端口：1

服务：tcpmux

说明：这显示有人在寻找sgi irix机器。irix是实现tcpmux的主要提供者，默认情况下tcpmux在这种系统中被打开。irix机器在发布是含有几个默认的无密码的帐户，如：ip、guest uucp、nuucp、demos 、tutor、diag、outofbox等。许多管理员在安装后忘记删除这些帐户。因此hacker在internet上搜索tcpmux并利用这些帐户。

端口：7

服务：echo

说明：能看到许多人搜索fraggle放大器时，发送到x.x.x.0和x.x.x.255的信息。

端口：19

服务：character generator

说明：这是一种仅仅发送字符的服务。udp版本将会在收到udp包后回应含有\*\*字符的包。tcp连接时会发送含有\*\*字符的数据流直到连接关闭。hacker利用ip欺骗可以发动dos攻击。伪造两个chargen服务器之间的udp包。同样fraggle dos攻击向目标地址的这个端口广播一个带有伪造受害者ip的数据包，受害者为了回应这些数据而过载。

端口：21

服务：ftp

说明：ftp服务器所开放的端口，用于上传、下载。最常见的攻击者用于寻找打开anonymous的ftp服务器的方法。这些服务器带有可读写的目录。木马doly trojan、fore、invisible ftp、webex、wincrash和blade runner所开放的端口。

端口：22

服务：ssh

说明：pcanywhere建立的tcp和这一端口的连接可能是为了寻找ssh。这一服务有许多弱点，如果配置成特定的模式，许多使用rsaref库的版本就会有不少的漏洞存在。

端口：23

服务：telnet

说明：远程登录，入侵者在搜索远程登录unix的服务。大多数情况下扫描这一端口是为了找到机器运行的操作系统。还有使用其他技术，入侵者也会找到密码。木马tiny telnet server就开放这个端口。

端口：25

服务：smtp

说明：smtp服务器所开放的端口，用于发送邮件。入侵者寻找smtp服务器是为了传递他们的spam。入侵者的帐户被关闭，他们需要连接到高带宽的e－mail服务器上，将简单的信息传递到不同的地址。木马antigen、email password sender、haebu coceda、shtrilitz stealth、winpc、winspy都开放这个端口。

端口：31

服务：msg authentication

说明：木马master paradise、hackers paradise开放此端口。

端口：42

服务：wins replication

说明：wins复制

端口：53

服务：domain name server（dns）

说明：dns服务器所开放的端口，入侵者可能是试图进行区域传递（tcp），欺骗dns（udp）或隐藏其他的通信。因此防火墙常常过滤或记录此端口。

端口：67

服务：bootstrap protocol server

说明：通过dsl和cable modem的防火墙常会看见大量发送到广播地址255.255.255.255的数据。这些机器在向dhcp服务器请求一个地址。hacker常进入它们，分配一个地址把自己作为局部路由器而发起大量中间人（man－in－middle）攻击。客户端向68端口广播请求配置，服务器向67端口广播回应请求。这种回应使用广播是因为客户端还不知道可以发送的ip地址。

端口：69

服务：trival file transfer

说明：许多服务器与bootp一起提供这项服务，便于从系统下载启动代码。但是它们常常由于错误配置而使入侵者能从系统中窃取任何 文件。它们也可用于系统写入文件。

端口：79

服务：finger server

说明：入侵者用于获得用户信息，查询操作系统，探测已知的缓冲区溢出错误，回应从自己机器到其他机器finger扫描。

端口：80

服务：http

说明：用于网页浏览。木马executor开放此端口。

端口：99

服务：metagram relay

说明：后门程序ncx99开放此端口。

端口：102

服务：message transfer agent(mta)－x.400 over tcp/ip

说明：消息传输代理。

端口：109

服务：post office protocol －version3

说明：pop3服务器开放此端口，用于接收邮件，客户端访问服务器端的邮件服务。pop3服务有许多公认的弱点。关于用户名和密码交 换缓冲区溢出的弱点至少有20个，这意味着入侵者可以在真正登陆前进入系统。成功登陆后还有其他缓冲区溢出错误。

端口：110

服务：sun公司的rpc服务所有端口

说明：常见rpc服务有rpc.mountd、nfs、rpc.statd、rpc.csmd、rpc.ttybd、amd等

端口：113

服务：authentication service

说明：这是一个许多计算机上运行的协议，用于鉴别tcp连接的用户。使用标准的这种服务可以获得许多计算机的信息。但是它可作为许多服务的记录器，尤其是ftp、pop、imap、smtp和irc等服务。通常如果有许多客户通过防火墙访问这些服务，将会看到许多这个端口的连接请求。记住，如果阻断这个端口客户端会感觉到在防火墙另一边与e－mail服务器的缓慢连接。许多防火墙支持tcp连接的阻断过程中发回rst。这将会停止缓慢的连接。

