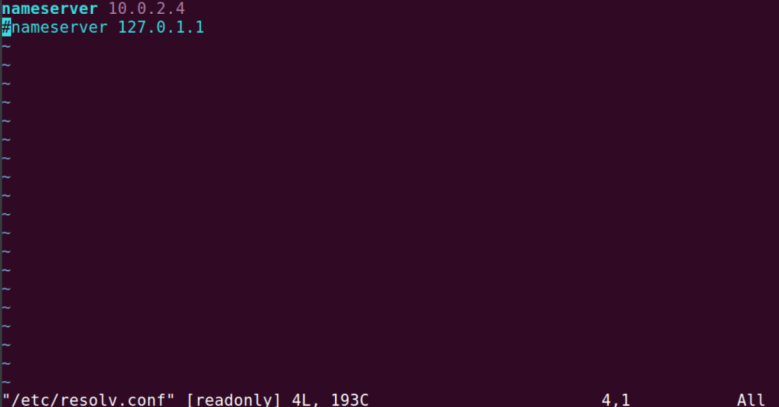
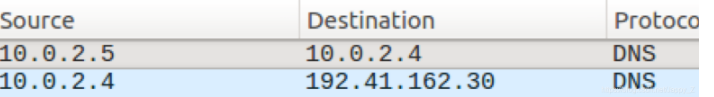
Local DNS Attack Lab 57117219尚林灏

Task1

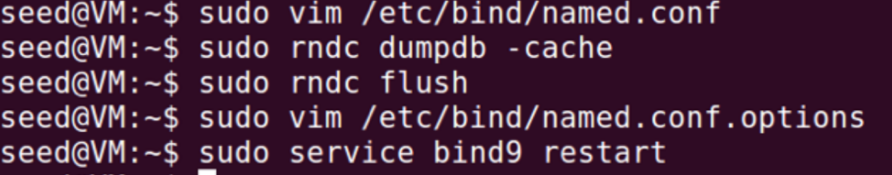
配置用户使用本地dns服务器，修改/etc/resolvconf/resolv.conf.d/head，开启虚拟机时，还要检查/etc/resolv.conf文件，将nameserver 127.0.1.1以及有时候会出现的fudan.edu.cn注释，保证只有一条nameserver指向本地服务器



用wireshark看向本地服务器发出的dns请求



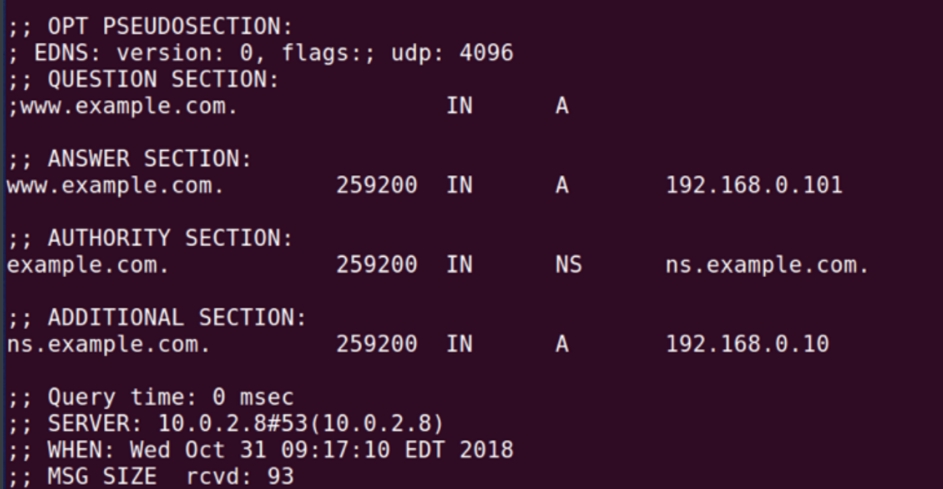
Task2



Task3

按照题⽬要求配置好了DNS Zone之后，在⽤户容器中请求解析 www.example.com 的IP

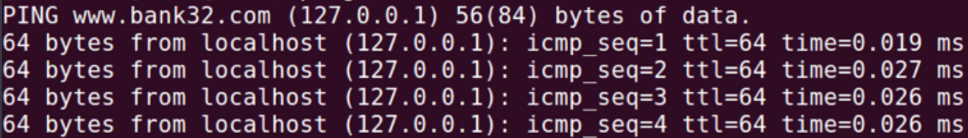
由于加入了zone，www.example.com会被解析到192.168.0.101

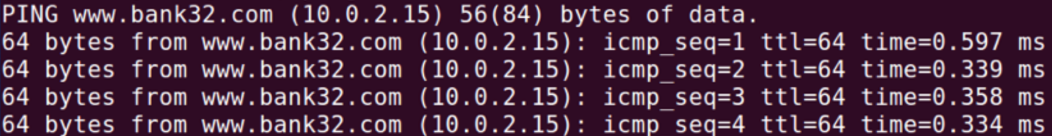


Task4

在修改 /etc/hosts ⽂件之前，在⽤户容器中 ping www.bank32.com。其IP是⼀个真实的外部IP。然后修改 /etc/hosts ⽂件，将 www.bank32.com 的IP写成 114.5.1.4 ，然后再次 ping

