

**入侵检测与数字取证**

**黄雨卓 57117205**

**LAB5**

2020年9月17日

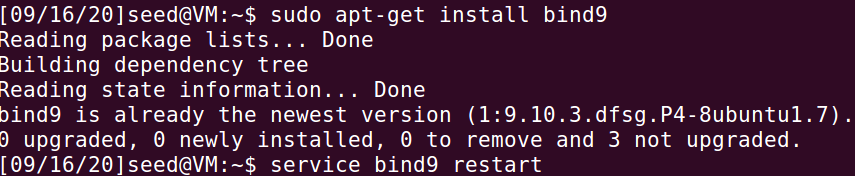
Local DNS Attack Lab

Task1: Conﬁgure the User Machine

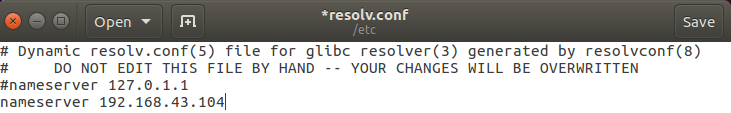
0用户机192.168.43.223

1 DNS服务器192.168.43.104

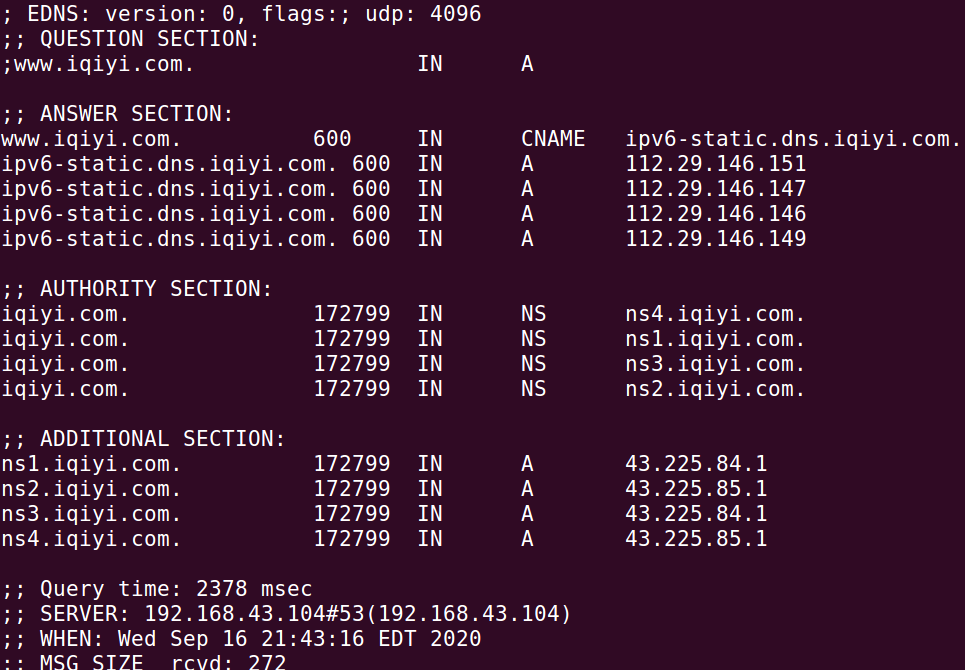
2攻击者192.168.43.45





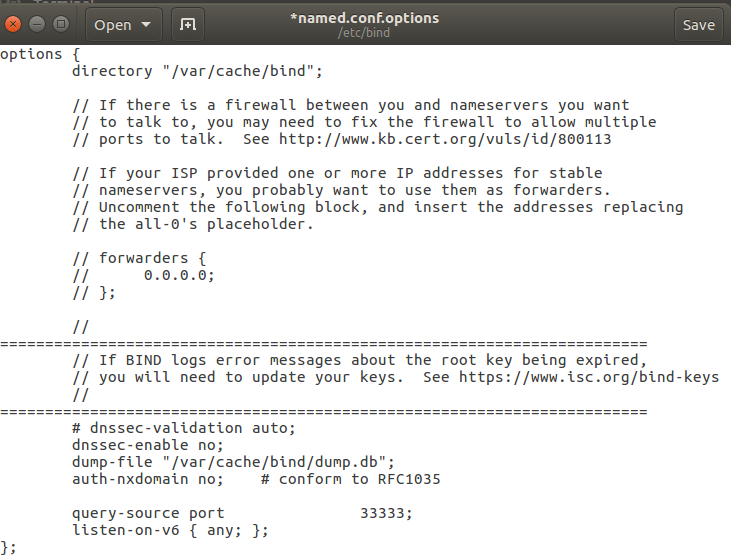


设置成功，用户机的DNS服务器已设为实验使用的DNS服务器



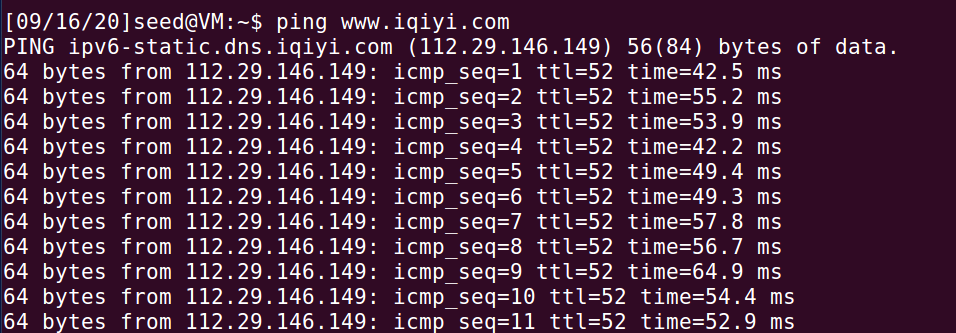
Task2: Setup a Local DNS Server



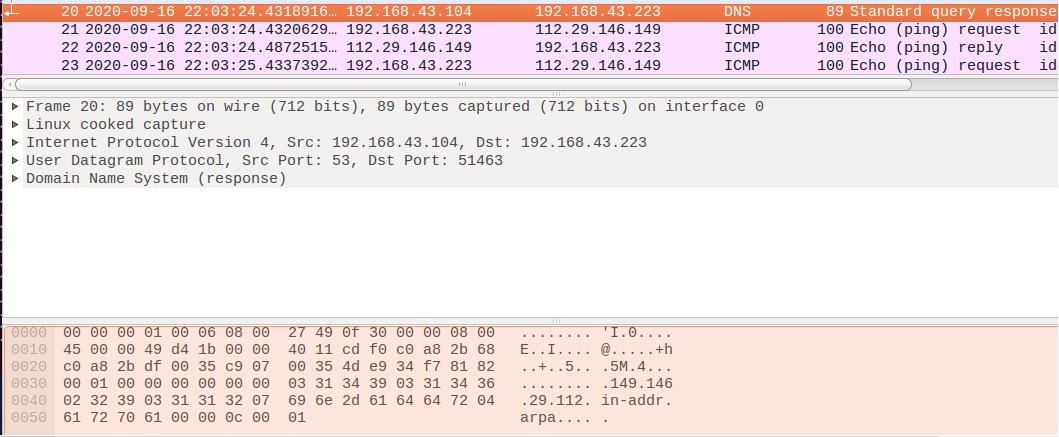


然后重启bind9

