常规的dns服务器无法保证来自服务器或客户端的数据是绝对可信的，而dnssec服务器可依靠创建的数字签名数据来检验其是可信的。

实验一：搭建dns服务器

首先安装dns服务器软件：BIND。

执行安装指令：

apt-get install bind9 dnsutils



cd /etc/bind

在里面创建文件db.example.com：

;

; BIND data file for local loopback interface

;

$TTL 604800

@ IN SOA ns.example.com. root.example.com. (

1 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

@ IN NS ns.example.com.

ns IN A 192.168.1.10

;also list other computers

box IN A 192.168.1.21

和db.192文件：

;

; BIND reverse data file for local loopback interface

;

$TTL 604800

@ IN SOA ns.example.com. root.example.com. (

2 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

@ IN NS ns.

10 IN PTR ns.example.com.

; also list other computers

21 IN PTR box.example.com.

修改**named.conf.local文件：**

zone "example.com" {

type master;

file "/etc/bind/db.example.com";

};

zone "1.168.192.in-addr.arpa" {

type master;

notify no;

file "/etc/bind/db.192";

};

**将named.conf.options文件中的**

//forwarders {

// 0.0.0.0;

// };

**替换为：**

forwarders {

1.2.3.4;

5.6.7.8;

};

**检验配置情况，结果如下：**

**named-checkconf**

**named-checkzone example.com /etc/bind/db.example.com**

**named-checkzone 1.168.192.in-addr.arpa. /etc/bind/db.192**



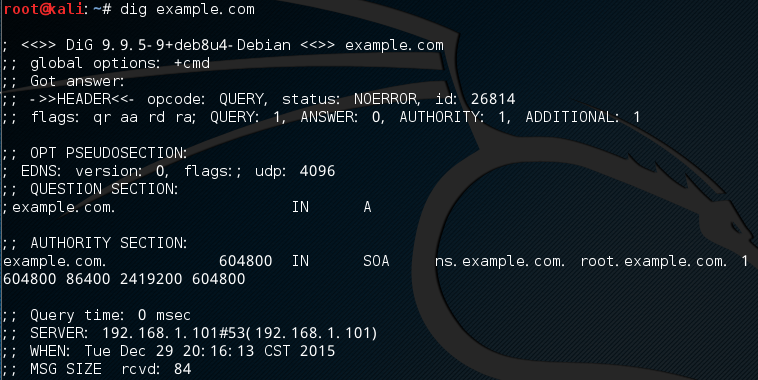
**打开服务器：**

**/etc/init.d/bind9 start**

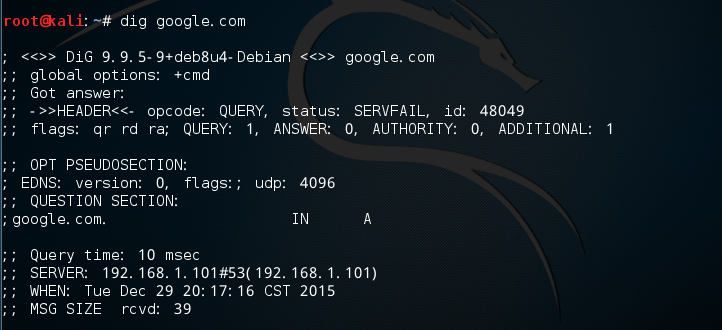


**执行指令：**

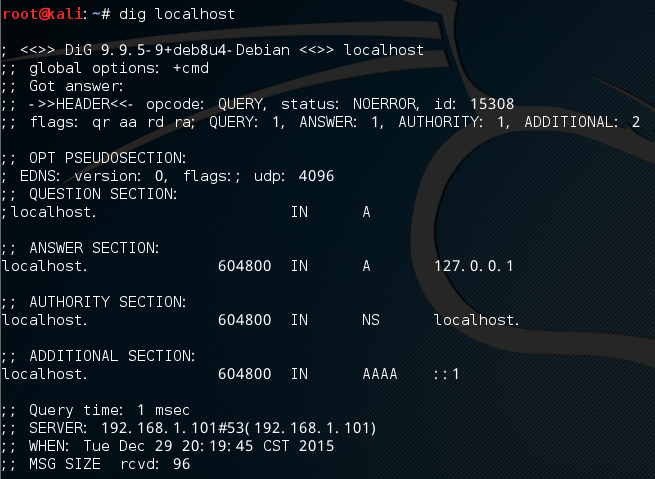
**dig example.com**



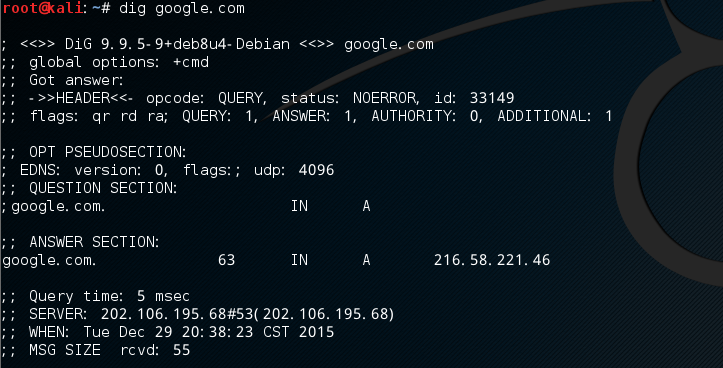
dig google.com



dig localhost



但dig的正常情况是这样的：



如此需要把庞大的数据量将dns数据导入其中，因此我偷了一次懒，索性将named.conf.options中改成：

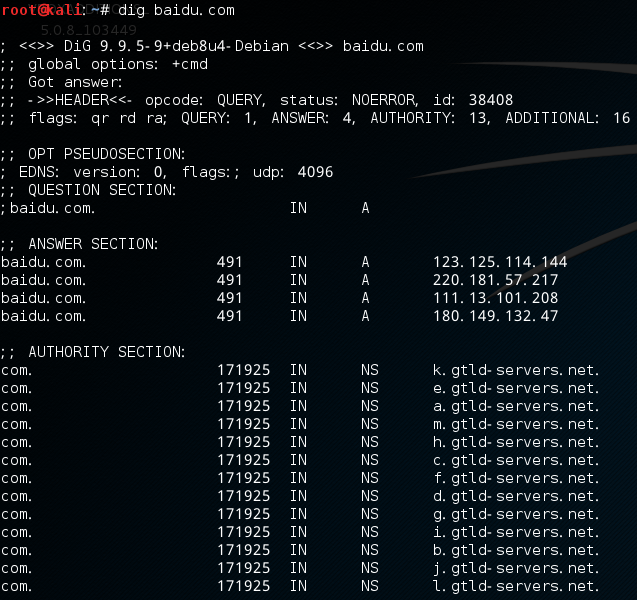
forwarders {

202.106.195.68;

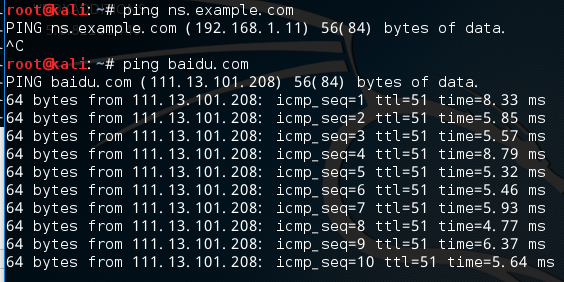
202.106.46.151;

};

这样就直接导入官方的dns地址解析了，如下图：



再度运行，发现dns已经成功解析：



至此一个可用的dns服务器以搭建完毕。