# 网络安全实验二

## DNS 攻击实验

华中科技大学网络空间安全学院

二零二一年四月

# 1 实验目的

DNS（域名系统）将主机名转换为 IP 地址（反之亦然）。此转换是通过 DNS 解析，在后台发生的。DNS 攻击以各种方式操纵此解析过程，意图将用户误导到其他目的地，这些目的地通常是恶意的。本实验的目的是了解此类攻击的工作原理。学生首先要设置并配置 DNS 服务器，然后尝试对同样位于实验环境中的目标主机进行各种 DNS 攻击。

攻击本地主机与攻击远程 DNS 服务器的困难是截然不同的。 因此，我们设置了两个实验，一个侧重于本地 DNS 攻击，另一个侧重于远程 DNS 攻击。本实验侧重于本地攻击。本实验包含以下主要内容：

- DNS 及其工作原理
- DNS 服务器设置
- DNS 缓存中毒攻击
- 欺骗 DNS 响应
- 数据包嗅探和欺骗
- Scapy 工具

# 2 实验环境

VMware Workstation 虚拟机。

Ubuntu 16.04 操作系统（SEEDUbuntu16.04）。

# 3 实验要求

熟悉 DNS 协议和工作原理。

掌握本地 DNS 欺骗攻击、DNS 缓存中毒攻击的原理。

使用本实验提供的虚拟机完成实验内容。

通过实验课的上机实验，演示给实验指导教师检查，并提交详细的实验报告。

# 4 实验内容

## 4.1 设置本地 DNS 服务器

本实验的主要目的是 DNS 攻击，我们的攻击目标是本地 DNS 服务器。显然，攻击真机是违法的，所以我们需要建立自己的 DNS 服务器来进行攻击实验。实验室环境需要三台独立的机器：一台作为被攻击者，一台作为 DNS 服务器，另一台作为攻击者。我们将在一台物理机器上运行这三个虚拟机。所有这些 VM 都将运行我们预先构建的 Ubuntu VM 映像。图 1 说明了实验环境的设置。 对于 VM 网络设置，如果使用的是 VirtualBox，请使用“NAT Network”作为每个 VM 的网络适配器。如果使用的是 Vmware，则默认的“NAT”设置就可以。

为简单起见，我们将所有这些 VM 放在同一网络上。在以下部分中，我们假设用户主机的 IP 地址为 10.0.2.18，DNS 服务器的 IP 为 10.0.2.16，攻击者计算机的 IP 为 10.0.2.17。我们需要配置用户机器和本地 DNS 服务器，对于攻击者计算机，VM 中的默认设置应该足够。

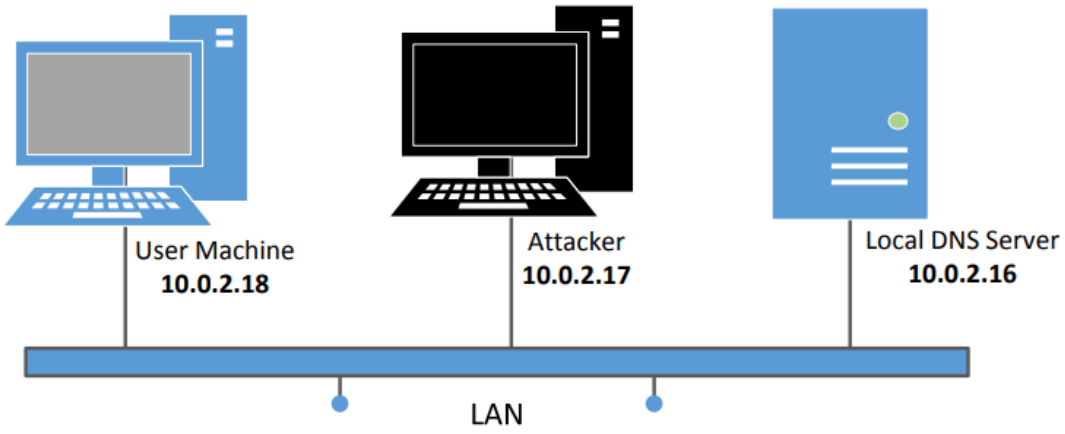


图 1 实验的环境设置

### 4.1.1 任务 1：配置用户计算机

在用户机器 10.0.2.18 上，我们需要使用 10.0.2.16 作为本地 DNS 服务器（默认情况下，DNS 服务器程序已在 SEED VM 中运行）。这是通过更改用户计算机的解析程序配置文件（/etc/resolv.conf）来实现的，因此将服务器 10.0.2.16 添加为文件中的第一个 nameserver 条目，即此服务器将用作主 DNS 服务器。

在完成配置用户计算机之后，使用 dig 命令从你选择的主机名获取 IP 地址。从响应中，请提供证据以证明响应确实来自您的服务器。如果您无法找到证据，则表明您的设置不成功。

### 4.1.2 任务 2：设置本地 DNS 服务器

对于本地 DNS 服务器，我们需要运行 DNS 服务器程序。最广泛使用的 DNS 服务器软件称为 BIND（Berkeley Internet Name Domain），顾名思义，它最初是在 20 世纪 80 年代早期在加州大学伯克利分校设计的。最新版本的 BIND 是 BIND 9，它于 2000 年首次发布。我们将展示如何为我们的实验环境配置 BIND 9。BIND 9 服务器程序已经安装在我们预先构建的 Ubuntu VM 映像中。

**第 1 步：配置 BIND 9 服务器。** BIND 9 从/etc/bind/named.conf 文件中获取其配置。这个文件是主要的配置文件，它通常包含几个"include"条目，即实际配置存储在那些 include 文件中。其中一个 include 文件称为/etc/bind/named.conf.options。这是我们通常设置配置选项的文件。让我们首先通过向选项块添加 dump-file 条目来设置与 DNS 缓存相关的选项：

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

如果要求 BIND 转储其缓存，则上述选项指定应转储缓存内容的位置。如果未指定此选项，BIND 会将缓存转储到名为/var/cache/bind/named_dump.db 的默认文件中。下面显示的两个命令与 DNS 缓存有关。第一个命令将缓存的内容转储到上面指定的文件，第二个命令清空缓存。

```
$ sudo rndc dumpdb -cache // Dump the cache to the sepcified file

$ sudo rndc flush // Flush the DNS cache
```

**第 2 步：关闭 DNSSEC。**引入 DNSSEC 是为了防止对 DNS 服务器的 spoofing 攻击。为了说明如果没有这种保护机制，攻击如何进行，我们需要关闭保护。这是通过修改 named.conf.options 文件来完成的：注释掉 dnssec-validation 条目，并添加一个 dnssec-enable 条目。

```
options {
        # dnssec-validation auto;
        dnssec-enable no;
};
```

**第 3 步：启动 DNS 服务器。**我们现在可以使用以下命令启动 DNS 服务器。每次对 DNS 配置进行修改时，都需要重新启动 DNS 服务器。以下命令将启动或重新启动 BIND 9 DNS 服务器。

```
$ sudo service bind9 restart
```

