盗用失败：而且由于网卡MAC地址的唯一确定性，可以根据MAC地址查出使用该MAC地址的网卡，进而查出非法盗用者。 目前，很多单位的内部网络，尤其是学校校园网都采用了MAC地址与IP地址的绑定技术。许多防火墙（硬件防火墙和软件防火墙）为了防止网络内部的IP地址被盗用，也都内置了MAC地址与IP地址的绑定功能。 从表面上看来，绑定MAC地址和IP地址可以防止内部IP地址被盗用，但实际上由于各层协议以及网卡驱动等实现技术，MAC地址与IP地址的绑定存在很大的缺陷，并不能真正防止内部IP地址被盗用。 2 破解MAC与IP地址绑定策略 2.1 IP地址和MAC地址简介 现行的TCP/IP网络是一个四层协议结构，从下往上依次为链路层、网络层、传输层和应用层。 Ethernet协议是链路层协议，使用的地址是MAC地址。MAC地址是Ethernet网卡在Ethernet中的硬件标志，网卡生产时将其存于网卡的EEPROM中。网卡的MAC地址各不相同，MAC地址可以唯一标志一块网卡。在Ethernet上传输的每个报文都含有发送该报文的网卡的MAC地址。 Ethernet根据Ethernet报文头中的源MAC地址和目的MAC来识别报文的发送端和接收端。IP协议应用于网络层，使用的地址为IP地址。使用IP协议进行通讯，每个IP报文头中必须含有源IP和目的IP地址，用以标志该IP报文的发送端和接收端。在Ethernet上使用IP协议传输报文时，IP报文作为Ethernet报文的数据。IP地址对于Ethernet交换机或处理器是透明的。用户可以根据实际网络的需要为网卡配置一个或多个IP地址。MAC地址和IP地址之间并不存在一一对应的关系。 MAC地址存储在网卡的EEPROM中并且唯一确定，但网卡驱动在发送Ethernet报文时，并不从EEPROM

中读取MAC地址，而是在内存中来建立一块缓存区，Ethernet报文从中读取源MAC地址。而且，用户可以通过操作系统修改实际发送的Ethernet报文中的源MAC地址。既然MAC地址可以修改，那么MAC地址与IP地址的绑定也就失去了它原有的意义。 2.2 破解方案 下图是破解试验的结构示意图。其内部服务器和外部服务器都提供Web服务，防火墙中实现了MAC地址和IP地址的绑定。报文中的源MAC地址与1P地址对如果无法与防火墙中设置的MAC地址与1P地址对匹配，将无法通过防火墙。主机2和内部服务器都是内部网络中的合法机器；主机1是为了做实验而新加入的机器。安装的操作系统是W2000企业版，网卡是3Com的。 试验需要修改主机1中网卡的MAC和IP地址为被盗用设备的MAC和IP地址。首先，在控制面板中选择“ 网络和拨号连接 ”，选中对应的网卡并点击鼠标右键，选择属性，在属性页的“ 常规 ”页中点击“ 配置 ”按钮。在配置属性页中选择“ 高级 ”，再在“ 属性 ”栏中选择“ Network Address ”，在“ 值 ”栏中选中输人框，然后在输人框中输人被盗用设备的MAC地址，MAC地址就修改成功了。 然后再将IP地址配置成被盗用设备的IP地址。盗用内部客户机IP地址：将主机1的MAC地址和IP地址分别修改为主机2的MAC地址和IP地址。主机1可以访问外部服务器，能够顺利地通过防火墙，访问权限与主机2没有分别。而且，与此同时主机2也可以正常地访问外部服务器，完全不受主机1的影响。无论是主机2还是防火墙都察觉不到主机1的存在。主机1 