UNIX 系统的安全管理策略和措施

严云洋 （淮阴工业专科学校计算机系 223001）

摘要：Unix 是一种被广泛应用的网络操作系统，但在使用中发现它存在安全漏洞。本文就此提出了 Unix 系统的安全防范策略及安全管理工具和保护措施。

关键词：Unix 网络安全 安全管理 策略 措施

一、引言

随着计算机网络技术的发展，网络系统已进入政治、经济、文化、军事等各领域，对网络安全性的要求也越来越高，良好的安全功能是保证用户利益的重要前提。网络操作系统（NOS—Network Operating System）用于管理计算机网络中的各种资源，实现资源共享，并为网络用户提供所需的各种服务，保证系统顺利地运行。因此 NOS 的安全性是网络安全的根本，实现网络系统的安全可靠，首先必须保证 NOS 的安全。目前流行的 NOS 有 Unix、NetWare、WindowsNT、Linux 等。本文分析了 Unix 采用的安全机制，指出了它可能存在的安全漏洞，提出了相应的安全防范策略和安全保护措施，然后给出了某些安全管理及安全保护工具软件及其在 Internet 上的下载地址。

二、Unix 系统的基本安全机制

在 Unix 系统中提供了用户帐号、文件系统权限和日志文件等基本的安全机制，这些安全机制存在一定的安全漏洞。

1. 用户帐号

用户帐号是用户的身份标志，最简单的形式就是用口令。在 Unix 系统内部，与用户帐号（用户口令）有关的信息，一般存储在 /etc/passwd 文件中。若非法用户获得了 /etc/passwd 文件，即使口令被加密成密文，但若安全强度不高，非法用户也可以采用“字典攻击”等方法获得用户口令。

2. 文件系统权限

文件系统的安全主要是通过设置文件的权限来实现的。每一个 Unix 的文件和 Unix 目录都有 3 个允许的比特位设置，分别定义文件的所有者、分组和其他人的使用权限，如只读、可写、可执行、允许 SUID、允许 SGID 等。需注意的是，权限为 SUID 和 SGID 的可执行文件，在程序运行中，会给进程赋予所有者的权限，若被入侵者利用，就会留下隐患，给入侵者的入侵提供了方便。

3. 日志文件

日志文件用来记录操作系统的使用状况。在 Unix 中比较重要的日志文件有：

（1）/user/adm/lastlog 文件：记录每个用户最后登录的时间，包括成功的和未成功的。这样用户每次登录后只要查看一下所用帐号的最后登录时间，就可以确定是否被盗用。

（2）/etc/utmp 和 /user/adm/wtmp（或 /etc/wtmp）文件：utmp 文件记录当前登录到系统的用户，wtmp 文件则同时记录用户的登录和注销。

（3）/user/adm/acct 文件：记录每个用户运行的每个命令，也称为系统记帐。

三、Unix 系统的安全防范

Unix 系统一开始就是一种开放式体系结构，紧密集成了通信服务，故存在一定的安全漏洞，因此会受到网络上非法用户的攻击，给系统造成一定的损失，但是只要系统采用一定的安全保护措施，完全可以大大提高 Unix 系统的安全性。也就是说必须要加强安全防范，特别是要针对一些可能的网络攻击，采取必要且相应的保护措施。

1. 网络攻击类型

（1）拒绝服务（Denial - of - Service）。网络入侵者采用具有破坏性的方法阻塞目标网络的资源，使网络暂时（或永久）瘫痪。比如黑客使用伪造的源地址发出 TCP / IP 请求从而使系统瘫痪。

（2）猛烈攻击（Brute - force attack）。这种攻击的目的是为了破译口令和加密的信息资源，如果使用一个高速处理器，入侵者可以利用各种口令组合（或者加密密钥），直到最终找到正确口令，并打开网络资源为止。这种方法通常涉及到字典攻击。

（3）社会工程攻击（Social - engineering attack）。这种攻击也许是最难防备的一种攻击方式。网上黑客呼叫用户，并装扮成技术支持人员，从而向他们索要用户的口

令。这是最简单也是最有效的一种攻击方式。

(4)被动攻击(Passive attack)。非法用户通过探测网络布线等方法,收集敏感数据或者认证信息,以便日后访问其他资源。

2. 网络安全防范策略

许多事例表明对网络的攻击既有非法用户,也有合法用户,因此既要防范外部攻击,也要加强内部保护。可实施以下策略。

(1)加强用户权限管理。为了保护 Unix 资源,首先要做的事就是采用最小权限方法,也就是给用户只授予他们完成特定任务所必需的服务器访问权限。实现方法是给用户帐户设置最小的许可权,这需要建立一个用户请求文件和资源访问许可权的程序,要求用户指定要处理的任务、任务的持续时间等。

