中南大學
CENTRAL SOUTH UNIVERSITY

网络安全

实验报告

学生姓名 马田瑶

学　　号 0906140124

专业班级 信息安全 **1401**

指导教师 王伟平

学　　院 信息科学与工程学院

完成时间 2016 年 12 月

实验二　本地 DNS 攻击

一、实验目的

通过实验 DNS 攻击过程，加深对 DNS 服务原理的理解。

二、实验内容

在 SEED Project 网站的指导下，通过查询资料，独立完成本地 DNS 攻击实验。

三、实验原理

DNS 服务器完成域名到 IP 的映射，攻击者可通过截获 DNS 发送给用户的应到包，修改对应的 IP 地址，将用户引到一个恶意的网站；或者攻击者可以篡改 DNS 服务器发出的询问包，从而在 DNS 服务器上有一个错误的映射。

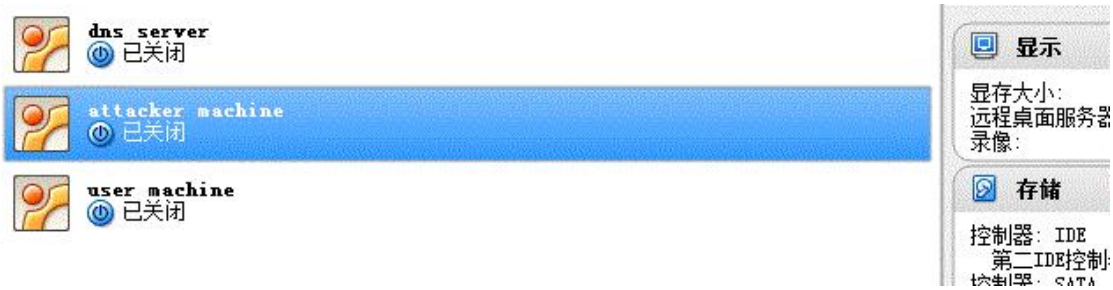
四、实验环境

VirtualBox　Ubuntu

五、实验步骤

1、按照 description 搭建环境

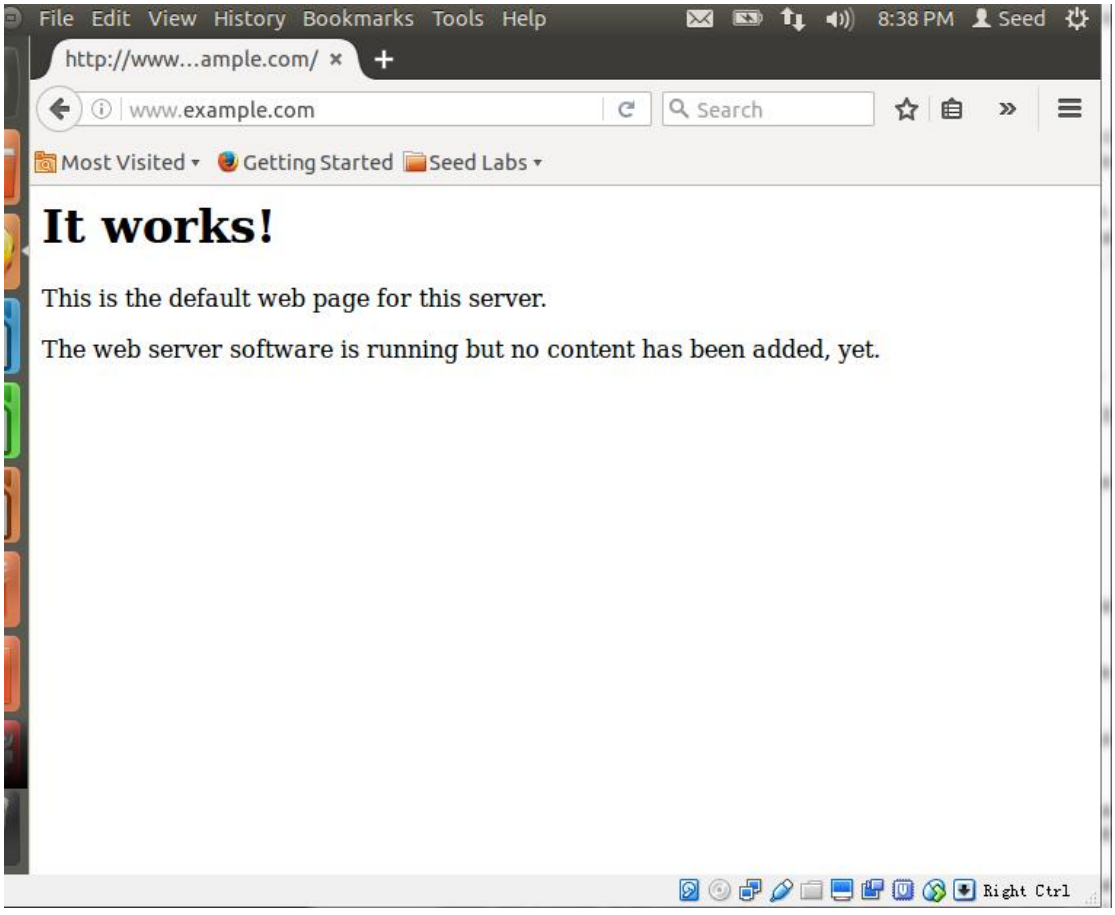
新建一个虚拟机，并以他为模板克隆出另外两个分别为 DNS 服务器，攻击者，被攻击者



