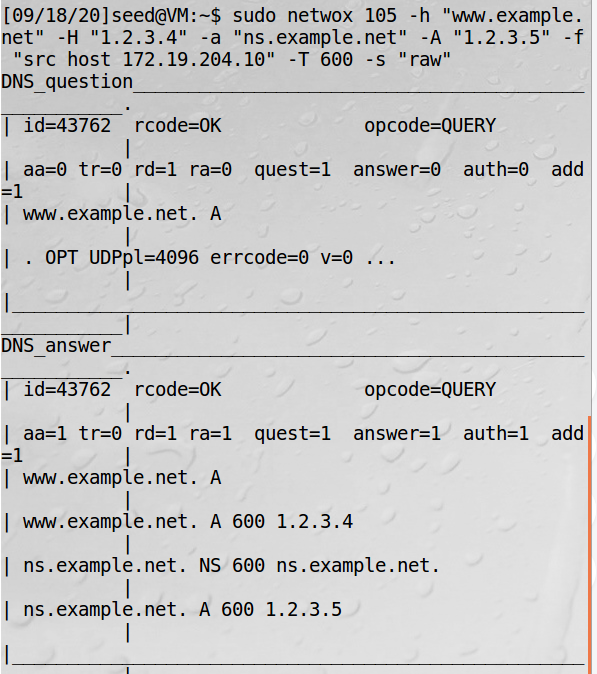
攻击成功，DNS查询结果为1.2.3.4。

**Task 6: DNS Cache Poisoning Attack**

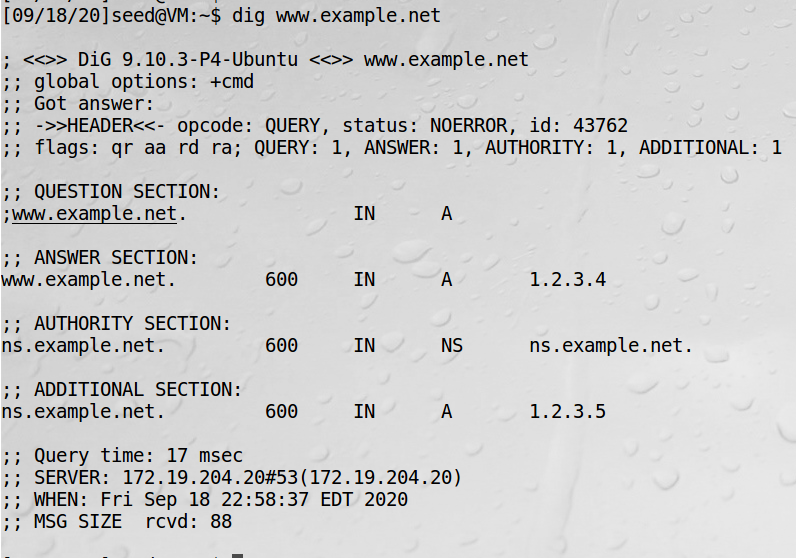
1. 清空本地DNS服务器缓存：



1. 在攻击机（主机C）中，用netwox 105伪造来自其他DNS服务器的报文发送给本地DNS服务器10.0.2.6，达到DNS缓存攻击的目的：



1. 用户机（主机A）中dig www.example.net：



1. 在本地DNS服务器（主机B）中执行命令，查看本地DNS服务器的缓存：



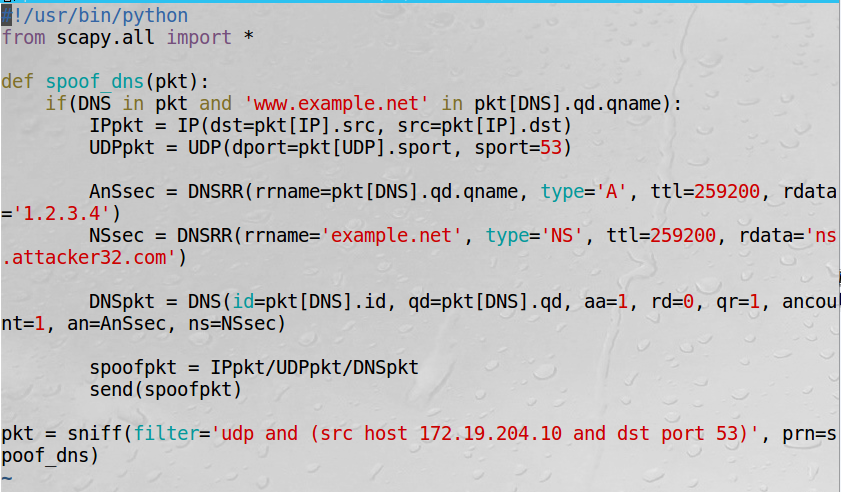
可以查看到对应条目。

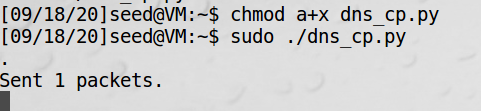
**Task 7: DNS Cache Poisoning: Targeting the Authority Section**

1. 清空本地DNS缓存：

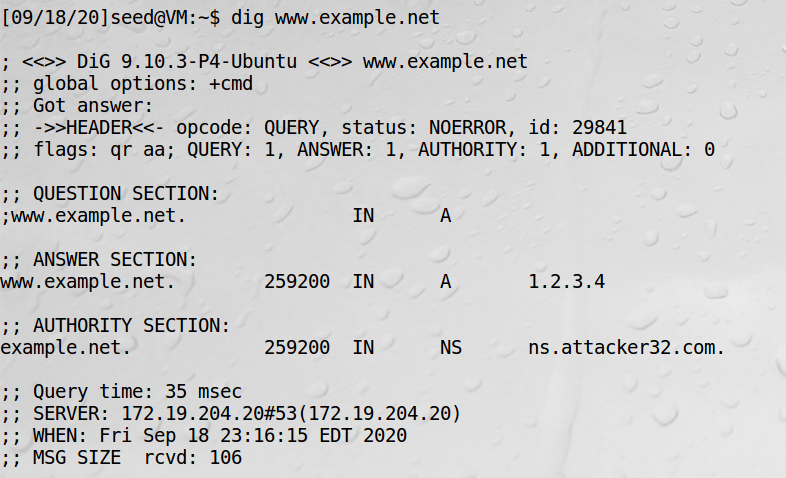


1. 编写程序并执行：





1. 用户机（主机A）中dig www.example.net：



发现answer为1.2.3.4，authority为ns.attacker32.com，攻击成功。说明DNS缓存中毒攻击不仅伪造了answer部分，还伪造了authority部分，将example.net域中任何主机名的查询服务指向了ns.attacker32.com。