

# 本地 DNS 攻击实验室

## 一、实验室概述

DNS（域名系统）是互联网的电话簿;它将主机名转换为 IP 地址（或 IP 地址到主机名）。这种翻译是通过 DNS 解析，发生在幕后。DNS Pharming 攻击以各种方式操纵这个解析过程，意图误导用户到其他目的地，这通常是恶意的。本实验的目的是了解这种情况攻击工作。学生将首先设置和配置 DNS 服务器[2]，然后他们将尝试各种 DNS

对同样在实验室环境中的目标的药物攻击。

攻击本地受害者与远程 DNS 服务器的困难是完全不同的。因此，我们已经开发了两个实验室，一个侧重于本地 DNS 攻击，另一个侧重于远程 DNS 攻击。本实验关注本地攻击。

## 二、实验室环境

我们需要设置实验室环境。为了简化实验室环境，我们让用户的计算机，DNS 服务器和攻击者的计算机在一台物理机上，但使用不同的虚拟机。本实验中使用的网站可以是任何网站。我们的配置是基于 Ubuntu，

这是我们在预构建的虚拟机中使用的操作系统。

我们设置了 DNS 服务器，用户计算机和攻击者机器同一个局域网。我们假设用户计算机的 IP 地址是 192.168.0.100，DNS 服务器的 IP 是 192.168.0.10，攻击者的 IP 为 192.168.0.200。

教师注：对于本实验，实验室会议是可取的，特别是如果学生不熟悉工具和环境。

## 三、实验过程

- 1.使用虚拟机软件。
- 2.使用 Wireshark，Netwag 和 Netwox 工具。
- 3.配置 DNS 服务器。

### 2.1 安装并配置 DNS 服务器

步骤 1: 安装 DNS 服务器。在 192.168.0.10, 我们使用安装 BIND9 [3]

DNS 服务器

以下命令:

1 我们假设教师已经在讲座中涵盖了攻击的概念, 所以我们不将它们包括进来

实验室会议。

SEED 实验室 - 本地 DNS 攻击实验室 2

受害者

DNS 服务器

(Apollo)

192.168.0.10

袭击者

192.168.0.200

.COM

DNS 服务器

用户

192.168.0.100

根

DNS 服务器

LAN 或虚拟网络

example.com

DNS 服务器

互联网

图 1: 实验室环境设置

```
# sudo apt-get install bind9
```

BIND9 服务器已经安装在我们预先构建的 Ubuntu 虚拟机映像中。

步骤 2: 创建 named.conf.options 文件。 DNS 服务器需要读取/ etc / bind /

named.conf 配置文件启动。此配置文件通常包括一个选项文件称为/ etc / bind / named.conf.options。请将以下内容添加到选项文件:

```
options {
```

```
dump-file"/var/cache/bind/dump.db";
```

```
};
```

应该注意，文件/var/cache/bind/dump.db 用于转储 DNS 服务器的缓存。

步骤 3：创建区域。假设我们拥有一个域：example.com，这意味着我们负责

用于提供关于 example.com 的最终答案。因此，我们需要在中创建一个区域

DNS 服务器通过添加以下内容到/etc/bind/named.conf。应该注意的是 example.com 域名保留供文档使用，不属于任何人，因此是安全使用它。

```
zone"example.com"{
```