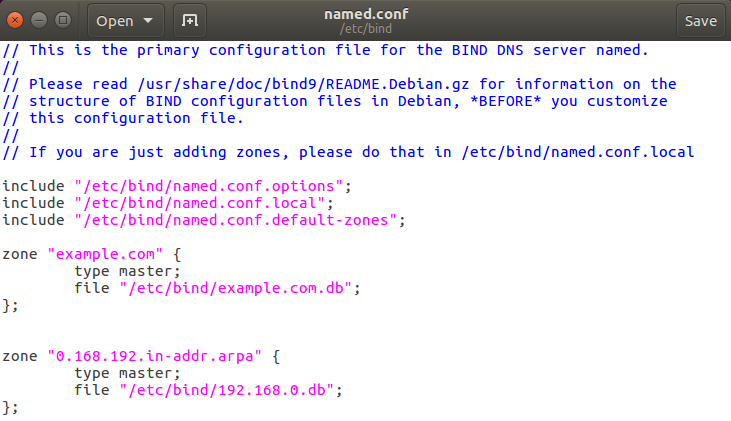
用户机连接www.iqiyi.com

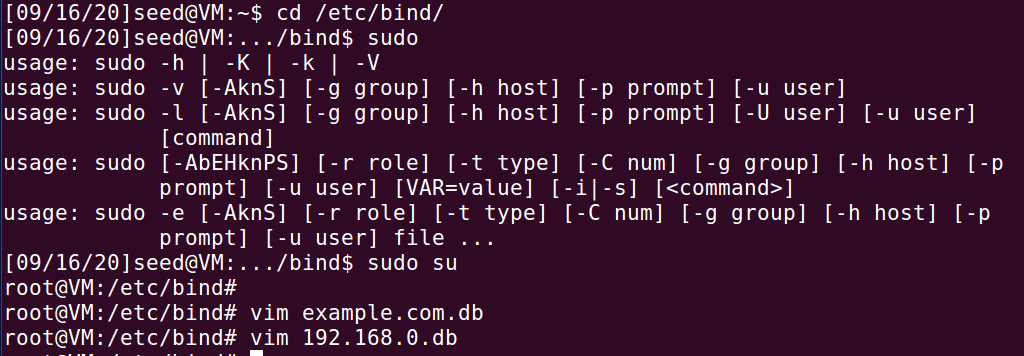


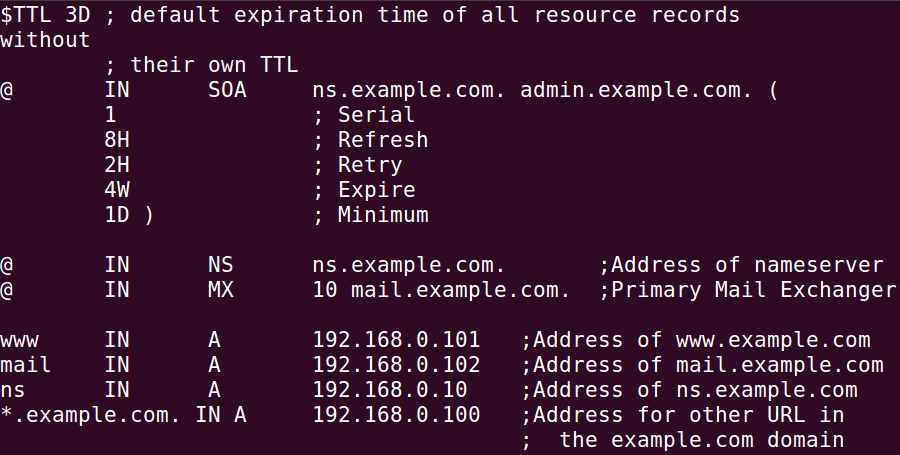
观察可得用户机优先连接我们配置的DNS服务器

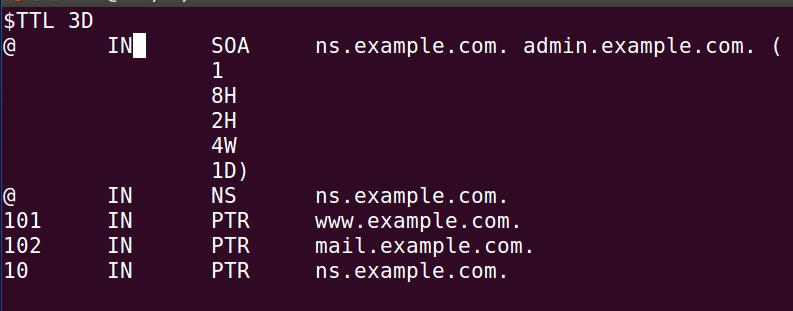


Task3: Host a Zone in the Local DNS Server









