网络 ARP 攻击

应用场景

由于局域网的网络流通不是根据 IP 地址进行，而是按照 MAC 地址进行传输。所以，那个伪造出来的 MAC 地址在主机上被改变成一个不存在的 MAC 地址，这样就会造成网络不通这就是一个简单的 ARP 欺骗，在该 ARP 欺骗中，我们实施的过程包括包捕获，包修改，包植入三个阶段；通过该过程理解 ARP 欺骗的过程及原理。

实验目标

- 能够通过包编辑器构造虚假 ARP 数据包
- 能够向目标主机发起 ARP 欺骗攻击
- 了解 ARP 欺骗的原理
- 能够根据原理思考并设计实验内容

实验环境

Server：Windows Server 2003

Client：Windows XP

Iris

实验拓扑

VM Server　　VM Client

实验过程指导

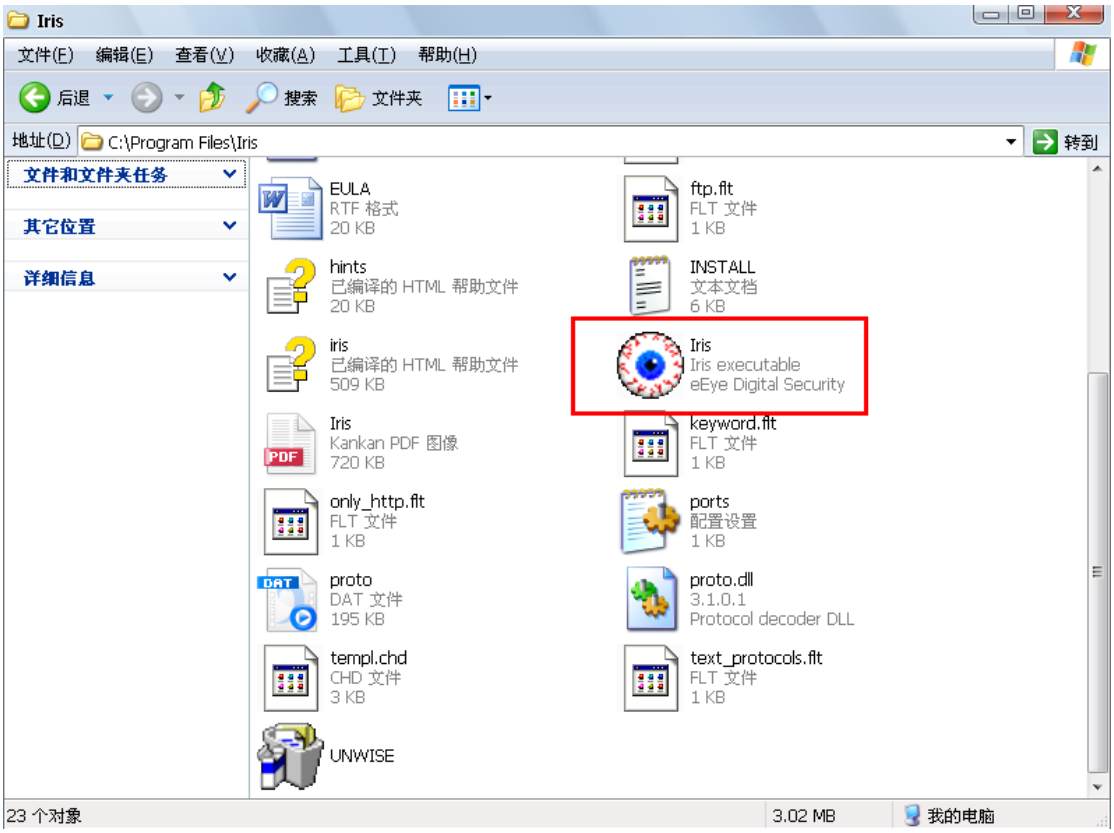
1　启动 Windows Server 2003 为服务器角色

2　在客户端通过 ping 命令对服务器 ip 进行检测

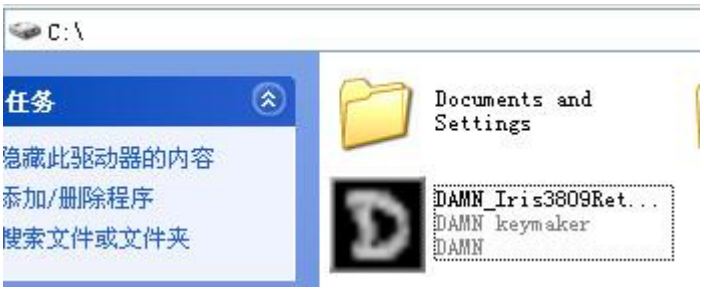
3　在客户端运行 arp　-a 查看 arp 缓存，获得服务器的 MAC 地址

```
C:\Documents and Settings\Administrator>arp -a

Interface: 10.1.1.99 --- 0x10003
  Internet Address      Physical Address      Type
  10.1.1.1              00-1a-a9-15-71-cf     dynamic
  10.1.1.90             00-16-76-1b-67-fb     dynamic

C:\Documents and Settings\Administrator>
```

