网络安全与端口攻略的详细解读一 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_140287.htm 按端口号可分为3大类：（1）公认端口（Well Known Ports）：从0到1023，它们紧密绑定（binding）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。 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 TCP Port Service Multiplexer 传输控制协议端口服务多路开关选择器 2 compressnet Management Utility compressnet 管理实用程序 3 compressnet Compression Process 压缩进程 5 rje Remote Job Entry 远程作业登录 7 echo Echo 回显 9 discard Discard 丢弃 11 systat Active Users 在线用户 13 daytime Daytime 时间 17 qotd Quote of the Day 每日引用 18 msp Message Send Protocol 消息发送协议 19 chargen Character Generator 字符发生器 20 ftp-data File Transfer[Default Data] 文件传输协议(默认数据口) 21 ftp File

Transfer[Control] 文件传输协议(控制) 22 ssh SSH Remote Login Protocol SSH远程登录协议 23 telnet Telnet 终端仿真协议 24 any private mail system 预留给个人用邮件系统 25 smtp Simple Mail Transfer 简单邮件发送协议 27 nsw-fe NSW User System FE NSW 用户系统现场工程师 29 msg-icp MSG ICP MSG ICP 31 msg-auth MSG Authentication MSG验证 33 dsp Display Support Protocol 显示支持协议 35 any private printer server 预留给个人打印机服务 37 time Time 时间 38 rap Route Access Protocol 路由访问协议 39 rlp Resource Location Protocol 资源定位协议 41 graphics Graphics 图形 42 nameserver WINS Host Name Server WINS 主机名服务 43 nicname Who Is "绰号" who is服务 44 mpm-flags MPM FLAGS Protocol MPM(消息处理模块)标志协议 45 mpm Message Processing Module [recv] 消息处理模块 46 mpm-snd MPM [default send] 消息处理模块(默认发送口) 47 ni-ftp NI FTP NI FTP 48 auditd Digital Audit Daemon 数码音频后台服务 49 tacacs Login Host Protocol (TACACS) TACACS登录主机协议