巧妙利用Linux系统IP伪装抵住黑客攻击 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/144/2021_2022__E5_B7_A7_E5_A6_99_E5_88_A9_E7_c103_144322.htm 防火墙可分为几种不同的安全等级。在Linux中，由于有许多不同的防火墙软件可供选择，安全性可低可高，最复杂的软件可提供几乎无法渗透的保护能力。不过，Linux核心本身内建了一种称作“ 伪装 ”的简单机制，除了最专门的黑客攻击外，可以抵挡住绝大部分的攻击行动。 当我们拨号接连上Internet后，我们的计算机会被赋给一个IP地址，可让网上的其他人回传资料到我们的计算机。黑客就是用你的IP来存取你计算机上的资料。Linux所用的“ IP伪装 ”法，就是把你的IP藏起来，不让网络上的其他人看到。有几组IP地址是特别保留给本地网络使用的，Internet骨干路由器并不能识别。像作者计算机的IP是192.168.1.127，但如果你把这个地址输入到你的浏览器中，相信什么也收不到，这是因为Internet骨干是不认得192.168.X.X这组IP的。在其他Intranet上有数不清的计算机，也是用同样的IP，由于你根本不能存取，当然不能侵入或破解了。 那么，解决Internet上的安全问题，看来似乎是一件简单的事，只要为你的计算机选一个别人无法存取的IP地址，就什么都解决了。错！因为当你浏览Internet时，同样也需要服务器将资料回传给你，否则你在屏幕上什么也看不到，而服务器只能将资料回传给在Internet骨干上登记的合法IP地址。“ IP伪装 ”就是用来解决此两难困境的技术。当你有一部安装Linux的计算机，设定要使用“ IP伪装 ”时，它会将内部与外部两个网络桥接起来，并自动解译由内往外或由外至

内的IP地址，通常这个动作称为网络地址转换。 实际上的"IP伪装"要比上述的还要复杂一些。基本上，“ IP伪装 ”服务器架设在两个网络之间。如果你用模拟的拨号调制解调器来存取Internet上的资料，这便是其中一个网络；你的内部网络通常会对应到一张以太网卡，这就是第二个网络。若你使用的是DSL调制解调器或缆线调制解调器(Cable Modem)，那么系统中将会有第二张以太网卡，代替了模拟调制解调器。
而Linux可以管理这些网络的每一个IP地址，因此，如果你有一部安装Windows的计算机（IP为192.168.1.25），位于第二个网络上（Ethernet eth1）的话，要存取位于Internet（Ethernet eth0）上的缆线调制解调器（207.176.253.15）时，Linux的“ IP伪装 ”就会拦截从你的浏览器所发出的所有TCP/IP封包，抽出原本的本地地址（192.168.1.25），再以真实地址（207.176.253.15）取代。接着，当服务器回传资料到207.176.253.15时，Linux也会自动拦截回传封包，并填回正确的本地地址（192.168.1.25）。 Linux可管理数台本地计算机（如Linux的“ IP伪装 ”示意图中的192.168.1.25与192.168.1.34），并处理每一个封包，而不致发生混淆。作者有一部安装SlackWare Linux的老486计算机，可同时处理由四部计算机送往缆线调制解调器的封包，而且速度不减少。 在第二版核心前，“ IP伪装 ”是以IP发送管理模块（IPFWADM，IP fw adm）来管理。第二版核心虽然提供了更快、也更复杂的IPCHAINS，但仍旧提供了IPFWADM wrapper来保持向下兼容性，因此，作者在本文中会以IPFWADM为例，来解说如何设定“ IP伪装 ”（您可至http：//metalab.unc.edu/mdw/HOWTO/IPCHAINS－HOWTO.html

