一、端口概念

在网络技术中，端口（Port）大致有两种意思：一是物理意义上的端口，比如，ADSL Modem、集线器、交换机、路由器用于连接其他网络设备的接口，如RJ-45端口、SC端口等等。二是逻辑意义上的端口，一般是指TCP/IP协议中的端口，端口号的范围从0到65535，比如用于浏览网页服务的80端口，用于FTP服务的21端口等等。

二、网络端口的分类

按端口号可分为3大类：（1）公认端口（Well-KnownPorts）：范围从0到1023（2）动态端口（Dynamic Ports）：范围从1024到65535
(2.1)注册端口（RegisteredPorts）：从1024到49151
(2.2)动态和/或私有端口（Dynamicand/orPrivatePorts）：：从49152到65535。

.....

.....

端口：0服务：Reserved说明：通常用于分析操作系统。这一方法能够工作是因为在一些系统中“0”是无效端口，当你试图使用通常的闭合端口连接它时将产生不同的结果。一种典型的扫描，使用IP地址为0.0.0.0，设置ACK位并在以太网层广播。

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包后回应含有垃圾字符的包。TCP连接时会发送含有垃圾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：Location 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RED HAT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。

端口：1025、1033服务：1025：network blackjack
1033：[NULL]说明：木马netspy开放这2个端口。

端口：1080服务：SOCKS说明：这一协议以通道方式穿过防火墙，允许防火墙后面的人通过一个IP地址访问INTERNET。理论上它应该只允许内部的通信向外到达INTERNET。但是由于错误的配置，它会允许位于防火墙外部的攻击穿过防火墙。WinGate常会发生这种错误，在加入IRC聊天室时常会看到这种情况。端口：1170服务：[NULL]说明：木马Streaming Audio Trojan、Psyber Stream
Server、Voice开放此端口。

端口：1234、1243、6711、6776服务：[NULL]说明：木马SubSeven2.0、Ultors Trojan开放1234、6776端口。木马SubSeven1.0/1.9开放1243、6711、6776端口。

端口：1245服务：[NULL]说明：木马Vodoo开放此端口。

端口：1433服务：SQL说明：Microsoft的SQL服务开放的端口。

端口：1492服务：stone-design-1说明：木马FTP99CMP开放此端口。

端口：1500服务：RPC client fixed port session queries说明：RPC客户固定端口会话查询

端口：1503服务：NetMeeting T.120说明：NetMeeting T.120

端口：1524服务：ingress说明：许多攻击脚本将安装一个后门SHELL于这个端口，尤其是针对SUN系统中Sendmail和RPC服务漏洞的脚本。如果刚安装了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。可以试试Telnet到用户的计算机上的这个端口，看看它是否会给你一个SHELL。连接到600/pcserver也存在这个问题。

端口：1600服务：issd说明：木马Shivka-Burka开放此端口。

端口：1720服务：NetMeeting说明：NetMeeting H.233 call Setup。

端口：1731服务：NetMeeting Audio Call Control说明：NetMeeting音频调用控制。

端口：1807服务：[NULL]说明：木马SpySender开放此端口。

端口：1981服务：[NULL]说明：木马ShockRave开放此端口。

端口：1999服务：cisco identification port说明：木马BackDoor开放此端口。

端口：2000服务：[NULL]说明：木马GirlFriend 1.3、Millenium 1.0开放此端口。

端口：2001服务：[NULL]说明：木马Millenium 1.0、Trojan Cow开放此端口。

端口：2023服务：xinuexpansion 4说明：木马Pass Ripper开放此端口。

端口：2049服务：NFS说明：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。

端口：2115服务：[NULL]说明：木马Bugs开放此端口。

端口：2140、3150服务：[NULL]说明：木马Deep Throat 1.0/3.0开放此端口。

端口：2500服务：RPC client using a fixed port session replication说明：应用固定端口会话复制的RPC客户

端口：2583服务：[NULL]说明：木马Wincrash 2.0开放此端口。

端口：2801服务：[NULL]说明：木马Phineas Phucker开放此端口。

端口：3024、4092服务：[NULL]说明：木马WinCrash开放此端口。

端口：3128服务：squid说明：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。也会看到搜索其他代理服务器的端口8000、8001、8080、8888。扫描这个端口的另一个原因是用户正在进入聊天室。其他用户也会检验这个端口以确定用户的机器是否支持代理。

