

## 实验二 DNS 攻击

### 一、实验目的

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。DNSPharming 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。

### 二、实验内容

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 DNS 本地攻击。

### 三、实验原理

设置和配置 DNS 服务器[，然后尝试各种 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。

### 四、实验环境

VirtualBox Ubuntu 实验室环境

### 五、实验过程

使用虚拟机软件。使用 Wireshark，Netwag 和 Netwox 工具。

配置 DNS 服务器。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。

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 {

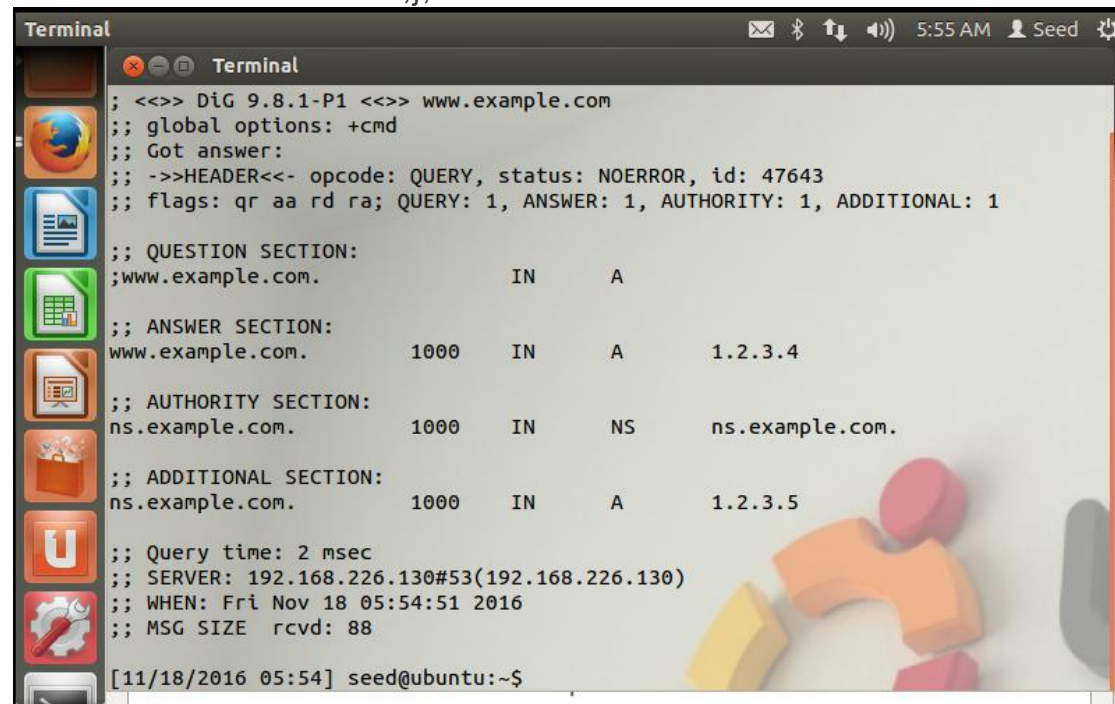
```
dump-file"/var/cache/bind/dump.db";};
```