**第 4 步：使用 DNS 服务器。** 现在，返回到您的用户计算机，并 ping 一台计算机，例如 www. google.com 和 www.facebook.com，并描述您的观察结果。请使用 Wireshark 显示 ping 命令触发的 DNS 查询。还请指出何时使用了 DNS 缓存。

### 4.1.3 任务 3：在本地 DNS 服务器中建一个区域

假设我们拥有一个域名，我们将负责提供有关该域名的响应。我们将使用本地 DNS 服务器作为域的权威名称服务器。在本实验中，我们将为 example.com 域设置为权威服务器。 此域名保留用于文档，并且不由任何人拥有，因此使用它是安全的。

**第 1 步：创建区域。** 我们需要在 DNS 服务器中创建两个区域条目，方法是将以下内容添加到/etc/bind/named.conf 中。第一个区域用于正向查找（从主机名到 IP），第二个区域用于反向查找（从 IP 到主机名）。应该注意的是，example.com 域名保留用于文档，并不归任何人所有，因此使用它是安全的。

```
zone "example.com" {
        type master;
        file "/etc/bind/example.com.db";
};
zone "0.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/192.168.0.db";

};
```

**第 2 步：设置正向查找区域文件。**上述区域定义中 file 关键字之后的文件名为区域文件，这是存储实际 DNS 解析的位置。 在/etc/bind/目录中，创建以下 example.com.db 区域文件。区域文件的语法可以参考 RFC 1035 了解详细信息。

（以上内容可能因为字符集的原因导致解析有问题，建议从下面的链接下载：

https://seedsecuritylabs.org/Labs_16.04/Networking/DNS_Local/example.com.db）

符号“@”是一种特殊符号，表示在 named.conf 中指定的原点（“zone”之后的字符串）。因此，'@'代表 example.com。该区域文件包含 7 个资源记录（RR），包括 SOA（开始授权）RR，NS（名称服务器）RR，MX（邮件交换器）RR 和 4A（主机地址）RR。

**第 3 步：设置反向查找区域文件。** 为了支持 DNS 反向查找，即从 IP 地址到主机名，我们还需要设置 DNS 反向查找文件。在/etc/bind/目录中，为 example.net 域创建以下反向 DNS 查找文件 192.168.0.db：

```
$TTL 3D

@ IN SOA ns.example.com. admin.example.com. (

1

8H

2H

4W

1D)

@ IN NS ns.example.com.

101 IN PTR www.example.com.

102 IN PTR mail.example.com.

10 IN PTR ns.example.com.
```

( 以上内容可能因为字符集的原因导致解析有问题，建议从 qq 群下载：

**第 4 步：重新启动 BIND 服务器并进行测试。**完成所有更改后，请记住重新启动 BIND 服务器。现在，返回用户计算机，并使用 dig 命令向本地 DNS 服务器询问 www. example.com 的 IP 地址。请描述并解释您的观察结果。

## 4.2 本地 DNS 攻击

对用户进行 DNS 攻击的主要目标是在用户尝试使用 A 的主机名到达机器 A 时将用户重定向到另一台机器 B. 例如，当用户尝试访问在线银行时，如果攻击者可以将用户重定向到看起来非常像银行主网站的恶意网站，则用户可能会被欺骗并泄露他/她的网上银行账户密码。

当用户在他/她的浏览器中键入 http://www.example.net 时，用户的计算机将发出 DNS 查询以找出该网站的 IP 地址。攻击者的目标是使用伪造的 DNS 回复欺骗用户的计算机，该回复将主机名解析为恶意 IP 地址。有几种方法可以发起这种 DNS 攻击。有关攻击过程的图示，请参见图 2。

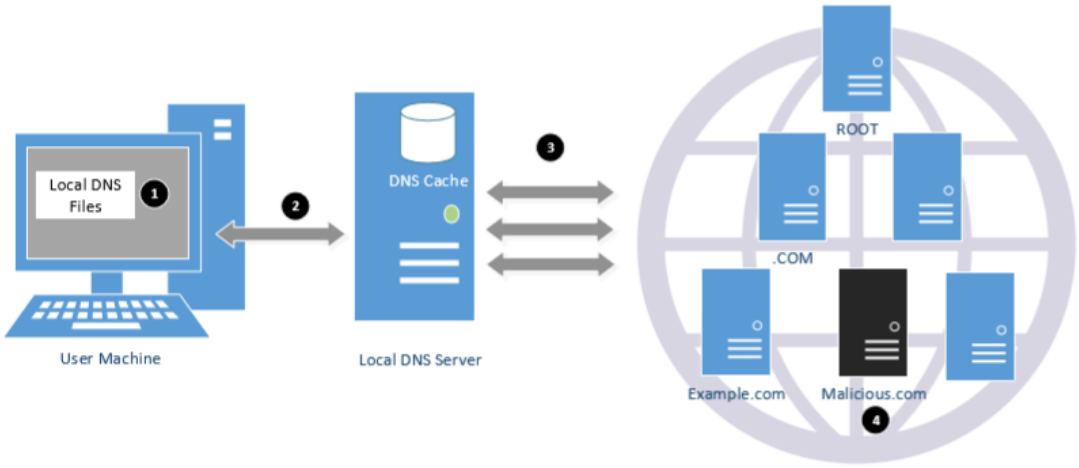


图 2 DNS 攻击

我们将在 example.net 域上发起一系列 DNS 攻击。 应该注意的是，我们使用 example.net 作为我们的目标域，而不是 example.com。后者已由我们自己的本地 DNS 服务器在设置中托管，因此不会为该域中的主机名发送 DNS 查询。

### 4.2.1 任务 4：修改主机文件

HOSTS 文件（/etc/hosts）中的主机名和 IP 地址对用于本地查找，它们优先考虑远程 DNS 查找。例如，如果用户计算机中的 HOSTS 文件中有以下条目，则 www.example.com 将在用户计算机中解析为 1.2.3.4 而不询问任何 DNS 服务器：

```
1.2.3.4    www.example.net
```

如果攻击者破坏了用户的计算机，他们可以修改 HOSTS 文件，以便在用户尝试访问 www.example.com 时将用户重定向到恶意站点。假设您已经破坏了一台计算机，请尝试使用此技术将 www.bank32.com 重定向到您选择的任何 IP 地址。

需要注意的是，dig 命令会忽略/etc/hosts，但会对 ping 命令和 Web 浏览器等生效。比较攻击前后获得的结果。

### 4.2.2 任务 5：直接欺骗用户响应

在此次攻击中，受害者的计算机尚未受到破坏，因此攻击者无法直接更改受

害者计算机上的 DNS 查询过程。但是，如果攻击者与受害者位于同一局域网，他们仍然可以造成巨大破坏。

当用户在 web 浏览器中键入 web 站点的名称(主机名，如 www.example.net)时，用户的计算机将向 DNS 服务器发出 DNS 请求，以解析主机名的 IP 地址。在听到这个 DNS 请求后，攻击者可以伪造一个虚假的 DNS 响应(见图 2.3)，如果这个虚假的 DNS 响应符合以下条件，用户的计算机将接受它:

