网络安全

安全技巧（六）

小未 主编

目　录

解读防火墙记录

本文将向你解释你在防火墙的记录（Log）中看到了什么？尤其是那些端口是什么意思？你将能利用这些信息做出判断：我是否受到了 Hacker 的攻击？他/她到底想要干什么？本文既适用于维护企业级防火墙的安全专家，又适用于使用个人防火墙的家庭用户。

现在个人防火墙开始流行起来，很多网友一旦看到报警就以为受到某种攻击，其实大多数情况并非如此。

一、目标端口 ZZZZ 是什么意思

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”(logfile)。这节将描述这些端口的意义。

端口可分为 3 大类：

1）公认端口（WellKnownPorts）：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（RegisteredPorts）：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(Dynamicand/orPrivatePorts)：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

"AssignedNumbers"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。WindowsNT 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。

6．http://www.tlsecurity.com/trojanh.htm

TLSecurity 的 Trojan 端口列表。与其它人的收藏不同，作者检验了其中的所有端口。

7．http://www.simovits.com/nyheter9902.html

TrojanHorse 探测。

二、通常对于防火墙的 TCP/UDP 端口扫描有哪些？

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。

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。

1tcpmux 这显示有人在寻找 SGIIrix 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。

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。(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“ResonateGlobalDispatch”，它与 DNS 的这一端口连接以确定最近的路由。

Harvest/squidcache 将从 3130 端口发送 UDPecho：“如果将 cache 的 source_pingon 选项打开，它将对原始主机的 UDPecho 端口回应一个 HITreply。”这将会产生许多这类数据包。

11sysstat 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，ICMPport11 通常是 ICMPtype=11

19chargen 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 fraggleDoS 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。

21ftp 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。

22sshPcAnywhere 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 0

x1600）位交换后是 0x0016（使进制的 22）。

23Telnet 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。

25smtp 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）。

53DNSHacker 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 68Bootp 和 DHCPUDP 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。

69TFTP(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。

79fingerHacker 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。

98linuxconf 这个程序提供 linuxboxen 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，历遍目录等）

109POP2 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。

110POP3 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。

111sunrpcportmaprpcbindSunRPCPortMapper/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。

113Identauth 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。

119NNTPnews 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。

135oc-servMSRPCend-pointmapperMicrosoft 在这个端口运行 DCERPCend-pointmapper 为它的 DCOM 服务。这与 UNIX111 端口的功能很相似。使用 DCOM 和/或 RPC 的服务利用机器上的 end-pointmapper 注册它们的位置。远端客户连接到机器时，它们查询 end-pointmapper 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 ExchangeServer 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。

137NetBIOSnameservicenbtstat(UDP)这是防火墙管理员最常见的信息，请仔细阅读文章后面的 NetBIOS 一

节

139NetBIOSFileandPrintSharing 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。在 Internet 上共享自己的硬盘是可能是最常见的问题。

大量针对这一端口始于 1999，后来逐渐变少。2000 年又有回升。一些 VBS（IE5VisualBasicScripting）开始将它们自己拷贝到这个端口，试图在这个端口繁殖。

143IMAP 和上面 POP3 的安全问题一样，许多 IMAP 服务器有缓冲区溢出漏洞运行登陆过程中进入。记住：一种 Linux 蠕虫（admw0rm）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被感染的用户。当 RadHat 在他们的 Linux 发布版本中默认允许 IMAP 后，这些漏洞变得流行起来。Morris 蠕虫以后这还是第一次广泛传播的蠕虫。

这一端口还被用于 IMAP2，但并不流行。

已有一些报道发现有些 0 到 143 端口的攻击源于脚本。

161SNMP(UDP)入侵者常探测的端口。SNMP 允许远程管理设备。所有配置和运行信息都储存在数据库中，通过 SNMP 客获得这些信息。许多管理员错误配置将它们暴露于 Internet。Crackers 将试图使用缺省的密码“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你的网络。Windows 机器常会因为错误配置将 HPJetDirectremotemanagement 软件使用 SNMP。HPOBJECTIDENTIFIER 将收到 SNMP 包。新版的 Win98 使用 SNMP 解析域名，你会看见这

种包在子网内广播（cablemodem,DSL）查询 sysName 和其它信息。

162SNMPtrap 可能是由于错误配置

177xdmcp 许多 Hacker 通过它访问 X-Windows 控制台，它同时需要打开 6000 端口。

513rwho 可能是从使用 cablemodem 或 DSL 登陆到的子网中的 UNIX 机器发出的广播。这些人为 Hacker 进入他们的系统提供了很有趣的信息。

553CORBAIIOP(UDP)如果你使用 cablemodem 或 DSLVLAN，你将会看到这个端口的广播。CORBA 是一种面向对象的 RPC（remoteprocedurecall）系统。Hacker 会利用这些信息进入系统。

600Pcserverbackdoor 请查看 1524 端口

一些玩 script 的孩子认为他们通过修改 ingreslock 和 pcserver 文件已经完全攻破了系统--AlanJ.Rosenthal.