查询使用IPCHAINS的方法，该页并有“IP伪装”更详尽的说明）。另外，某些应用程序如RealAudio与CU－SeeME所用的非标准封包，则需要特殊的模块，您同样可从上述网站得到相关信息。作者的服务器有两张以太网卡，在核心激活过程中，分别被设定在eth0与eth1。这两张卡均为SN2000式无跳脚的ISA适配卡，而且绝大多数的Linux都认得这两张卡。作者的以太网络初始化步骤在rc.inet1中设定，指令如下：
IPADDR="207.175.253.15" ＃换成您缆线调制解调器的IP地址。 NETMASK="255.255.255.0" ＃换成您的网络屏蔽。
NETWORK="207.175.253.0" ＃换成您的网络地址。
BROADCAST="207.175.253.255" ＃换成您的广播地址。
GATEWAY="207.175.253.254" ＃换成您的网关地址。 ＃用以上的宏来设定您的缆线调制解调器以太网卡 /sbin/ifconfig eth0 ＄{IPADDR} broadcast ＄ {BROADCAST} netmask ＄{NETMASK} ＃设定IP路由表 /sbin/route add －net ＄{NETWORK} netmask ＄ {NETMASK} eth0 ＃设定intranet以太网络卡eth1，不使用宏指令 /sbin/ifconfig eth1 192.168.1.254 broadcast 192.168.1.255 netmask 255.255.255.0 /sbin/route add －net 192.168.1.0 netmask 255.255.255.0 eth1 ＃接着设定IP fw adm初始化 /sbin/ipfwadm －F －p deny ＃拒绝以下位置之外的存取 ＃打开来自192.168.1.X的传送需求 /sbin/ipfwadm －F －a m －S 192.168.1.0/24 －D 0.0.0.0/0 /sbin/ipfwadm －M －s 600 30 120 就是这样！您系统的"IP伪装"现在应该可以正常工作了。如果您想得到更详细的信息，可以参考上面所提到的HOWTO，或是至http：//albali.aquanet.com.br/howtos/Bridge＋Firewall－4.html参考MINI HOWTO。另外关于安全性更高

的防火墙技术，则可在ftp
：//sunsite.unc.edu/pub/Linux/docs/HOWTO/Firewall
－HOWTO中找到资料。 半年来，56K模拟数据卡的价格突然跌降了不少。不过，大多数新的数据卡，其实是拿掉了板子上的控制用微处理器，因此会对系统的主CPU造成额外的负荷，而Linux并不支持这些“ WinModem ”卡。虽然Linux核心高手们，还是有能力为WinModem卡撰写驱动程序，但他们也很明白，为了省10元美金而对系统效能造成影响，绝对不是明智之举。 请确定您所使用的Modem卡，有跳脚可用来设定COM1、COM2、COM3与COM4，如此一来，这些数据卡才可在Linux下正常工作。您可在http：//www.o2.net/～gromitkc/winmodem.html中找到与Linux兼容的数据卡的完整列表。 当作者在撰写本篇文章时，曾花了点时间测试各种不同的数据卡。Linux支持即插即用装置，所以我买了一块由Amjet生产的无跳脚数据卡，才又发现另一个令人困扰的问题。 作者测试用的PC是一部老旧的486，用的是1994年版的AMI BIOS。在插上这块即插即用数据卡后，计算机便无法开机了，画面上出现的是“ 主硬盘发生故障 ”（Primary hard disk failure）。经检查，发现即插即用的BIOS居然将原应保留给硬盘控制器的15号中断，配给了数据卡。最后作者放弃了在旧计算机上使用即插即用产品，因为不值得为这些事花时间。所以，请您注意在购买数据卡之前，先看清楚是否有调整COM1到COM4的跳脚。 在作者的布告板（http
：//trevormarshall.com/BYTE/）上，看到有几位朋友询问是否可以用多条拨号线来改善Internet的上网速度。这里最好的例子是128K ISDN，它同时运用两条56K通道，以达到128K的速

度。当ISP提供这样的服务时，其实会配置两条独立的线路连到同一个IP上。 您可以看到，虽然Linux上有EQL这类模块，可让您在计算机上同时使用两块数据卡，但除非ISP对两组拨号连线提供同一个IP，否则这两块数据卡也只是对送出资料有帮助而已。 如果您拨接的是一般的ISP PPP线路，那么您会得到一个IP地址，从服务器回传的封包才能在数百万台计算机中找到您；而您每次拨入ISP时，都会得到一个不同的IP地址。 你的浏览器所送出的封包中，也包含供服务器资料回传的本地IP地址。EQL可将这些外传的封包，分散到不同的ISP线路上，但当资料回传时，却只能通过一个IP地址接收，也就是浏览器认为正在使用的那个地址。若是使用ISDN，那么ISP会处理这个问题；一些ISP会为多组线路的拨号接入提供相应的IP地址，但价钱非常昂贵。 在追求速度时，请别忽略了Linux防火墙的效率。在作者办公室有六位使用者通过“ IP伪装 ”防火墙，去存取一部56K模拟调制解调器，工作情况十分良好，只有在有人下载大文件时速度才会变慢。在您决定要加装多条ISP拨号线之前，可以先架设一部"IP伪装"服务器试试。Windows处理多重IP的方式并非十分有效率，而将Windows网络与调制解调器隔开，效能的增进将会让您惊讶不已。 简而言之，Linux所用的“ IP伪装 ”法，就是把你的IP藏起来，不让网络上的其他人看到。 