

# 实验二 **DNS**协议漏洞利用实验

---

网安2101-2102 张云鹤

网安2103-2104 梅松

信安2101-2102 肖凌

信安2103-2104 陈凯

密码2101-2102 董枫

网安本硕博 2101 王美珍

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

---

- 登陆vmcourse平台：
  - <https://222.20.126.111>
  - 虚拟机系统：ubuntu 20.04(seed20.04)
- ubuntu系统的用户密码
  - 虚拟机用户：ubuntu ， 密码：123456
  - 容器server用户：root ， 密码：123456
- 实验采用一个虚拟机，多个容器来完成

# docker容器的使用

---

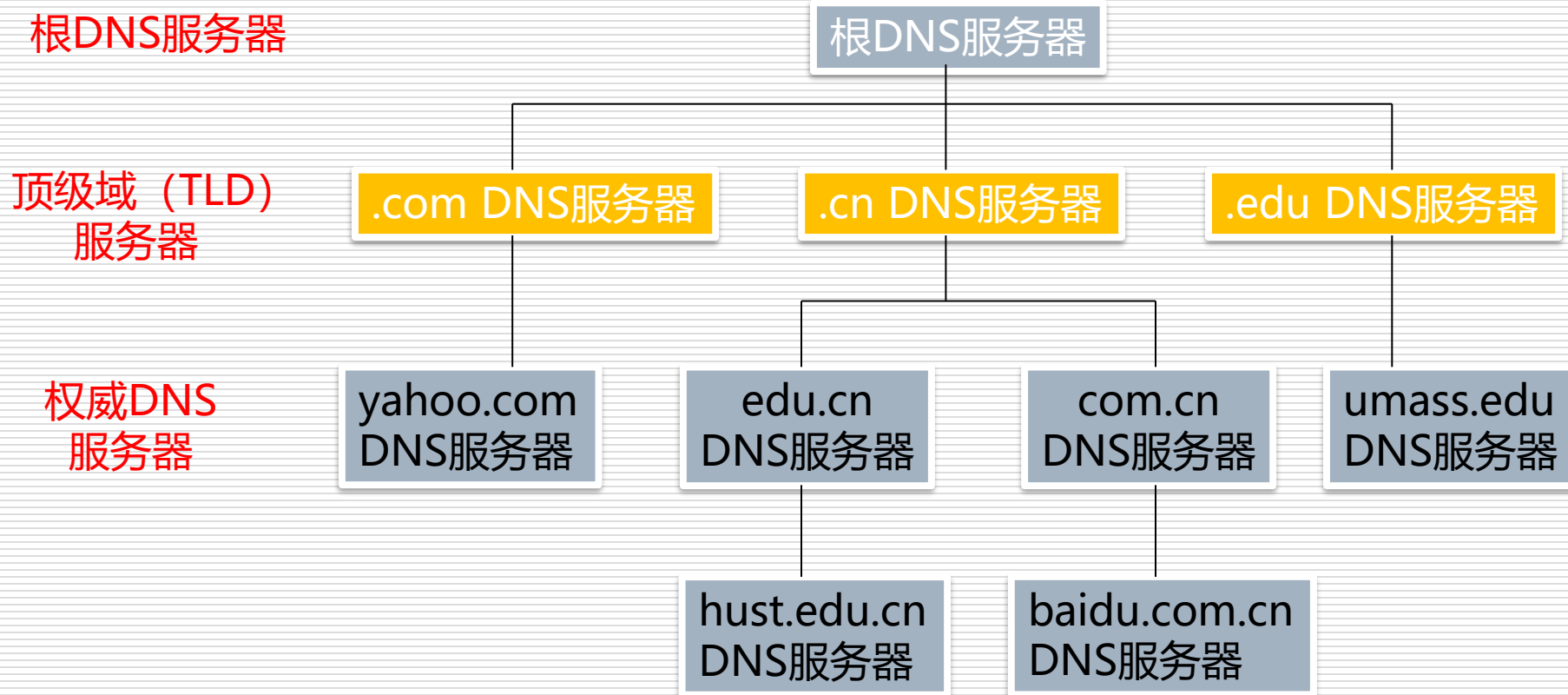
- 容器查看
    - `docker ps -a`, 可以看到已有两个容器: user, dns
  - 容器启用/停止
    - `docker start/stop 容器名`
  - 进入容器的命令行
    - `docker exec -it 容器名 /bin/bash`
  - 删除容器(实验未完成前不要删除)
    - `docker rm 容器名`
  - 主机和容器之间拷贝数据
    - `docker cp 容器名称:路径 主机路径`
    - `docker cp 主机路径 容器名称:路径`
-

