# 实验二 DNS协议漏洞利用实验

王美珍、梅松、张云鹤

华中科技大学网络空间安全学院

# 主要内容

- 实验目的
- 实验环境
- 实验内容
- 实验要求

# 1 实验目的

- 本实验的学习目标是让学生获得有关协议漏洞的第一手经验，以及针对这些漏洞的攻击。
- **TCP/IP**协议中的漏洞代表了协议设计和实现中的一种特殊类型的漏洞，它们提供了宝贵的教训
- 重点学习**DNS**协议的漏洞以及如何利用漏洞进行攻击

# 2 实验环境

- Ubuntu Seed虚拟机下载地址：
  - QQ群空间
- 虚拟机软件：vmware (15.5.0及兼容版本) + vmware tools
- ubuntu系统的用户密码

  普通用户： seed 密码:dees

  超级用户：root 密码：seedubuntu
- 实验采用一个虚拟机，多个容器来完成

# docker容器的使用

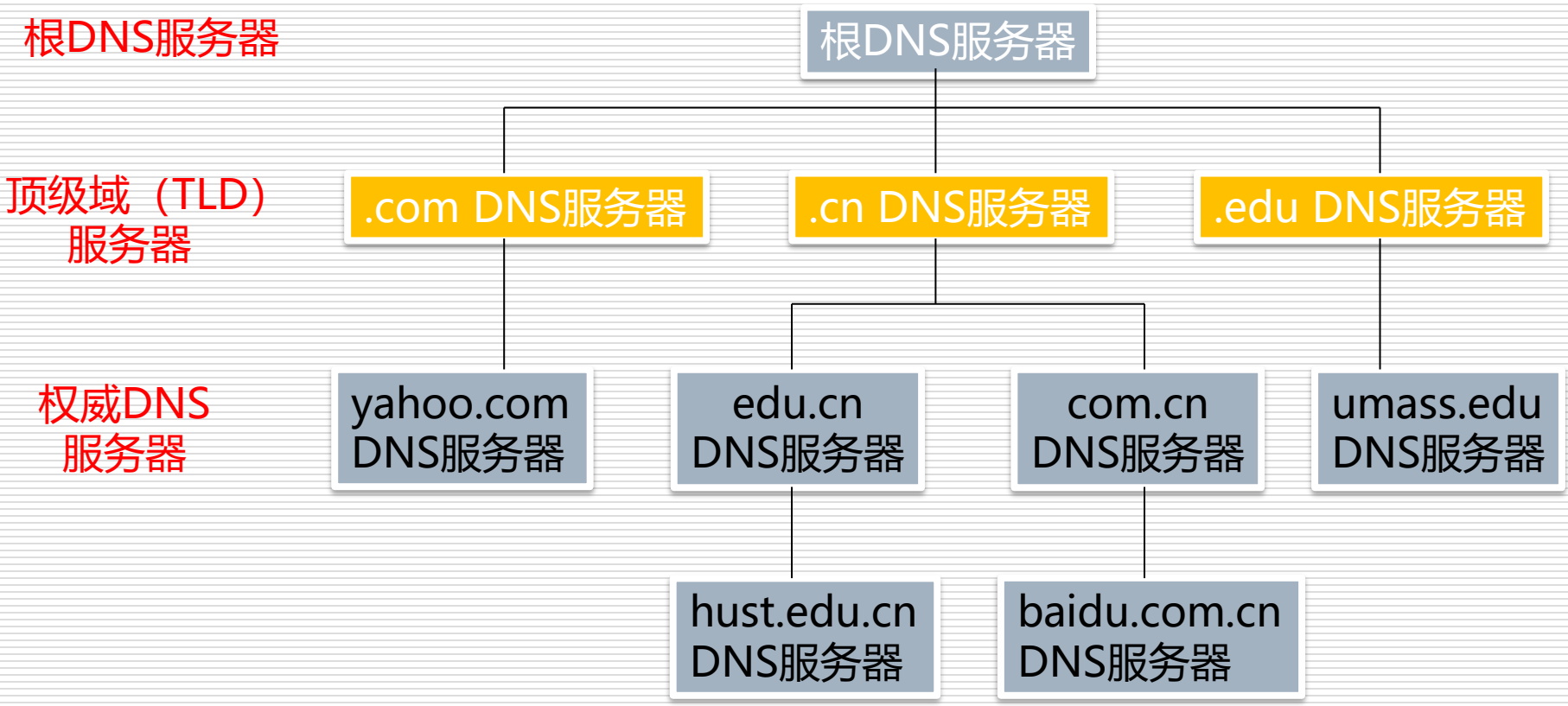
- 容器查看
  - docker ps –a，可以看到已有一个server
- 容器创建
  - docker run -it --name=server ~~--privileged~~ “seedubuntu” /bin/bash
- 容器启用/停止
  - docker start/stop 容器名
- 进入容器的命令行
  - docker exec –it 容器名 /bin/bash
- 删除容器(实验未完成前不要删除）
  - docker rm 容器名

