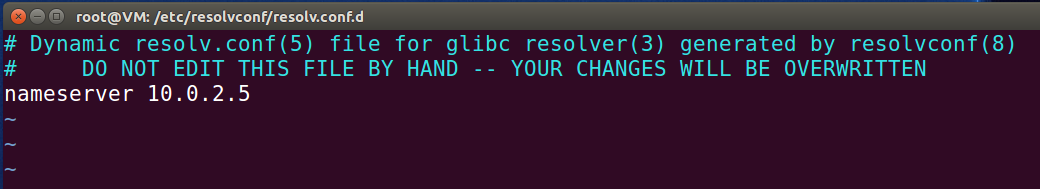
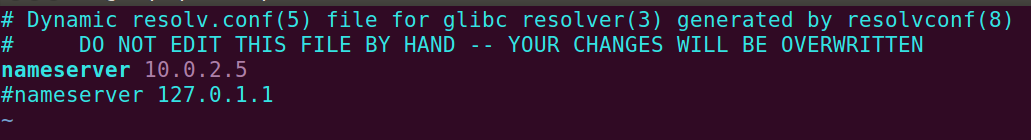
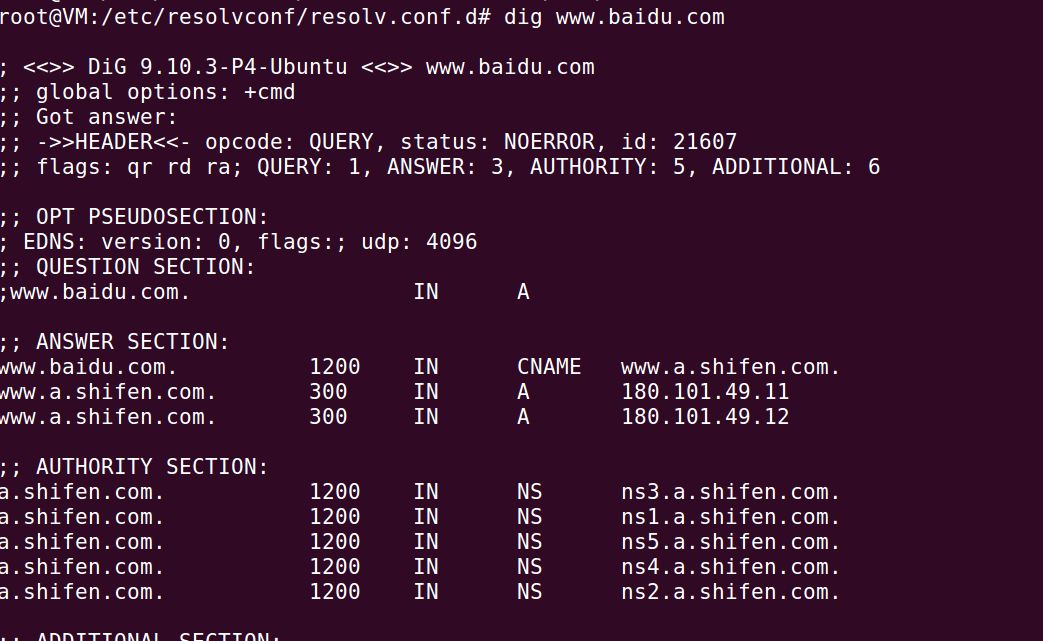
**Task1: Conﬁgure the UserMachine**

修改文件

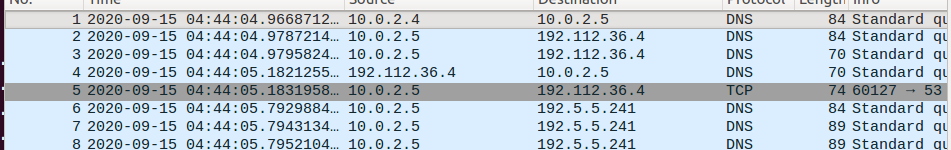




dig“www.baidu.com”