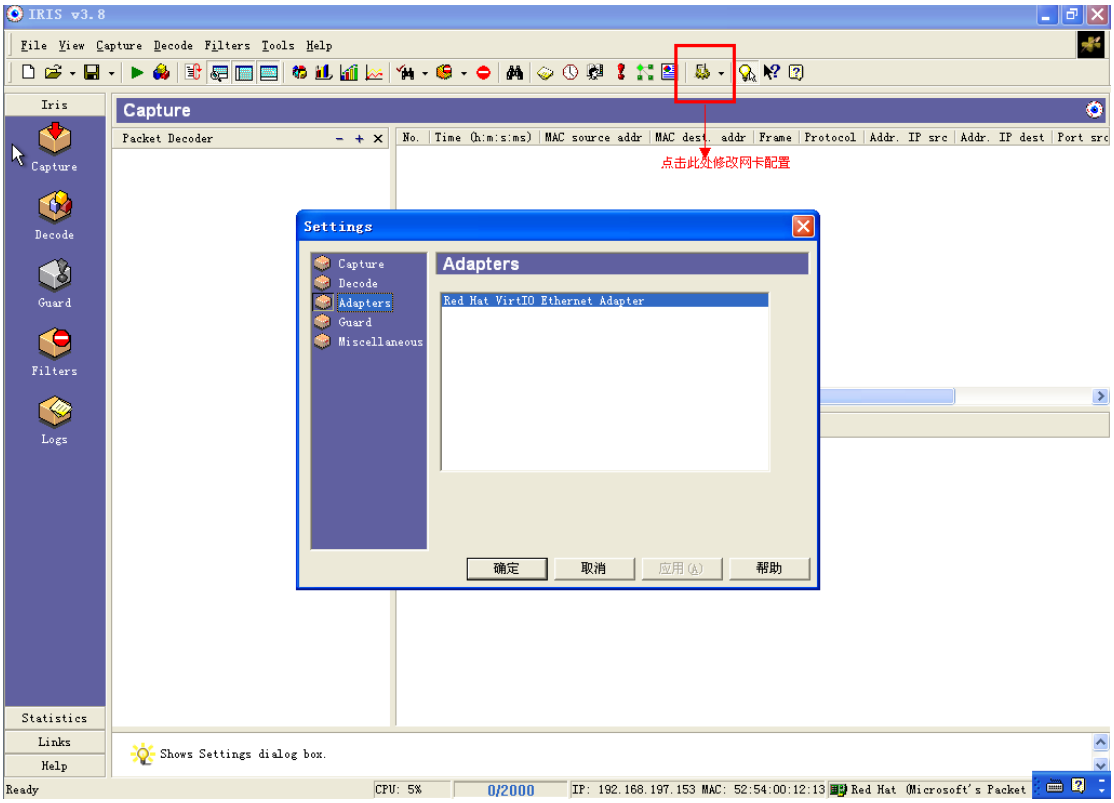
4　在客户端的 C:\Program Files\Iris 中启动 Iris，



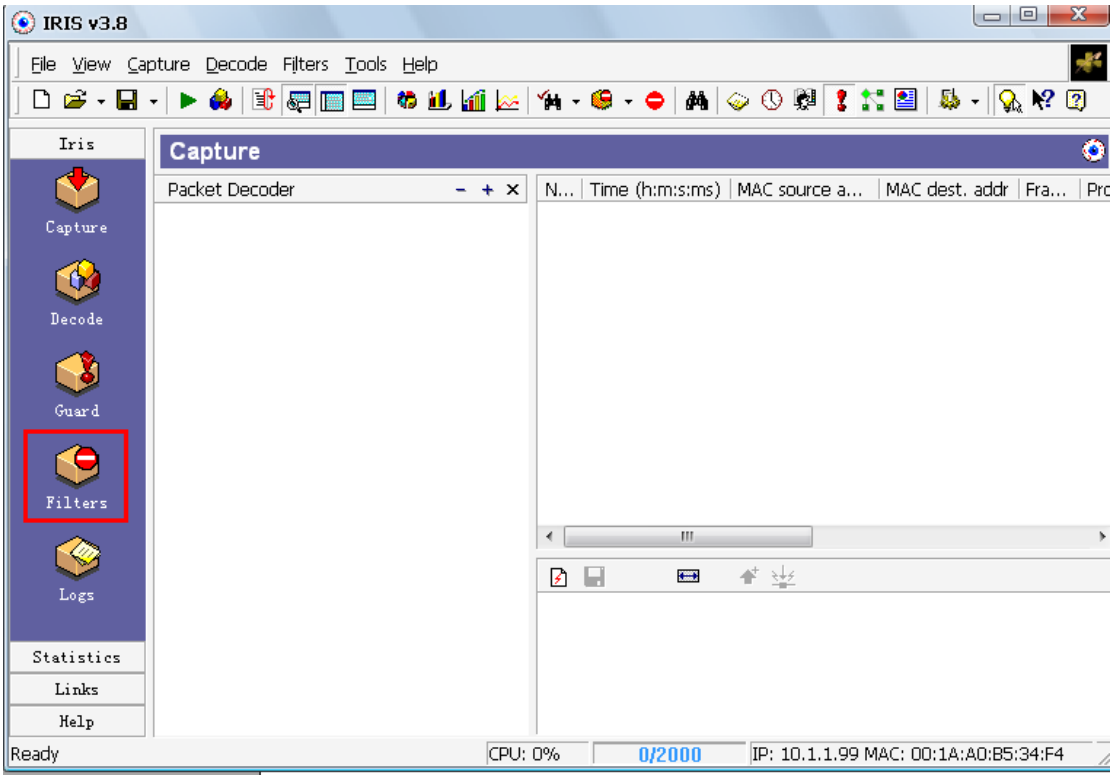