1.源 IP 地址必须匹配 DNS 服务器的 IP 地址。

2.目标 IP 地址必须与用户机器的 IP 地址匹配。

3.源端口号(UDP 端口)必须与发送 DNS 请求的端口号匹配(通用端口 53)。

4.目标端口号必须与发送 DNS 请求的端口号匹配。

5.UDP 校验和必须计算正确。

6.事务 ID 必须匹配 DNS 请求中的事务 ID。

7.应答的问题部分中的域名必须与请求的问题部分中的域名匹配。

8.回答部分中的域名必须与 DNS 请求的问题部分中的域名匹配。

9.用户的计算机必须在接收到合法的 DNS 响应之前接收攻击者的 DNS 响应。

为了满足标准 1 到 8，攻击者可以嗅探受害者发送的 DNS 请求消息; 然后，他们可以创建虚假的 DNS 响应，并在真正的 DNS 服务器之前发回给受害者。Netwox 工具 105 提供用于进行这种嗅探和响应的实用程序。我们可以在回复数据包中组成任意 DNS 回答。此外，我们可以使用“filter”” 字段来指定要嗅探的数据包类型。例如，通过使用“src host 10.0.2.18”，我们可以将嗅探的范围限制为仅来自主机 10.0.2.18 的数据包。该工具的手册如下所述：

表 2.1 netwox 工具 105 的用法

```
Title: Sniff and send DNS answers
    Usage: netwox 105 -h data -H ip -a data -A ip [-d device]
                      [-T uint32] [-f filter] [-s spoofip]
    Parameters:
    -h|--hostname data     hostname
    -H|--hostnameip ip     IP address
    -a|--authns data       authoritative nameserver
    -A|--authnsip ip       authns IP
    -d|--device device     device name
    -T|--ttl uint32        ttl in seconds
    -f|--filter filter     pcap filter
    -s|--spoofip spoofip   IP spoof initialization type
```

当攻击程序正在运行时，在用户计算机上，您可以代表用户运行 dig 命令。此命令触发用户计算机向本地 DNS 服务器发送 DNS 查询，该 DNS 服务器最终会向 example.net 域的权威名称服务器发送 DNS 查询（如果缓存不包含答案）。如果您的攻击成功，您应该能够在回复中看到您的欺骗信息。比较攻击前后获得

的结果。

### 4.2.3 任务 6：DNS 缓存中毒攻击

上述攻击针对用户的计算机。为了实现持久的效果，每当用户的机器发送到 www.example.net 的 DNS 查询时，攻击者的机器必须发出欺骗性的 DNS 响应，这可能不那么有效；有一种更好的方法，可以通过定位 DNS 服务器而不是用户的计算机来进行攻击。

当 DNS 服务器 Apollo 收到查询时，如果主机名不在 Apollo 的域中，它将要求其他 DNS 服务器解析主机名。 请注意，在我们的实验设置中，我们的 DNS 服务器的域名是 example.com; 因此，对于其他域（例如 example.net）的 DNS 查询，DNS 服务器 Apollo 将询问其他 DNS 服务器。但是，在 Apollo 询问其他 DNS 服务器之前，它首先从自己的缓存中寻找答案; 如果有答案，DNS 服务器 Apollo 将简单地回复其缓存中的信息。如果答案不在缓存中，DNS 服务器将尝试从其他 DNS 服务器获得答案。 当 Apollo 得到答案时，它会将答案存储在缓存中，因此下次无需询问其他 DNS 服务器。 见图 3。

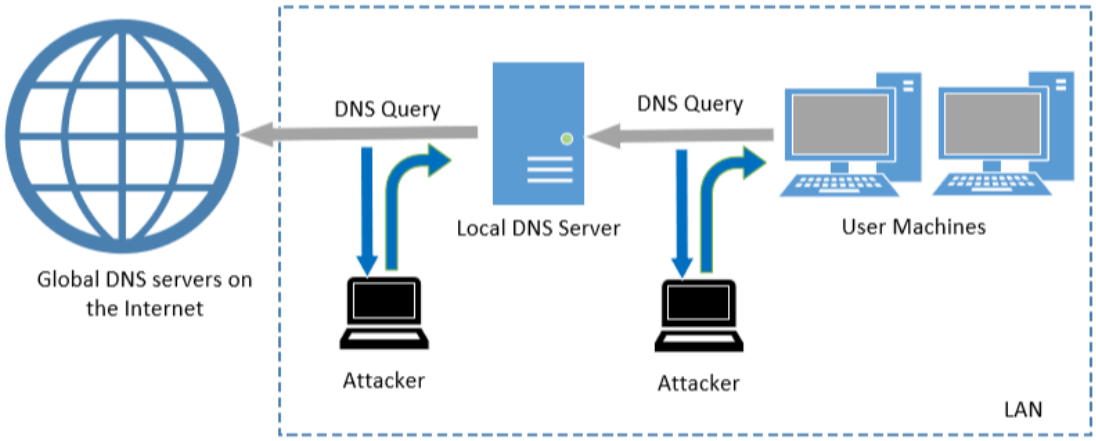


图 3 本地 DNS 中毒攻击

因此，如果攻击者可以欺骗来自其他 DNS 服务器的响应，Apollo 会将欺骗性响应保留在其缓存中一段时间。下次，当用户的计算机想要解析相同的主机名时，Apollo 将使用缓存中的欺骗响应进行回复。这样，攻击者只需要欺骗一次，就能将影响持续到缓存的信息到期为止。 此攻击称为 DNS 缓存中毒。

我们可以使用相同的工具（Netwox 105）进行此攻击。在攻击之前，请确保 DNS 服务器的缓存为空。 您可以使用以下命令刷新缓存：

```
$ sudo rndc flush
```

此攻击与之前的攻击之间的区别在于我们现在欺骗对 DNS 服务器的响应，因此我们将过滤器字段设置为“src host 10.2.0.16”，这是其它 DNS 服务器的 IP 地址。我们还使用 ttl 字段（生存时间）来指示我们希望假答案保留在 DNS 服务器缓存中的时间。DNS 服务器中毒后，我们可以停止 Netwox 105 程序。如果我们将 ttl 设置为 600（秒），那么 DNS 服务器将在接下来的 10 分钟内继续发出假回复。

注意：请在 *spoofip* 字段中选择 *raw*; 否则，Netwox 105 将对被欺骗的 IP 地址也进行 MAC 地址欺骗。为了获得 MAC 地址，该工具发出 ARP 请求，询问欺骗 IP 的 MAC 地址。此欺骗 IP 地址通常是外部 DNS 服务器的 IP 地址，该服务器不在同一 LAN 上。因此，没有主机会回复 ARP 请求。该工具将在没有 MAC 地址的情况下等待 ARP 回复一段时间。 这个等待会使工具发出欺骗性响应延迟。如果实际的 DNS 响应早于欺骗响应，则攻击将失败。这就是为什么你需要让工具不要欺骗 MAC 地址。

通过在目标主机名上运行 dig 命令时使用 Wireshark 观察 DNS 流量，可以判断 DNS 服务器是否中毒。您还应该转储本地 DNS 服务器的缓存，以检查是否缓存了欺骗性回复。要转储和查看 DNS 服务器的缓存，请发出以下命令：

```
$ sudo rndc dumpdb -cache
$ sudo cat /var/cache/bind/dump.db
```