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



```
Terminal
; <<>> DiG 9.8.1-P1 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47643
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.example.com.                IN      A

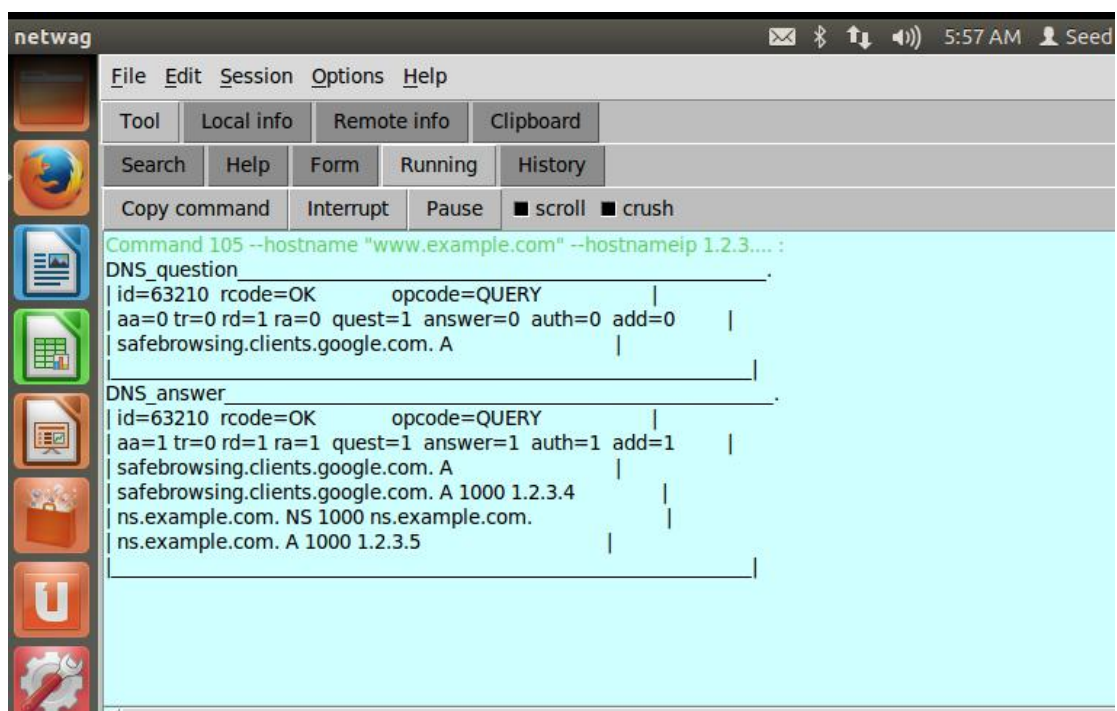
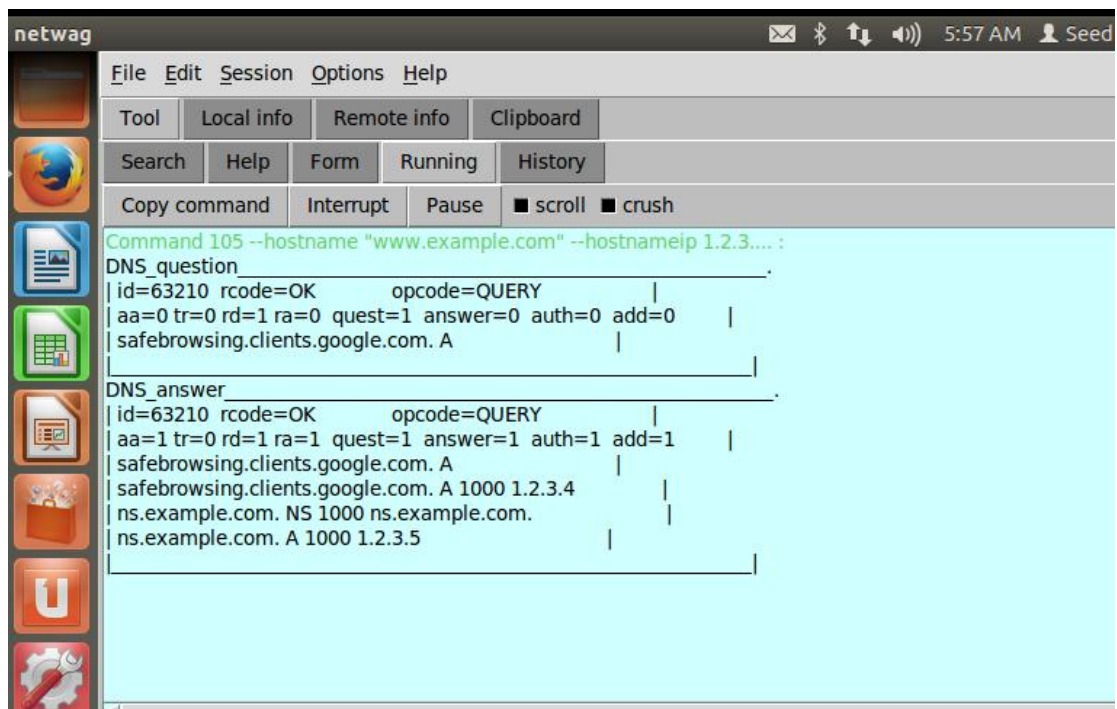
;; ANSWER SECTION:
www.example.com.                1000    IN      A      1.2.3.4

;; AUTHORITY SECTION:
ns.example.com.                 1000    IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.                 1000    IN      A      1.2.3.5

;; Query time: 2 msec
;; SERVER: 192.168.226.130#53(192.168.226.130)
;; WHEN: Fri Nov 18 05:54:51 2016
;; MSG SIZE rcvd: 88

[11/18/2016 05:54] seed@ubuntu:~$
```



## 六、实验感想

通过本次实验，了解了 DNS 攻击的原理，因为对文件的操作较多，其实对具体文件作用并不太清楚，只是机械的操作，希望以后能加深理解，进而对种类丰富的 DNS 攻击有更深的领悟。