5　运行 DAMN_Iris3809 文件生成 Iris 所需要信息。



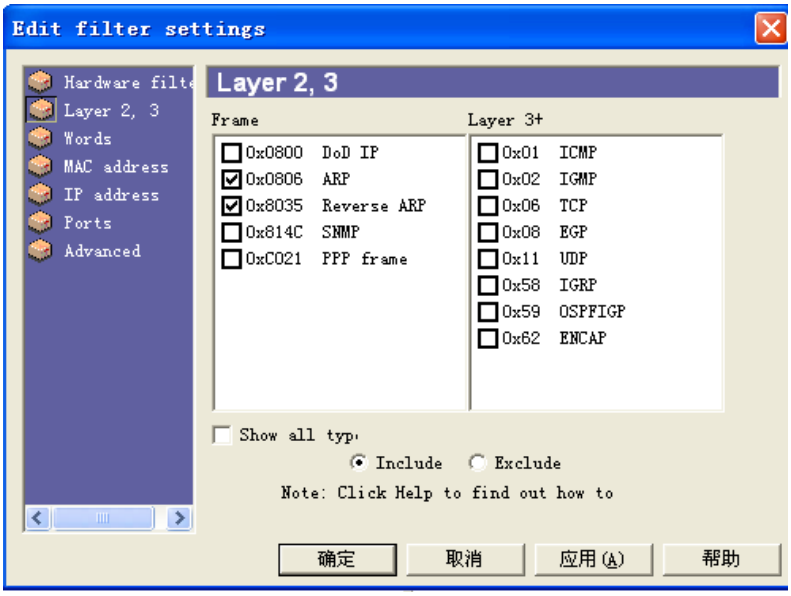
6　在 Iris 中进行网卡配置。选择左侧的 Adapters。在右侧选择要进行捕获的网卡。点击确定。