# 3 实验内容

---

- ☐ **DNS**本地攻击
- ☐ **DNS**远程攻击

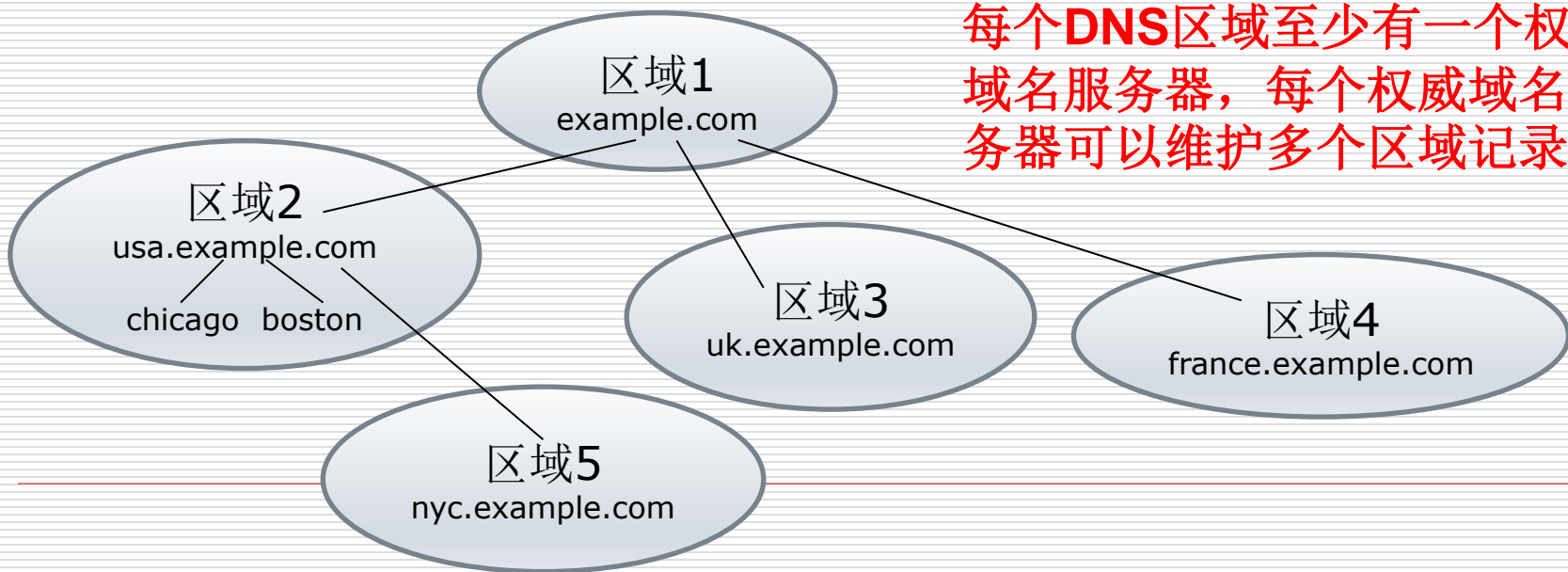
# 域名系统



# 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

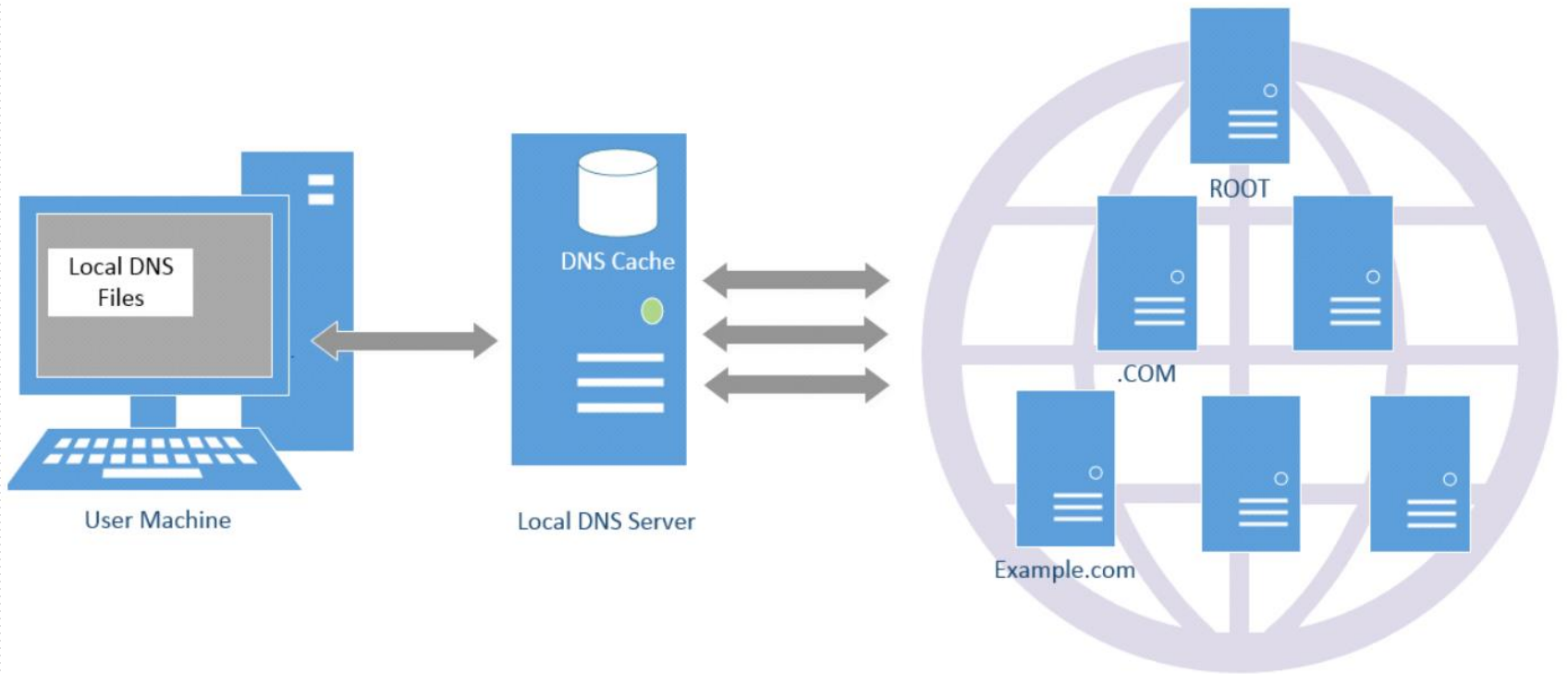
每个**DNS**区域至少有一个权威域名服务器，每个权威域名服务器可以维护多个区域记录





# 本地DNS服务器

---



# 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
-

# 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查询举例

---

## 查询权威域名服务器

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

(Only a portion of the reply is shown here)