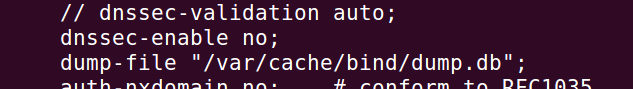


使用wireshark抓包，发现seed1（user）向seed3（server）发出了DNS包，成功



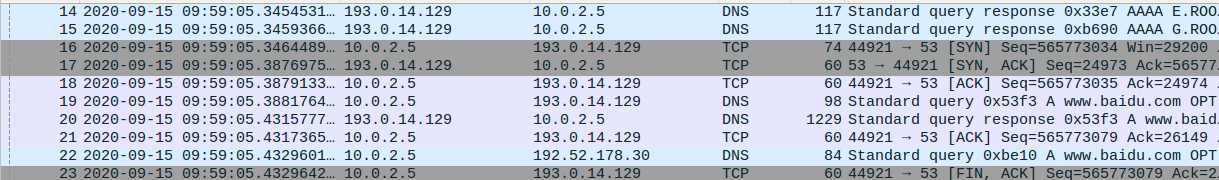
**Task2: Set up a Local DNS Server**

按步骤进入并修改相关文件

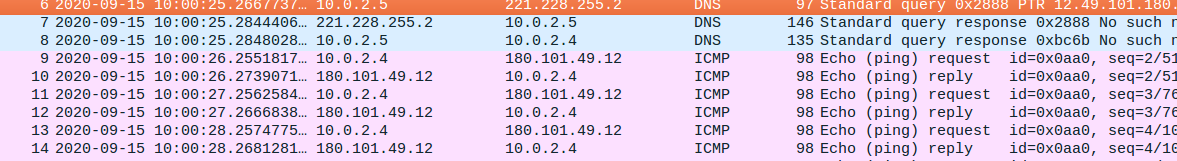




第一次访问baidu时出现了许多tcp报文，按常理应该是udp报文

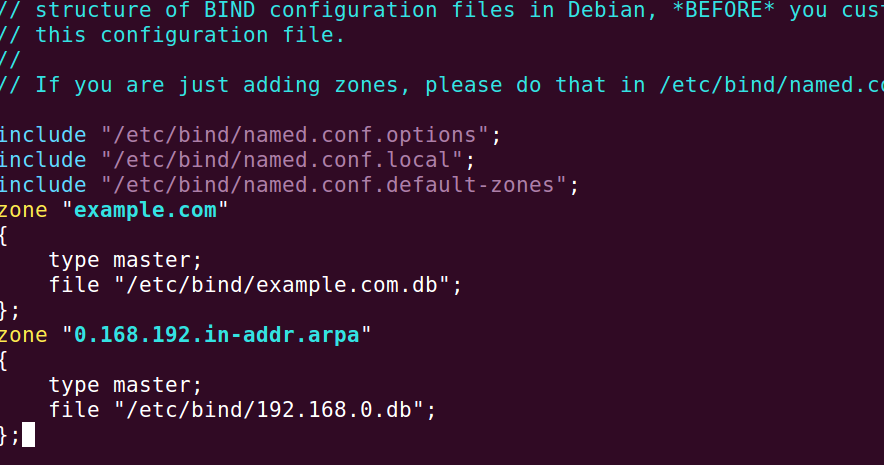


再次访问，就没有tcp报文，说明使用了缓存。

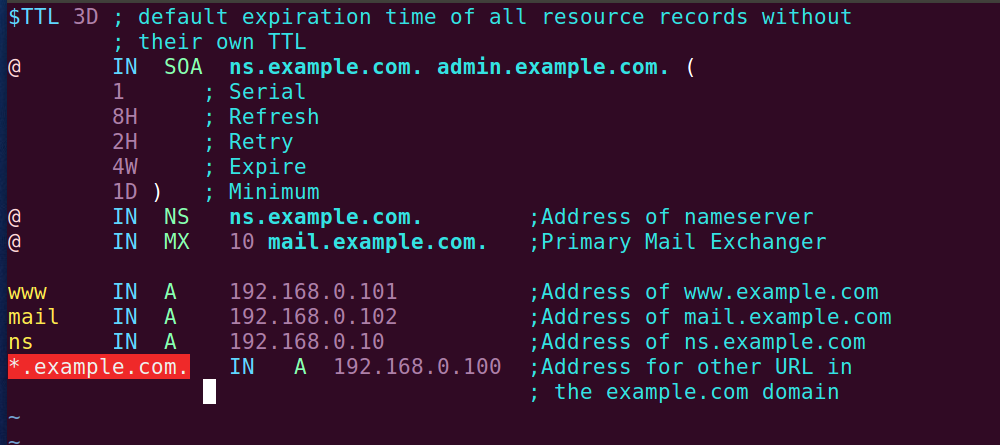


**Task 3: Host a Zone in the Local DNS Server**

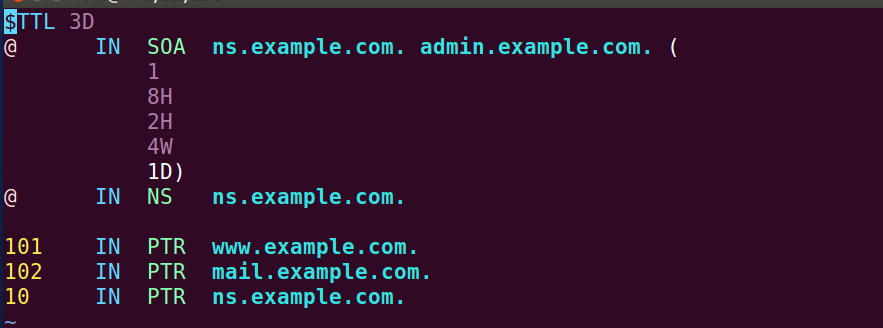