7 点击 Iris 左侧的 Filters 设置过滤器



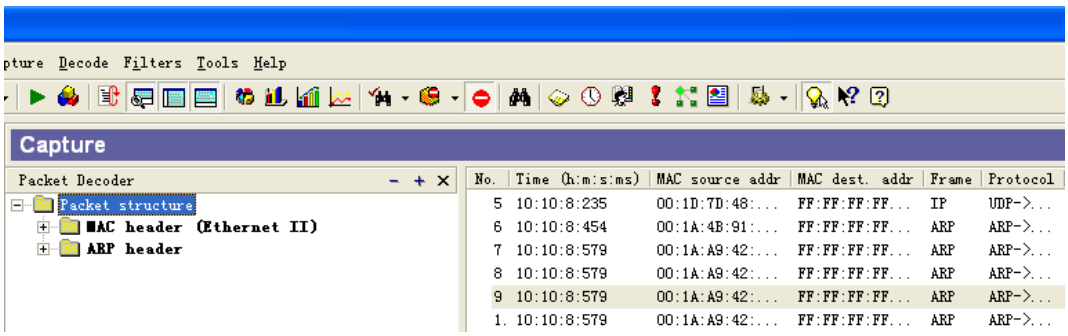
8 选择 ARP 和反向 ARP，从而对网络中的 ARP 数据包进行监听



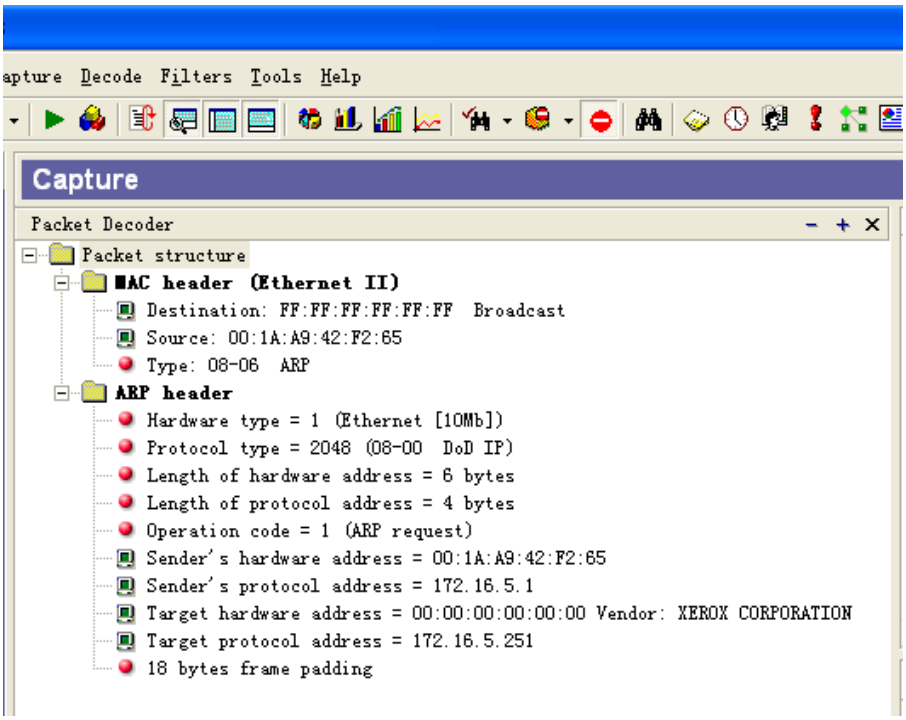
9 确定之后点击开始，开始捕获网络中的数据包

10 禁用服务器端网卡。再启用服务器端网卡。使之产生 ARP 报文。

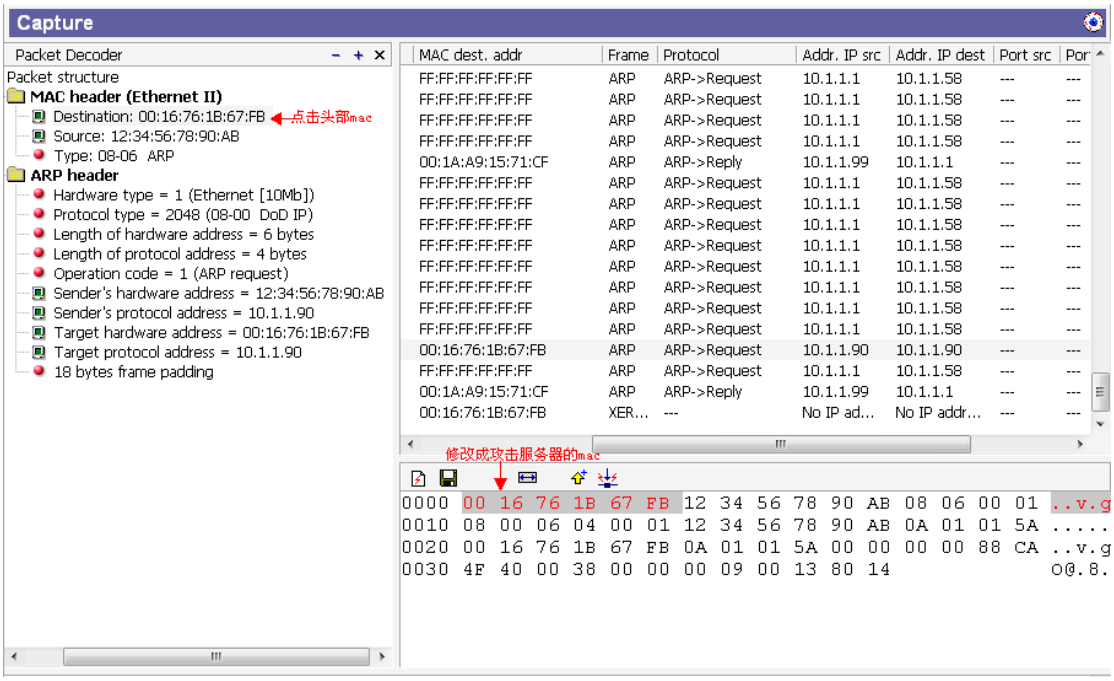