635mountdLinux 的 mountdBug。这是人们扫描的一个流行的 Bug。大多数对这个端口的扫描是基于 UDP 的，但基于 TCP 的 mountd 有所增加（mountd 同时运行于两个端口）。记住，mountd 可运行于任何端口（到底在哪个端口，需要在端口 111 做 portmap 查询），只是 Linux 默认为 635 端口，就象 NFS 通常运行于 2049 端口。

1024 许多人问这个端口是干什么的。它是动态端口的开始。许多程序并不在乎用哪个端口连接网络，它们请求操作系统为它们分配“下一个闲置端口”。基于这一点分配从端口 1024 开始。这意味着第一个向系统请求分配动态端口的程序将被分配端口 1024。为了验证这一点，你可以重启机器，打开 Telnet，再打开一个窗口运行“natstat-a”，你将会看到 Telnet 被分配 1024 端口。请

求的程序越多，动态端口也越多。操作系统分配的端口将逐渐变大。再来一遍，当你浏览 Web 页时用“ netstat ”查看，每个 Web 页需要一个新端口。

Version0.4.1,June20,2000

http://www.robertgraham.com/pubs/firewall-seen.html

Copyright1998-2000byRobertGraham(mailto:firewall-seen1@robertgraham.com

Allrightsreserved.Thisdocumentmayonlybereproduced(wholeor

inpart)fornon-commercialpurposes.Allreproductionsmust

containthiscopyrightnoticeandmustnotbealtered,exceptby

permissionoftheauthor.

1025 参见 1024

1026 参见 1024

1080SOCKS

这一协议以管道方式穿过防火墙，允许防火墙后面的许多人通过一个 IP 地址访问 Internet。理论上它应该只允许内部的通信向外达到 Internet。但是由于错误的配置，它会允许 Hacker/Cracker 的位于防火墙外部的攻击穿过防火墙。或者简单地回应位于 Internet 上的计算机，从而掩饰他们对你的直接攻击。WinGate 是一种常见的 Windows 个人防火墙，常会发生上述的错误配置。在加入 IRC 聊天室时常会看到这种情况。

1114SQL

系统本身很少扫描这个端口，但常常是 sscan 脚本

的一部分。

1243Sub-7 木马（TCP）

参见 Subseven 部分。

1524ingreslock 后门

许多攻击脚本将安装一个后门 Shell 于这个端口(尤其是那些针对 Sun 系统中 Sendmail 和 RPC 服务漏洞的脚本，如 statd,ttdbserver 和 cmsd)。如果你刚刚安装了你的防火墙就看到在这个端口上的连接企图，很可能是上述原因。你可以试试 Telnet 到你的机器上的这个端口，看看它是否会给你一个 Shell。连接到 600/pcserver 也存在这个问题。

2049NFS

NFS 程序常运行于这个端口。通常需要访问 portmapper 查询这个服务运行于哪个端口，但是大部分情况是安装后 NFS 运行于这个端口，Hacker/Cracker 因而可以闭开 portmapper 直接测试这个端口。

3128squid

这是 SquidHTTP 代理服务器的默认端口。攻击者扫描这个端口是为了搜寻一个代理服务器而匿名访问 Internet。你也会看到搜索其它代理服务器的端口：8000/8001/8080/8888。扫描这一端口的另一原因是：用户正在进入聊天室。其它用户（或服务器本身）也会检验这个端口以确定用户的机器是否支持代理。请查看 5.3 节。

5632pcAnywere

你会看到很多这个端口的扫描，这依赖于你所在的位置。当用户打开 pcAnywere 时，它会自动扫描局域网 C 类网以寻找可能得代理(译者 指 agent 而不是 proxy)。Hacker/cracker 也会寻找开放这种服务的机器，所以应该

查看这种扫描的源地址。一些搜寻 pcAnywere 的扫描常包含端口 22 的 UDP 数据包。参见拨号扫描。

6776Sub-7artifact

这个端口是从 Sub-7 主端口分离出来的用于传送数据的端口。例如当控制者通过电话线控制另一台机器，而被控机器挂断时你将会看到这种情况。因此当另一人以此 IP 拨入时，他们将会看到持续的，在这个端口的连接企图。（译者：即看到防火墙报告这一端口的连接企图时，并不表示你已被 Sub-7 控制。）

6970RealAudio

RealAudio 客户将从服务器的 6970-7170 的 UDP 端口接收音频数据流。这是由 TCP7070 端口外向控制连接设置的。

13223PowWow

PowWow 是 TribalVoice 的聊天程序。它允许用户在此端口打开私人聊天的连接。这一程序对于建立连接非常具有“进攻性”。它会“驻扎”在这一 TCP 端口等待回应。这造成类似心跳间隔的连接企图。如果你是一个拨号用户，从另一个聊天者手中“继承”了 IP 地址这种情况就会发生：好象很多不同的人在测试这一端口。这一协议使用“OPNG”作为其连接企图的前四个字节。

