安全知识：解读防火墙日志记录 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/460/2021_2022__E5_AE_89_E5_85_A8_E7_9F_A5_E8_c100_460852.htm 如今个人防火墙已经越来越多的应用于用户的计算机上，但您真的可以驾驭您的防火墙吗？它的性能可以被用户最大限度的发挥出来吗？本文将详细介绍个人防火墙的日志的详细信息，有效保护用户的计算机。 一、目标端口 所有穿过防火墙的通讯都是连接的一个部分。一个连接包含一对相互“ 交谈 ”的IP地址以及一对与IP地址对应的端口。目标端口通常意味着正被连接的某种服务。当防火墙阻挡（block）某个连接时，它会将目标端口“ 记录在案 ”。 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/私有端口（Dynamic/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。 从哪里获得更全面的端口信息： 1.ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers "Assigned Numbers" RFC，端口分配的官方来源。 2.http://advice.networkice.com/advice/Exploits/Ports/ 端口数据库，包含许多系统弱点的端口。 3./etc/services UNIX 系统中文

件/etc/services包含通常使用的UNIX端口分配列表。Windows NT中该文件位于%systemroot%/system32/drivers/etc/services. 4.http://www.con.wesleyan.edu/~triemer/network/docservs.html 特定的协议与端口。
5.http://www.chebucto.ns.ca/~rakerman/trojan-port-table.html 描述了许多端口。 二、通常对防火墙的TCP/UDP端口扫描有哪些？ 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。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。 7 Echo 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机器的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；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 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（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 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。 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