实验二 windows 下 dns 欺骗实验

实验目的：

1.在 ARP 欺骗技术的基础上进行 DNS 欺骗。

2.了解 DNS 欺骗的基本原理。

3.熟悉 DNS 欺骗的工具使用，完成实验过程。

实验要求：

1、复习网络层次及协议对应关系，协议封装，重点对 dns 协议数据结构进行分析；

2、工具及软件选用：安装 cain 软件并做相应的设置；

3、明确 dns 协议的缺陷，制定模拟 dns 攻击方法；

4、实施 dns 协议模拟攻击与攻击结果检查；

实验原理：

1.DNS 欺骗原理介绍

1.1.DNS 基本概念

DNS 是指：域名服务器(Domain Name Server)，该系统用于命名组织到域层次结构中的计算机和网络服务，通过用户友好的名称查找计算机和服务。当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与之相关的其他信息，如 IP 地址。在 Internet 上域名与 IP 地址之间是一一对应的，域名虽然便于人们记忆，但机器之间只能互相认识 IP 地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。一般来说，打开控制面板-->网络拨号连接--->本地连接属性-->Internet 协议（TCP/IP)属性-->可以进入 IP 和 DNS 服务器地址的设置。用户可以自行设置该机器的 DNS 服务器地址（首选 DNS 服务器和备选 DNS 服务器），若选择“自动分配”，则可以自动获取 DNS 服务器地址。DNS 服务器地址也可以通过“ipconfig”命令查看到。

1.2.DNS 欺骗原理介绍

首先先了解正常 DNS 请求的过程：

1) 用户在浏览器中输入需要访问的网址

2) 计算机将会向 DNS 服务器发出请求

3) DNS 服务器经过处理分析得到该网址对应的 IP 地址

4) DNS 将 IP 地址返回到发出请求的计算机

5) 此时，用户正常登陆到所需要访问的网址

而 DNS 欺骗是这样一种中间人攻击形式，它是攻击者冒充域名服务器的一种欺骗行为，DNS 欺骗其实并不是真的“黑掉”了对方的网站，而是冒名顶替、招摇撞骗罢了。被 DNS 欺骗以后的 DNS 请求的过程变为:

1) 用户在浏览器中输入需要访问的网址

2) 计算机将会向 DNS 服务器发出请求(这里注意：实际上你发起的请求被发送到了攻击者那里)

3) 攻击者对请求处理进行伪造 DNS 回复报告，返回给计算机的是攻击者指定的 IP 地址

4) 此时，用户访问到的网址并不是他之前写入的网址，而是掉入攻击者设置的“陷阱网站”

DNS 欺骗可以使得用户访问某个网站的时候跳转到“陷阱网站”，也可以通过设置使得用户访问任一网址都跳转到“陷阱网址”。通过 DNS 欺骗，攻击者可以通过陷阱网站获取用户的用户名、密码或信用卡号等信息，或将在自己的网站上“挂马”。获取用户更多信息，从而控制用户机器。 DNS 欺骗的实现一般通过 DNS 服务器高速缓存中毒（DNS Cache Poisoning）或者 DNS ID 欺骗（DNS ID Spoofing）来实现。

1.3.DNS 服务器高速缓存中毒

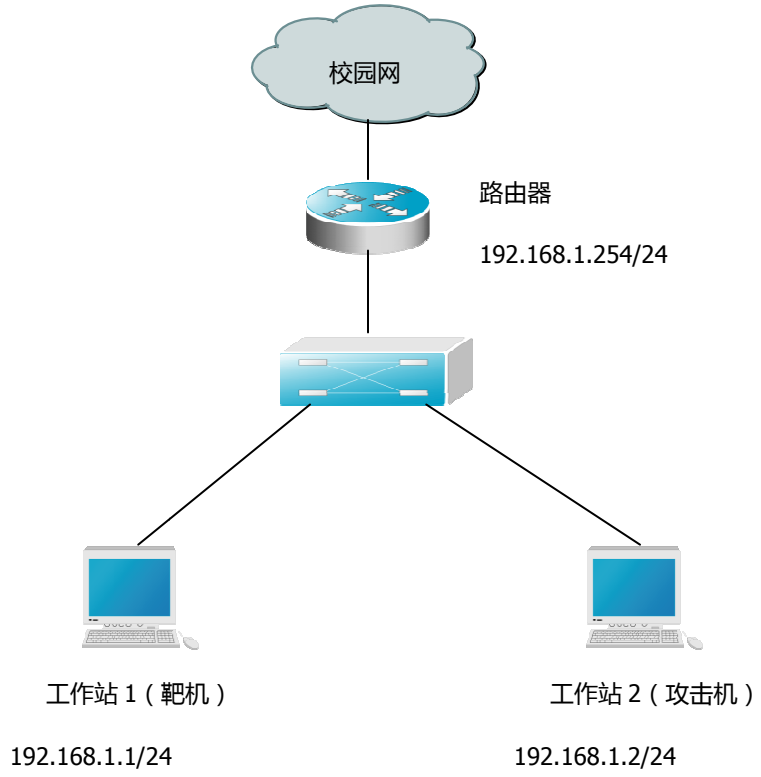
DNS 服务器有一个高速缓冲存储器（cache），它使得服务器可以存储 DNS 记录一段时间。一台 DNS 服务器只会记录本身所属域中的授权的主机，如果它想要知道其它的，在自身域以外主机的信息，就必须向信息持有者（另一台 DNS 服务器）发送请求，同时，为了不每次都发送请求，这台 DNS 服务器会将另一台 DNS 服务器返回的信息又记录下来。