### 4.2.4 任务 7：DNS 缓存中毒：针对授权区域部分

在上一个任务中，我们的 DNS 缓存中毒攻击仅影响一个主机名，即 www.example.net。 如果用户试图获取另一个主机名的 IP 地址，例如 mail.example.net，我们需要再次发起攻击。 如果我们发起一次可能影响整个 example.net 域的攻击，效率会更高。

我们的想法是使用 DNS 回复中的授权区域部分。当我们欺骗回复时，除了欺骗答案（在 Answer 部分），我们还在授权区域部分添加以下内容。当此条目由本地 DNS 服务器缓存时，ns.attacker32.com 将用作名称服务器，以便将来查询 example.net 域中的任何主机名。由于 attacker32.com 是由攻击者控制的计算机，因此它可以为任何查询提供伪造答案。

```
;; AUTHORITY SECTION:
example.net.      259200     IN      NS      attacker32.com.
```

此任务的目的就是进行这样的攻击。你需要证明你可以获得本地 DNS 服务器缓存的上述条目。缓存中毒后，在 example.net 域中的任何主机名上运行 dig 命令，并使用 Wireshark 观察 DNS 查询的位置。应该注意的是，attacker32.com 并不存在，攻击者可以在攻击者机器上搭建了该服务器。因此，您将无法从中获得答案，但您的 Wireshark 流量应该能够告诉您攻击是否成功。

需要使用 Scapy 执行此任务。有关示例代码，请参阅 4.2.7 节。

### 4.2.5 任务 8：针对另一个域

在上一次攻击中，我们成功使本地 DNS 服务器缓存中毒，因此 attacker32.com 成为 example.com 域的名称服务器。受到这一成功的启发，我们希望将其影响扩展到其他领域。 也就是说，在由 www.example.net 查询触发的欺骗性响应中，我们希望在“授权”部分添加其他条目（请参阅下文），因此 attacker32.com 也可用作 google.com 的名称服务器。

```
;; AUTHORITY SECTION:
example.net.    259200    IN    NS    attacker32.com.
google.com.     259200    IN    NS    attacker32.com.
```

请使用 Scapy 在您的本地 DNS 服务器上发起此类攻击；描述和解释你观察到的结果。 应该注意的是，我们正在攻击的查询仍然是对 example.net 的查询，而不是 google.com 的查询。

### 4.2.6 任务 9：针对附加部分

在 DNS 回复中，有一个名为 Additional Section 的部分，用于提供其他信息。实际上，它主要用于为某些主机名提供 IP 地址，特别是对于出现在“AUTHORITY”部分的主机名。此任务的目标是欺骗本节中的某些条目，并查看它们是否由目标本地 DNS 服务器成功缓存。特别是，在响应 www.example.net 的查询时，除了“答案”部分中的条目外，我们还在欺骗性回复中添加以下条目：

```
;; AUTHORITY SECTION:
example.net.        259200    IN    NS    attacker32.com.
example.net.        259200    IN    NS    ns.example.net.

;; ADDITIONAL SECTION:
attacker32.com.     259200    IN    A     1.2.3.4  ①
ns.example.net.     259200    IN    A     5.6.7.8  ②
www.facebook.com. 259200      IN    A     3.4.5.6  ③
```

条目①和②与权限部分中的主机名相关。条目③与回复中的任何条目完全无关，但它为用户提供了“亲切”的帮助，因此他们无需查找 Facebook 的 IP 地址。请使用 Scapy 来欺骗这样的 DNS 回复。您的工作是报告成功缓存了哪些条目，以及哪些条目不会被缓存，请解释原因。

### 4.2.7 代码示例

在本实验中，多个任务都需要使用 Scapy。Ubuntu 虚拟机中如果没有安装

scapy 的话，可以使用下面的命令进行安装：

$sudo apt-get install python-scapy

以下示例代码显示了如何监听 DNS 查询，然后伪造 DNS 回复，其中包含“响应”部分中的记录，“权限”部分中的两个记录和“附加”部分中的两个记录。

```
#!/usr/bin/python
from scapy.all import *

def spoof_dns(pkt):
    if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
        # Swap the source and destination IP address
        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)

        # Swap the source and destination port number
        UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)

        # The Answer Section
        Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',
                 ttl=259200, rdata='10.0.2.5')

        # The Authority Section
        NSsec1 = DNSRR(rrname='example.net', type='NS',
                 ttl=259200, rdata='ns1.example.net')
        NSsec2 = DNSRR(rrname='example.net', type='NS',
                 ttl=259200, rdata='ns2.example.net')

        # The Additional Section
        Addsec1 = DNSRR(rrname='ns1.example.net', type='A',
                ttl=259200, rdata='1.2.3.4')
        Addsec2 = DNSRR(rrname='ns2.example.net', type='A',
                 ttl=259200, rdata='5.6.7.8')

        # Construct the DNS packet

    DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,①
                 qdcount=1, ancount=1, nscount=2, arcount=2,
                 an=Anssec, ns=NSsec1/NSsec2, ar=Addsec1/Addsec2)

        # Construct the entire IP packet and send it out
        spoofpkt = IPpkt/UDPpkt/DNSpkt
        send(spoofpkt)

# Sniff UDP query packets and invoke spoof_dns().
```

```
pkt = sniff(filter='udp and dst port 53', prn=spoof_dns)
```

第 ① 行构造 DNS 载荷，包括 DNS 头部和数据，DNS 载荷的每个字段说明如下：

id: 传输 id,需要跟 DNS 请求报文保持一致；

qd: 查询域，需要跟 DNS 请求报文保持一致；

aa: 授权回答（1 表示在响应报文中包括授权回答）

rd: 递归要求（0 表示禁用递归查询）

qr: 查询响应 bit（1 表示响应）

qdcount: 查询域数量

ancount: 在 answer 部分的记录数

nscount: 在授权（权限）部分的记录数

arcount: 在附加部分的记录数

an: answer 部分

ns: 授权部分

ar: 附加部分

## 4.3 远程 DNS 攻击实验

本实验主要研究一种特殊的 DNS 欺骗攻击技术，称为 DNS 缓存中毒攻击。在上一个实验中，我们设计了在本地网络环境中进行相同攻击的活动，即攻击者和受害者 DNS 服务器位于同一个网络上，因此可以嗅探数据包。在这个远程攻击实验室中，包嗅探是不可能的，因此攻击比本地攻击更具挑战性。

DNS 欺骗攻击的主要目标是，当用户试图使用 A 的主机名访问机器 A 时，将用户重定向到另一台机器 B。例如，假设 www.example.com 是一个在线银行站点。当用户试图使用正确的 URL www.example.com 访问此站点时，如果攻击者能够将用户重定向到与 www.example.com 非常相似的恶意 web 站点，用户可能会被愚弄，并将其凭据泄露给攻击者。