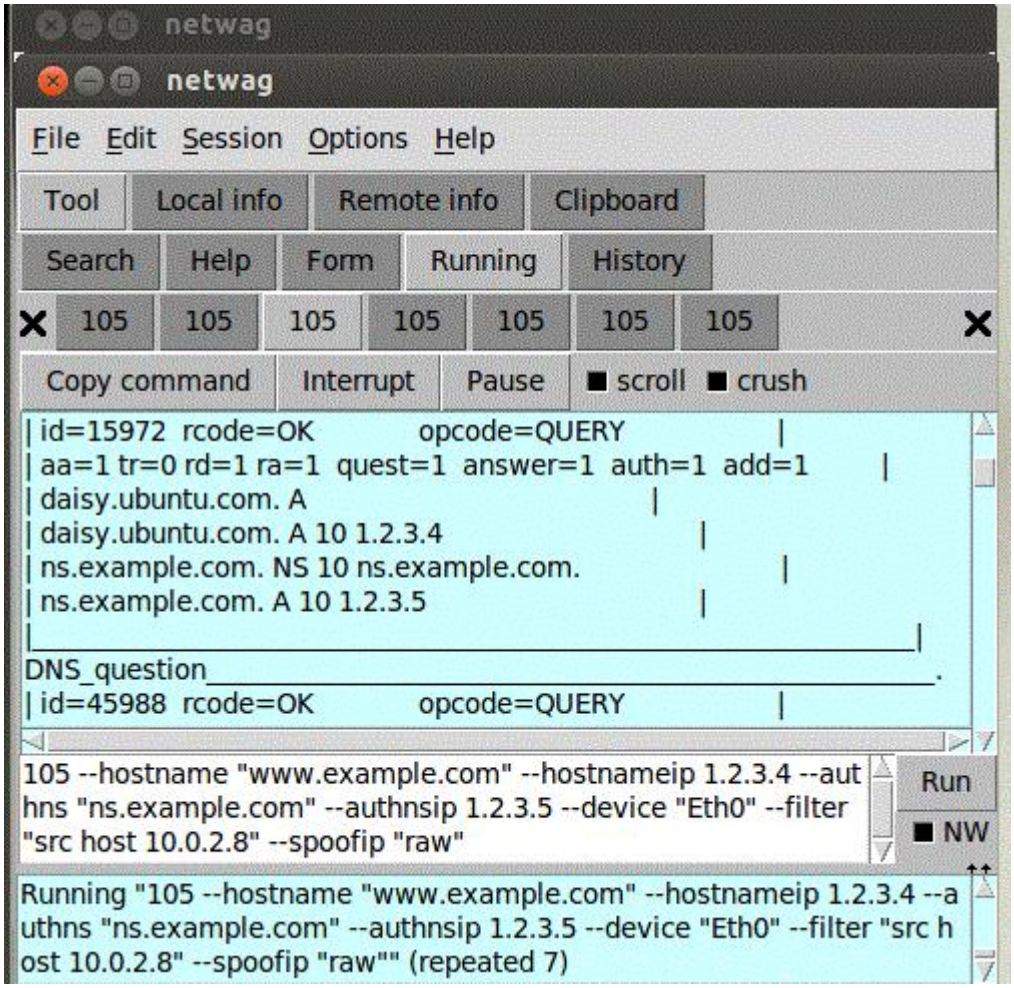
2、攻击者已控制被攻击者的电脑，修改了文件中 example.com 的 ip

```
127.0.0.1       www.SQLLabCollabtive.com

127.0.0.1       www.XSSLabCollabtive.com

127.0.0.1       www.SOPLab.com
127.0.0.1       www.SOPLabAttacker.com
127.0.0.1       www.SOPLabCollabtive.com

127.0.0.1       www.OriginalphpMyAdmin.com

127.0.0.1       www.CSRFLabElgg.com
127.0.0.1       www.XSSLabElgg.com
127.0.0.1       www.SeedLabElgg.com
10.0.2.5        www.heartbleedlabelgg.com
127.0.0.1       www.WTLabElgg.com

127.0.0.1       www.wtmobilestore.com
127.0.0.1       www.wtshoestore.com
127.0.0.1       www.wtelectronicsstore.com
127.0.0.1       www.wtcamerastore.com

127.0.0.1       www.wtlabadserver.com
1.2.3.4         www.example.com
```