会捕获到网卡状态变化引起的 arp 消息



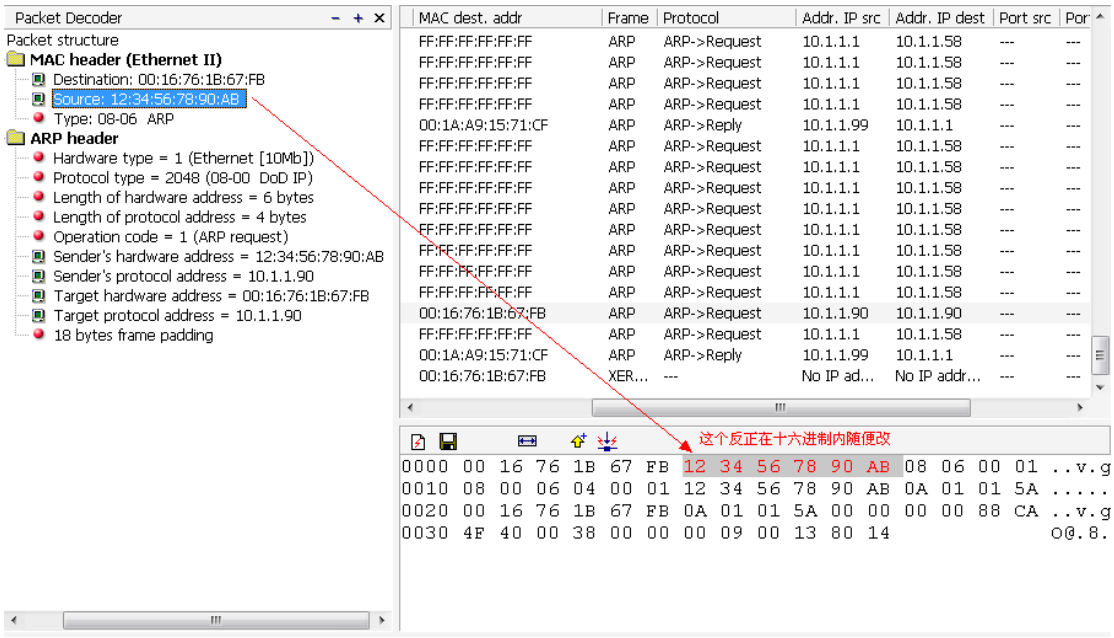
11 在其中随意选择右边一个 ARP 请求的数据包，在左侧的包编辑器中打开展开细项。



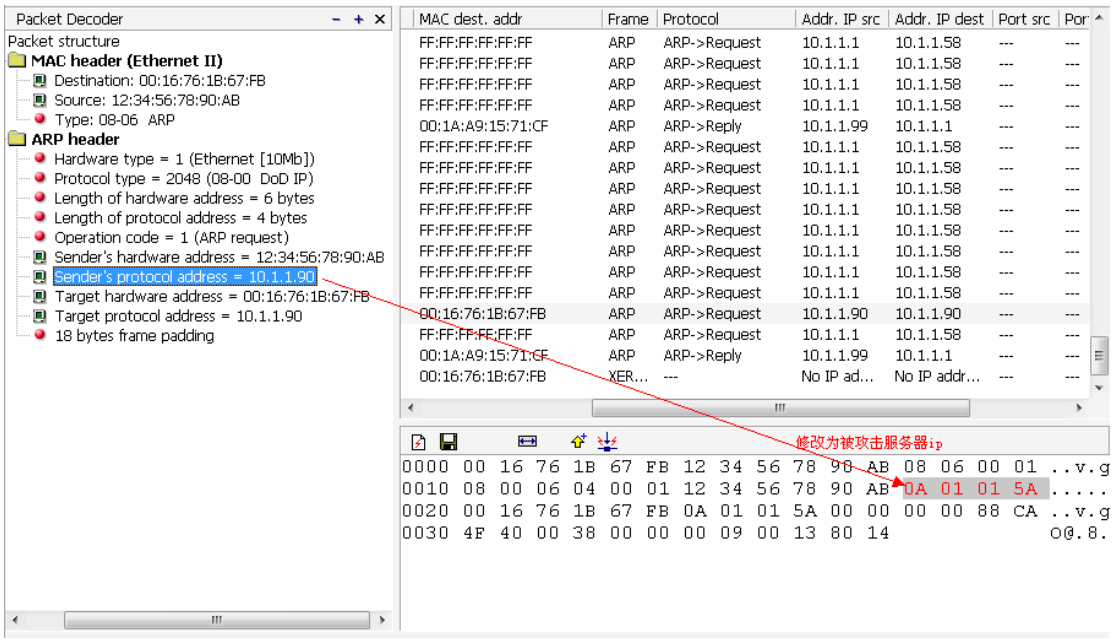
12 点击 MAC 头中的 Destination 选项，将该数据包 MAC 头信息中目的 MAC 改为欲攻击服务器的 MAC（服务器 MAC 地址通过在客户端运行 arp –a 查看）