17027Conducent

这是一个外向连接。这是由于公司内部有人安装了带有 Conducent"adbot"的共享软件。Conducent"adbot"是为共享软件显示广告服务的。使用这种服务的一种流行的软件是 Pkware。有人试验：阻断这一外向连接不会有任何问题，但是封掉 IP 地址本身将会导致 adbots 持续在每秒内试图连接多次而导致连接过载：

机器会不断试图解析 DNS 名—ads.conducent.com，即 IP 地址 216.33.210.40；216.33.199.77；216.33.199.80；216.33.199.81；216.33.210.41。（译者：不知 NetAnts 使用的 Radiate 是否也有这种现象）

27374Sub-7 木马(TCP)

参见 Subseven 部分。

30100NetSphere 木马(TCP)

通常这一端口的扫描是为了寻找中了 NetSphere 木马。

31337BackOrifice“elite”

Hacker 中 31337 读做“elite”/ei 'li:t/（译者：法语，译为中坚力量，精华。即 3=E,1=L,7=T）。因此许多后门程序运行于这一端口。其中最有名的是 BackOrifice。曾经一段时间内这是 Internet 上最常见的扫描。现在它的流行越来越少，其它的木马程序越来越流行。

31789Hack-a-tack

这一端口的 UDP 通讯通常是由于"Hack-a-tack"远程访问木马（RAT,RemoteAccessTrojan）。这种木马包含内置的 31790 端口扫描器，因此任何 31789 端口到 317890 端口的连接意味着已经有这种入侵。（31789 端口是控制连接，317890 端口是文件传输连接）

32770~32900RPC 服务

SunSolaris 的 RPC 服务在这一范围内。详细的说：早期版本的 Solaris（2.5.1 之前）将 portmapper 置于这一范围内，即使低端口被防火墙封闭仍然允许 Hacker/cracker 访问这一端口。扫描这一范围内的端口不是为了寻找 portmapper，就是为了寻找可被攻击的已知的 RPC 服务。

33434~33600traceroute

如果你看到这一端口范围内的 UDP 数据包（且只在此范围之内）则可能是由于 traceroute。参见 traceroute 部分。

41508Inoculan

早期版本的 Inoculan 会在子网内产生大量的 UDP 通讯用于识别彼此。参见

http://www.circlemud.org/~jelson/software/udpsend.html

http://www.ccd.bnl.gov/nss/tips/inoculan/index.html

(二）下面的这些源端口意味着什么？

端口 1~1024 是保留端口，所以它们几乎不会是源端口。但有一些例外，例如来自 NAT 机器的连接。参见 1.9。

常看见紧接着 1024 的端口，它们是系统分配给那些并不在乎使用哪个端口连接的应用程序的“动态端口”。

ServerClient 服务描述

1-5/tcp 动态 FTP1-5 端口意味着 sscan 脚本

20/tcp 动态 FTPFTP 服务器传送文件的端口

53 动态 FTPDNS 从这个端口发送 UDP 回应。你也可能看见源/目标端口的 TCP 连接。

123 动态 S/NTP 简单网络时间协议（S/NTP）服务器运行的端口。它们也会发送到这个端口的广播。

27910~27961/udp 动态 QuakeQuake 或 Quake 引擎驱动的游戏在这一端口运行其服务器。因此来自这一端

口范围的 UDP 包或发送至这一端口范围的 UDP 包通常是游戏。

61000 以上动态 FTP61000 以上的端口可能来自 Lin

uxNAT 服务器（IPMasquerade）

三、我发现一种对于同一系列端口的扫描来自于 Internet 上变化很大的源地址这通常是由于“诱骗”扫描（decoyscan），如 nmap。其中一个是攻击者，其它的则不是。

利用防火墙规则和协议分析我们可以追踪他们是谁？例如：如果你 ping 每个系统，你就可以将获得的 TTL 与那些连接企图相匹配。这样你至少可以哪一个是“诱骗”扫描（TTL 应该匹配，如果不匹配则他们是被“诱骗”了）。不过，新版本的扫描器会将攻击者自身的 TTL 随机化，这样要找出他们回更困难。

你可以进一步研究你的防火墙记录，寻找在同一子网中被诱骗的地址（人）。你通常会发现攻击者刚刚试图对你连接，而被诱骗者不会。

四、特洛伊木马扫描是指什么？

特洛伊木马攻击的第一步是将木马程序放置到用户的机器上。常见的伎俩有：

1)将木马程序发布在 Newsgroup 中，声称这是另一种程序。

2)广泛散布带有附件的 E-mail

3)在其 Web 上发布木马程序

4)通过即时通讯软件或聊天系统发布木马程序（ICQ,AIM,IRC 等）

5)伪造 ISP（如 AOL）的 E-mail 哄骗用户执行程序（如软件升级）

6)通过“文件与打印共享”将程序 Copy 至启动组

下一步将寻找可被控制的机器。最大的问题是上述方法无法告知 Hacker/Cracker 受害者的机器在哪里。因