事实上，一台 DNS 服务器只会记录本身所属域的授权主机，如果想查询自身域外的主机信息，就必须向信息持有者(另一台 DNS 服务器)发送请求，同时，为了不每次都发送请求，这台 DNS 服务器会把这条记录记到缓存中，以便下次查询时，直接从缓存中调取。攻击者此时就是打了缓存的主意。通过欺骗的手法，修改了缓存中的正确信息。

1.4.DNS ID 欺骗（DNS ID Spoofing）

当主机 A 向它所在的域的 DNS 服务器询问一个域名的 IP 地址时，主机 A 会分配一个随机数(Transaction ID)，这个数也会出现在 DNS 服务器返回的信息里，主机 A 通过对比这个数是否一致来判断信息是否有效。漏洞出现了，于是便产生了类似于 ARP 欺骗的手法，通过截获此 ID，然后伪造一个 DNS 回复，但是此回复包含了攻击提供的伪造的 IP。

实验拓扑



实验工具与软件：

1、攻击软件 cain；

2、S2126G（一台）；PC 机（三台）；R1700（一台）；直连线（4 条）

实验步骤

1、 按照拓扑图正确的连线并对路由器做正确的配置

登录路由器，进入路由器特权用户配置模式

1）设置路由器接口 ip

R1700-1#configure terminal

R1700-1(config)#int fa 1/1

R1700-1(config-if)#ip address dhcp //从校园网路由器中得到 IP 地址

R1700-1(config-if)#exit

R1700-1(config)#sh ip interface brief //查看接口 ip，看 fa1/1 是否得到了地址

Interface	IP-Address(Pri)	OK?	Status
serial 1/2	no address	YES	DOWN
serial 1/3	no address	YES	DOWN
FastEthernet 1/0	no address	YES	DOWN
FastEthernet 1/1	100.64.186.43/17	YES	UP
Null 0	no address	YES	UP

R1700-1(config)#int fa 1/0 //设置内网接口 ip 并启用

R1700-1(config-if)#ip add 192.168.1.254 255.255.255.0

R1700-1(config-if)#no shutdown

R1700-1(config-if)#exit

R1700-1(config)#sh ip int b //再次查看接口 ip

Interface	IP-Address(Pri)	OK?	Status
serial 1/2	no address	YES	DOWN
serial 1/3	no address	YES	DOWN
FastEthernet 1/0	192.168.1.254/24	YES	UP
FastEthernet 1/1	100.64.186.43/17	YES	UP
Null 0	no address	YES	UP