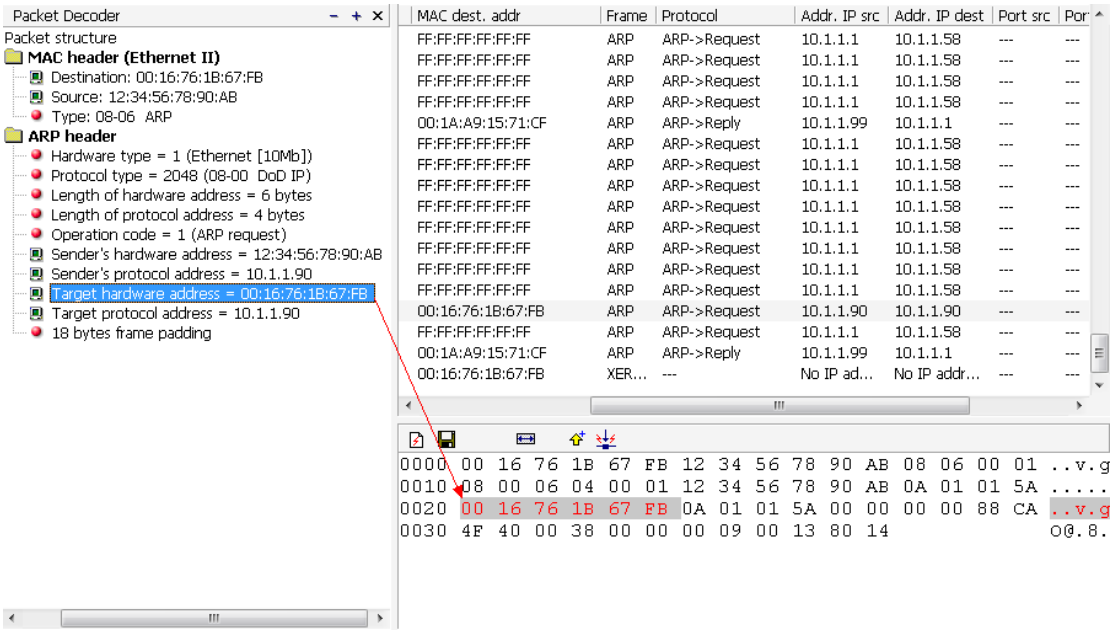
13 并且将 ARP 头部的发送 MAC 修改为虚假 MAC（虚假 MAC 随意指定，建议改变真 MAC 的后两位），