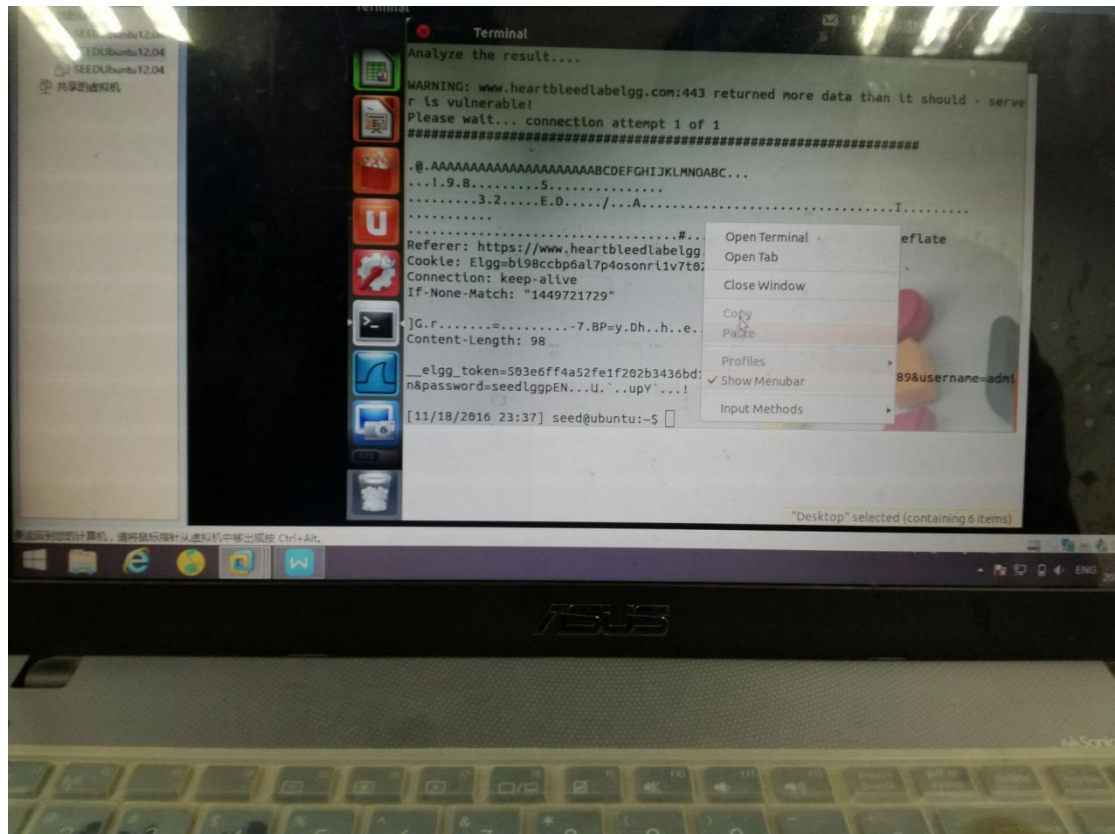
```
文件"/var/cache/bind/example.com.db";};
```

```
区域"0.168.192.in-addr.arpa"{
```