# 实验环境截图

# 3 实验内容

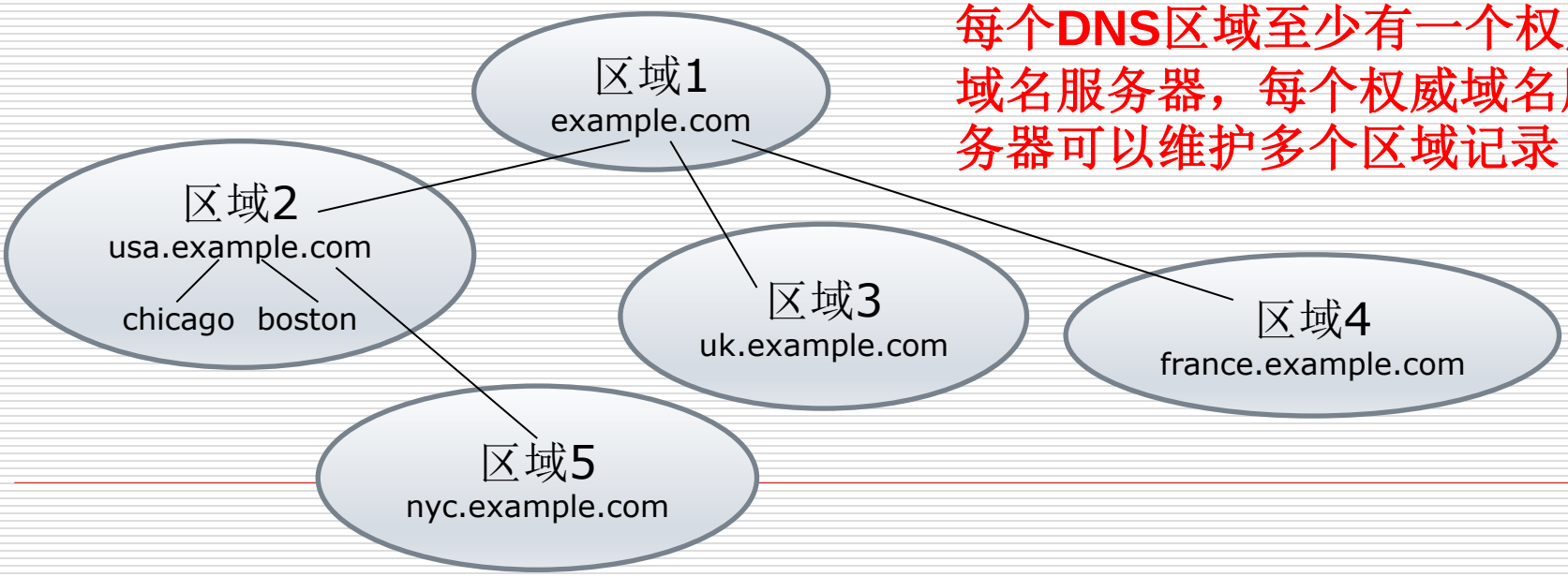
- DNS本地攻击
- DNS远程攻击

# 域名系统


根DNS服务器
根DNS服务器
顶级域（TLD）服务器
.com DNS服务器
.cn DNS服务器
.edu DNS服务器
权威DNS服务器
yahoo.com DNS服务器
edu.cn DNS服务器
com.cn DNS服务器
umass.edu DNS服务器
hust.edu.cn DNS服务器
baidu.com.cn DNS服务器