2）把路由器设置成 NAT 设备

R1700-1(config)#int fa 1/0 //设置内部端口

R1700-1(config-if)#ip nat inside

R1700-1(config-if)#exit

R1700-1(config)#int fa 1/1 //设置外部端口

R1700-1(config-if)#ip nat outside

R1700-1(config-if)#exit

//定义合法 IP 地址池

R1700-1(config)#ip nat pool onlyone 100.64.186.43 100.64.186.43 prefix-length 17

//定义内部网络中允许访问 Internet 的访问列表

R1700-1(config)#access-list 1 permit 192.168.1.0 0.0.0.255

//以端口复用方式，将访问列表 1 中的私有 IP 地址转换为 onlyone IP 地址池中定义的合法 IP 地址。

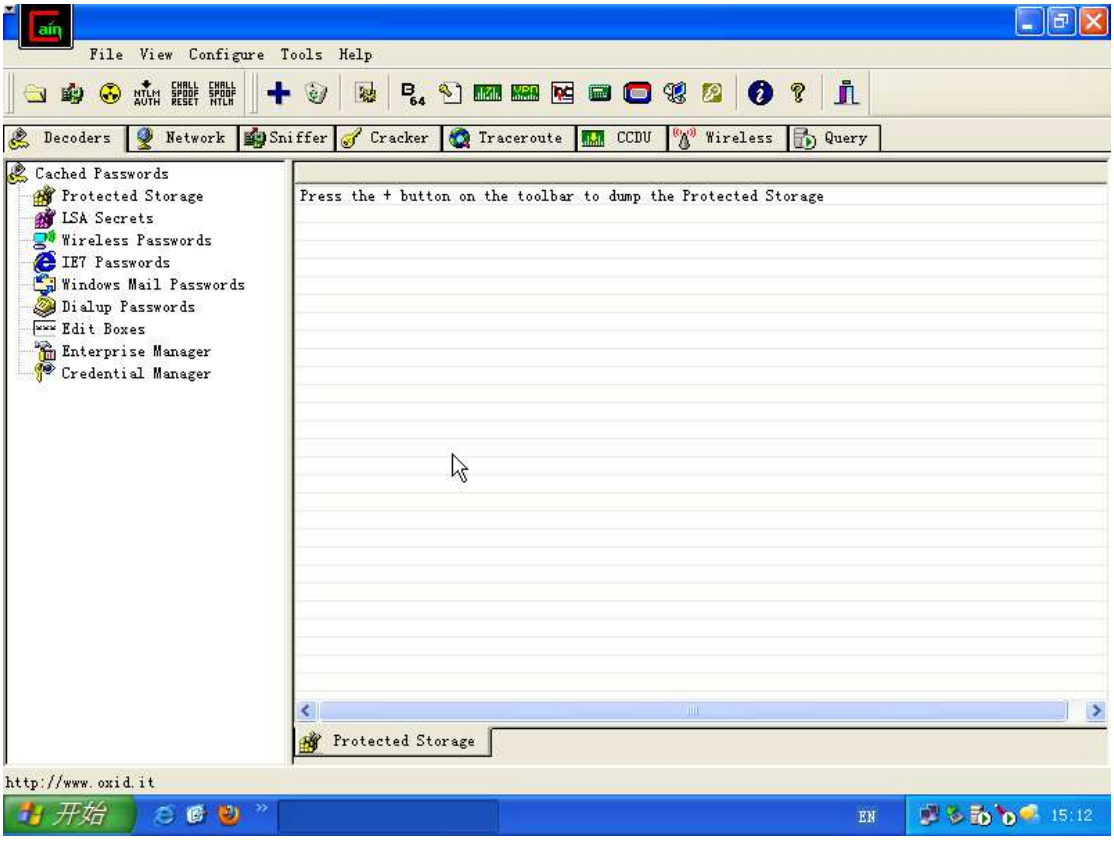
R1700-1(config)#ip nat inside source list 1 pool onlyone overload

2、正确设置攻击机和靶机（注意是修改本地连接 2 的地址）的 ip 地址和网关（网关为路由器内网接口 ip：192.168.1.254）并关闭本地连接 1（注意首先关闭路由器登录窗口），在任何一台工作站上启用 IE 并登录上校园网（登录校园网时有些延迟），如图：

