Linux用防火墙伪装抵挡黑客攻击（1） PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/462/2021_2022_Linux_E7_94_A8_E9_98_c103_462215.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，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）。 100Test 下载频道开通，各类考试题目直接下载。详细请