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

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

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

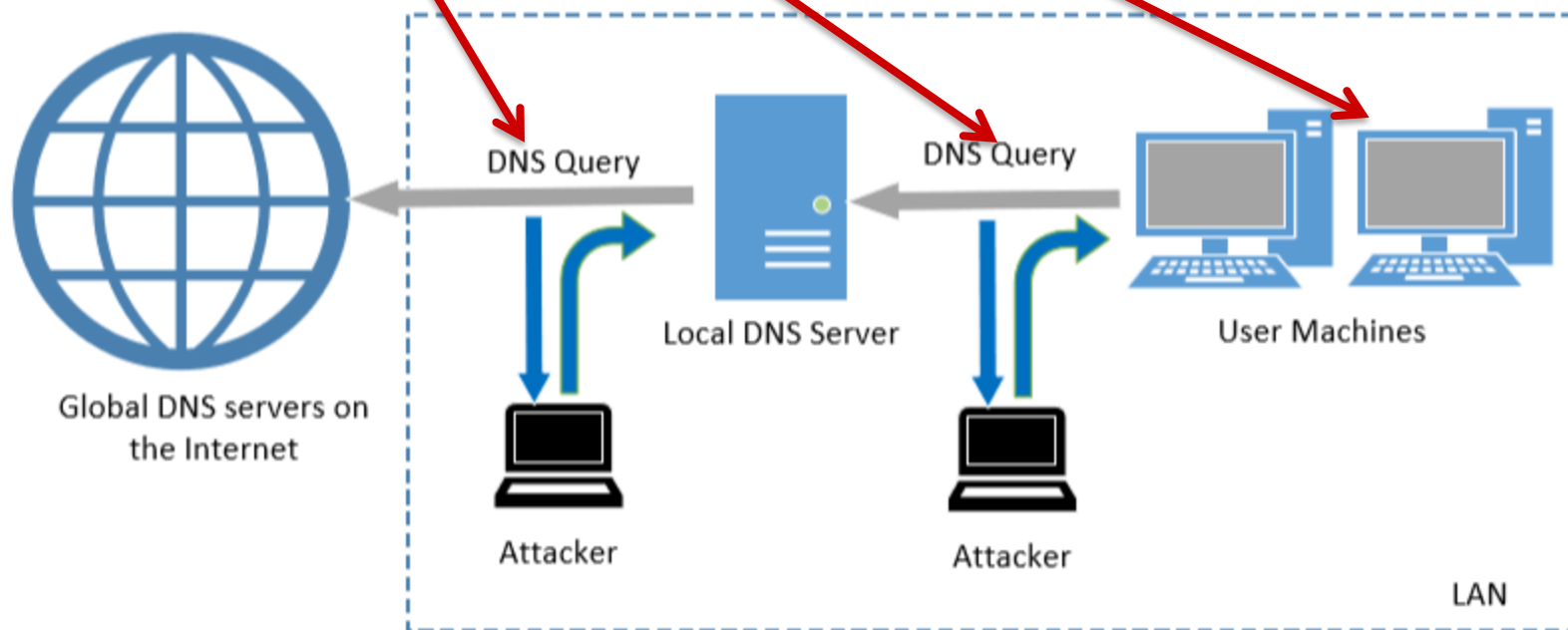
```
;; QUESTION SECTION:
;www.example.net.      IN      A
```