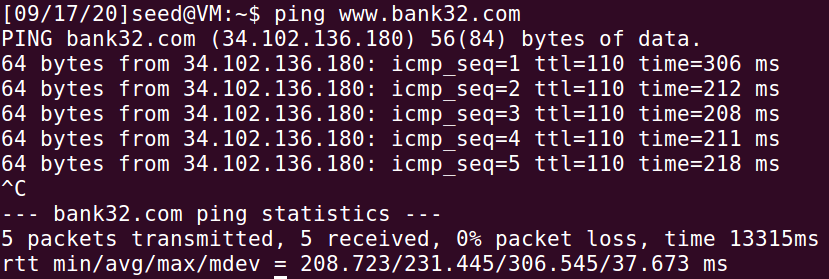


连不上，莫得办法

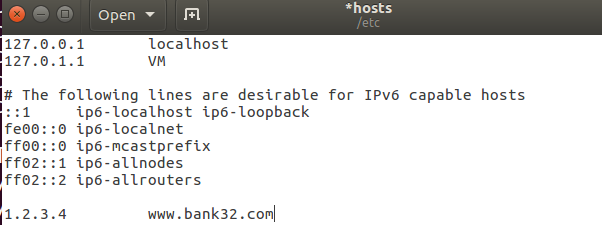


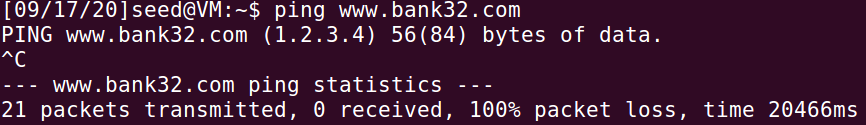
Task4: Modifying the Host File

攻击前

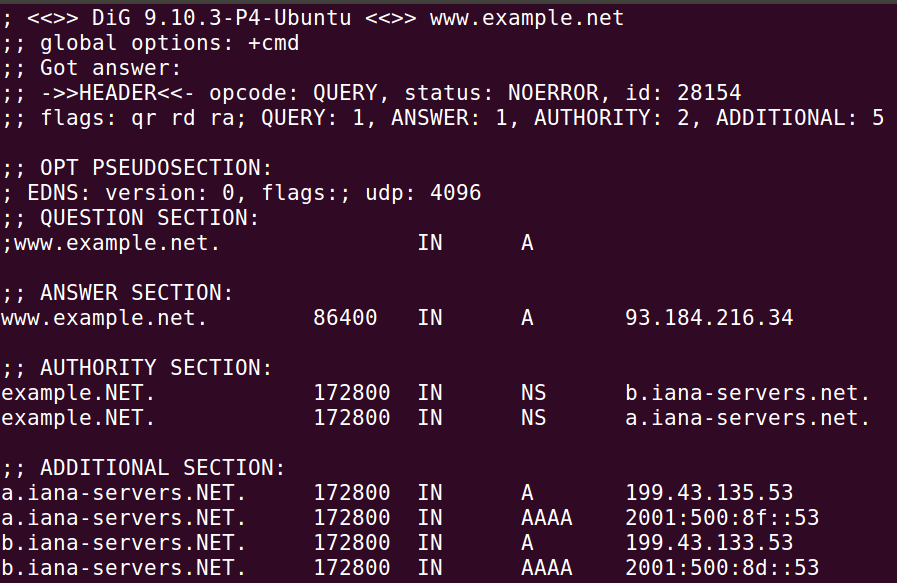


攻击后IP地址变为1.2.3.4

