 3.2 Strobe（超级优化TCP端口检测程序） strobe是一个TCP端口扫描器，它可以记录指定机器的所有开放端口。strobe运行速度快（其作者声称在适中的时间内，便可扫描整个一个国家的机器）。 strobe的主要特点是，它能快速识别指定机器上正在运行什么服务。strobe的主要不足是这类信息是很有限的，一次strobe攻击充其量可以提供给"入侵者"一个粗略的指南，告诉什么服务可以被攻击。但是，strobe用扩展的行命令选项弥补了这个不足。比如，在用大量指定端口扫描主机时，你可以禁止所有重复的端口描述（仅打印首次端口定义）。其他选项包括：■定义起始和终止端口 ■定义在多长时间内接收不到端口或主机响应，便终止这次扫描。 ■定义使用的socket号码 ■定义strobe要捕捉的目标主机的文件 在获得strobe的同时，必然获得手册页面，这对于Solaris 2.3是一个明显的问题，为了防止发生问题，必须禁止使用getpeername()。在行命令中加入-g标志就可以实现这一目的。同时，尽管strobe没有对远程主机进行广泛测试，但它留下的痕迹与早期的ISS一样明显，被strobe扫描过的主机会知道这一切（这非常象在/var/adm/messages文件中执行连接请求）。3.3 SATAN（安全管理员的网络分析工具） SATAN是为UNIX设计的，它主要是用C和Perl语言编写的（为了用户界面的友好性，还用了一些HTML技术）。它能在许多类UNIX平台上运行，有些根本不需要移植，而在其他平台上也只是略作移植。 在Linux上

运行SATAN有一个特殊问题，应用于原系统的某些规则在Linus平台上会引起系统失效的致命缺陷；在tcp-scan模块中实现0select()调用也会产生问题；最后要说的是，如果用户扫描一个完整子网，则会引进反向fping爆炸，也即套接字（socket）缓冲溢出。但是，有一个站点不但包含了用于Linux的、改进的SATAN二进制代码，还包含了diff文件。SATAN用于扫描远程主机的许多已知的漏洞，其中包括但并不限于下列这些漏洞： ■FTPD脆弱性和可写的FTP目录 ■NFS脆弱性 ■NIS脆弱性 ■RSH脆弱性 ■Sendmail ■X服务器脆弱性 SATAN的安装和其他应用程序一样，每个平台上的SATAN目录可能略有不同，但一般都是/satan-1.1.1。安装的第一步（在阅读了使用文档说明后）是运行Perl程序reconfig。这个程序搜索各种不同的组成成分，并定义目录路径。如果它不能找到或定义一个浏览器。则运行失败，那些把浏览器安装在非标准目录中（并且没有在PATH中进行设置）的用户将不得不手工进行设置。同样，那些没有用DNS（未在自己机器上运行DNS）的用户也必须在/satan-1.1.1/conf/satan.cf中进行下列设置：$dont_use_nslookuo=1；在解决了全部路径问题后，用户可以在分布式系统上运行安装程序（IRIX或SunOS），我建议要非常仔细地观察编译，以找出错误。 SATAN比一般扫描器需要更多一些的资源，尤其是在内存和处理器功能方面要求更高一些。如果你在运行SATAN时速度很慢，可以尝试几种解决办法。最直接的办法就是扩大内存和提高处理器能力，但是，如果这种办法不行，我建议用下面两种方法：一是尽可能地删除其他进程；二是把你一次扫描主机的数量限制

在100台以下。最后说明的一点是，对于没有强大的视频支持或内存资源有限的主机，SATAN有一个行命令接口，这一点很重要。 3.4 Jakal Jakal是一个秘密扫描器，也就是就，它可以扫描一个区域（在防火墙后面），而不留下任何痕迹。 秘密扫描器工作时会产生"半扫描"（half scans），它启动（但从不完成）与目标主机的SYN/ACK过程。从根本上讲，秘密扫描器绕过了防火墙，并且避开了端口扫描探测器，识别出在防火墙后面运行的是什么服务。（这里包括了像Courtney和GAbriel这样的精制扫描探测器）。