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

---

# 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）

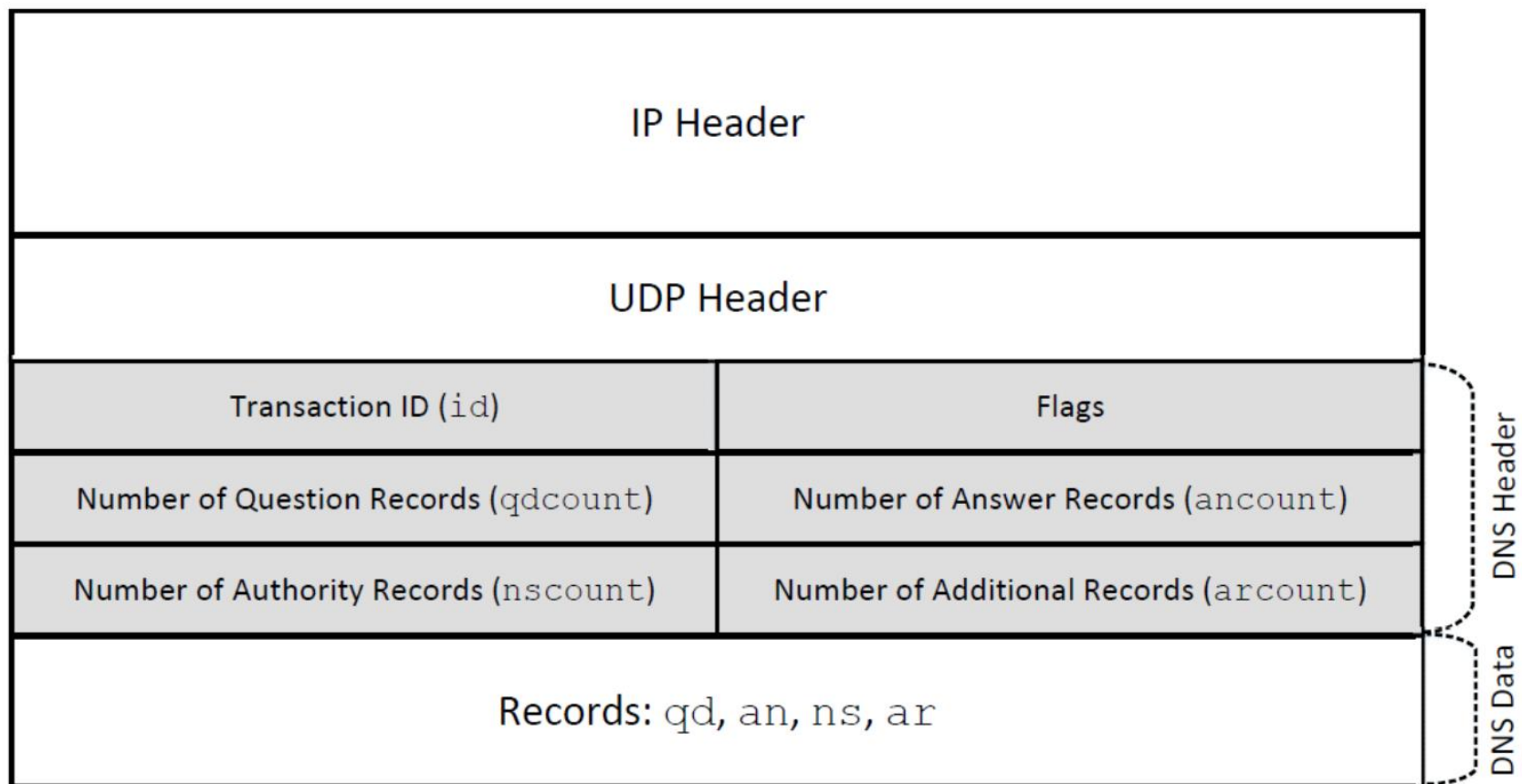


# DNS本地攻击

---

- 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



# 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( rname = old_dns.qd.qname, \
                        type = ?? , \
                        rdata = ?? , \
                        ttl = 259200)

        dns = DNS( id = old_dns.id, \
                   aa=1, qr=1, qdcount=??, ancourt=??, \
                   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