在这个实验中，我们使用域名 www.example.com 作为攻击目标。需要注意的是，example.com 域名是保留给文档使用的，而没有分配给何真正的公司。www.example.com 的真实 IP 地址为 93.184.216.34，其名称服务器由互联网名称与数字地址分配机构(ICANN)管理。当用户在该对该域名使用上运行 dig 命令或在浏览器中键入该名称时，用户的机器将向其本地 DNS 服务器发送一个 DNS 查询，该服务器最终将从 example.com 的名称服务器请求 IP 地址。

这次攻击的目标是对本地 DNS 服务器进行 DNS 缓存中毒攻击,这样当用户运行 dig 命令找到 www.example.com 的 IP 地址,最终本地 DNS 服务器会到攻击者的名称服务器 ns.dnslabattacker.net 上获取这个 IP 地址,所以返回的 IP 地址可以是攻击者决定的任何数字。结果，用户将被引导到攻击者的 web 站点，而不是真实的 www.example.com。

这种攻击有两个任务：缓存中毒和结果验证。在第一个任务中，学生需要使用户的本地 DNS 服务器 Apollo 的 DNS 缓存中毒。这样，在 Apollo 的 DNS 缓存中，将 ns.dnslabattacker.net 设置为 example.com 域的名称服务器，而不是该域注册的权威名称服务器。在第二项任务中，学生需要展示攻击的影响。更具体地说，它们需要从用户的机器上运行“dig www.example.com”命令，返回的结果必须是一个假的 IP 地址。

### 4.3.1 配置本地 DNS 服务器 Apollo

**删除 example.com 区域：**如果之前做过本地 DNS 攻击实验，那么可能已经在 example.com 域配置了本地 DNS 服务器 Apollo。在这个实验中，这个 DNS 服务器不会使用该域，所以请从/etc/bind/name .conf 中删除它的对应区域。（建议注释掉 example.com 域的记录，而不是删除，避免重复性工作）

步骤 4:启动 DNS 服务器。我们现在可以使用以下命令启动 DNS 服务器:

```
% sudo /etc/init.d/bind9 restart
```

或

```
% sudo service bind9 restart
```

### 4.3.2 远程缓存中毒

在此任务中，攻击者向受害者 DNS 服务器(Apollo)发送 DNS 查询请求，从而触发 Apollo 的 DNS 查询。查询可能经过一个根 DNS 服务器，即.com DNS 服务器，最终结果将从 example.com 的 DNS 服务器返回。完整的 DNS 查询过程如图 4 所示。

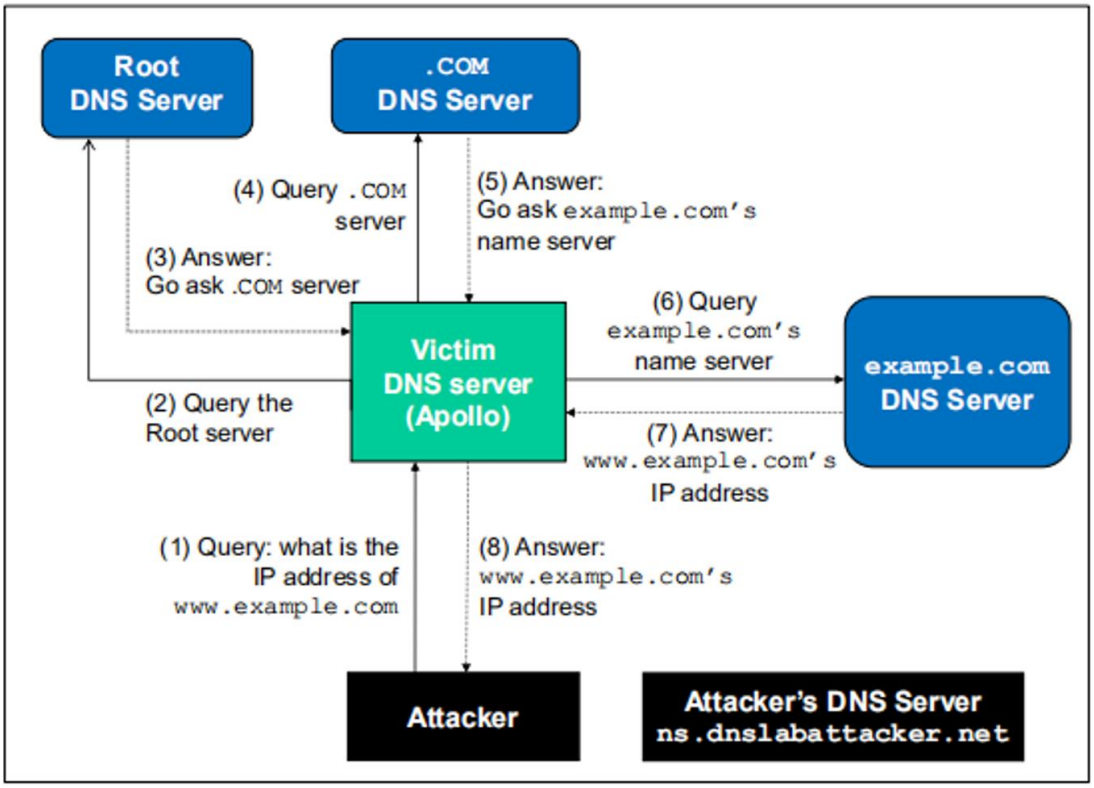


图 4 完整的 DNS 查询过程

如果 example.com 的名称服务器信息已经被 Apollo 缓存，查询将不会通过根或.COM 服务器，如图 5 所示。在这个实验室中，图 5 中描述的情况更为常见，所以我们将使用这个图作为描述攻击机制的基础。

