网络安全与端口攻略的详细解读八 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_140263.htm 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REDHAT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。 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