SEED 实验室 - 本地 DNS 攻击实验室 3

```
文件"/var/cache/bind/192.168.0";};
```

实验截图：

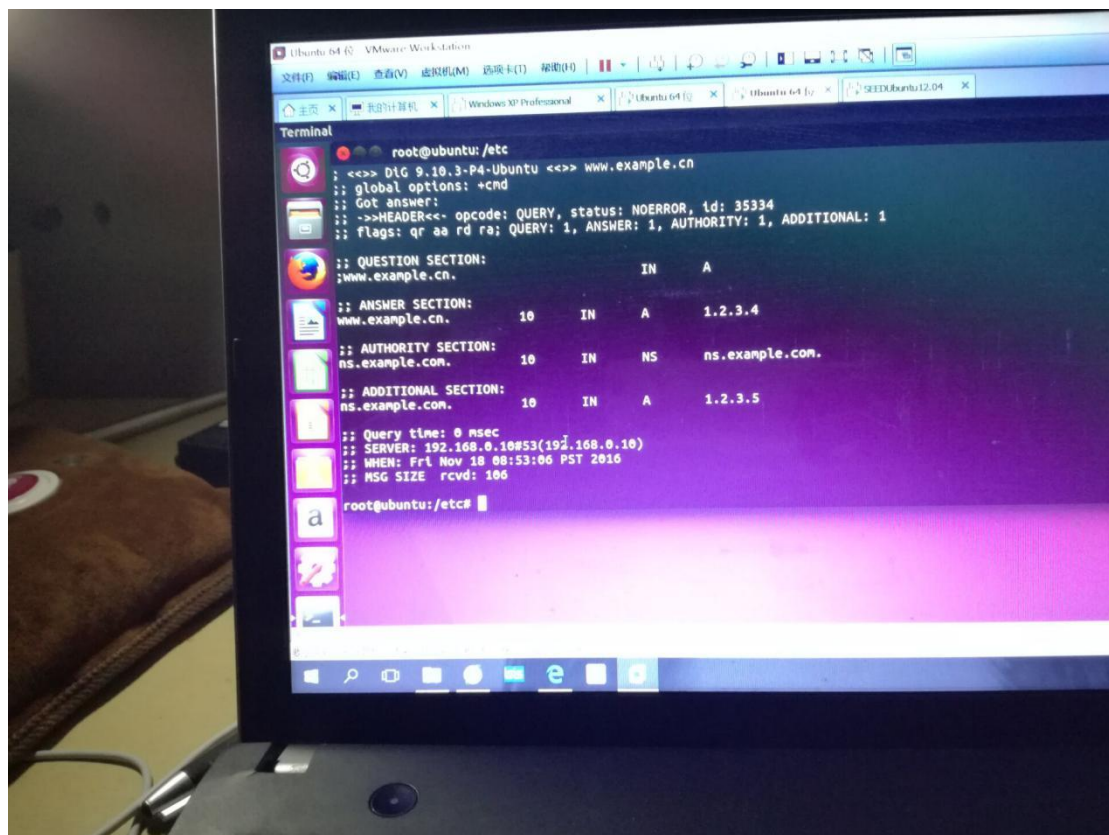
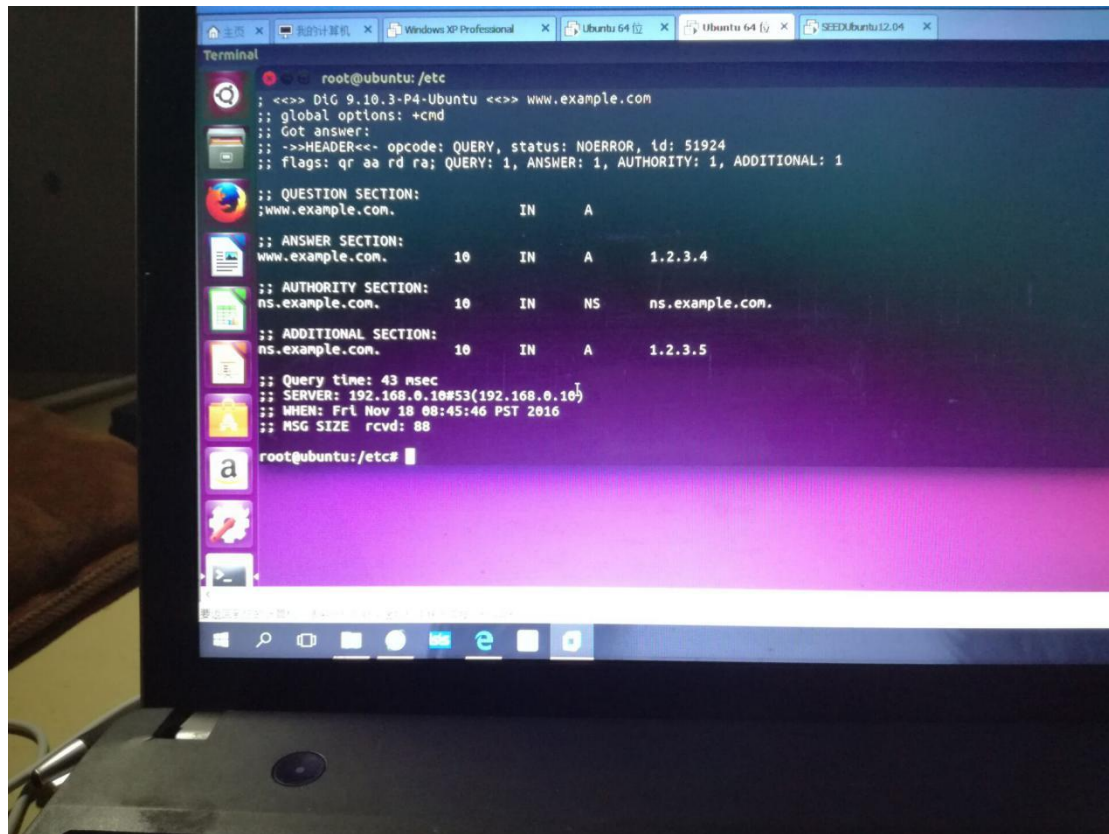


```
ntu:/etc# ifconfig ens33 192.168.0.200
ntu:/etc# ifconfig ens33 192.168.0.100
ntu:/etc# dig www.example.com

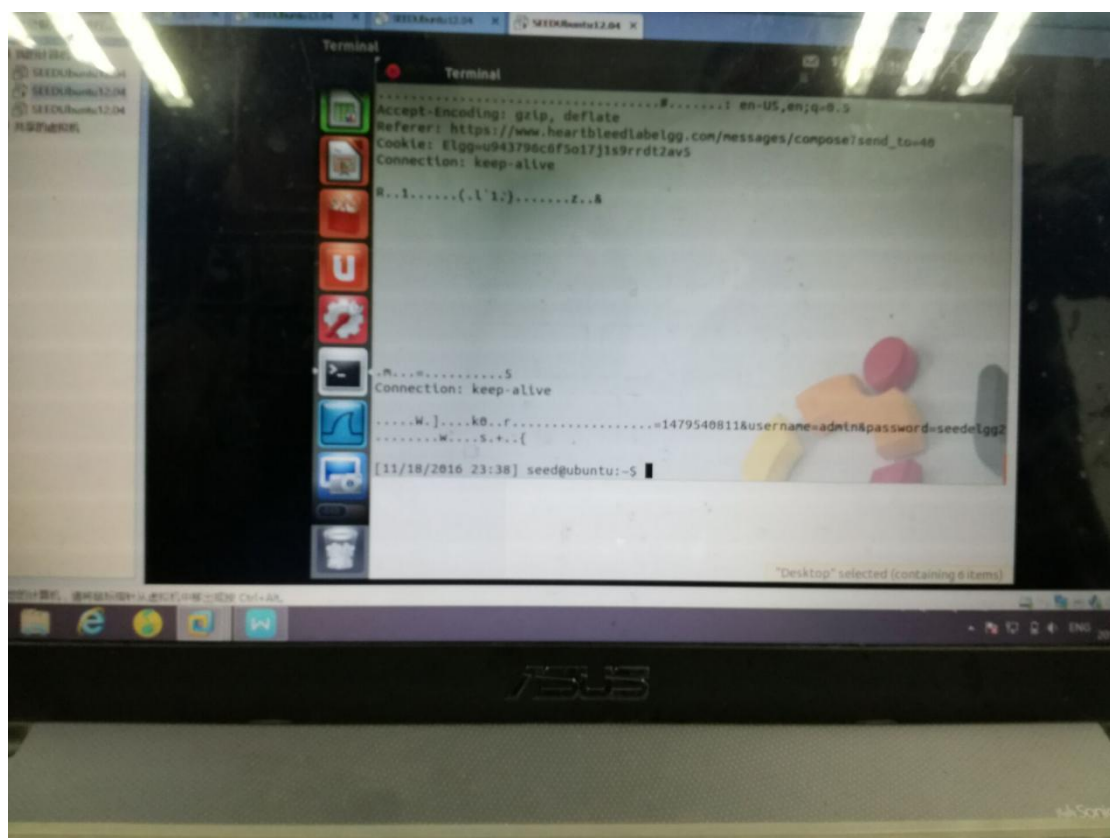