(2)加强口令管理和更新。口令是较容易出现问题的地方,即使被加密,也容易受到"猛烈攻击"。因此,一方面要强制使用安全口令(使用非字母数字字符,如 + | } # % * @等符号,大小写字母混用,规定最小长度 - 不少于 6 位等),使用强加密算法;另一方面要主动定期使用检查程序(如 Crack - 在 Internet 上可容易得到的一个程序,用于对用户口令进行字典攻击) 检查口令是否安全,也就是对/etc/passwd 文件运行检查程序。若口令不安全,需及时更换口令。还可以采用一定的技术手段,增加字典攻击的难度,如改变加密算法(如 Unix 中的 crypt (3)算法)中的加密参数,然后加密口令,这样除非攻击者同样改变了此参数,否则就得不到正确的结果。Crack 可以在 ftp://ftp.cert.org/pub/tools/crack/处下载。

(3)建立健全广泛的记录和监视机制。对网络的运行过程进行记录和监视,以便记录可疑的网络活动,阻止以后的入侵者侵入系统。更为重要的是,还可以跟踪甚至识别成功的侵入系统的入侵者。

(4)设置防火墙。将网络内部分为多个子网,可以阻止或延缓入侵者的入侵。在内部网络与外部网络的接口处,可以设置防火墙,从而提高内部网络的安全系数。

(5)定期进行安全审查。Unix 系统安全是变化的,没有固定的模式,所以网络保护也应该是动态的。作为 Unix 系统的管理员也要尝试定期攻击 Unix 服务器,这样既可以分析和探索别人攻击的思维方式,又可以发现安全保护机制中存在的潜在问题。

(6)制定相应的灾难恢复计划。没有一种安全策略是十全十美的,因此有必要制定相应的灾难恢复计划,以便在受到恶意攻击以后,采取相应的对策,尽可能减少损失。

3. 加强网络服务安全的手段和工具

(1)使用记录工具,记录对 Unix 系统的访问。大多数现成的 Unix 应用可以通过 Syslog 记录事件,这是 Unix 的集中记录工具。可以每天扫描记录文件/var/adm/messaged,并可配置 Syslog 以便把高优先级的事件转送给有关人员处理。另一个有用工具是 TCP Wrappers,这是一种免费的安全工具,可以解决 Unix 网络安全中的监视和过滤问题。其监视功能非常有用,所有 TCP 连接试图(无论是成功的还是不成功的),都可以记录到一个文本文件里,具体内容包括源地址、目的地址、TCP 端口和请求时间等。可通过监视 TCP Wrappers 的记录,查看未遂连接试图,并可以通过配置,由 TCP Wrappers 来根据某些因素,如源或目的 TCP 端口、IP 地址等接受或者拒绝 TCP 连接。下载 TCP Wrappers 的地址:ftp://ftp.win.tue.nl/pub/security。

(2)Telnet 服务。由于用 Telnet 登录时,用户名和口令是明文传输,这就可能被网上 其他用户截获。入侵者也常常使用 Telnet 对系统发动猛烈攻击。入侵者可较容易地编写一个脚本,通过破译不同的口令来试图和远程服务建立 Telnet 连接。因此可以使 Telnet 精灵进程在多次连接试图失败之后产生一定的延迟,延迟时间应和未遂的注册次数成正比,从而防止入侵。还有一种加强 Telnet 服务口令安全的方法,就是每次使用不同的口令,这可通过 S/KEY 工具实现。S/KEY 系统建立在一次性口令基础之上,然后生成一系列口令,用户可以使用这些口令远程访问 Unix 服务器,且不需要特殊的客户机软件。S/KEY 的认证算法使得入侵者无法预测下一个口令内容。S/KEY 的信息可以访问 http://yak.net/skey/。

(3)NFS(Network File System)服务。允许工作站通过网络共享一个或多个服务器输出的文件系统。早期的 NFS 协议使用 RPC(Remote Procedure Call)设施进行客户机 - - 服务器数据交换。问题是用户不经登录就可以阅读或者更改存储在 NFS 服务器上的文件,使得 NFS 服务器很容易受到攻击。为此,要确保基于 Unix 的所有 NFS 服务器支持 Secure RPC。与传统的 RPC 不同的是,Secure RPC 使用 DES (Data Encryption Standard)加密算法和指数密钥交换(exponential key exchange)技术验证每个 NFS RPC 请求的身份。其具体工作方式是:当用户登录到某台工作站,login(或 rlogin)程序从 NIS(Network Information System)数据库获得一个记录。其中共包含了三项内容:用户名、用户公钥,以及用于口令加密的用户私钥。然后使用用户提供的口令解密获得其私钥(在 Secure RPC4.1 以上版本中,私钥被保存在内存中的 Keyserver 进程中)。接着,工作站和服务器用自己的私钥和对方的公钥产生一个 Session Key 。此后,工作站随机产生一个 56 位的 Conversation key ,用 Session Key 加密后传给服务器。在随后的登录过程中,均使用 Conver-

sation key 进行加密。在数据传输过程中,服务器通过以下的推理确认用户身份:用户传送的包是用 Conversation Key 加密的;只有知道用户的私钥才能产生 Conversation Key;只有知道用户的口令才能解开加密的私钥。使用 NFS,还应注意以下几点:尽可能以只读方式输出文件系统;仅将必须输出的文件系统输出给需要访问的客户;不要输出本机的可执行文件,或仅以只读方式输出;不要输出所有人都可以写的目录;不要输出用户的 home 目录;将需要保护的文件的 owner 设为 root,权限设为 755(或 644),这样即使工作站上的 root 帐号被攻破,NFS 服务器上的文件仍能受到保护;可使用 fsirand 程序,增加伪造文件句柄的难度,使用方法是