现在所有内网工作站都能上网了。

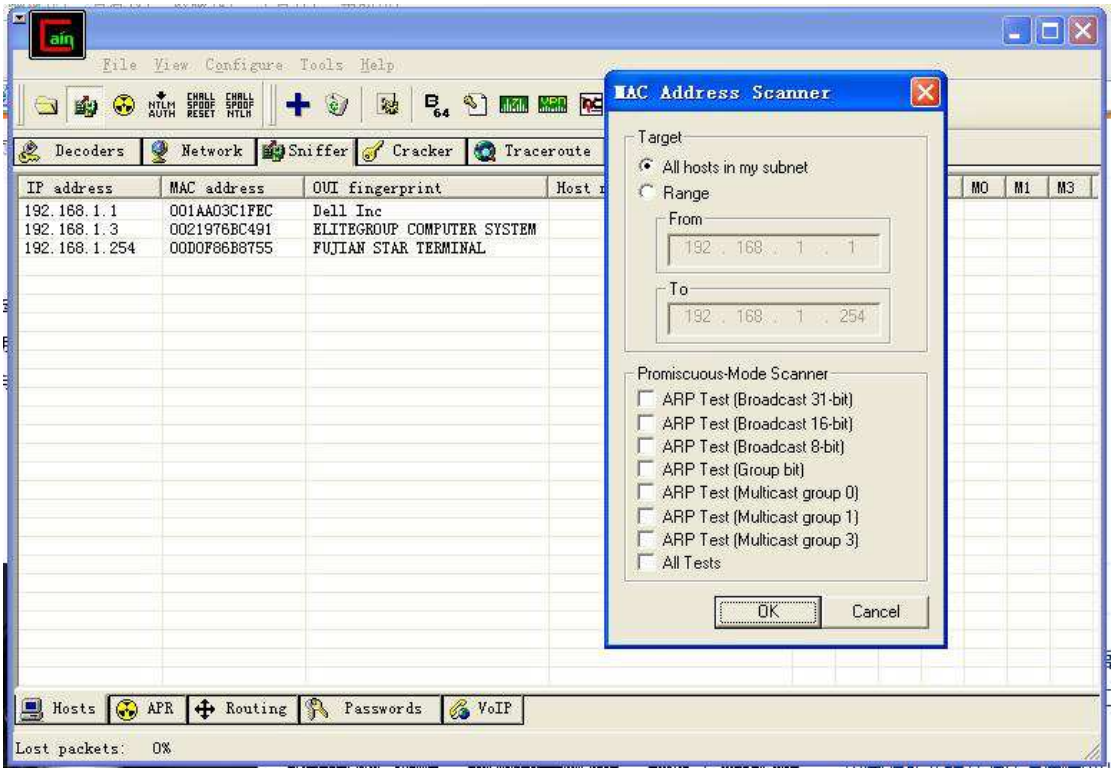
2、在攻击机上安装 cain 软件并实施攻击

1）安装好 cain 软件，其中 WinPcap 软件可以装也可以不用安装，并启动 cain 软件如下图所示：

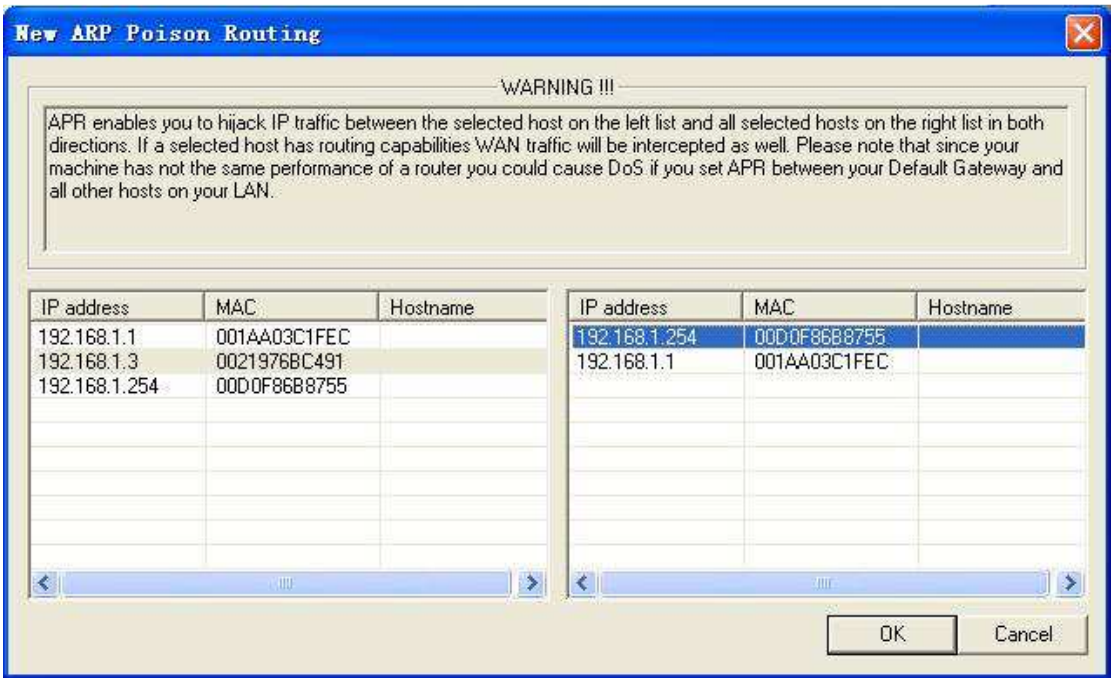


cain 功能很多，本实验仅对本实验中所用到的功能进行讲解，其余功能可以自学了解、尝试。