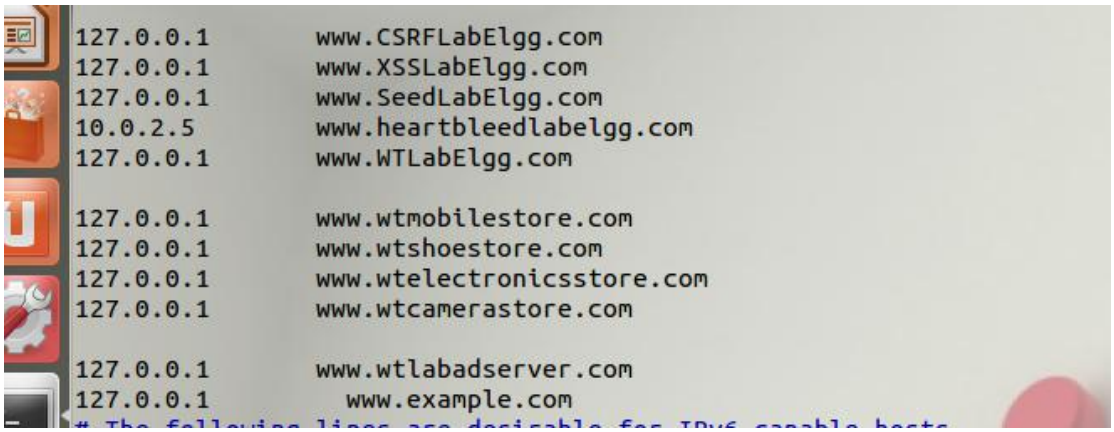
访问该网站



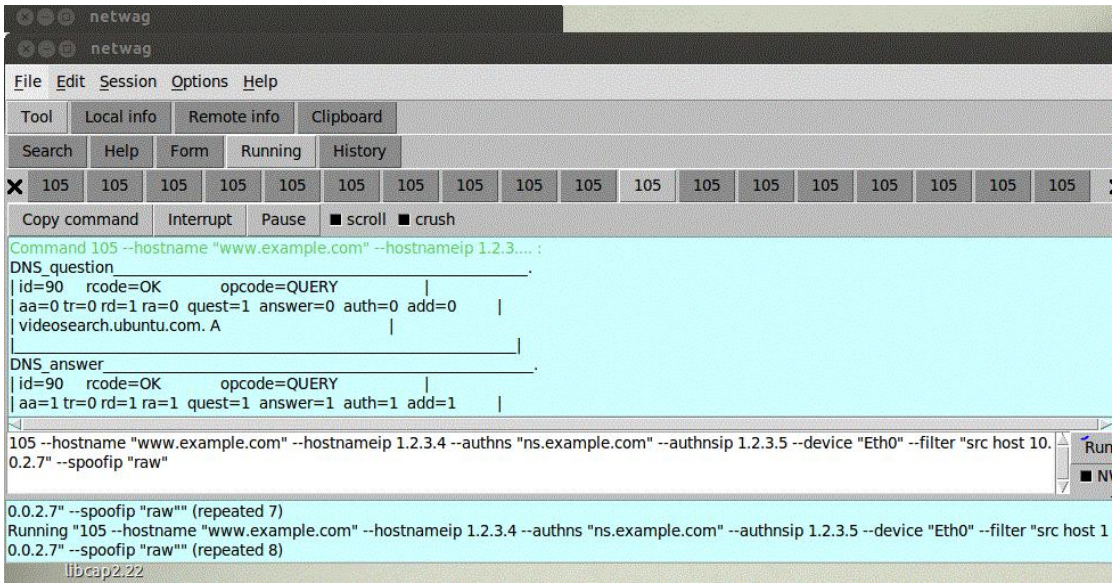
3、攻击者截获 DNS 发出的应答包并修改 ip 为 1.2.3.4



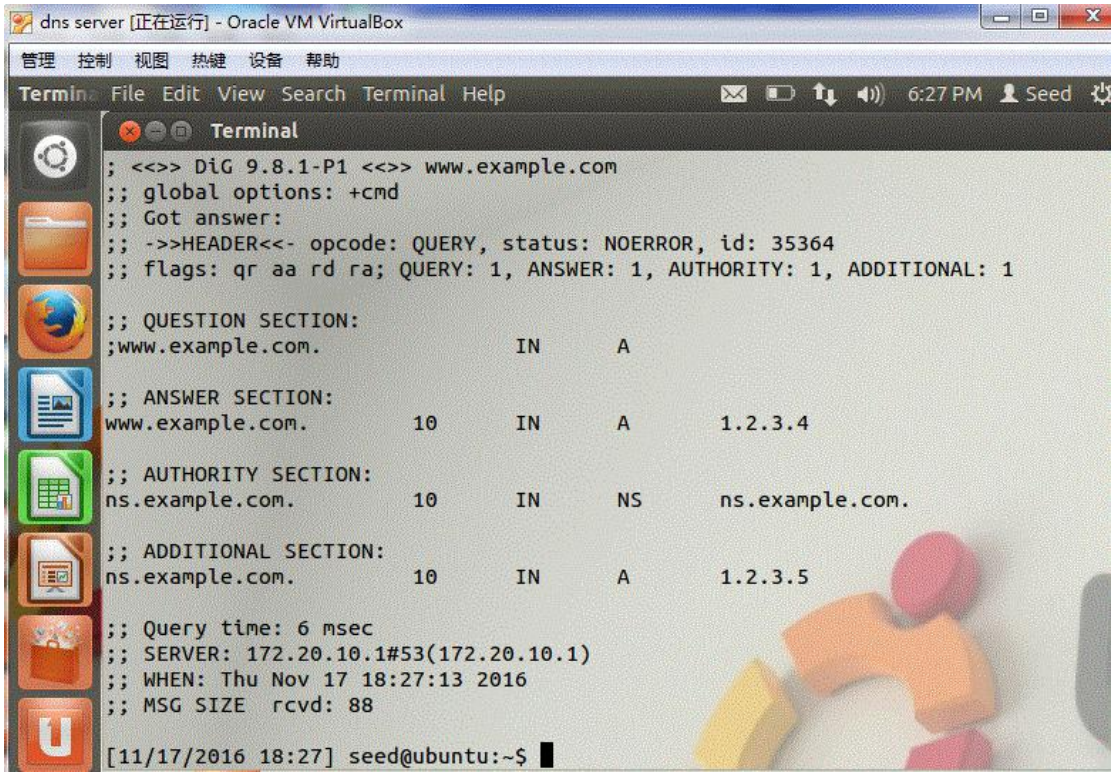
被攻击者再次查询 ip



4、攻击者修改 DNS 服务器发出的包,是的 DNS 服务器上 example.com 对应的 ip 地址是错误的



DNS 服务器收到包后,再次查询 ip



六、攻击原理

攻击者通过捕包，构造假包，篡改 ip，使得被攻击者获得一个假的 ip 地址，从而进入恶意的网站。

六、实验总结

通过此次试验，我对 DNS 的攻击过程有了了解，以前只是知道 DNS 可以将域名解析为 ip 地址，并不知到攻击的原理，实验后，我不仅对 DNS 的服务过程有了更深的认识，对 Ubuntu 的使用也更加熟练，对 Linux 的学习有很大的帮助。