

端口知识及被攻击方法 PDF转换可能丢失图片或格式，建议
阅读原文

https://www.100test.com/kao_ti2020/245/2021_2022__E7_AB_AF_E5_8F_A3_E7_9F_A5_E8_c97_245830.htm 端口可分为3大类：1

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。常见

端口详解及部分攻击策略：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SGI Irix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。Irix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UDP echo：“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ICMP type=11 19 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包。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Crackers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

ssh PcAnywhere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make-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（二进制的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 DNS Hacker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DHCP UDP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linux boxen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，遍历目录等）。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 RPC PortMapper/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：rpc.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RST，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://comp.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。

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