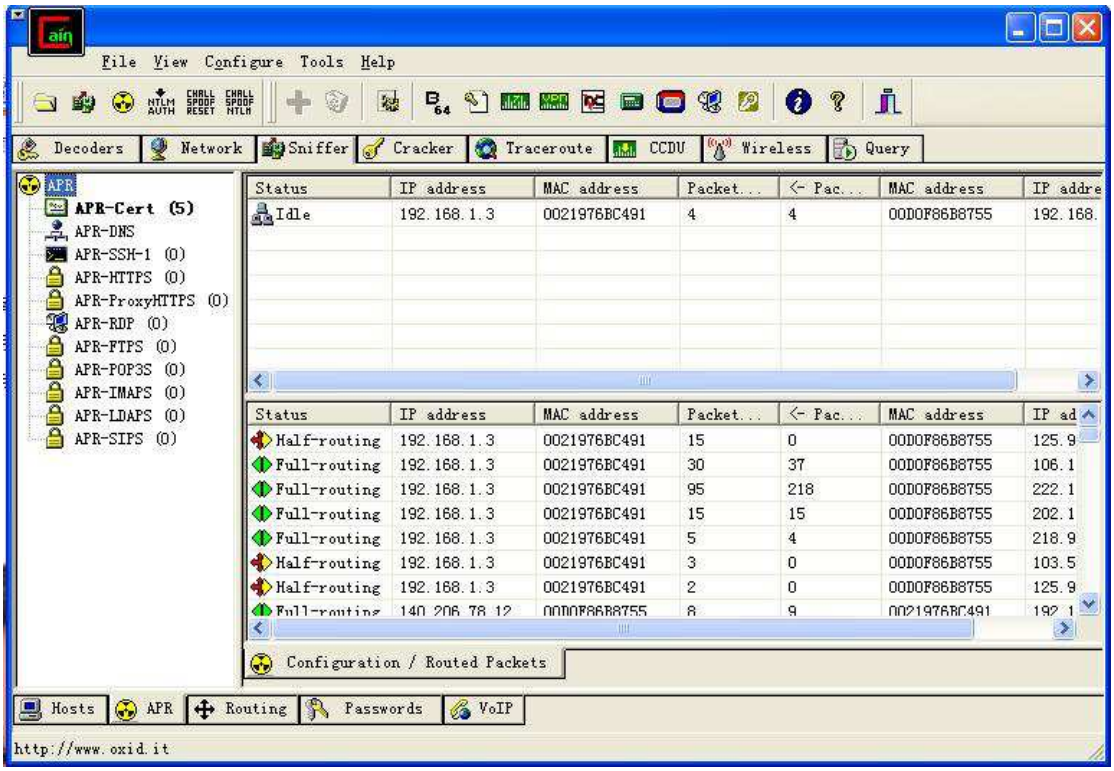
2）设置好相应参数后，点击“确定”，返回到 Cain 主界面，（这里无需设置任何参数）按下下图左侧红框内的“start/stop sniffer”快捷按钮，再点击右侧红框中的“Add to list”按钮，可以对主机所在的整个网络或指定网络进行嗅探。本实验选择对整个局域网进行嗅探，选择“All hosts in my subnet”，点击“OK”。主界面将出现在指定区域内扫描到得主机 IP、MAC 地址等信息。如下图所示：