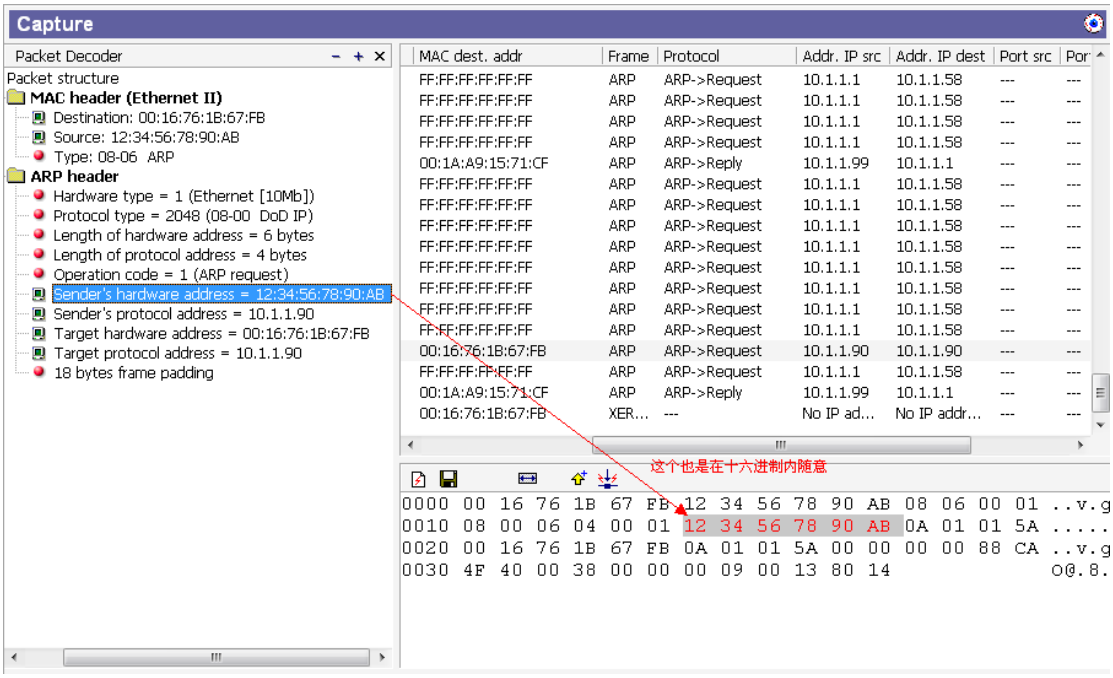


14 发送 IP 与欲攻击的服务器 IP 一致（这里服务器 ip 是 10.1.1.90）

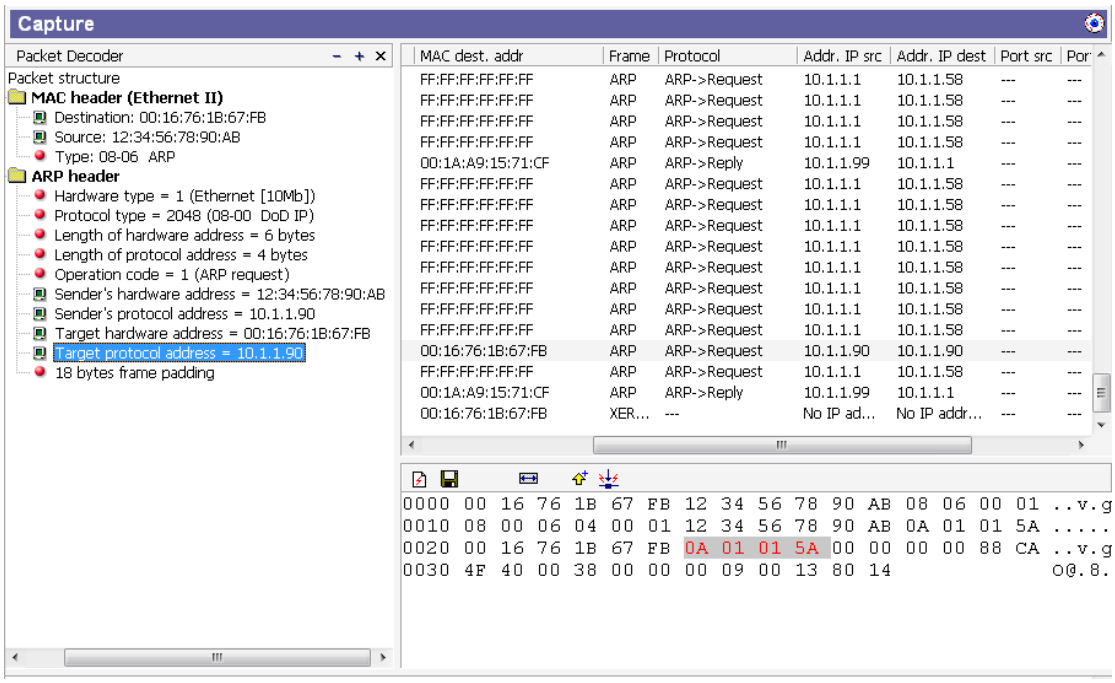


15 目标 MAC 和目标 MAC 需要按被攻击的服务器进行设定。

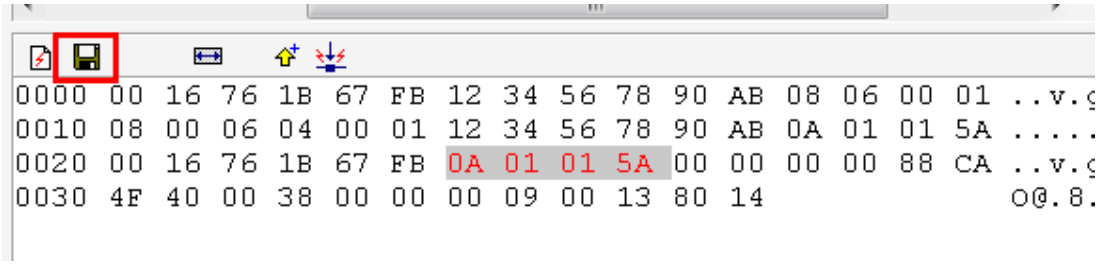


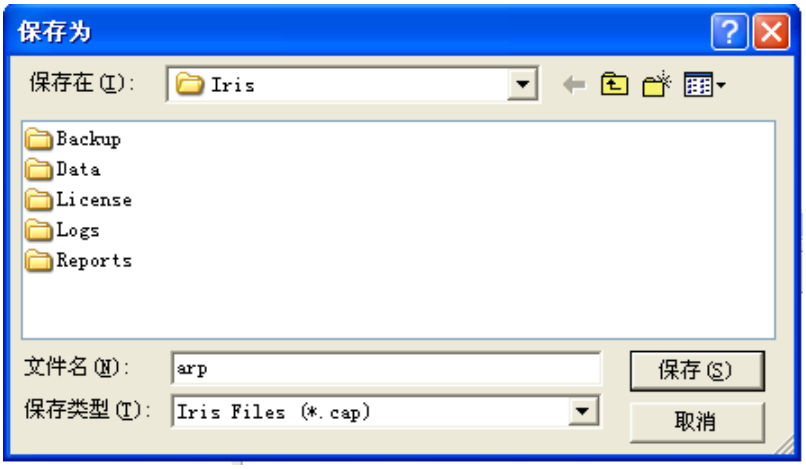


16 目标地址改为被攻击服务端的 mac。目标 ip 改成被攻击服务端 ip 地址

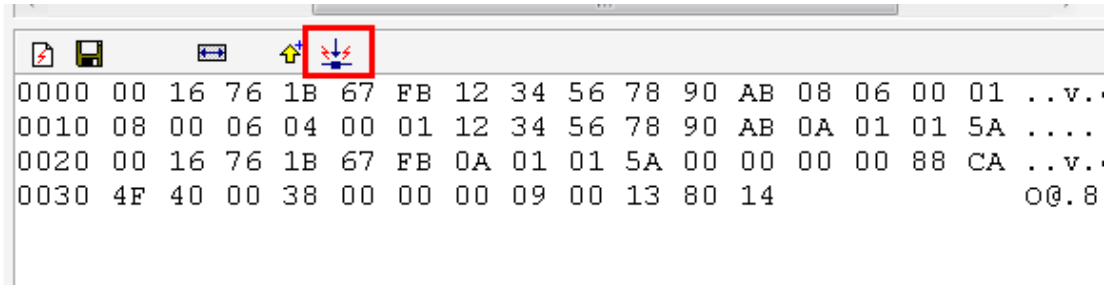


17 设定后，将该数据包保存