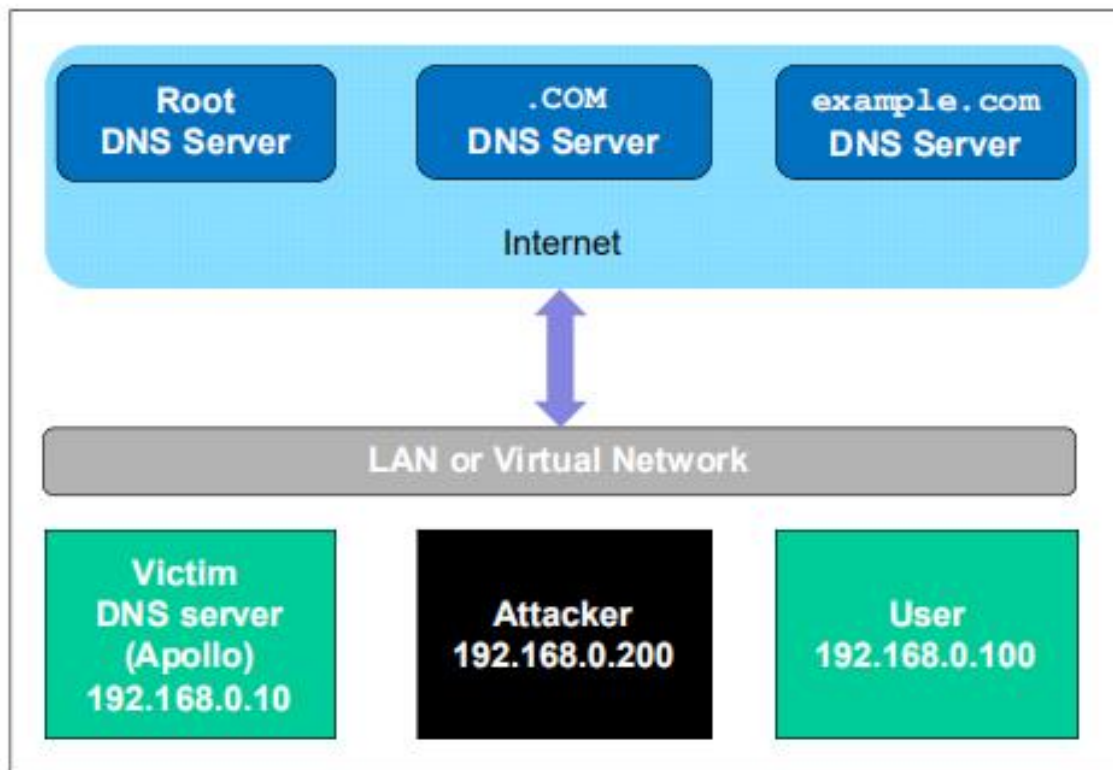


Figure 1: The Lab Environment Setup

- 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

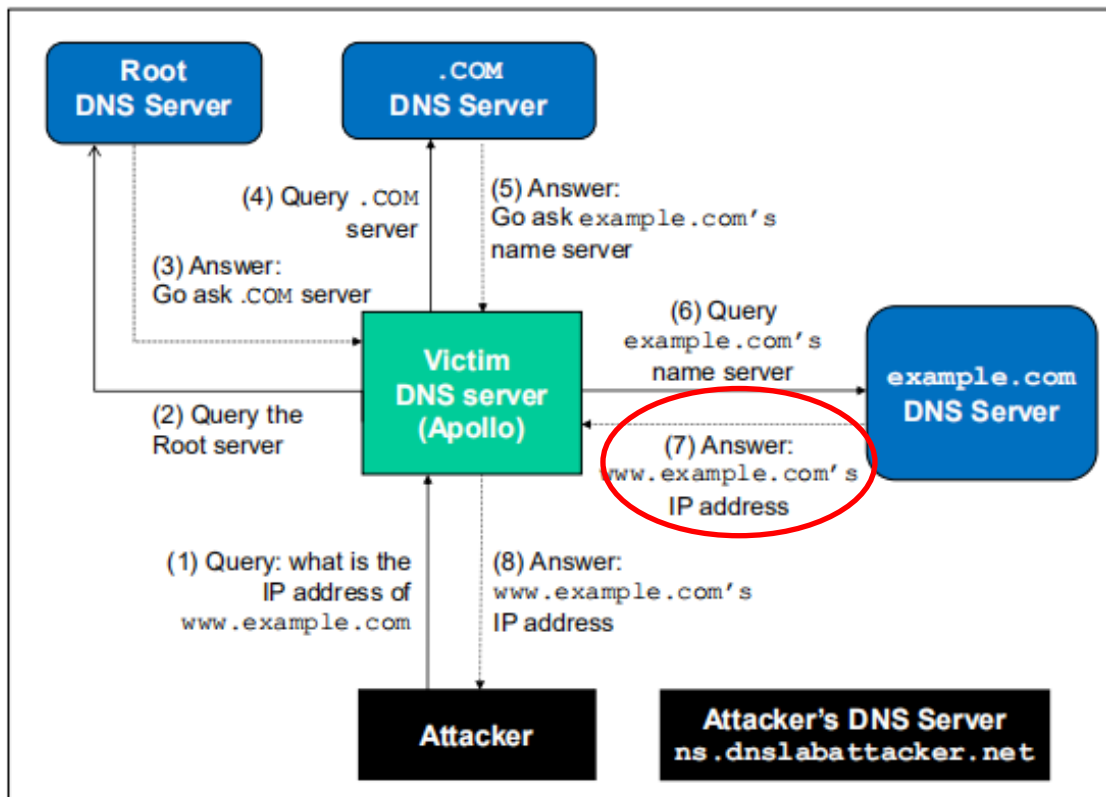
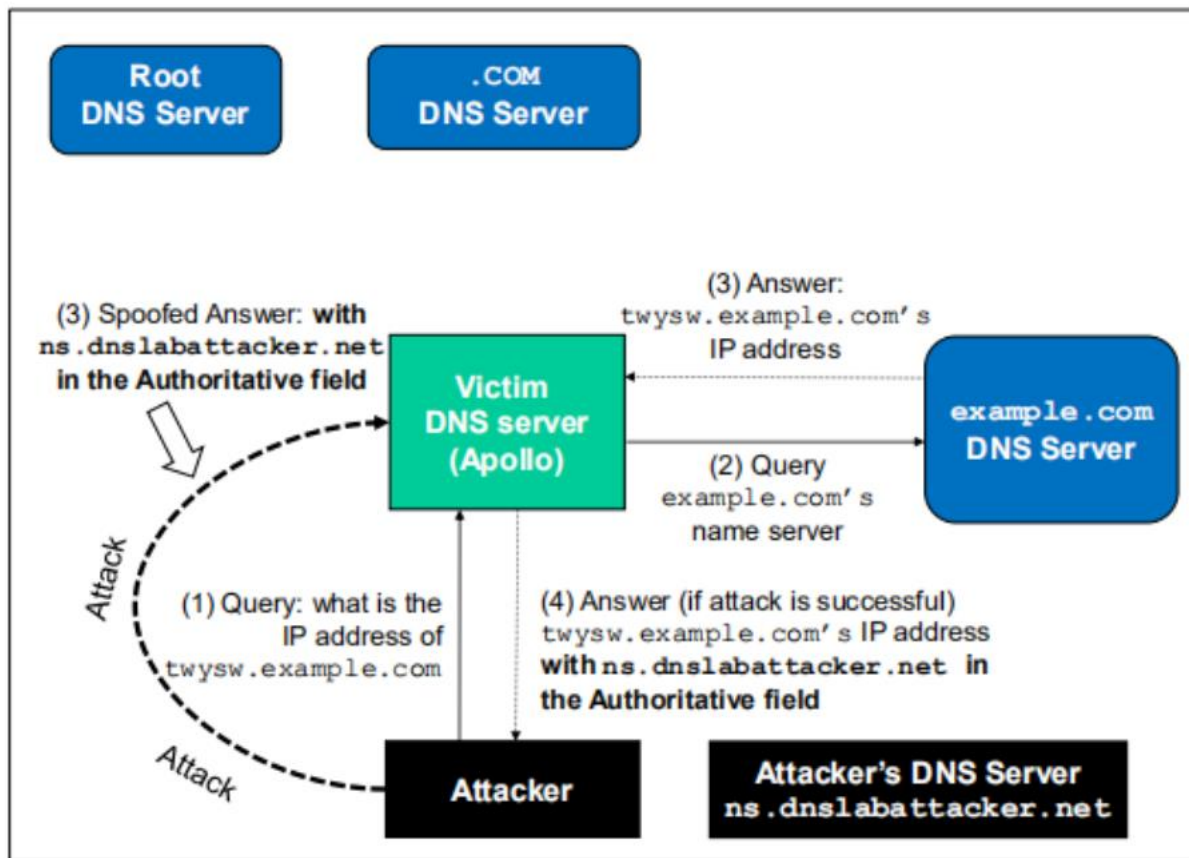


Figure 2: The complete DNS query process

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, 实验之前一定看清楚测评的要求, 实验成功以后及时提交测评

## 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，提交习题测评。
  - 远程缓冲中毒实验时，伪造的响应报文中，**ns.dnslabattack.net**的名字改为“**ns.hust-cse.net**”，相应的配置文件也要自行修改
  - 本次实验不需要提交报告
-

## 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:  
<https://seedsecuritylabs.org/>
  - ❑ **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

---