反击ARP欺骗，我和网络执法官的战斗 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/255/2021_2022__E5_8F_8D_E5_87_BBARP_E6_c67_255814.htm 作为一名校园网管理员，笔者近期接二连三地接到用户不能正常上网的举报，使得我们焦头烂额。经过进一步调查，终于发现了故障的真相。 首先说明一下我校的网络拓扑结构：在一台三层主交换机上划分了VLAN，VLAN1使用普通的二层交换机，连接学生宿舍的网络。使用192.168.0.0作为网络地址，并在主交换机上做了MAC地址与IP地址的绑定，避免学生自行修改IP地址造成地址冲突。学生的计算机全部连接到普通的二层交换机上。 故障现象 某台计算机会突然不能连接到服务器或其他客户机，重启后恢复正常，短时间后，又出现该状况。查看本地连接状态发现只有发出的数据包而没有返回的数据包。根据以往的经验，该症状与MAC地址绑定错误相同，于是在交换机上查看，发现一切正常，只是该IP地址没有数据流量。同时，在网络中的网管软件监听到大量未知MAC地址的数据包出现。 故障分析 综合考虑，我们认为有伪造MAC地址的情况出现。我们重点查找Windows系统下的嗅探软件，并以著名的Winpcap和Libpcap为重点，最终的焦点定位在一款叫做“网络执法官”的软件上。 我们立即下载该软件进行安装，发现其基于Winpcap。因为Winpcap的资料相对较多，我们没有试图对该软件进行反编译，而只对其基本功能进行了测试，发现其工作方式有三种，并进行了基本测试： 1. 生成IP地址冲突 在该模式下，软件产生一个虚拟的MAC地址，并利用这个MAC地址伪造和被攻击机器的IP地址相同的数据包，从

而使被攻击机器不断出现IP地址冲突对话框，但由于该MAC地址是伪造的，所以被攻击机器无法发现是哪个机器进行了攻击。 2. 断开被攻击机器与网关的联系 在该模式下，软件对被攻击机和网关机都产生一个ARP的“ 欺骗 ”，使得两者不能正确获知对方的MAC地址，从而不能正常通讯。但被攻击机器和局域网内其他主机可以进行通讯。 3. 断开被攻击机器与所有其他主机的联系 在该模式下，软件对被攻击机器和局域网内所有主机（包括网关）都进行“ ARP欺骗 ”，被攻击机器不能和任何机器通讯。但本主机不能和被攻击机断开联系（该软件不会欺骗本身主机），所以如果该软件如果安装在网关机上，就失去了网络管理功能。 明显的，这是一种“ ARP欺骗 ”的攻击。而ARP协议位于TCP/IP协议中的网络层，主要功能是将广域网的IP地址寻址转换成局域网中的MAC地址寻址。所以，如果我们破坏了IP/MAC地址的转换，被攻击的主机就不能在局域网中进行通讯了（因为没有其他主机“ 认识 ”它了）。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com