网络安全与端口攻略的详细解读十一 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_140250.htm 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)常见命令和端口列表网络基础知识!端口对照,常用命令! 常用端口

对照表！ 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。