攻防入门：全面认识你的网络端口 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/181/2021_2022__E6_94_BB_E9_98_B2_E5_85_A5_E9_c101_181849.htm 端口可分为3大类：1） 公认端口（Well Known Ports）：从0到1023，它们紧密绑定于一些服务。通常这些端口的通讯明确表明了某种服 务的协议。例如：80端口实际上总是HTTP通讯。 2） 注册端口（Registered Ports）：从1024到49151。它们松散地绑定于一些服务。也就是说有许多服务绑定于这些端口，这些端口同样用于许多其它目的。例如：许多系统处理动态端口从1024左右开始。 3） 动态和/或私有端口（Dynamic and/or Private Ports）：从49152到65535。理论上，不应为服务分配这些端口。实际上，机器通常从1024起分配动态端口。但也有例外：SUN的RPC端口从32768开始。 本节讲述通常TCP/UDP端口扫描在防火墙记录中的信息。记住：并不存在所谓ICMP端口。如果你对解读ICMP数据感兴趣，请参看本文的其它部分。0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 图使用一种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。 1 tcpmux 这显示有人在寻找SGIIrix机器。Irix是实现tcpmux的主要提供者，缺省情况下tcpmux在这种系统中被打开。Iris机器在发布时含有几个缺省的无密码的帐户，如lp,guest, uucp, nuucp, demos, tutor, diag, EZsetup, OutOfBox, 和4Dgifts。许多管理员安装后忘记删除这些帐户。因此Hacker们在Internet上搜索tcpmux 并利用这些帐户。 7Echo你能看到许多人们搜索Fraggle放大器时，

发送到x.x.x.0和x.x.x.255的信息。常见的一种DoS攻击是echo循环（echo-loop），攻击者伪造从一个机器发送到另一个UDP数据包，而两个机器分别以它们最快的方式回应这些数据包。（参见Chargen） 另一种东西是由DoubleClick在词端口建立的TCP连接。有一种产品叫做Resonate Global Dispatch ”，它与DNS的这一端口连接以确定最近的路由 。Harvest/squid cache将从3130端口发送UDPecho：“ 如果将cache的source_ping on选项打开，它将对原始主机的UDP echo端口回应一个HIT reply。 ”这将会产生许多这类数据包 。 11 sysstat这是一种UNIX服务，它会列出机器上所有正在运行的进程以及是什么启动了这些进程。这为入侵者提供了许多信息而威胁机器的安全，如暴露已知某些弱点或帐户的程序。这与UNIX系统中“ ps ”命令的结果相似再说一遍 ：ICMP没有端口，ICMP port 11通常是ICMPtype=1119 chargen 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知道连接关闭。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由于服务器企图回应两个服务器之间的无限的往返数据通讯一个chargen和echo将导致服务器过载。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。 21 ftp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。Hackers或tackers利用这些服务器作为传送warez (私有程序) 和pr0n(故意拼错词而避免被搜索引擎分类)的节点。 22 sshPcAnywhere建立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库的版本有不少漏洞。（建议在其它端口运行ssh）还应该注意的是ssh工具包带有一个称为ake-ssh-known-hosts的程序。它会扫描整个域的ssh主机。你有时会被使用这一程序的人无意中扫描到。UDP（而不是TCP）与另一端的5632端口相连意味着存在搜索pcAnywhere的扫描。5632（十六进制的0x1600）位交换后是0x0016（使进制的22）。 23 Telnet入侵者在搜索远程登陆UNIX的服务。大多数情况下入侵者扫描这一端口是为了找到机器运行的操作系统。此外使用其它技术，入侵者会找到密码。 25 smtp攻击者（spammer）寻找SMTP服务器是为了传递他们的spam。入侵者的帐户总被关闭，他们需要拨号连接到高带宽的e-mail服务器上，将简单的信息传递到不同的地址。SMTP服务器（尤其是sendmail）是进入系统的最常用方法之一，因为它们必须完整的暴露于Internet且邮件的路由是复杂的（暴露 复杂=弱点）。 53 DNSHacker或crackers可能是试图进行区域传递（TCP），欺骗DNS（UDP）或隐藏其它通讯。因此防火墙常常过滤或记录53端口。 需要注意的是你常会看到53端口做为UDP源端口。不稳定的防火墙通常允许这种通讯并假设这是对DNS查询的回复。Hacker常使用这种方法穿透防火墙。 67和68 Bootp和DHCPUDP上的Bootp/DHCP：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分配。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的“ 中间人 ”（man-in-middle）攻击。客户端向68端口（bootps）广播请求配置，服务器向67端口