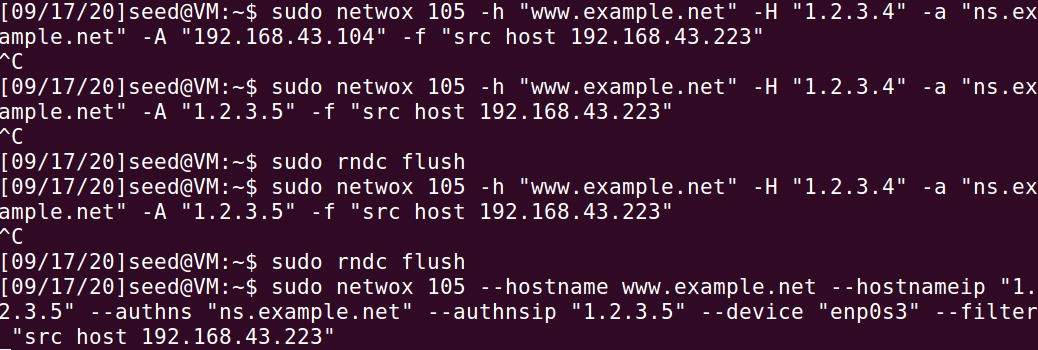




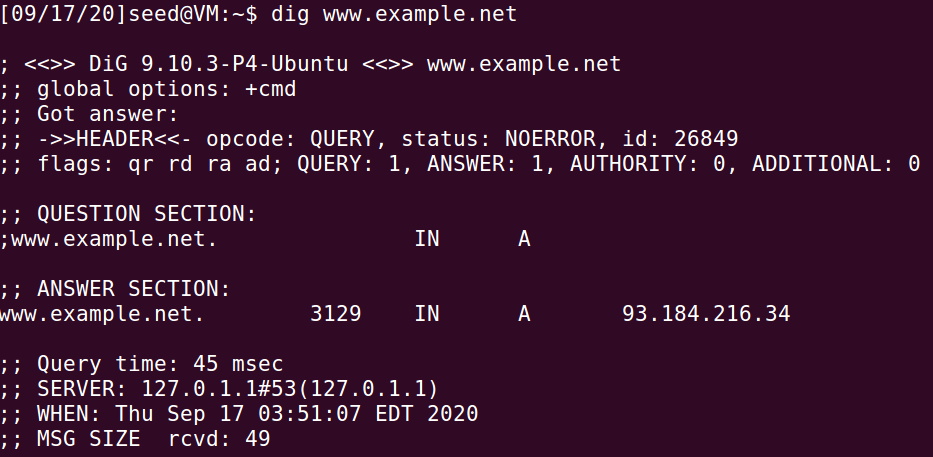
Task5: Directly Spooﬁng Response to User





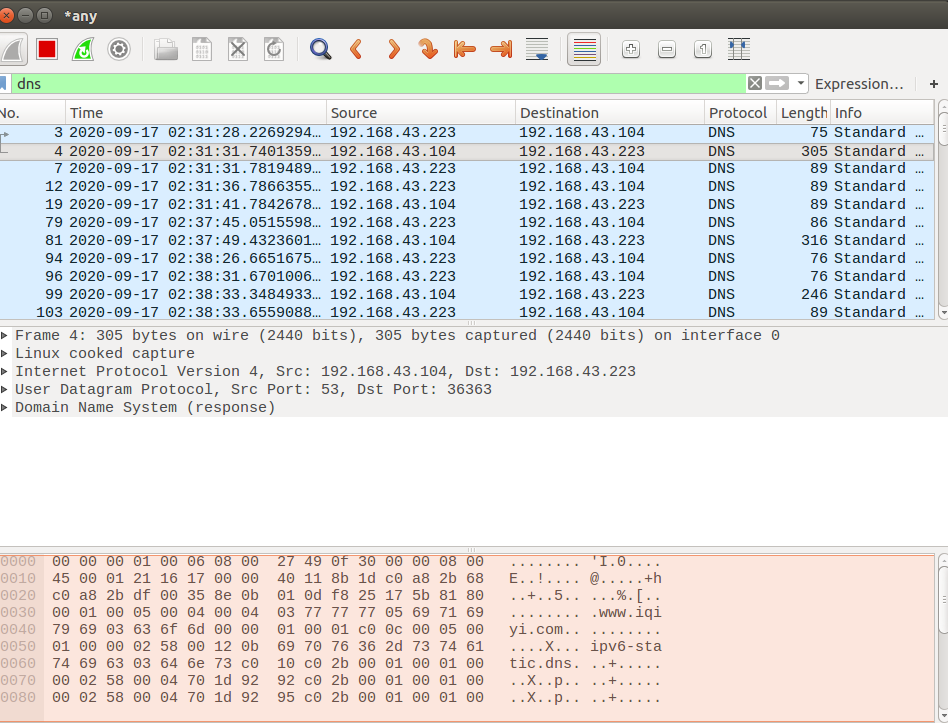


Task6: DNS Cache Poisoning Attack









Task7: DNS Cache Poisoning: Targeting the Authority Section