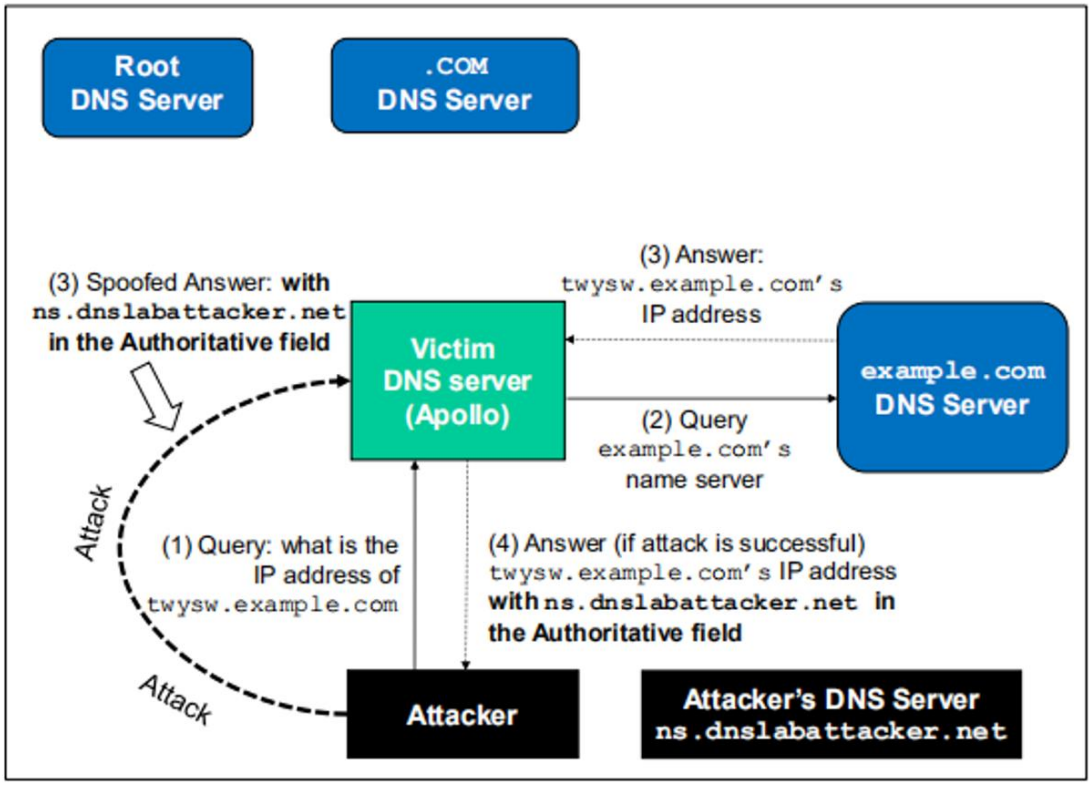


图 5 当 example.com 的名字服务器被缓存时 DNS 查询过程

当 Apollo 等待来自 example.com 名称服务器的 DNS 响应时，攻击者可以向 Apollo 发送伪造的响应，假装响应来自 example.com 名称服务器。如果伪造的回复先到达，Apollo 将接受它，攻击就会成功。

本地 DNS 攻击实验，是假定攻击者和 DNS 服务器位于同一个 LAN 上，即，攻击者可以观察 DNS 服务器发出的 DNS 查询消息。当攻击者和 DNS 服务器不在同一个 LAN 上时，缓存中毒攻击将变得更加困难。造成这种困难的主要原因是 DNS 响应包中的事务 ID 必须与查询包中的事务 ID 匹配。由于查询中的事务 ID 通常是随机生成的，在不查看查询包的情况下，攻击者很难知道正确的事务 ID。

显然，攻击者可以猜测事务 ID。由于 ID 的大小只有 16 位，如果攻击者可以在攻击窗口内伪造 K 个响应(即在合法响应到达之前)，成功的概率为 K / 2^16。发出数百个伪造的响应是可行的，因此攻击者不需要太多的尝试就可以成功。

然而，上述假设的攻击忽略了缓存效应。实际上，如果攻击者没有幸运地在真正的响应包到达之前做出正确的猜测，正确的信息将被 DNS 服务器缓存一段时间。这种缓存效果使得攻击者不可能伪造对相同域名的另一个响应，因为 DNS 服务器不会在缓存超时之前发出针对该域名的另一个 DNS 查询。要伪造相同域名上的另一个响应，攻击者必须等待该域名上的另一个 DNS 查询，这意味着他/她必须等待缓存超时。等待时间可以是几个小时或几天。

Kaminsky 攻击：Dan Kaminsky 提出了一种优雅的技术来克服缓存效应。通过 Kaminsky 攻击，攻击者将能够不需要等待而持续攻击同一个域名上的 DNS 服务器，所以攻击可以在很短的时间内成功。攻击的细节在[1]中描述。在这个任务中，我们将尝试这种攻击方法。参照图 3 以下步骤概述了该攻击：

1. 攻击者向 DNS 服务器 Apollo 查询 example.com 中不存在的名称，例如 twysw.example.com，其中 twysw 是一个随机名称。

2. 由于该映射在 Apollo 的 DNS 缓存中不可用，因此 Apollo 向 example.com 域的名称服务器发送 DNS 查询。

3. 当 Apollo 等待响应时，攻击者会向 Apollo 发送一个欺骗的 DNS 响应[6]流，每个响应都尝试一个不同的事务 ID，并希望其中一个是正确的。在响应中，攻击者不仅为 twysw.example.com 提供了一个 IP 解析，还提供了一个“Authoritative Nameservers”记录，指示 ns.dnslabattacker.net 作为 example.com 域的名称服务器。如果欺骗响应击败了实际响应，并且事务 ID 与查询中的事务 ID 匹配，Apollo 将接受并缓存欺骗响应，从而破坏 Apollo 的 DNS 缓存。

4. 即使欺骗 DNS 响应失败(例如,事务 ID 不匹配或者是太迟了),这并不重要,因为下一次,攻击者将查询一个不同的名称,所以 Apollo 发送另一个查询,给攻击者另一个机会做欺骗攻击。这有效地消除了缓存效果。

5. 如果攻击成功，在 Apollo 的 DNS 缓存中，example.com 的名称服务器将被攻击者的名称服务器 ns.dnslabattacker.net 替换。为了证明这次攻击的成功，学生们需要证明这样的记录在 Apollo 的 DNS 缓存中。图 5 显示了中毒的 DNS 缓存的示例。

## 攻击配置：

我们需要对这个任务进行如下配置:

1. 配置攻击机器：我们需要配置攻击机器，使它使用目标 DNS 服务器(即 Apollo）作为它的默认 DNS 服务器。有关说明请参阅第 4.1.1 节。

2. 源端口：一些 DNS 服务器现在在 DNS 查询中随机化源端口号;这使得攻击更加困难。不幸的是，许多 DNS 服务器仍然使用可预测的源端口号。为了简单起见，我们假设源端口号是一个固定的数字。我们可以将所有 DNS 查询的源端口设置为 33333。这可以通过将以下选项添加到 Apollo 的 /etc/bind/name.conf.options 文件里：

```
query-source port 33333
```

3. DNSSEC：现在，大多数 DNS 服务器都采用了一种名为“DNSSEC”的

保护方案，旨在抵抗 DNS 缓存中毒攻击。如果你不关掉它，你的攻击将是极其困难的。在这个实验，我们将关闭它。这可以通过改变 Apollo 的文件/etc/bind/named.conf..option 来实现。请找到“dnssec-validation auto”行，将其注释掉，然后添加新行。见以下：

```
//dnssec-validation auto;
dnssec-enable no;
```

4. 刷新缓存。清空 Apollo 的 DNS 缓存，重启 DNS 服务器。

实现 Kaminsky 攻击是相当具有挑战性的，因此将其分解为三个子任务：伪造 DNS 请求包、伪造 DNS 响应包、实施攻击。

1）**子任务 1：伪造 DNS 请求包：**此子任务侧重于伪造 DNS 请求。为了完成攻击，我们（作为攻击者）需要触发目标 DNS 服务器发送 DNS 查询，因此我们就有机会欺骗 DNS 响应。这个过程需要多次尝试才能成功，因此必须自动化这个过程。第一步是编写一个程序，将 DNS 查询发送到目标 DNS 服务器，每次在查询字段中使用不同的主机名。我们的工作就是编写这个程序，并使用 Wireshark 查看发送的查询请求，触发目标 DNS 服务器来发送 DNS 查询。不需要很快地发送 DNS 查询，所以我们可以使用外部程序来完成这项工作，而不是在 C 程序中实现所有内容。例如，可以使用 system（）调用 dig 程序：

```
system(“dig xyz.example.com”);
```

