[Lab 1 Local DNS Attack Lab 2](#_Toc51230309)

[task 1 Conﬁgure the User Machine 2](#_Toc51230310)

[task 2 Set up a Local DNS Server 2](#_Toc51230311)

[task 3 Host a Zone in the Local DNS Server 3](#_Toc51230312)

[task4 Modifying the Host File 3](#_Toc51230313)

[task 5 Directly Spooﬁng Response to User 5](#_Toc51230314)

[task 6 DNS Cache Poisoning Attack 7](#_Toc51230315)

[task 7 DNS Cache Poisoning: Targeting the Authority Section 8](#_Toc51230316)

# Lab 1 Local DNS Attack Lab

## task 1 Conﬁgure the User Machine

手机屏幕截图

描述已自动生成手机屏幕的截图

描述已自动生成  
user虚拟机配置好了，可以看到此时本地的DNS服务器为首选服务器。

## task 2 Set up a Local DNS Server

手机屏幕截图

描述已自动生成

手机屏幕截图

描述已自动生成

cache使用之后，域名解析就有确定结果了 而不是想之前没有返回answer。

## task 3 Host a Zone in the Local DNS Server

电脑屏幕的照片上有文字

描述已自动生成

可以看到DNSVM配置完成后，解析出来我们配置好的结果。

## task4 Modifying the Host File

图片包含 桌子, 游戏机, 人们

描述已自动生成

电脑屏幕的照片上有文字

描述已自动生成

在修改hosts之前，可以看到ping命令和dig命令对[www.bank32.com](http://www.bank32.com)的解析结果一致。

现在修改hosts文件：

手机屏幕截图

描述已自动生成

图片包含 键盘, 电脑

描述已自动生成电脑屏幕的照片上有文字

描述已自动生成

可以看到两次结果不一致，这次ping命令解析的结果被修改为hosts文件中的值。

## task 5 Directly Spooﬁng Response to User

攻击开始前：

屏幕上有字

描述已自动生成

attackerVM上的命令为：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

屏幕上有字

描述已自动生成手机屏幕的截图

描述已自动生成

可以看到userVM被成功欺骗至220.181.38.148（这是baidu的网址）。

## task 6 DNS Cache Poisoning Attack

在用户VM上执行dig example.net

图片包含 文字, 游戏机

描述已自动生成

在攻击VM上执行如下命令

电脑屏幕的截图

描述已自动生成

最后在DNSVM上看到cache中的记录已经变成被欺骗后的结果。实验成功。



## task 7 DNS Cache Poisoning: Targeting the Authority Section

在userVM上：

手机屏幕的截图

描述已自动生成

在attackerVM上：

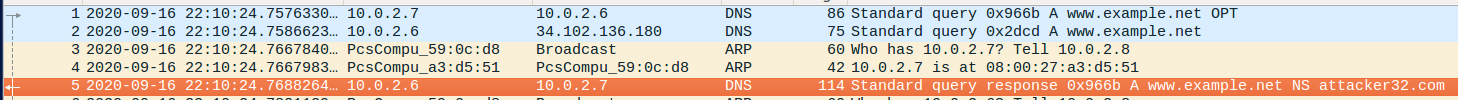
手机屏幕截图

描述已自动生成

在DNSVM上的local cache中记录：

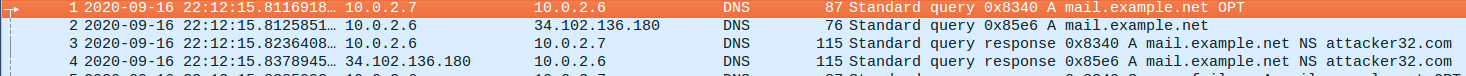


在userVM上访问[www.example.net](http://www.example.net) 抓包结果如图：



可以看到已经被转向到访问attacker32.com了。

在userVM上访问[mail.example.net](http://www.example.net) 抓包结果如图：



结果一样被转向访问attacker32.com。

实验成功