Create zones



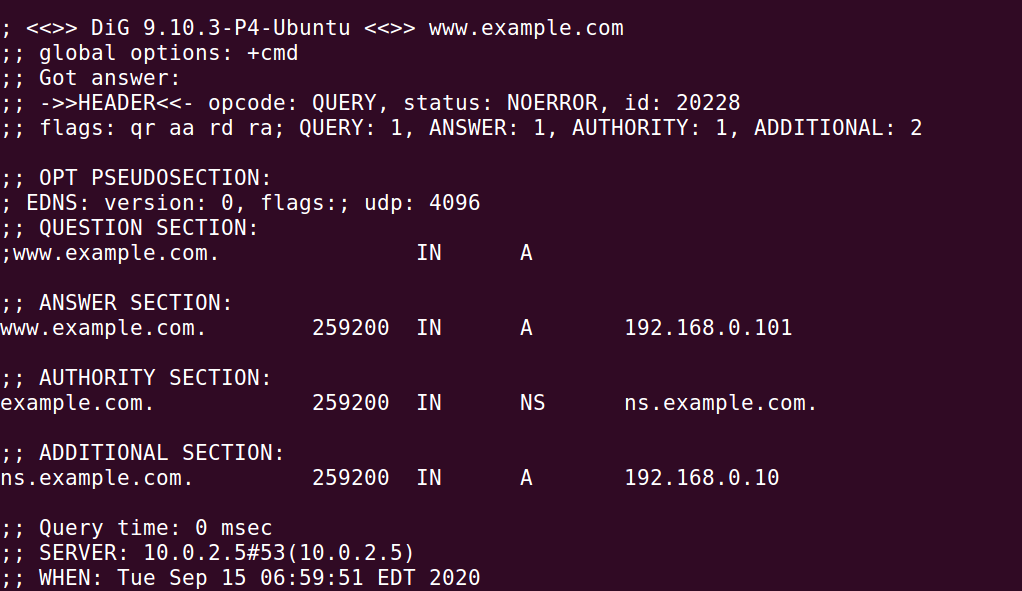
Setup the forward lookup zone ﬁle



Set up the reverse lookup zone ﬁle

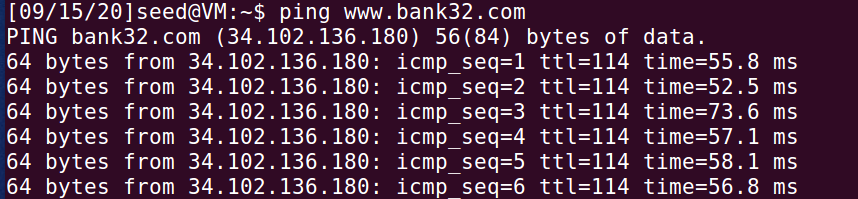


Restart the BIND server and test，dig“www.example.com”,指向了192.168.0.101，成功

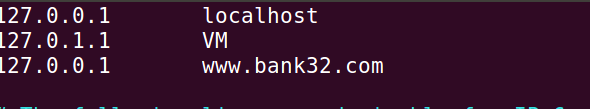
****

**Task4: Modifying the HostFile**

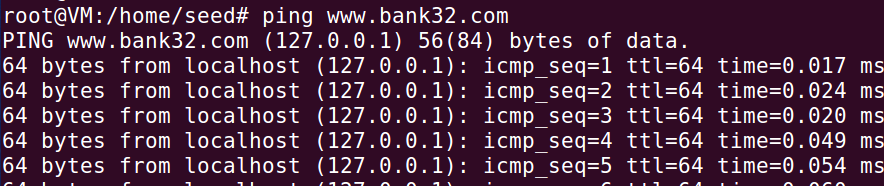
实现进行前，先ping“www.bank32.com”,发现ip为34.102.136.108