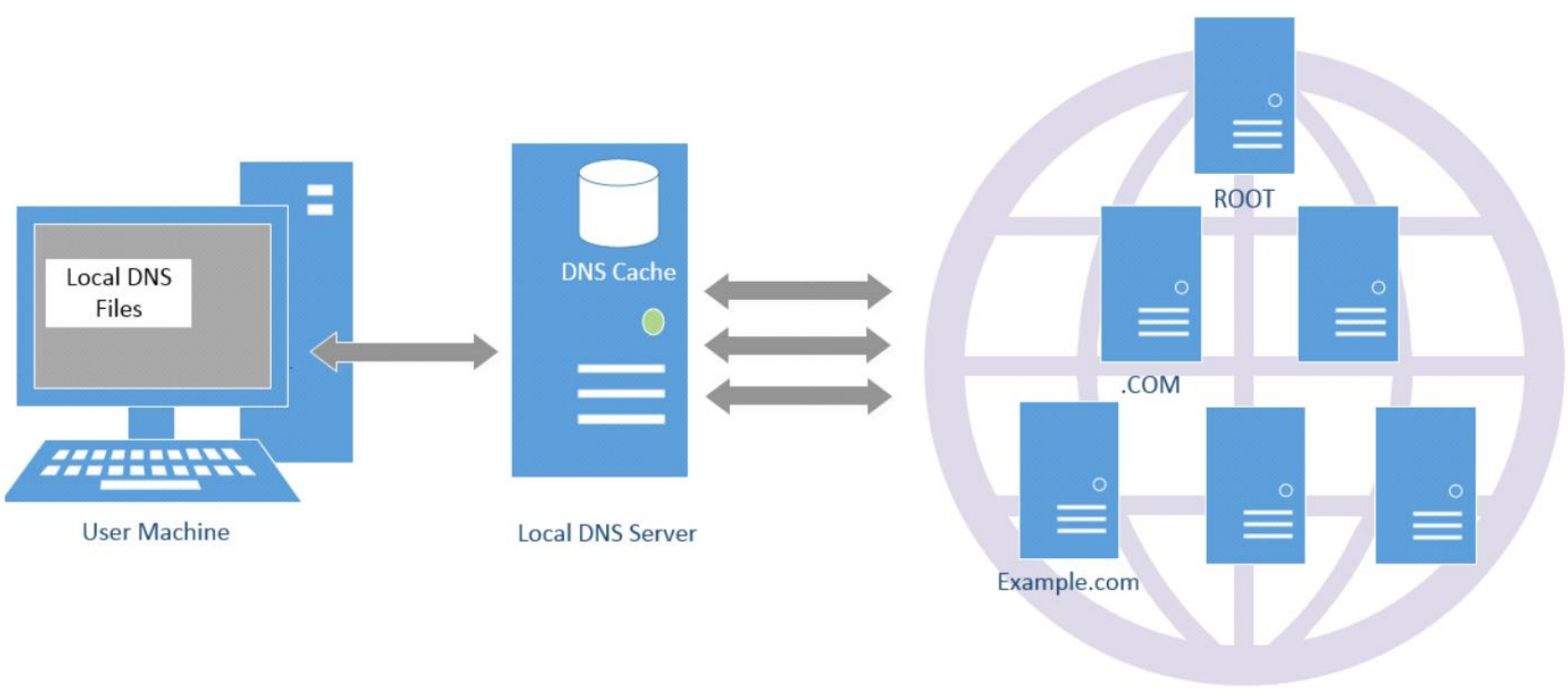
# DNS区域和权威域名服务器

- 一个DNS区域把树状域内临近的域名和子域组织起来，并将管理权限分配给实体。
  - 例如：example.com是一个国际企业，有很多子域名：usa.example.com、uk.example.com




每个DNS区域至少有一个权威域名服务器，每个权威域名服务器可以维护多个区域记录

# 本地DNS服务器


Local DNS
Files
User Machine
DNS Cache
Local DNS Server
ROOT
.COM
Example.com

# DNS迭代查询

- 查询**www.example.net**
  - 查询根域名服务器
  - 查询.net域名服务器
  - 查询.example.net域名服务器

```
seed@ubuntu:~$ dig @a.root-servers.net www.example.net
```

```
seed@ubuntu:~$ dig @m.gtld-servers.net www.example.net
```

```
seed@ubuntu:$ dig @a.iana-servers.net www.example.net

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

;; ANSWER SECTION:
www.example.net.   86400 IN    A     93.184.216.34
```