端口：3129服务：[NULL]说明：木马Master Paradise开放此端口。

端口：3150服务：[NULL]说明：木马The Invasor开放此端口。

端口：3210、4321服务：[NULL]说明：木马SchoolBus开放此端口

端口：3333服务：dec-notes说明：木马Prosiak开放此端口

端口：3389服务：超级终端说明：WINDOWS 2000终端开放此端口。

端口：3700服务：[NULL]说明：木马Portal of Doom开放此端口

端口：3996、4060服务：[NULL]说明：木马RemoteAnything开放此端口

端口：4000服务：QQ客户端说明：腾讯QQ客户端开放此端口。

端口：4092服务：[NULL]说明：木马WinCrash开放此端口。

端口：4590服务：[NULL]说明：木马ICQTrojan开放此端口。

端口：5000、5001、5321、50505服务：[NULL]说明：木马blazer5开放5000端口。木马Sockets de Troie开放5000、5001、5321、50505端口。

端口：5400、5401、5402服务：[NULL]说明：木马Blade Runner开放此端口。

端口：5550服务：[NULL]说明：木马xtcp开放此端口。

端口：5569服务：[NULL]说明：木马Robo-Hack开放此端口。

端口：5632服务：pcAnywere说明：有时会看到很多这个端口的扫描，这依赖于用户所在的位置。当用户打开pcAnywere时，它会自动扫描局域网C类网以寻找可能的代理（这里的代理是指agent而不是proxy）。入侵者也会寻找开放这种服务的计算机。，所以应该查看这种扫描的源地址。一些搜寻pcAnywere的扫描包常含端口22的UDP数据包。

端口：5742服务：[NULL]说明：木马WinCrash1.03开放此端口。

端口：6267服务：[NULL]说明：木马广外女生开放此端口。

端口：6400服务：[NULL]说明：木马The tHing开放此端口。

端口：6670、6671服务：[NULL]说明：木马Deep Throat开放6670端口。而Deep Throat 3.0开放6671端口。

端口：6883服务：[NULL]说明：木马DeltaSource开放此端口。

端口：6969服务：[NULL]说明：木马Gatecrasher、Priority开放此端口。

端口：6970服务：RealAudio说明：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TCP-7070端口外向控制连接设置的。

端口：7000服务：[NULL]说明：木马Remote Grab开放此端口。

端口：7300、7301、7306、7307、7308服务：[NULL]说明：木马NetMonitor开放此端口。另外NetSpy1.0也开放7306端口。

端口：7323服务：[NULL]说明：Sygate服务器端。

端口：7626服务：[NULL]说明：木马Giscier开放此端口。

端口：7789服务：[NULL]说明：木马ICKiller开放此端口。

端口：8000服务：OICQ说明：腾讯QQ服务器端开放此端口。

端口：8010服务：Wingate说明：Wingate代理开放此端口。

端口：8080服务：代理端口说明：WWW代理开放此端口。

端口：9400、9401、9402服务：[NULL]说明：木马Incommand 1.0开放此端口。

端口：9872、9873、9874、9875、10067、10167服务：[NULL]说明：木马Portal of Doom开放此端口。

端口：9989服务：[NULL]说明：木马iNi-Killer开放此端口。

端口：11000服务：[NULL]说明：木马SennaSpy开放此端口。

端口：11223服务：[NULL]说明：木马Progenic trojan开放此端口。

端口：12076、61466服务：[NULL]说明：木马Telecommando开放此端口。page]