修改hsot文件

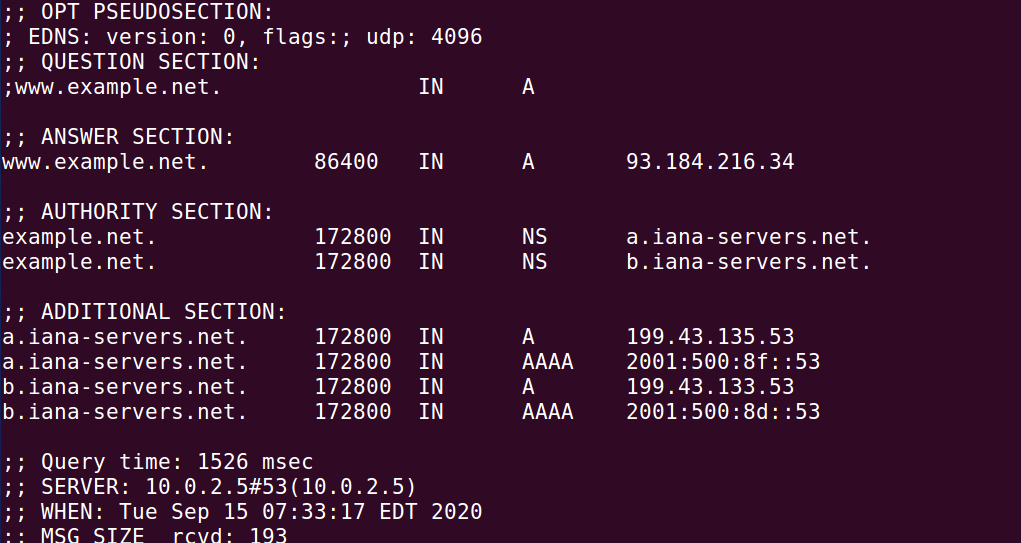


再次ping该网址，发现ip已经变成了127.0.0.1，成功

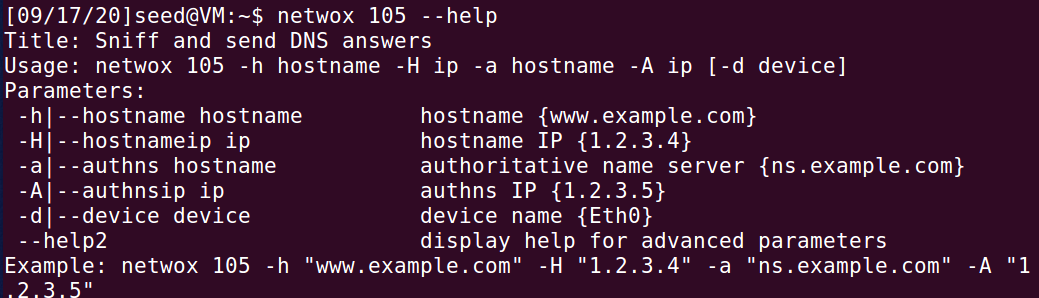


**Task5: Directly Spooﬁng Response to User**

运行攻击程序之前

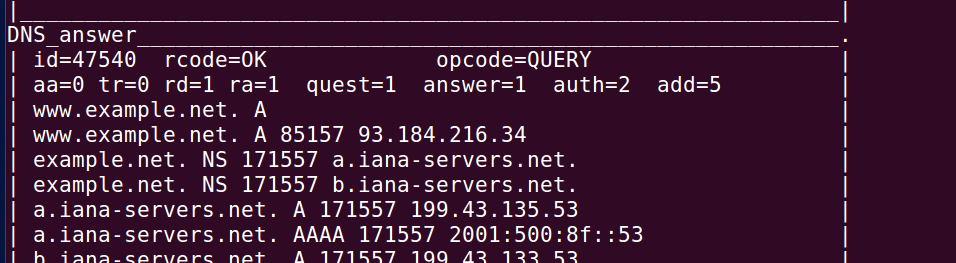


使用netwox 105 --help



模仿构造攻击程序