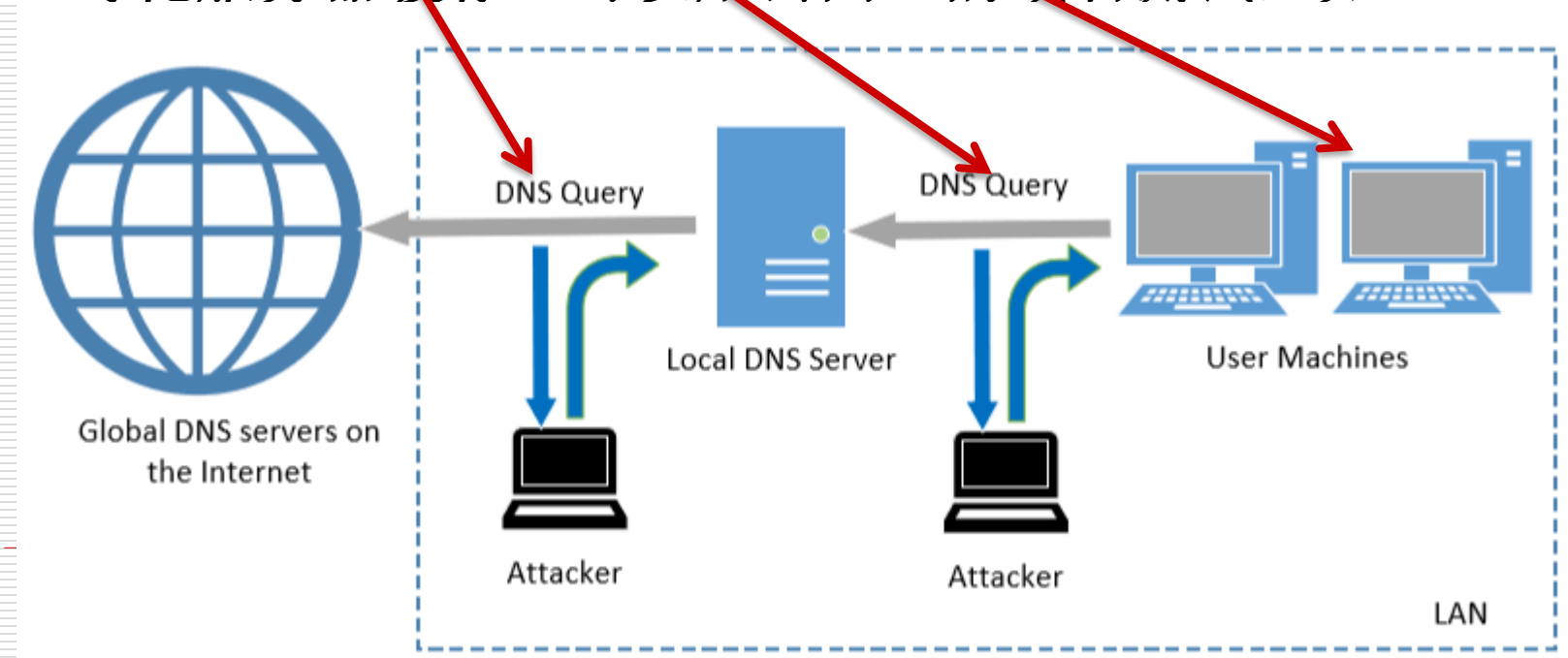
```
b.iana-servers.net. 172800 IN A     199.43.133.53
```

# DNS根域名服务器

| Hostname | IP Addresses | Manager |
|---|---|---|
| a.root-servers.net | 198.41.0.4, 2001:503:ba3e::2:30 | VeriSign, Inc. |
| b.root-servers.net | 192.228.79.201 | University of Southern California (ISI) |
| c.root-servers.net | 192.33.4.12 | Cogent Communications |
| d.root-servers.net | 199.7.91.13, 2001:500:2d::d | University of Maryland |
| e.root-servers.net | 192.203.230.10 | NASA (Ames Research Center) |
| f.root-servers.net | 192.5.5.241, 2001:500:2f::f | Internet Systems Consortium, Inc. |
| g.root-servers.net | 192.112.36.4 | US Department of Defence (NIC) |
| h.root-servers.net | 128.63.2.53, 2001:500:1::803f:235 | US Army (Research Lab) |
| i.root-servers.net | 192.36.148.17, 2001:7fe::53 | Netnod |
| j.root-servers.net | 192.58.128.30, 2001:503:c27::2:30 | VeriSign, Inc. |
| k.root-servers.net | 193.0.14.129, 2001:7fd::1 | RIPE NCC |
| l.root-servers.net | 199.7.83.42, 2001:500:3::42 | ICANN |
| m.root-servers.net | 202.12.27.33, 2001:dc3::35 | WIDE Project |

# DNS攻击

- 攻击用户主机：修改/etc/hosts，或/etc/resolv.conf
- 欺骗用户响应：伪造来自服务器的响应包，在真的服务器响应到达用户主机之前
- DNS缓存中毒攻击：伪装其它服务器到服务器的响应，毒化服务器缓存（可以用公网上的域名测试，如baidu）