（bootpc）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。69 TFTP(UDP) 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。但是它们常常错误配置而从系统提供任何文件，如密码文件。它们也可用于向系统写入文件 79 finger Hacker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它机器finger扫描。 98 linuxconf 这个程序提供linuxboxen的简单管理。通过整合的HTTP服务器在98端口提供基于Web界面的服务。它已发现有许多安全问题。一些版本setuidroot，信任局域网，在/tmp下建立Internet可访问的文件，LANG环境变量有缓冲区溢出。 此外因为它包含整合的服务器，许多典型的HTTP漏洞可 能存在（缓冲区溢出，历遍目录等）109 POP2并不象POP3那样有名，但许多服务器同时提供两种服务（向后兼容）。在同一个服务器上POP3的漏洞在POP2中同样存在。110 POP3用于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Hacker可以在真正登陆前进入系统）。成功登陆后还有其它缓冲区溢出错误。 111 sunrpc portmap rpcbind Sun RPCPortMapper/RPCBIND。访问portmapper是扫描系统查看允许哪些RPC服务的最早的一步。常 见RPC服务有：pc.mountd, NFS, rpc.statd, rpc.csmd, rpc.ttybd, amd等。入侵者发现了允许的RPC服务将转向提供 服务的特定端口测试漏洞。记住一定要记录线路中的daemon, IDS, 或sniffer，你可以发现入侵者正使用什么程序访问以便发现到底发生了什么。 113 Ident auth .这是一个许多机器上运行的协议，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机器的信息（会被Hacker利用）。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，你将会看到许多这个端口的连接请求。记住，如果你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。许多防火墙支持在TCP连接的阻断过程中发回T，着将回停止这一缓慢的连接。 119 NNTP news新闻组传输协议，承载USENET通讯。当你链接到诸如：news.security.firewalls/. 的地址时通常使用这个端口。这个端口的连接企图通常是人们在寻找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。 135 oc-serv MS RPC end-point mapper 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/或RPC的服务利用 机器上的end-point mapper注册它们的位置。远端客户连接到机器时，它们查询end-point mapper找到服务的位置。同样Hacker扫描机器的这个端口是为了找到诸如：这个机器上运 行Exchange Server吗？是什么版本？ 这个端口除了被用来查询服务（如使用epdump）还可以被用于直接攻击。有一些DoS攻 击直接针对这个端口。 137 NetBIOS name service nbtstat (UDP)这是防火墙管理员最常见的信息，请仔细阅读文章后面的NetBIOS一节 139 NetBIOS File and Print Sharing 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。在Internet上共享自己的硬盘是可能