Umount/dev/hdl

Fsirand/dev/hdl

(4)NIS(Network Information System)服务。这是一个分布式数据系统,它使计算机能够通过网络共享 password 文件、group 文件、主机表和一些类似的资源。通过 NIS 和 NFS,整个网络中所有工作站的操作就好象在使用单个计算机系统,而且其中过程对用户是透明的。但在 NIS 系统中,用户可以编写程序模仿 ypserv 响应 ypbind 的请求,从而获取用户的口令。因此,NIS 客户最好使用 ypbind 的 secure 选项,不接受非特权端口(即端口号小于 1024)的 ypserv 响应。

5. FTP 服务。与 Telnet 类似,用户名和口令也是明文传输,为此可以修改/etc/ftpusers 文件,指定不允许通过 ftp 进行远程登录的用户。使用匿名 ftp 服务,任何人都可以随意注册并下载(有时还可以上载)文件,如果不需要匿名 ftp 服务,可把 username ftp 从/etc/passwd 文件里删除掉;如果必须提供匿名 FTP 服务,要把它安装在本网络之外的机器,这个地方一般称为停火区(DMZ)

(6)POP—3 服务。因为邮件用户的口令是按明文方式传送到网络里,入侵者可很容易截获到用户名/口令,并用于非法访问很多网络资源。解决的方法是安装支持 Authenticated POP(APOP)命令的 POP－3 服务器。APOP 是 POP－3 命令集的最新扩展,用户可以在把口令发送到服务器之前,采用对时间很敏感的单向加密功能,加密口令,因而不采用明文方式发送口令。支持 APOP 命令的 Unix POP－3 精灵进程,可在 http://eudora.qualcomm.com/free/servers.html 下下载,是免费的。

(7)Sendmail 服务。旧版本的 Sendmail 邮件传输代理存在安全漏洞。检查 Sendmail 是否存在安全漏洞的方法是:先 Telnet 到 smpt 端口,即 telnet localhost smpt,成功后键入 wiz、debug、kill 命令。解决的方法最好是安装并配置 Sendmail 分发站分发的最新版本的 Sendmail,下载地址 http://www.sendmail.org。也可以使用 Qmail 来替代 Sendmail,Qmail 是最新的易于配置的邮件传输代理。它支持 Sendmail 的大多数功能。Qmail 下载地址:http://www.qmail.org。

(8)WWW 服务。Web 安全必须关注,要加强 HTTP 服务器的安全保护。无论使用哪种 HTTP 服务器,都要特别留意 Common Gateway Interface(CGI)脚本。这些脚本是可执行程序,一般位于服务器的 CGI－BIN 目录下。在配置 Web 服务器时,要确保可执行脚本只保存在此目录里,从而可以加强脚本安全。可在 http://www.apache.org 下载最新版本的 Apache 服务器软件。

(9)finger 服务。使用 finger 命令,可以查看本地或远程系统中的当前登录用户的详细信息。但这也为入侵者提供了成功入侵的机会。因此,最好禁止使用 finger。

(10)安全的远程访问的工具 SSH。SSH(Secure Shell)软件包的安全性强于 Telnet,它具有强力远程主机认证机制,因而可以降低入侵者通过 DNS 或者 IP 地址欺骗手段模仿客户机的可能性。SSH 还支持多种端到端加密协议,如 DES,Triple－DES,IDEA 和 Blowfish 等,从而有利于进一步保证整个通信的安全。IETF 正在定义 SSH 的第二个版本,它将成为通过不安全的公共网络进行远程安全注册的 Internet 标准。使用 SSH 时应禁用 Telnet 和 Rlogin 服务。SSH 软件包可免费下载,下载地址:http://www.ssh.fi/。

四、结束语

针对 Unix 服务器采取适当的安全保护措施可以降低风险,但不能彻底消除安全隐患,这是因为 Unix 是一种非常复杂的操作系统,再加之 Unix 操作系统的广泛使用,也使得 Unix 成为了被研究得最透彻的操作系统。而入侵者发动的攻击也是极其复杂的,故保护 Unix 系统安全的关键是制定切实可行的安全防范策略,并使安全措施多样化,在加固 IP 级安全(如安装 IP 包过滤防火墙)之后,还要加固传输(TCP)层和应用层的安全。

参考文献

[1] Simson Garfinkel, Gene Spaffor. 实用 UNIX 和 Internet 安全技术. 王启智,申功迈,单和平等译. 北京:电子工业出版社,1999.1

[2] 龚俭. 计算机网络安全概论. 南京:东南大学计算机系,1997.10

(来稿时间:1999 年 5 月)