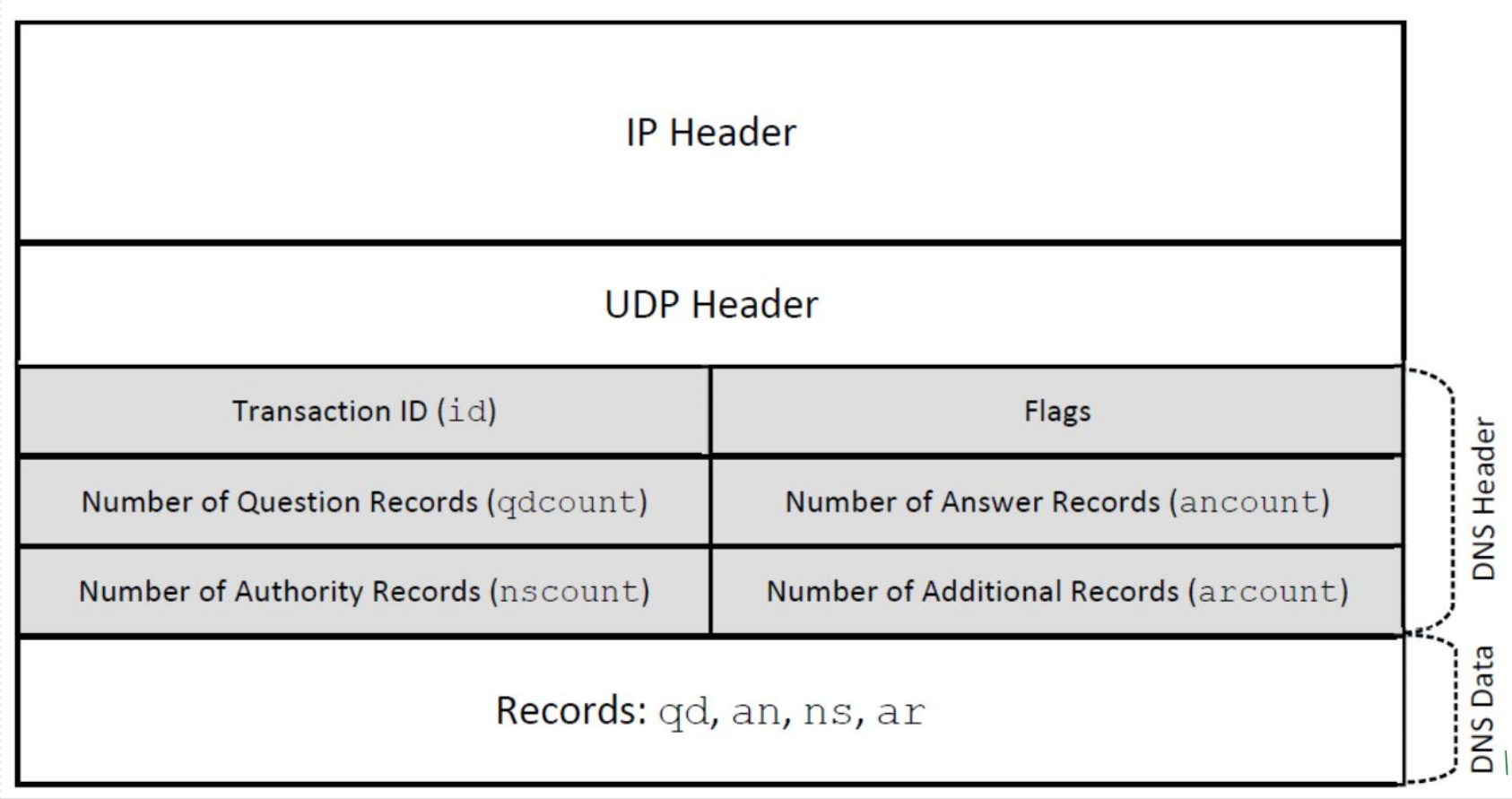
# DNS本地攻击

- 攻击者和用户机或本地**DNS**服务器同一**LAN**，攻击者可以嗅探网络流量

- 攻击用户主机，欺骗用户响应
  - netwox 105

  （建议欺骗外网的域名，不要用www.example.com)
- 攻击**DNS**服务器，**DNS**缓存中毒攻击
  - netwox 105
  - scapy

# 构造DNS报文


IP Header
UDP Header
Transaction ID (id)
Flags
Number of Question Records (qdcount)
Number of Answer Records (ancount)
Number of Authority Records (nscount)
Number of Additional Records (arcount)
Records: qd, an, ns, ar
DNS Header
DNS Data

