网络安全与端口攻略的详细解读七 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/140/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c100_140267.htm 1080 SOCKS 这一协议以管道方式穿过防火墙，允许防火墙后面的许多人通过一个IP地址访问Internet。理论上它应该只允许内部的通信向外达到Internet。但是由于错误的配置，它会允许Hacker/Cracker的位于防火墙外部的攻击穿过防火墙。或者简单地回应位于Internet上的计算机，从而掩饰他们对你的直接攻击。WinGate是一种常见的Windows个人防火墙，常会发生上述的错误配置。在加入IRC聊天室时常会看到这种情况。 1114 SQL 系统本身很少扫描这个端口，但常常是sscan脚本的一部分。 1243 Sub-7木马（TCP） 1524 ingreslock 后门许多攻击脚本将安装一个后门Shell于这个端口（尤其是那些针对Sun系统中sendmail和RPC服务漏洞的脚本，如statd, ttdbserver和cmsd）。如果你刚刚安装了你的防火墙就看到在这个端口上的连接企图，很可能是上述原因。你可以试试Telnet到你的机器上的这个端口，看看它是否会给你一个Shell。连接到600/pcserver也存在这个问题。 2049 NFS NFS程序常运行于这个端口。通常需要访问portmapper查询这个服务运行于哪个端口，但是大部分情况是安装后NFS运行于这个端口，Hacker/Cracker因而可以闭开portmapper直接测试这个端口。 3128 squid 这是Squid HTTP代理服务器的默认端口。攻击者扫描这个端口是为了搜寻一个代理服务器而匿名访问Internet。你也会看到搜索其它代理服务器的端口：8000/8001/8080/8888。扫描这一端口的另一原因是：用户正在进入聊天室。其它用户（或服

务器本身）也会检验这个端口以确定用户的机器是否支持代理。 5632 pcAnywere 你会看到很多这个端口的扫描，这依赖于你所在的位置。当用户打开pcAnywere时，它会自动扫描局域网C类网以寻找可能得代理（译者：指agent而不是proxy）。Hacker/cracker也会寻找开放这种服务的机器，所以应该查看这种扫描的源地址。一些搜寻pcAnywere的扫描常包含端口22的UDP数据包。 6776 Sub-7 artifact 这个端口是从Sub-7主端口分离出来的用于传送数据的端口。例如当控制者通过电话线控制另一台机器，而被控机器挂断时你将会看到这种情况。因此当另一人以此IP拨入时，他们将会看到持续的，在这个端口的连接企图。（译者：即看到防火墙报告这一端口的连接企图时，并不表示你已被Sub-7控制。） 6970 RealAudio RealAudio客户将从服务器的6970-7170的UDP端口接收音频数据流。这是由TCP7070端口外向控制连接设置的。 13223 PowWow PowWow 是Tribal Voice的聊天程序。它允许用户在此端口打开私人聊天的连接。这一程序对于建立连接非常具有“ 进攻性 ”。它会“ 驻扎 ”在这一TCP端口等待回应。这造成类似心跳间隔的连接企图。如果你是一个拨号用户，从另一个聊天者手中“ 继承 ”了IP地址这种情况就会发生：好象很多不同的人在测试这一端口。这一协议使用“ OPNG ”作为其连接企图的前四个字节。 17027 Conducent 这是一个外向连接。这是由于公司内部有人安装了带有Conducent "adbot" 的共享软件。Conducent "adbot"是为共享软件显示广告服务的。使用这种服务的一种流行的软件是Pkware。有人试验：阻断这一外向连接不会有任何问题，但是封掉IP地址本身将会导致adbots持续在每秒内试图连接多

次而导致连接过载： 机器会不断试图解析DNS名ads.conducent.com，即IP地址216.33.210.40 ；216.33.199.77 ；216.33.199.80；216.33.199.81；216.33.210.41。（译者：不知NetAnts使用的Radiate是否也有这种现象） 27374 Sub-7木马(TCP) 30100 NetSphere木马(TCP) 通常这一端口的扫描是为了寻找中了NetSphere木马。 31337 Back Orifice “ elite ” Hacker中31337读做 “ elite ” /ei ’ li:t/（译者：法语，译为中坚力量，精华。即3=E, 1=L, 7=T）。因此许多后门程序运行于这一端口。其中最有名的是Back Orifice。曾经一段时间内这是Internet上最常见的扫描。现在它的流行越来越少，其它的木马程序越来越流行。 31789 Hack-a-tack 这一端口的UDP通讯通常是由于"Hack-a-tack"远程访问木马（RAT, Remote Access Trojan）。这种木马包含内置的31790端口扫描器，因此任何31789端口到317890端口的连接意味着已经有这种入侵。（31789端口是控制连接，317890端口是文件传输连接） 32770~32900 RPC服务 Sun Solaris的RPC服务在这一范围内。详细的说：早期版本的Solaris（2.5.1之前）将portmapper置于这一范围内，即使低端口被防火墙封闭仍然允许Hacker/cracker访问这一端口。扫描这一范围内的端口不是为了寻找portmapper，就是为了寻找可被攻击的已知的RPC服务。 33434~33600 traceroute 如果你看到这一端口范围内的UDP数据包（且只在此范围之内）则可能是由于traceroute 