端口：119

服务：network news transfer protocol

说明：news新闻组传输协议，承载usenet通信。这个端口的连接通常是人们在寻找usenet服务器。多数isp限制，只有他们的客户才能访问他们的新闻组服务器。打开新闻组服务器将允许发/读任何人的帖子，访问被限制的新闻组服务器，匿名发帖或发送spam。

端口：135

服务：本地 service

说明：microsoft在这个端口运行dce rpc end－point mapper为它的dcom服务。这与unix 111端口的功能很相似。使用dcom和rpc的服务利用计算机上的end－point mapper注册它们的位置。远端客户连接到计算机时，它们查找end－point mapper找到服务的位置。hacker扫描计算机的这个端口是为了找到这个计算机上运行exchange server吗？什么版本？还有些dos攻击直接针对这个端口。

端口：137、138、139

服务：netbios name service

说明：其中137、138是udp端口，当通过网上邻居传输文件时用这个端口。而139端口：通过这个端口进入的连接试图获得netbios/smb服务。这个协议被用于windows文件和打印机共享和samba。还有wins regisrtation也用它。

端口：143

服务：interim mail access protocol v2

说明：和pop3的安全问题一样，许多imap服务器存在有缓冲区溢出漏洞。记住：一种linux蠕虫（admv0rm）会通过这个端口繁殖，因此许多这个端口的扫描来自不知情的已经被感染的用户。当redhat在他们的linux发布版本中默认允许imap后，这些漏洞变的很流行。这一端口还被用于imap2，但并不流行。

端口：161

服务：snmp

说明：snmp允许远程管理设备。所有配置和运行信息的储存在数据库中，通过snmp可获得这些信息。许多管理员的错误配置将被暴露在internet。cackers将试图使用默认的密码public、private访问系统。他们可能会试验所有可能的组合。snmp包可能会被错误的指向用户的网络。

端口：177

服务：x display manager control protocol

说明：许多入侵者通过它访问x－windows操作台，它同时需要打开6000端口。

端口：389

服务：ldap、ils

说明：轻型目录访问协议和netmeeting internet locator server共用这一端口。

端口：443

服务：https

说明：网页浏览端口，能提供加密和通过安全端口传输的另一种http。

端口：456

服务：【null】

说明：木马hackers paradise开放此端口。

端口：513

服务：login,remote login

说明：是从使用cable modem或dsl登陆到子网中的unix计算机发出的广播。这些人为入侵者进入他们的系统提供了信息。

端口：544

服务：【null】

说明：kerberos kshell

端口：548

服务：macintosh,file services(afp/ip)

说明：macintosh,文件服务。

端口：553

服务：corba iiop （udp）

说明：使用cable modem、dsl或vlan将会看到这个端口的广播。corba是一种面向对象的rpc系统。入侵者可以利用这些信息进入系统。

端口：555

服务：dsf

说明：木马phase1.0、stealth spy、inikiller开放此端口。

端口：568

服务：membership dpa

说明：成员资格 dpa。

端口：569

服务：membership msn

说明：成员资格 msn。

端口：635

服务：mountd

说明：linux的mountd bug。这是扫描的一个流行bug。大多数对这个端口的扫描是基于udp的，但是基于tcp的mountd有所增加（mountd同时运行于两个端口）。记住mountd可运行于任何端口（到底是哪个端口，需要在端口111做portmap查询），只是linux默认端口是635，就像nfs通常运行于2049端口。

端口：636

服务：ldap

说明：ssl（secure sockets layer）

端口：666

服务：doom id software

说明：木马attack ftp、satanz backdoor开放此端口

端口：993

服务：imap

说明：ssl（secure sockets layer）

端口：1001、1011

服务：【null】

说明：木马silencer、webex开放1001端口。木马doly trojan开放1011端口。

端口：1024

服务：reserved

说明：它是动态端口的开始，许多程序并不在乎用哪个端口连接网络，它们请求系统为它们分配下一个闲置端口。基于这一点分配从端口1024开始。这就是说第一个向系统发出请求的会分配到1024端口。你可以重启机器，打开telnet，再打开一个窗口运行natstat －a 将会看到telnet被分配1024端口。还有sql session也用此端口和5000端口