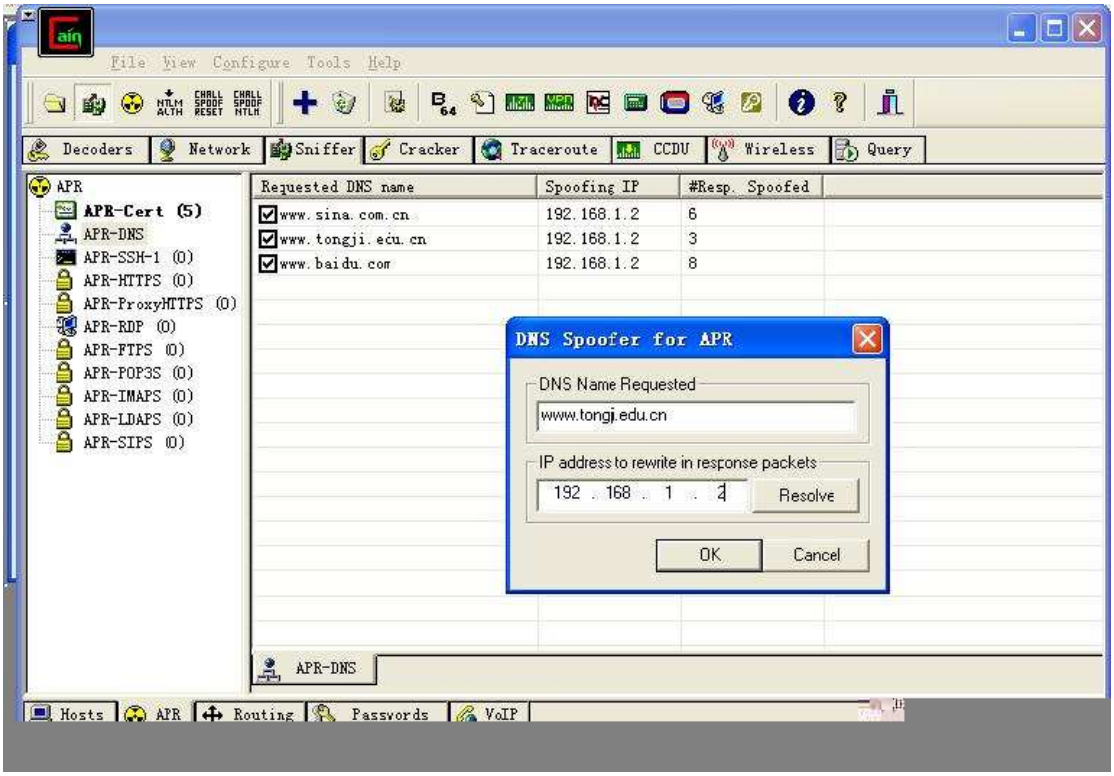
3）选择 Cain 主界面下端的 APR 标签，点击下图上方红框，随后点击“Add to list”快捷按键，在选项框中选择进行嗅探的 ip 地址。左边选择被欺骗的主机即靶机，再在右边选择网关。ARP 能够在左边列表中被选的主机和所有在右边选中的主机之间双向劫持 IP 包。在该实验中首先在左侧列表中选择靶机的 ip 地址：192.168.1.1，然后右侧列表即会出现其他 IP 地址，若在右侧选择网关 192.168.1.254，这样就可以截获所有从靶机发出到广域网的数据包信息。点击“OK”。如下图所示：