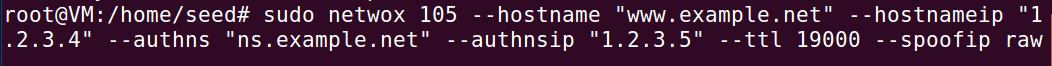
但攻击好像没有成功

**Task6: DNS Cache Poisoning Attack**

清除缓存



攻击程序

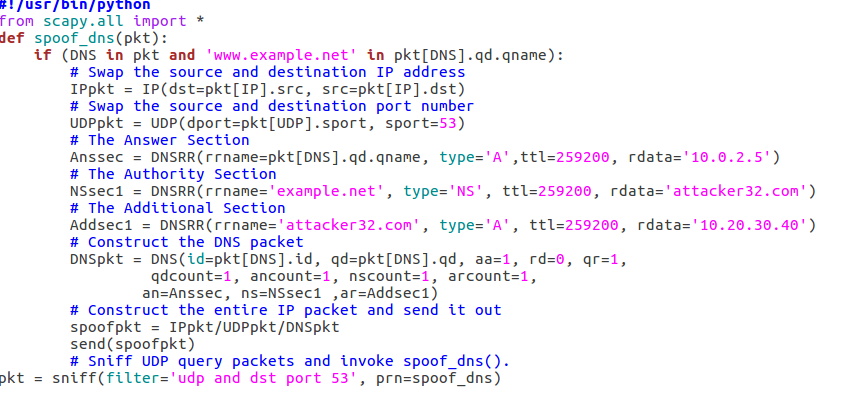


bad cache，攻击也没成功



**Task7: DNS Cache Poisoning: Targeting the Authority Section**

模仿构造攻击脚本



但攻击没能成功，task5-7都是bad cache，不知道哪里出现了问题