# Scapy构造DNS报文

```
>>> ls(DNS)
length     : ShortField (Cond)                   = (None)
id         : ShortField                          = (0)
qr         : BitField (1 bit)                    = (0)
opcode     : BitEnumField (4 bits)               = (0)
aa         : BitField (1 bit)                    = (0)
tc         : BitField (1 bit)                    = (0)
rd         : BitField (1 bit)                    = (1)
ra         : BitField (1 bit)                    = (0)
z          : BitField (1 bit)                    = (0)
ad         : BitField (1 bit)                    = (0)
cd         : BitField (1 bit)                    = (0)
rcode      : BitEnumField (4 bits)               = (0)
qdcount    : DNSRRCountField                     = (None)
ancount    : DNSRRCountField                     = (None)
nscount    : DNSRRCountField                     = (None)
arcount    : DNSRRCountField                     = (None)
qd         : DNSQRField                          = (None)
an         : DNSRRField                          = (None)
ns         : DNSRRField                          = (None)
ar         : DNSRRField                          = (None)
```

# DNS记录格式(RFC 1035)

**Question Record**

| Name | Record Type | Class |
|---|---|---|
| twysw.example.com | "A" Record 0x0001 | Internet 0x0001 |

**Answer Record**

| Name | Record Type | Class | Time to Live | Data Length | Data: IP Address |
|---|---|---|---|---|---|
| twysw.example.com | "A" Record 0x0001 | Internet 0x0001 | 0x00002000 (seconds) | 0x0004 | 1.2.3.4 |

**Authority Record**

| Name | Record Type | Class | Time to Live | Data Length | Data: Name Server |
|---|---|---|---|---|---|
| example.com | "NS" Record 0x0002 | Internet 0x0001 | 0x00002000 (seconds) | 0x0017 | ns.dnslabattacker.net |

Representation in the packet
(Total: 0x17 bytes)

| 2 | n | s | 14 | d | n | s | l | a | b | a | t | t | a | c | k | e | r | 3 | n | e | t | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

# 用scapy构造DNS报文

## ❖ DNSQR Class

```
>>> ls(DNSQR)
qname      : DNSStrField                    = (b'www.example.com')
qtype      : ShortEnumField                 = (1)
qclass     : ShortEnumField                 = (1)
```

## ❖ DNSRR Class

```
>>> ls(DNSRR)
rrname     : DNSStrField                    = (b'.')
type       : ShortEnumField                 = (1)
rclass     : ShortEnumField                 = (1)
ttl        : IntField                       = (0)
rdlen      : FieldLenField                  = (None)
rdata      : MultipleTypeField              = (b'')
```

# 本地DNS缓存中毒攻击

```
local_dns_srv = "10.0.2.7"

def spoof_dns(pkt):
  if (DNS in pkt and 'example.com' in pkt[DNS].qd.qname.decode('utf-8')):
    old_ip  = pkt[IP]
    old_udp = pkt[UDP]
    old_dns = pkt[DNS]

    ip  = IP  ( dst   = ?? ,     \
                src   = ??  )

    udp = UDP ( dport = ?? ,  \
                sport = 53 )

    Anssec = DNSRR( rrname = old_dns.qd.qname, \
                    type   = ?? ,              \
                    rdata  = ?? ,        \
                    ttl    = 259200)

    dns = DNS( id = old_dns.id,                    \
               aa=1, qr=1, qdcount=??, ancount=??,  \
               qd = old_dns.qd,                    \
               an = ??)

    spoofpkt = ???
    send(spoofpkt)

f = 'udp and (src host {} and dst port 53)'.format(local_dns_srv)
pkt=sniff(filter=f, prn=spoof_dns)
```