是最常见的问题。 大量针对这一端口始于1999，后来逐渐变少。2000年又有回升。一些VBS（IE5 VisualBasicScripting）开始将它们自己拷贝到这个端口，试图在这个端口繁殖。143 IMAP和上面POP3的安全问题一样，许多IMAP服务器有缓冲区溢出漏洞运行登陆过程中进入。记住：一种Linux蠕虫（admw0rm）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被感染的用户。当RadHat在他们的Linux发布版本中默认允许IMAP后，这些漏洞变得流行起来。Morris蠕虫以后这还是第一次广泛传播的蠕虫。这一端口还被用于IMAP2，但并不流行。 已有一些报道发现有些0到143端口的攻击源于脚本。 161 SNMP(UDP)入侵者常探测的端口。SNMP允许远程管理设备。所有配置和运行信息都储存在数据库中，通过SNMP客获得这些信息。许多管理员错误配置将它们暴露于Internet。Crackers将试图使用缺省的密码“ 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你的网络。Windows机器常会因为错误配置将HP JetDirect rmote management软件使用SNMP。HP OBJECT IDENTIFIER将收到SNMP包。新版的Win98使用SNMP解析域名，你会看见这种包在子网内广播（cable modem, DSL）查询sysName和其它信息。 162 SNMP trap 可能是由于错误配置 177 xdmcp 许多Hacker通过它访问X-Windows控制台，它同时需要打开6000端口。 513 rwho 可能是从使用cable modem或DSL登陆到的子网中的UNIX机器发出的广播。这些人为Hacker进入他们的系统提供 了很有趣的信息 553 CORBA IIOP (UDP) 如果你使用cable modem或DSL VLAN，你将会看到这个端口的广播。CORBA是一种面向对

象的RPC（remote procedure call）系统。Hacker会利用这些信息进入系统。 600 Pcserver backdoor 请查看1524端口一些玩script的孩子认为他们通过修改ingreslock和pcserver文件已经完全攻破了系统-- Alan J. Rosenthal. 635 mountd Linux的mountd Bug。这是人们扫描的一个流行的Bug。大多数对这个端口的扫描是基于UDP的，但基于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（到底在哪个端口，需要在端口111做portmap查询），只是Linux默认为635端口，就象NFS通常运行于2049端口。 1024 许多人问这个端口是干什么的。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，它们请求操作系统为它们分配“ 下一个闲置端口 ”。基于这一点分配从端口1024开始。这意味着第一个向系统请求分配动态端口的程序将被分配端口1024。为了验证这一点，你可以重启机器，打开Telnet，再打开一个窗口运行“ natstat -a ”，你将会看到Telnet被分配1024端口。请求的程序越多，动态端口也越多。操作系统分配的端口将逐渐变大。再来一遍，当你浏览Web页时用“ netstat ”查看，每个Web页需要一个新端口。 1025 参见1024 1026 参见1024 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）参见Subseven部分。 1524 ingreslock后门 许多攻击脚本将安装一个后门Sh*ll 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Sh*ll 。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杏谖飧龆丝冢?acker/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： 000/8001/8080/8888。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。请查看5.3节。 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。参见拨号扫描。 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) 参见Subseven部分。 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 “ eliteHacker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。参见traceroute分。 41508 Inoculan早期版本的Inoculan会在子网内产生大量的UDP通讯用于识别彼此。参见http://www.circlemud.org/~jelson/software/udpsend.html http://www.ccd.bnl.gov/nss/tips/inoculan/index.html端口1~1024是保留端口，所以它们几乎不会是源端口。但有一些例外，例如来自NAT机器的连接。 常看见紧接着1024的端口，它们是系统分配给那些并不在乎使用哪个端口连接的应用程序的“ 动态端口 ”。 Server Client 服务描述 1-5/tcp 动态 FTP 1-5端口意味着sscan脚本 20/tcp 动态 FTP FTP服务器传送文件的端口 53 动态 FTP DNS从这个端口发送UDP回应。你也可能看见源/目标端口的TCP连接。 123 动态 S/NTP 简单网络时间协议（S/NTP）服务器运行的端口。它们也会发送到这个端口的广播。 27910~27961/udp 动态 Quake Quake或Quake引擎驱动的游戏在这一端口运行其服务器。因此来自这一端口范围的UDP包或发送至这一端口范围的UDP包通常是游戏。 61000

以上 动态 FTP 61000以上的端口可能来自Linux NAT服务器（IP asquerade） 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com