端口：12223服务：[NULL]说明：木马Hack'99 KeyLogger开放此端口。

端口：12345、12346服务：[NULL]说明：木马NetBus1.60/1.70、GabanBus开放此端口。

端口：12361服务：[NULL]说明：木马Whack-a-mole开放此端口。

端口：13223服务：PowWow说明：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攻击性。它会驻扎在这个TCP端口等回应。造成类似心跳间隔的连接请求。如果一个拨号用户从另一个聊天者手中继承了IP地址就会发生好象有很多不同的人在测试这个端口的情况。这一协议使用OPNG作为其连接请求的前4个字节。

端口：16969服务：[NULL]说明：木马Priority开放此端口。

端口：17027服务：Conducent说明：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。

端口：19191服务：[NULL]说明：木马蓝色火焰开放此端口。

端口：20000、20001服务：[NULL]说明：木马Millennium开放此端口。

端口：20034服务：[NULL]说明：木马NetBus Pro开放此端口。

端口：21554服务：[NULL]说明：木马GirlFriend开放此端口。

端口：22222服务：[NULL]说明：木马Prosiak开放此端口。

端口：23456服务：[NULL]说明：木马Evil FTP、Ugly FTP开放此端口。

端口：26274、47262服务：[NULL]说明：木马Delta开放此端口。

端口：27374服务：[NULL]说明：木马Subseven 2.1开放此端口。

端口：30100服务：[NULL]说明：木马NetSphere开放此端口。

端口：30303服务：[NULL]说明：木马Socket23开放此端口。

端口：30999服务：[NULL]说明：木马Kuang开放此端口。

端口：31337、31338服务：[NULL]说明：木马BO(Back Orifice)开放此端口。另外木马DeepBO也开放31338端口。

端口：31339服务：[NULL]说明：木马NetSpy DK开放此端口。

端口：31666服务：[NULL]说明：木马BOWhack开放此端口。

端口：33333服务：[NULL]说明：木马Prosiak开放此端口。

端口：34324服务：[NULL]说明：木马Tiny Telnet Server、BigGluck、TN开放此端口。

端口：40412服务：[NULL]说明：木马The Spy开放此端口。

端口：40421、40422、40423、40426、服务：[NULL]说明：木马Masters Paradise开放此端口。

端口：43210、54321服务：[NULL]说明：木马SchoolBus 1.0/2.0开放此端口。

端口：44445服务：[NULL]说明：木马Happypig开放此端口。

端口：50766服务：[NULL]说明：木马Fore开放此端口。

端口：53001服务：[NULL]说明：木马Remote Windows Shutdown开放此端口。

端口：65000服务：[NULL]说明：木马Devil 1.03开放此端口。

端口：88说明：Kerberos krb5。另外TCP的88端口也是这个用途。

端口：137说明：SQL Named Pipes encryption over other protocols name lookup(其他协议名称查找上的SQL命名管道加密技术)和SQL RPC encryption over other protocols name lookup(其他协议名称查找上的SQL RPC加密技术)和Wins NetBT name service(WINS NetBT名称服务)和Wins Proxy都用这个端口。

端口：161说明：Simple Network Management Protocol(SMTP)（简单网络管理协议）。

端口：162说明：SNMP Trap（SNMP陷阱）

端口：445说明：Common Internet File System(CIFS)（公共Internet文件系统）

端口：464说明：Kerberos kpasswd(v5)。另外TCP的464端口也是这个用途。

端口：500说明：Internet Key Exchange(IKE)（Internet密钥交换）

端口：1645、1812说明：Remot Authentication Dial-In User Service(RADIUS)authentication(Routing and Remote Access)(远程认证拨号用户服务)

端口：1646、1813说明：RADIUS accounting(Routing and Remote Access)(RADIUS记帐（路由和远程访问））

端口：1701说明：Layer Two Tunneling Protocol(L2TP)(第2层隧道协议)

端口：1801、3527说明：Microsoft Message Queue Server(Microsoft消息队列服务器)。还有TCP的135、1801、2101、2103、2105也是同样的用途。

端口：2504说明：Network Load Balancing(网络平衡负荷)