首先需要向 Apollo 发送 DNS 查询，在 example.com 域中查询一些随机主机名。每次查询发出后，攻击者需要在很短的时间内伪造大量的 DNS 响应包，希望其中一个具有正确的事务 ID，并在真实响应之前到达目标。

**2）子任务 2：伪造 DNS 响应包：**在 Kaminsky 攻击中，需要伪造 DNS 回复。性能对于攻击的成功至关重要，因此最好用 C 语言编写程序。我们提供了一个名为 udp.c 的示例代码，其中显示了如何构造 DNS 数据包。

1. 修改 udp.c 程序时，需要用正确的值填充每个 DNS 字段。为理解每个字段中的值，可以使用 Wireshark 捕获几个 DNS 查询和响应包。

2. DNS 响应包细节：构造一个正确的 DNS 响应包并不容易。我们做了一个

样本包来帮助理解。图 6 是示例响应包的屏幕截图:10.0.2.6 是本地 DNS 服务器地址，199.43.132.53 是 example.com 的真实域名服务器。突出显示的字节是原始 UDP 有效负载数据，需要弄清它们是什么。关于每个字节如何工作的细节在附录 a 中有详细的解释。响应包中使用了几种技术，比如字符串指针偏移量来缩短包的长度。你可能不需要使用这种技术，但它在实际的包中非常常见。

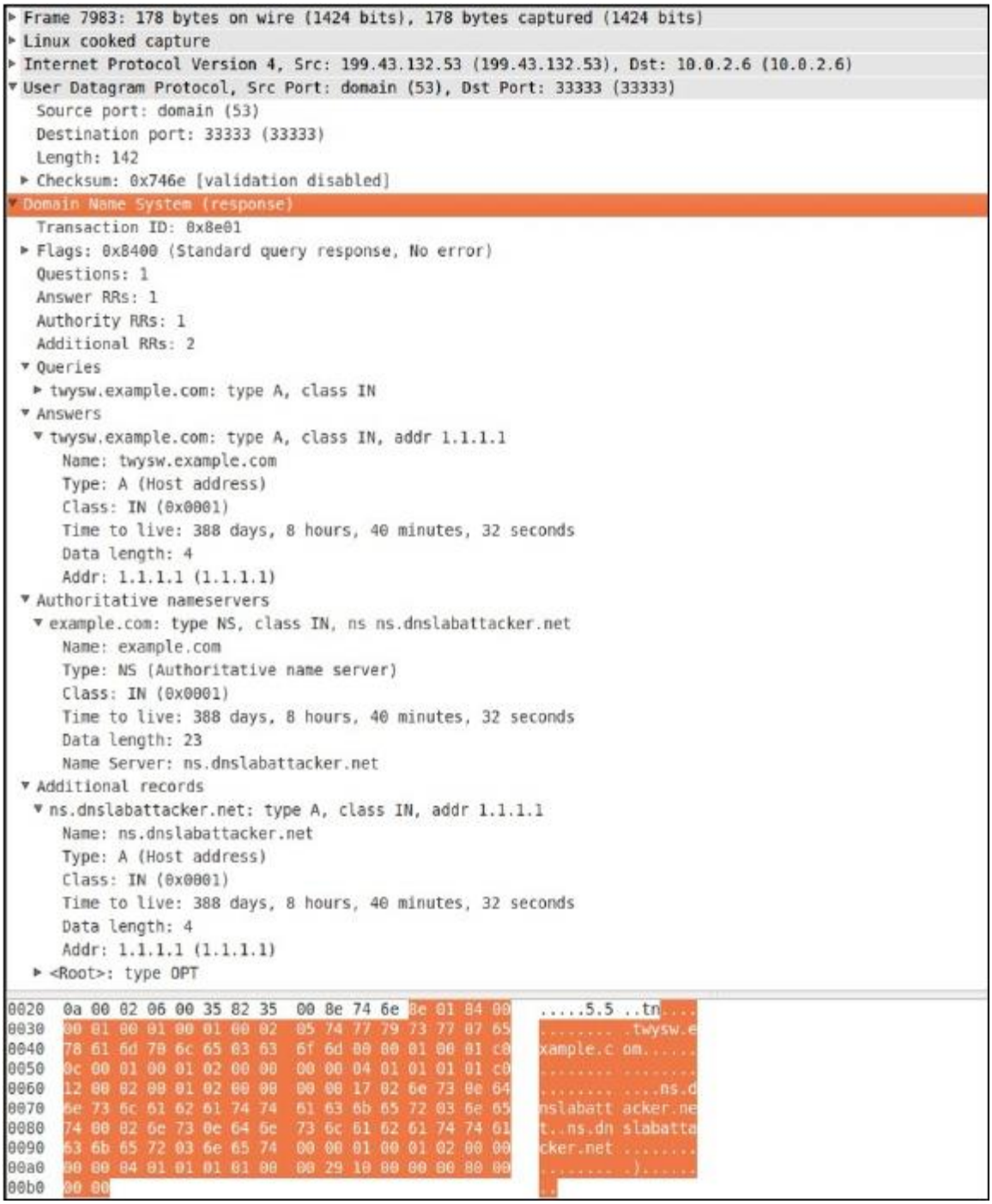


图 6: DNS 响应报文示例

3）**子任务 3：Kaminsky 攻击**。现在我们可以把所有的东西放在一起进行 Kaminsky 攻击。启动攻击，检查 dump.db 文件，查看你的欺骗 DNS 响应是否已被 DNS 服务器成功接受。参见图 7 中的示例。

```
                        172660  NS      h.gtld-servers.net.
                        172660  NS      i.gtld-servers.net.
                        172660  NS      j.gtld-servers.net.
                        172660  NS      k.gtld-servers.net.
                        172660  NS      l.gtld-servers.net.
                        172660  NS      m.gtld-servers.net.
; additional
                        86260   DS      30909 8 2 (
                                        E2D3C916F6DEEAC73294E8268FB5885044A8
                                        33FC5459588F4A9184CFC41A5766 )
; additional
                        86260   RRSIG   DS 8 1 86400 20141201170000 (
                                        20141124160000 22603 .
                                        LtkTupSuz/aOGV4FxKx0wnEdfutvv4xcM8YC
                                        BWlAL2DlGIumuQGbKTE6RUm91+k6B2WXcdgo
                                        u/EsAKnyFx4lj/f9iPsiIvgda950rEadmCxd
                                        xYkwnVMNkoV5sDfyev4NYwxfy3tai6ro0ngS
                                        TQCm5NrWr+r/Q8XhIhDCLYKDeks= )
; authauthority
example.com.            172660  NS      ns.dnslabattacker.net.
; additional
                        86260   DS      31589 8 1 (
                                        3490A6806D47F17A34C29E2CE80E8A999FFB
                                        E4BE )
                        86260   DS      31589 8 2 (
                                        CDE0D742D6998AA554A92D890F8184C698CF
                                        AC8A26FA59875A990C03E576343C )
; additional
                        86260   RRSIG   DS 8 2 86400 20141128051526 (
                                        20141121040526 48758 com.
                                        e2Zclaahc5xiHjzEj+prLZm5Qs0IWTPfEMa/
                                        VhoOguxIfupGnebs206WffE3Pc+ZjQp+QNzN
                                        Nv33N/Kg4WymFg9soQxJpXFeYrcnkNmkaXh8
                                        T5Rva4/M5+stP/tENNfiQuZG6klQECiNC9CA
                                        r5QckZNJExCN+7mZLuc/C4BufQQ= )
```