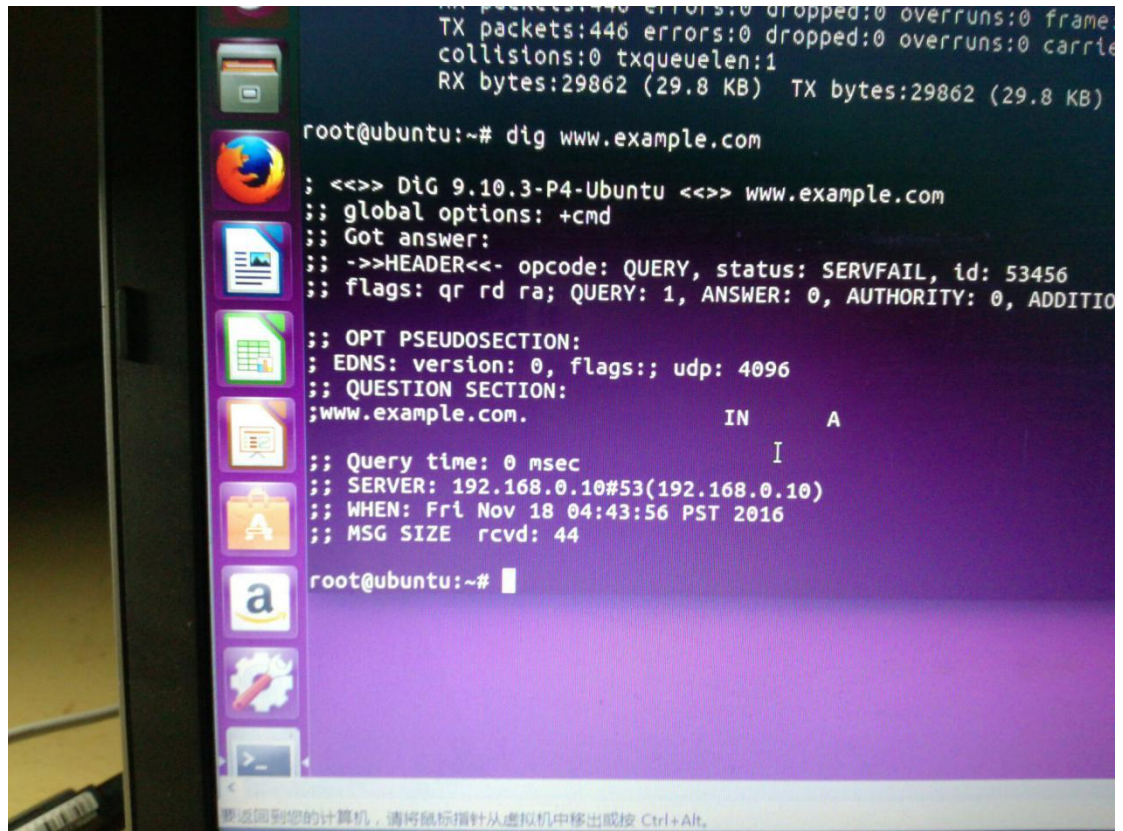
; <>> www.example.com
options: +cmd
answer:
HEADER<<- opcode: QUERY, status: SERVFAIL, id: 38045
: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

PSEUDOSECTION:
version: 0, flags:; udp: 4096
QUESTION SECTION:
example.com.                IN      A

y time: 6 msec
ER: 192.168.0.10#53(192.168.0.10)
: Fri Nov 18 07:46:45 PST 2016
SIZE rcvd: 44
untu:/etc#
```







## 四、实验总结

我们认为，在这学期的实验中，在收获知识的同时，还收获了阅历，收获了成熟，在此过程中，我们通过查找大量资料，请教老师，以及不懈的努力，不仅培养了独立思考、动手操作的能力，在各种其它能力上也都有了提高。更重要的是，在实验课上，我们学会了很多学习的方法。而这是日后最实用的，真的是受益匪浅。要面对社会的挑战，只有不断的学习、实践，再学习、再实践。