 arp病毒攻击后的影响 有时，局域网内大家突然都不可以上网，使用抓包工具可以发现有个别机器在不停的发送arp广播包。这种情况一般都是内网的某台机器中了arp病毒，然后这台机器便不断的发送欺骗包给所有机器来冒充网关，这样其他机器就会把这个中毒的机器当作网关而把数据包发给它，而它在接到数据包后又没有转发数据包到真正的网关去，所以造成大家都无法上网。 一般的，arp病毒使用欺骗的手段是为了窃听内网中所有的通信数据以达到它的某种目的。 由于一般的arp病毒在发送欺骗包时会修改自身的mac地址，这使我们在快速排查中毒机器有一定困难。但这可以通过mac与ip绑定的方式解决，即所有内网机器的ip都通与mac绑定的方式分配，这样所有未登记的不合法mac就无法连接到内网了。 如果局域网内已经有网关欺骗而导致无法上网时，我们还可以通过在本机上绑定网关的mac地址和ip来解决欺骗问题。但此步需要一个条件，即你要知道真实的网关ip和mac地址。操作如下： 防范arp病毒攻击方法一：(此方法对linux和windows都适用) 1，列出局域网内所有机器的mac地址,如果此步列出的路由表中网关ip 和网关mac地址与真实不符，就也证明你已经被网关欺骗了。 arp -a 2，绑定mac地址 arp -s 192.168.1.1 00:07:E9:xx:xx:xx 注意：这里192.168.1.1有可能有换成hostname，假如你的网关设置了hostname的话。 防范arp病毒攻击方法二：(适用于linux) 1，创建一个/etc/ethers文件，比如你要绑定网关，那就

在/etc/ethers里写上： 192.168.1.1 00:07:E9:xx:xx:xx 然后执行 arp -f 操作完成你可以使用arp -a查看当前的arp缓存表，如果列表显示正确，那么你的绑定操作已成功，如果还有绑定其它机器的话，比如ftp等，那就继续添加记录。 说明：此处的192.168.1.1为你的网关地址，00:07:E9:xx:xx:xx为你的网关mac地址。 注意：Linux和Widows上的MAC地址格式不同。Linux表示为：AA:AA:AA:AA:AA:AA，Windows表示为：AA-AA-AA-AA-AA-AA。 注意：每次重启机器后需要重新绑定mac地址，你可以写一个自动脚本后加到自启动项目中。另外，mac地址的绑定需要双向的，即机器a绑定了机器b，机器b也要绑定机器a，这样防范arp病毒攻击才会有效。 防范arp病毒攻击的方法有很多，本文知识介绍了比较实用的两种，而且是针对linux和windows两种不同系统的办法，所以使用时一定要看清系统，对症下药。 百考试题温馨提示：本内容来源于网络，仅代表作者个人观点，与本站立场无关，仅供您学习交流使用。其中可能有部分文章经过多次转载而造成文章内容缺失、错误或文章作者不详等问题，请您谅解。如有侵犯您的权利，请联系我们，本站会立即予以处理。 编辑特别推荐: #0000ff>如何选购Linux可以搭配的机器之RAM考量 #0000ff>linuxln命令详解 #0000ff>nginx关于服务静态文件的配置 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