# DNS远程攻击

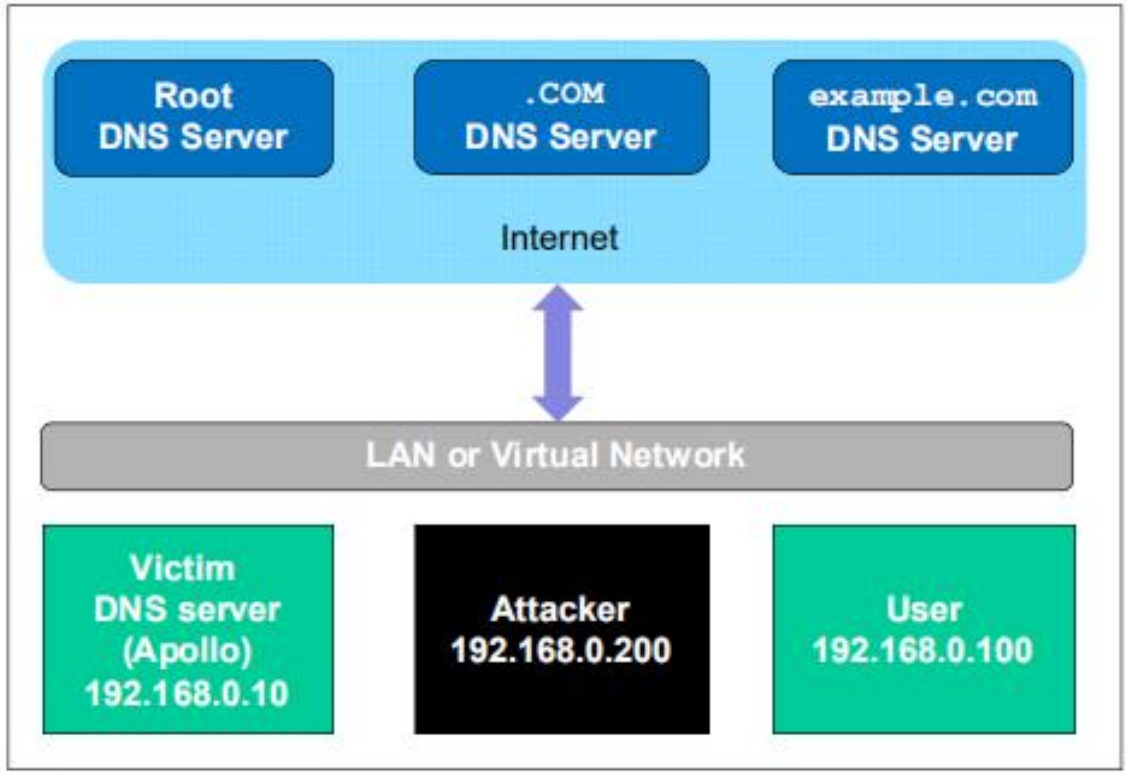



Figure 1: The Lab Environment Setup

- 攻击者不能嗅探到DNS服务器和用户之间的数据
- 远程缓存中毒

# 远程缓存中毒

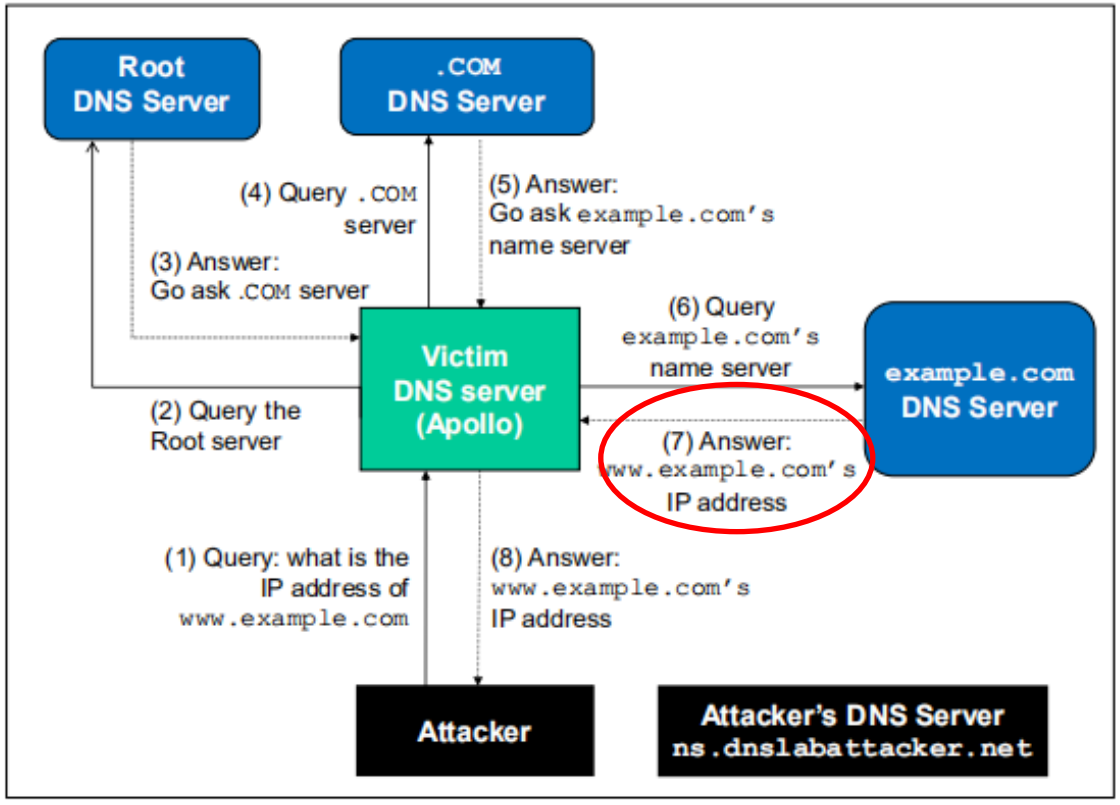
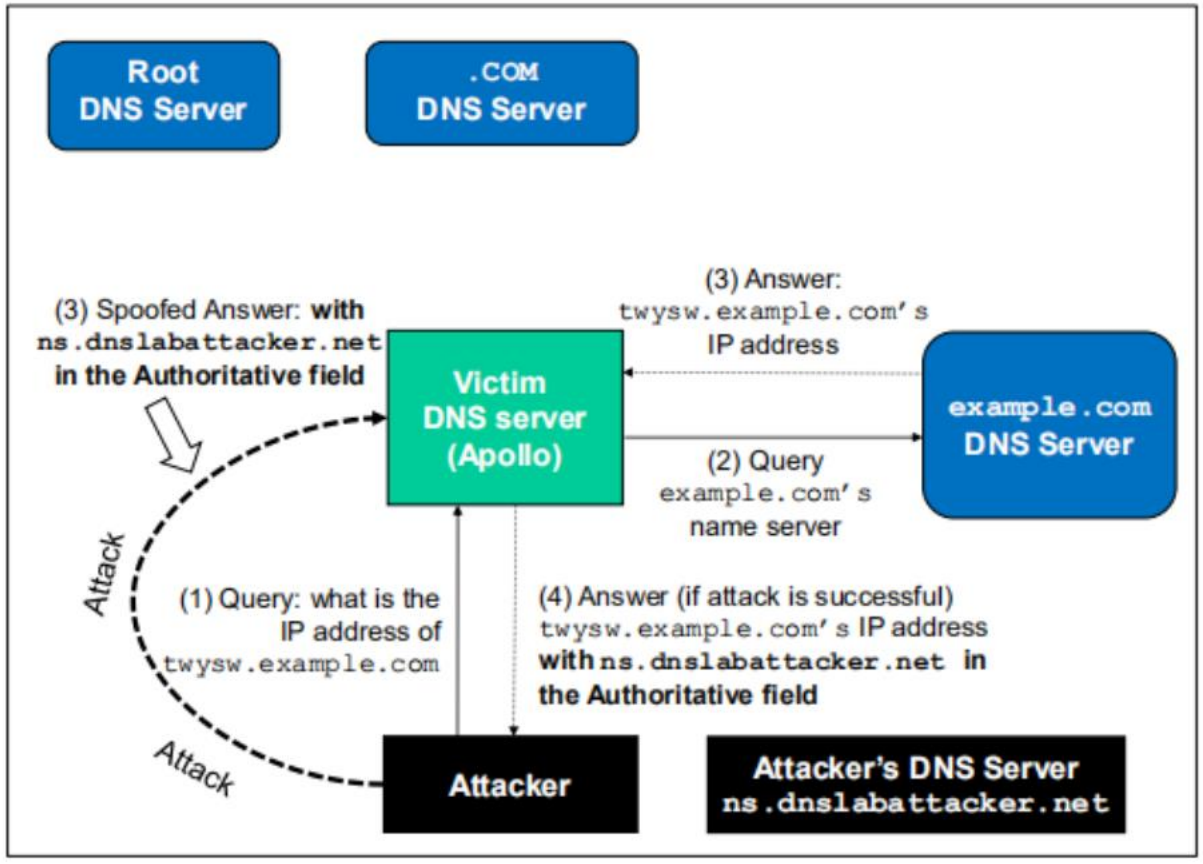



Figure 2: The complete DNS query process

当Apollo等待example.com DNS服务器的应答时，攻击者伪造DNS响应

# 远程缓存中毒




- 难点1：猜对事务ID
  解决：事务ID 16位，范围有限

- 难点2：缓存效应
  解决：Kaminsky攻击，查询包含不同名字的域名

此实验可能需要尝试多次才能成功一次，实验过程中一定要及时保存结果的截图

# 4 实验要求

- 按照实验指导手册，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，回答超星平台的问题，提交作业。
- 本次实验不需要提交报告
- 注意保存实验过程中的截包数据和屏幕截屏，超星平台作业需要提交。

# 参考资料：

- 杜文亮. 计算机安全导论：深度实践. 高等教育出版社
- **SEED**实验室网站：

  http://www.cis.syr.edu/~wedu/seed/
- **Scapy**中文手册

  https://wizardforcel.gitbooks.io/scapy-docs/content/

# 常见错误

**1. service bind9 start**

提示加载**liblwres.so.141**动态库失败，权限不够

解决**: docker run**后面不带**--privileged**参数

**2. Service bind9 start**

启动失败，无错误原因提示

查看错误信息：**named –d 3 –f –g**

一般是配置文件语法错误引起的