图 7 DNS 缓存中毒成功后的示例

### 4.3.3 结果验证

如果攻击成功，Apollo 的 DNS 缓存将如图 7 所示，即， example.com 的 NS 记录就变成了 ns.dnslabattacker.net。为了确保袭击确实成功，我们在用户机器上运行 dig 命令来询问 www.example.com 的 IP 地址。

当 Apollo 收到 DNS 查询时，它在缓存中搜索 example.com 的 NS 记录，并且找到 ns.dnslabattacker.net。因此，它将向 ns.dnslabattacker.net 发送 DNS 查询。但是，在发送查询之前，它需要知道 ns.dnslabattacker.net 的 IP 地址。这是通过发出一个单独的 DNS 查询来完成的。这就是我们遇到麻烦的地方。

域名 dnslabattacker.net 实际上并不存在。我们为这个实验的目的创建了这个名称。Apollo 很快就会发现这一点，并将 NS 条目标记为无效，然后就从中毒的缓存中恢复正常。有人可能会说，再伪造 DNS 响应时，我们可以使用额外的记录为 ns.dnslabattacker.net 提供 IP 地址。图 7 中的示例响应包实际上做到了这一点。不幸的是，这个额外的记录将不会被 Apollo 接受。请思考原因并在你的实验报告中给出你的解释(提示:考虑区域)。

两种方法可以解决这个问题，所以我们可以显示我们缓存中毒攻击成功的影

响(攻击确实成功了，问题是我们不能显示它):

**使用真实的域名：**如果你一个真实的域，并且可以配置它的 DNS，那么你的工作很容易。只需在 NS 记录中使用你自己的域名，而不是 dnslabattacker.net。请参考本地 DNS 攻击的设置部分来配置 DNS 服务器，以便它能够回答 example.com 域名的查询。

**使用假域名：**如果没有真正的域名，仍然可以使用我们的假域名 ns.dnslabattacker.net 进行演示。我们只需要在 Apollo 上做一些额外的配置，这样它就可以将 dnslabattacker.net 识别为一个真实的域。我们可以将 ns.dnslabattacker.net 的 IP 地址添加到 Apollo 的 DNS 配置中，因此 Apollo 不需要从一个不存在的域请求这个主机名的 IP 地址。

**（1）配置本地 DNS 服务器**

我们首先配置受害者的 DNS 服务器 Apollo。在/etc/bind/文件夹中找到 named.conf.default-zones 文件，并添加以下条目:

```
zone "ns.dnslabattacker.net" {
      type master;
      file "/etc/bind/db.attacker";
};
```

创建文件/etc/bind/db.attacker，并将以下内容放入其中。我们让 ns.dnslabattacker.net 指向攻击者机器(192.168.0.200)。我们已经在实验网站链接了文件 db.attacker。

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@   IN  SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@   IN  NS  ns.dnslabattacker.net.
@   IN  A   192.168.0.200
@   IN  AAAA    ::1
```

(上述红色标注的 ip 地址可以根据攻击者的实际 ip 修改)

一旦设置完成，如果缓存中毒攻击成功，发送给 Apollo 的关于 example.com

主机名的任何 DNS 查询都将被发送到攻击者的机器 192.168.0.200。

**（2）配置攻击者机器**

我们需要在 192.168.0.200 上配置 DNS 服务器，这样它就可以回答域 example.com 的查询。在 192.168.0.200 的/etc/bin /named.conf.local 中添加以下条目：

```
zone "example.com" {
      type master;
      file "/etc/bind/example.com.zone";
};
```

创建一个名为/etc/bind/example.com.zone 的文件，并使用以下内容填充它。

```
$TTL 3D
  @              IN          SOA ns.example.com. admin.example.com. (
2008111001
8H
2H
4W
1D)
@              IN          NS          ns.dnslabattacker.net.
@              IN          MX          10 mail.example.com.
www            IN          A           1.1.1.1
mail           IN          A           1.1.1.2
*.example.com  IN          A           1.1.1.100
```

配置完成后，不要忘记同时重启 Apollo 和攻击者的 DNS 服务器;否则，修改将不生效。如果一切都做得很好，您可以使用像“在用户机器上 dig www.example.com”这样的命令。答案将是 1.1.1.1，这正是我们放在上面文件中的。

# 5 实验报告

学生需要提交一份详细的实验报告，描述他们所做的和所观察到的。报告应包括支持观察所见的证据。证据包括包跟踪、屏幕截图等。

注意:请不要忘记回答 Task 2 中的问题，即为什么附加字段中的 ns.dnslabattacker.net 的 IP 地址不被受害者 DNS 服务器接受。

# 参考文献

[1] D. Schneider. Fresh Phish, How a recently discovered flaw in the Internet's Domain Name System makes it easy for scammers to lure you to fake Web sites. IEEE Spectrum, 2008 http:

[2] RFC 1035 Domain Names - Implementation and Specification : http://www.rfc-base.org/rfc-1035.html

[3] DNS HOWTO : http://www.tldp.org/HOWTO/DNS-HOWTO.html

[4] Pharming Guide : http://www.technicalinfo.net/papers/Pharming.html

[5] DNS Cache Poisoning: http://www.secureworks.com/resources/articles/other articles/dns-cache--poisoning/

[6] DNS Client Spoof: http://evan.stasis.org/odds/dns-client spoofing.txt

# 附录 DNS 响应包的详细信息

0x8e 0x01 transaction ID

0x84 0x00 flags:means a no-error answer

0x00 0x01 Questions No. (1 question session)

0x00 0x01 Answer No. (1 answer session)

0x00 0x01 Authority No. (1 authority session)

0x00 0x02 Additional No. (2 additional sessions)

query session: eggdd.example.com:type A, class IN

0x05 5 characters follow

0x74 t

0x77 w

0x79 y

0x73 s

0x77 w

0x07 7 characters follow

0x65 e

0x78 x

0x61 a

0x6d m

0x70 p

0x6c l

0x65 e

0x03 3 characters

0x63 c

0x6f o

0x6d m

0x00 end of the string

0x00 0x01 type:A(address)

0x00 0x01 Class:IN

the Answer session:

0xc0 first two bits set to 1 to notify this is a pointer for a name string, not a standard

string as before

0x0c the offset of the start point: here from transaction ID field to the name string

12 bytes. The string will shows from the offset point to the end of the string

0x00 0x01 type:A

0x00 0x01 Class:IN

0x02 0x00 0x00 0x00 time to live

0x00 0x04 DataLength:4 bytes

0x01 0x01 x01 0x01 1.1.1.1

Authoritative Nameservers session:

0xC0 first two bits set to 1 to notify this is a pointer for a name string,