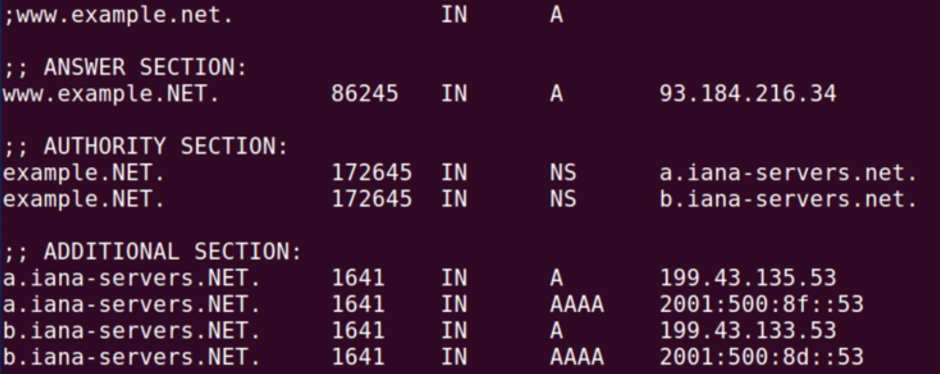
www.bank32.com



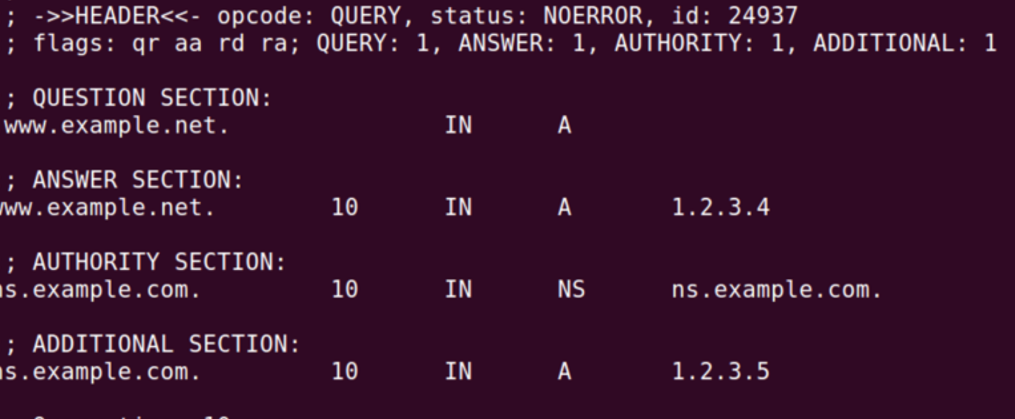


Task5

运行攻击程序之前

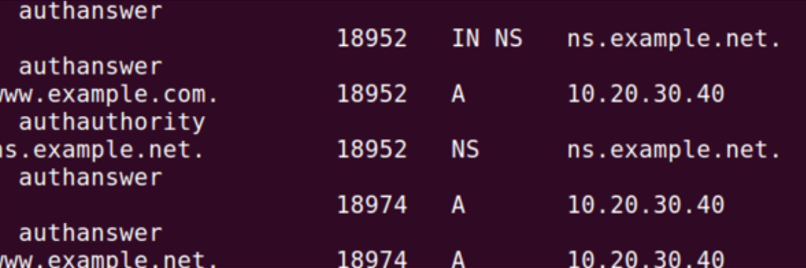


运行攻击程序之后



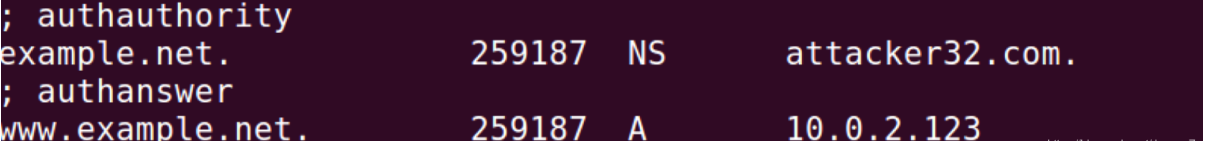
Task6

根据提示以network 105 --help可以构造出命令，其中–hostnameip "10.20.30.40"是将"www.example.net"映射到地址，–authnsip "10.20.30.50"是指"ns.example.net"这个dns服务器在该ip地址，由下图可以看到cache文件夹已经含有我们期望的信息



Task7

执行 sudo vim /var/cache/bind/dump.db后，查看dns缓存，发现成功缓存



运行wireshark发现example.net的域名下所有网站都会被解析到199.43.133.53(attacker32.com)的dns服务器