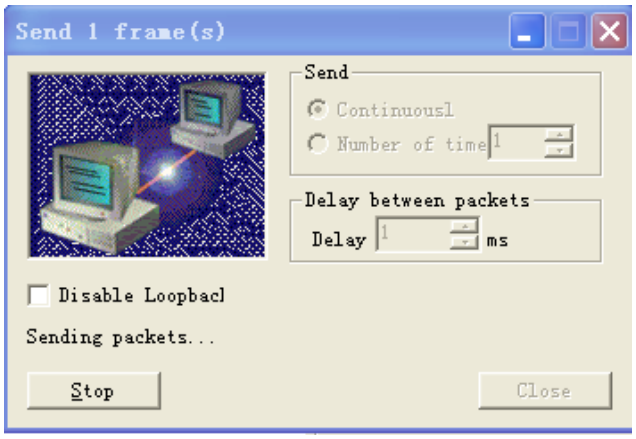




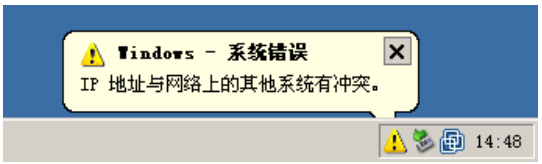
18 在网络上连续不断发送此数据包



19 如下图所示选择持续发送。



20 服务端报错，并且该对话框不间断弹出，该无法无法正常提供服务。



总结：

我们捕获到的任一个 ARP 数据包，将其目标 MAC、目标 IP、原 IP 都改为要攻击的主机地址。将原 MAC 随意填写。会导致收到这个数据包的主机认为网络上有别人跟他使用相同的 IP。从而导致冲突并无法正常访问网络。

试思考，如果将攻击目标改为网内的交换机。攻击内容为将网关或代理服务器的地址替换成自己的地址进行欺骗。则网内的 DNS 及到外网的服务访问都会出现中断的情况。因为所有的到外网的数据都流向了攻击机。