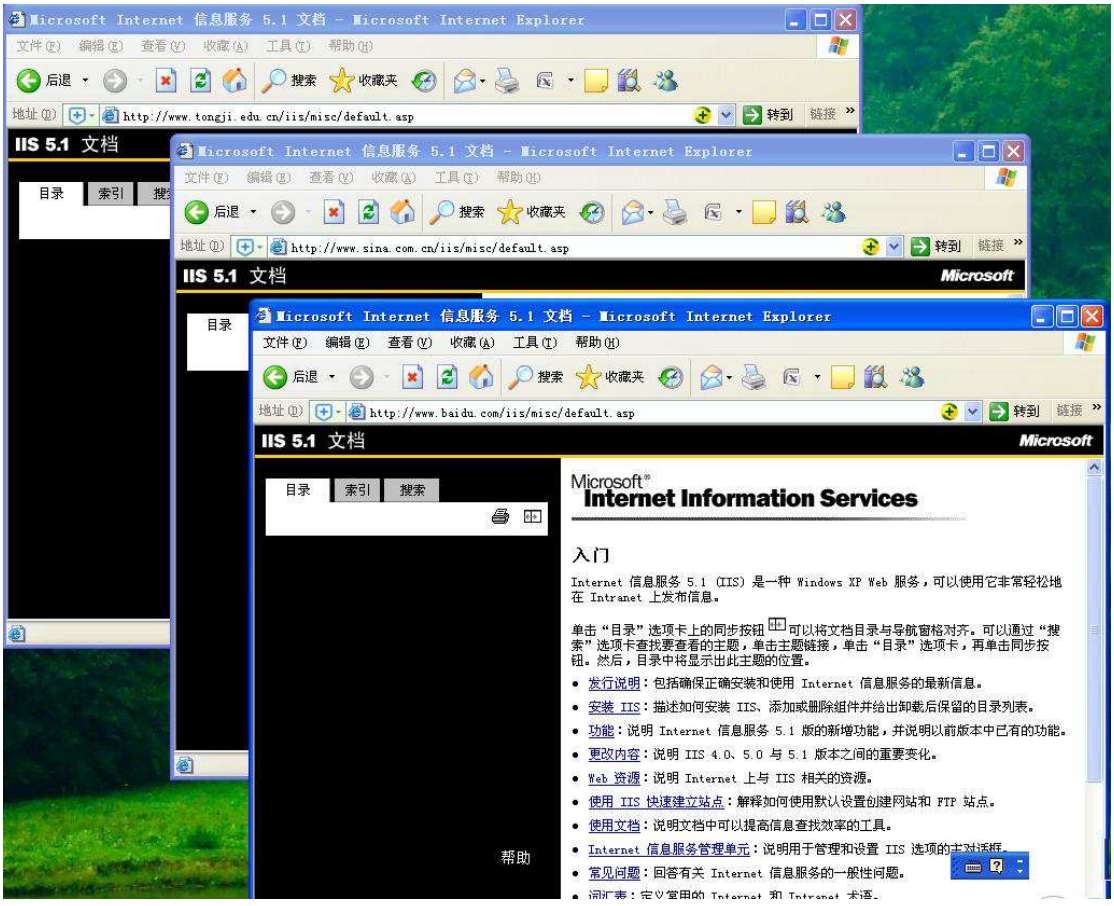
4） 在 Cain 界面上可以看到形成的欺骗列表，此时在状态一栏中显示“idle”，接着点击工具栏上的“Start/Stop ARP”快捷按钮，状态将变为“poisoning”，开始捕获。此时，在靶机上进行上网操作，在攻击机的 Cain 界面上会看到显示捕获数



5） 下面开始 ARP_DNS 欺骗。选择 Cain 界面左侧栏目中的“ARP_DNS”标签，点击下图红框内的“Add to list”，弹出对话框：在 DNS 名称请求处填入被欺骗主机要访问的网址，在回应包中输入欺骗的网址 IP（“陷阱网址”，这里为攻击机的 ip），点击“OK”设置完毕。如下图：



6）检查是否欺骗成功。此时，靶机访问网址,进入的不是想进入的网址，而是跳转到预设的页面，欺骗成功。如图：



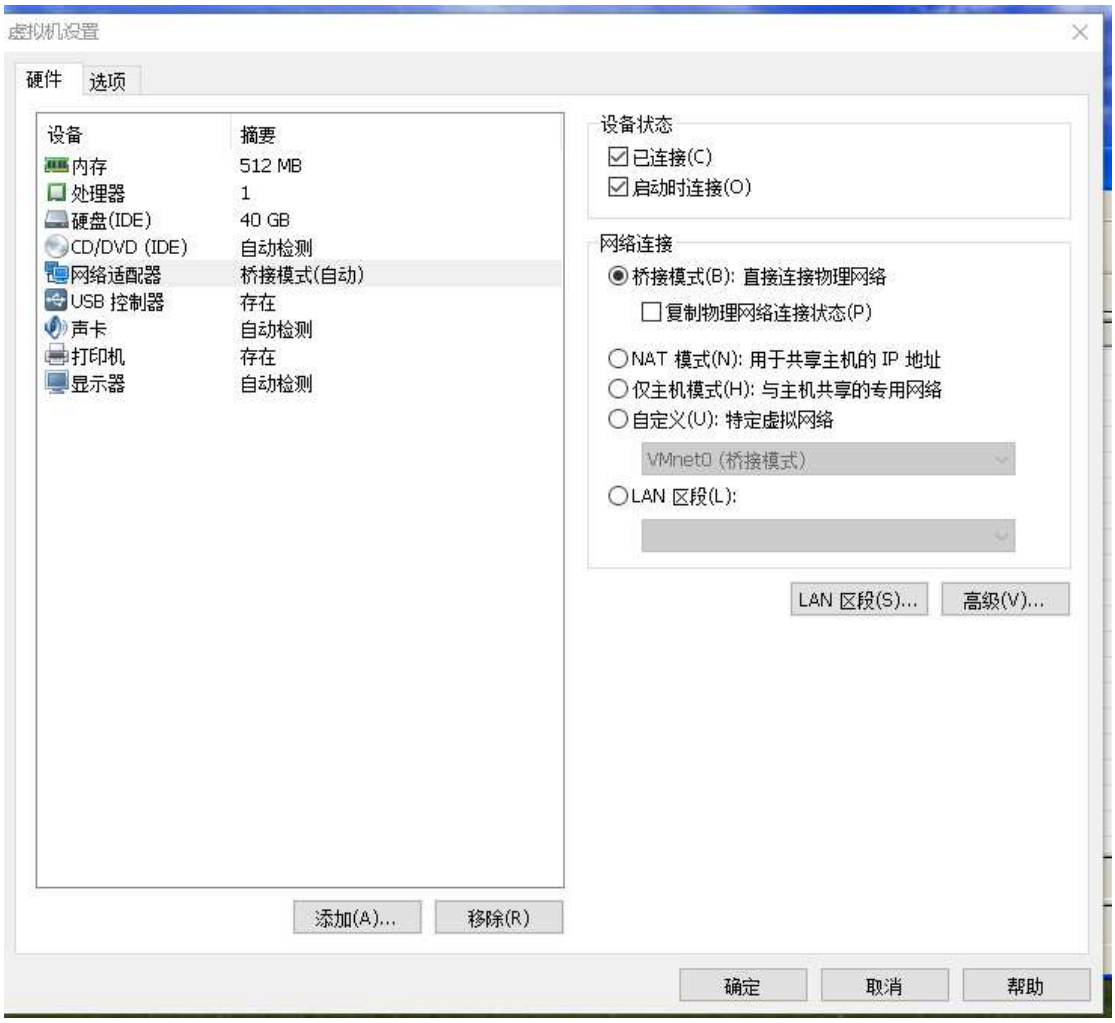
如没有出现此页面，表示在本地缓存中存在正确的网址，这里必须清除缓存，可以修护网卡也可以重启网卡。

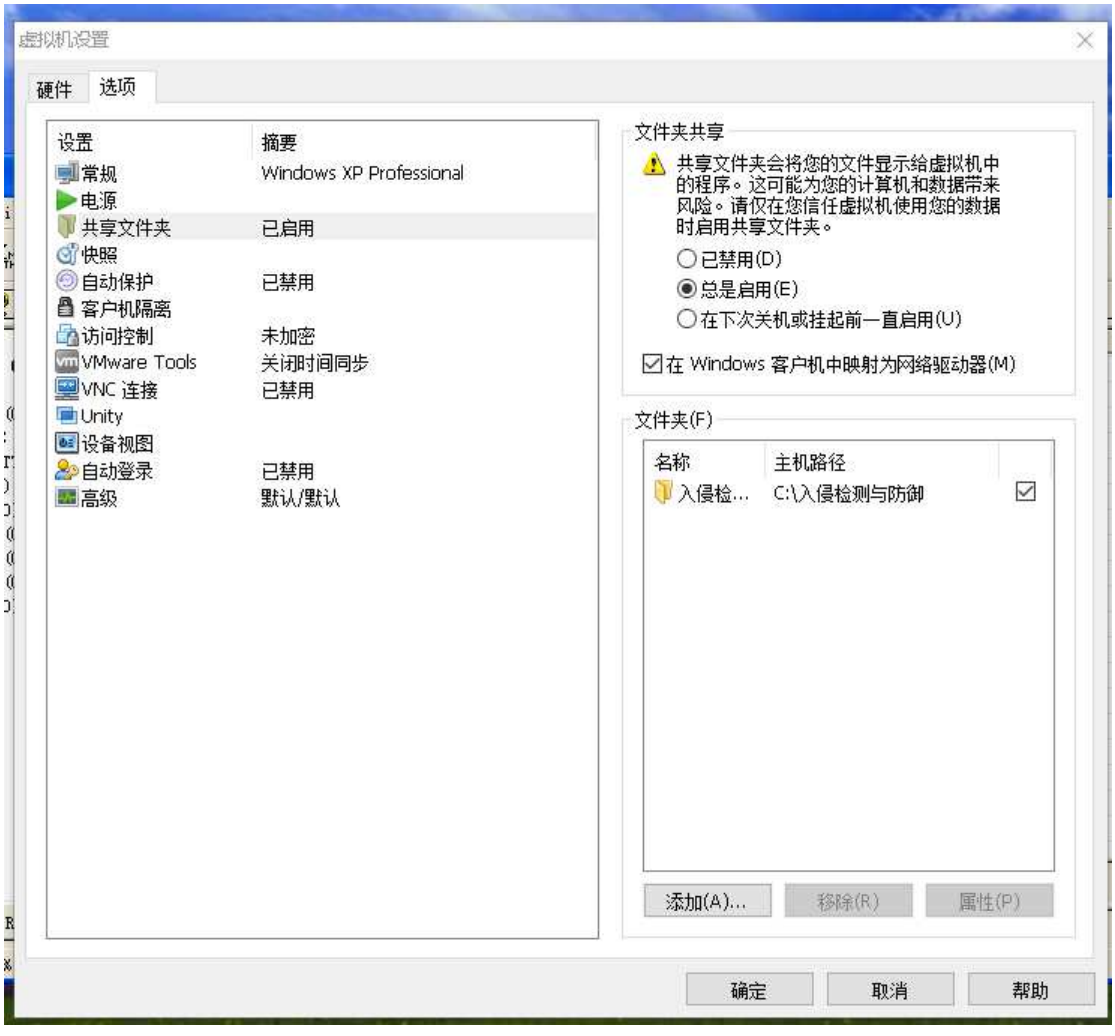
注意事项：

- 由于 cain 软件 win10 中出现问题，所以改为虚拟机，在虚拟机上启动 winxp，在启动 winxp 前进行下列步骤：

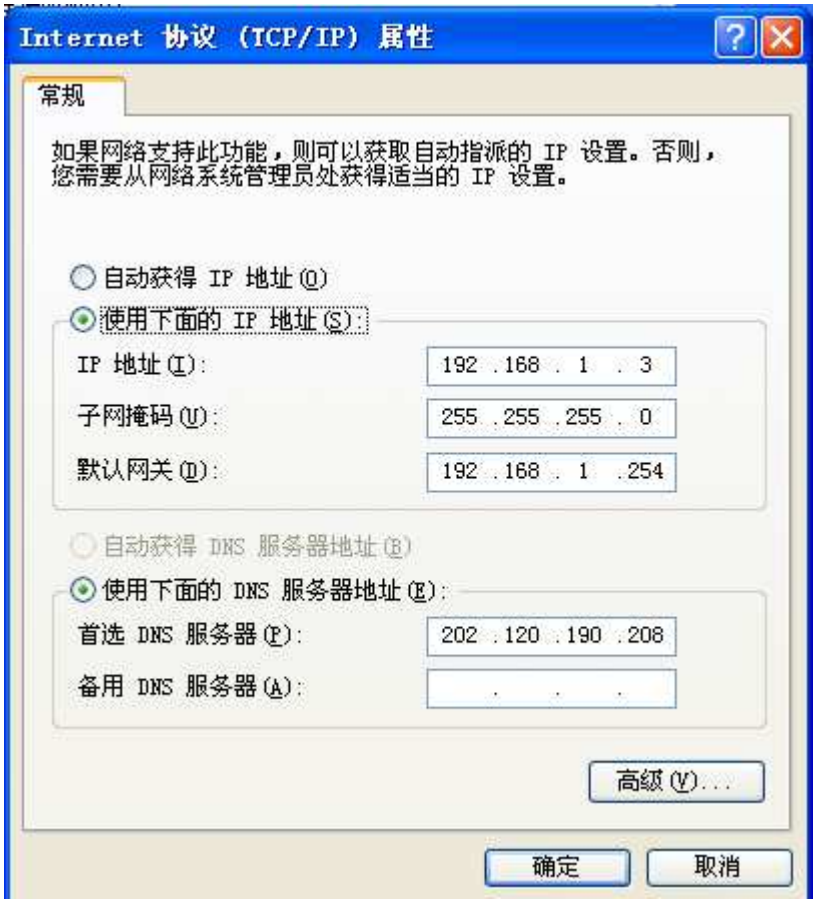
  （1） 单击 vmware 菜单“编辑”，选择“虚拟网络编制器”，在弹出界面中选择“vmnet0”，并单击“桥接模式”，在桥接到下拉框中选择第二块网卡“Realtek …”，如下图所示：

  （2） 选择“winxp 虚拟机”单击右键，选择设置，在弹出对话框中按下图进行设置；


虚拟机设置
硬件
选项
设备
摘要
内存
512 MB
处理器
1
硬盘(IDE)
40 GB
CD/DVD (IDE)
自动检测
网络适配器
桥接模式(自动)
USB 控制器
存在
声卡
自动检测
打印机
存在
显示器
自动检测
添加(A)...
移除(R)
设备状态
已连接(C)
启动时连接(O)
网络连接
桥接模式(B): 直接连接物理网络
复制物理网络连接状态(P)
NAT 模式(N): 用于共享主机的 IP 地址
仅主机模式(H): 与主机共享的专用网络
自定义(U): 特定虚拟网络
VMnet0 (桥接模式)
LAN 区段(L):
LAN 区段(S)...
高级(V)...
确定
取消
帮助


虚拟机设置
硬件
选项
设置
摘要
常规
Windows XP Professional
电源
共享文件夹
已启用
快照
自动保护
已禁用
客户机隔离
访问控制
未加密
VMware Tools
关闭时间同步
VNC 连接
已禁用
Unity
设备视图
自动登录
已禁用
高级
默认/默认
文件夹共享
共享文件夹会将您的文件显示给虚拟机中的程序。这可能为您的计算机和数据带来风险。请仅在您信任虚拟机使用您的数据时启用共享文件夹。
已禁用(D)
总是启用(E)
在下次关机或挂起前一直启用(U)
在 Windows 客户机中映射为网络驱动器(M)
文件夹(F)
名称
主机路径
入侵检...
C:\入侵检测与防御
添加(A)...
移除(R)
属性(P)
确定
取消
帮助

- 设置好后，启动 winxp，先把 xp 中的防火墙取消，如果 win10 中有防火墙都要取消掉，设置 xp 中的网卡并给网卡设置 ip 地址，地址和主机地址同一网段，dns、网关和主机一样，如下图：



在 xp 中现在能 ping 通主机、网关和被攻击机的 ip 地址了，且能上网，注意是在 xp 中按照 cain 软件。

- 在 xp 中安装 iis 并设置网站，在被攻击机中浏览网页选择 IE。其他步骤不变。

心得与体会