第 19 卷第 4 期　　广西科学院学报　　Vol. 19, No. 4
2003 年 11 月　　Journal of Guangxi Academy of Sciences　　November 2003

浅谈基于主机的网络安全管理

Brief Introduction to Security Management of Network Based on Host

罗　程

Luo Cheng

（广西大学信息网络中心　南宁　530004）

(Centre of Information & Network, Guangxi University, Nanning, 530004)

摘要　从 UNIX 服务器安全管理的角度，基于主机的日常安全管理应采用基本安全措施、系统访问 IP 过滤措施、入侵检测系统、MD5加密算法加解密和 AIDE 检查系统等技术手段。文中以广西大学校园网为例，介绍网络服务器的主要安全设置。

关键词　网络安全　入侵检测　AIDE

中图法分类号　TP393.08

Abstract　To protect UNIX server from network intrusion, some security methods including the basic security, IP filter, intrusion detection system, Message-Digest Algorithm 5 and Advanced Intrusion Detection Environment are introduced. The major security settings for network server is also introduced with the example of campus-wide network in Guangxi University.

Key words　network security, intrusion detection, AIDE

随着网络应用的不断深入，网络安全这一课题日益呈现出其重要性。现成的黑客工具越来越多，功能也越来越完备，使得完成攻击的操作不断简化，所需的时间大幅度缩短。攻击者利用操作系统或应用程序的漏洞、网络设置的不当、开放的端口、容易猜测的口令、一些可以获取系统信息却没有及时被屏蔽的系统命令、系统缓冲区溢出等等各种各样的手段方法获得管理权限，并且破坏系统日志，使系统管理员不能通过日志审计获得入侵信息。这种潜在的威胁是非常可怕的，必须采取有力的措施保护自己的网络和机器免受侵扰。本文从 UNIX 服务器安全管理的角度出发，讨论了一些必要的安全防范的技术手段。

1　基本的安全措施

据统计，一半以上的安全问题出自于系统内部管理的漏洞，即绝大部分安全漏洞是系统管理员的操作失误或遗漏导致的，也就是说许多毛病可以通过管理的角度来防止。首先，尽可能快的安装系统厂商提供的升级补丁，许多的补丁是针对系统安全方面的 Bug 的。仔细检查 inetd 提供的服务，去除一些不必要的服务程序，尤其是显示过多系统信息的程序，如 finger

2003-01-20 收稿，2003-04-02修回。

等；尽可能关闭服务对 RPC 的支持，防止远程攻击；严格控制用户对系统的使用权限，避免使用简单易猜的密码；对 TELNET、FTP 等服务器使用 SSH 提供的安全通道；修改系统用户执行程序堆栈参数，防止缓冲区溢出等等。

2　系统访问 IP 过滤

基于主机访问的 IP 过滤，实际上就是构建软件防火墙。针对进、出服务器 IP 数据包提供的过滤功能，有效抑制非授权网段的访问和一些特别指定协议的控制。系统管理员可以使用如 IP-Filter 类型的防火墙软件，根据需要设置一个进、出的过滤规则列表，对进、出该主机的 IP 包队列进行检查。系统按照既定的过滤规则对 IP 包进行匹配。过滤规则可针对具体的 IP、网段，可针对协议、协议的某些关键字，或者针对具体某个端口设置。同时，过滤规则中还可以设置对过滤情况进行记录，形成日志。系统管理员借助该日志可以分析和统计 IP 包的进出情况。

3　入侵检测系统

入侵检测就是通过对系统数据的分析，发现非授权的网络访问和攻击行为，随之定位入侵，达到控制和防止入侵的目的。

3.1　入侵检测系统的分类

入侵检测的首要问题就是从哪里提取包含入侵信息的数据。入侵检测系统根据其提取入侵数据的入口点分为基于网络的入侵检测和基于主机的入侵检测。

（1）基于网络的入侵检测。从网上提取数据，可以对一个子网进行检测，也可对多个子网协同检测，对通信数据进行监听、采集。这种方法获取的信息量大，实时性高，但原始的信息包居多，分析量大，主要针对对象是 IP 欺骗、DNS 欺骗、sniffer 攻击等利用网络协议攻击的行为。基于网络的入侵检测系统已经成为众多网络公司研究开发的一个重要产品。

（2）基于主机的入侵检测。从单个主机上提取数据，仅是针对本机系统内部的信息，直接面向操作系统和应用层，对系统日志等审计记录进行监视、分析，效率较高，判断的准确性也高，主要针对利用操作系统和应用程序的漏洞及运行特征进行的攻击行为。

3.2　基于主机的入侵检测系统的结构

基于主机的入侵检测系统机构由3个部分组成。

（1）信息采集模块。需采集的信息包括操作系统、应用系统、网络配置，来源为各种系统和网络的日志文件，系统中稳定的目录和文件配置部分，等等。其中关键在于所收集到的信息的可靠性和正确性。

（2）信息分析模块。对由信息采集模块采集回来的信息进行相应的分析比较。有3种方法：模式匹配，统计分析和完整性分析。其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。完整性分析利用强有力的加密机制称为消息摘要函数（如 MD5）。它能识别哪怕是微小的变化。完整性分析主要关注某个文件或对象是否被更改。

（3）反应模块。对上述采集、分析后的结果作出相应的反应。

4　MD5加密算法

MD5的全称是 Message-Digest Algorithm 5（信息－摘要算法），它的作用是让大容量信息

在用数字签名软件签署私人密钥前被“压缩”成一种保密的格式。

MD5算法具体来说是对输入的数据进行补位，确保信息的字节长度加上448后能被512整除。然后，一个以64位二进制表示的信息的最初长度被添加进来。信息被处理成512位的迭代结构区块，每一区块又被划分为16个32位子块，经过了一系列的处理后，算法的输出由4个32位区块组成，将这4个32位区块级联后将生成一个128位散列值，也就是人们常说的 MD5信息摘要。

任意文件经过 MD5（信息摘要）计算都会产生一个唯一的128位的报文摘要，当文件发生改变时，这个报文摘要也会随之改变。利用 MD5这个特性，可以对一个文件进行一致性和完整性校验。MD5将整个文件当作一个文本信息，通过其不可逆的字符串变换算法，产生了这个唯一的 MD5信息摘要。如果在以后传播这个文件的过程中，无论文件的内容发生了任何形式的改变（包括人为修改或者下载过程中线路不稳定引起的传输错误等），只要对这个文件重新计算 MD5时就会发现信息摘要不相同，由此可以确定文件已经不正确。

MD5被广泛地用于加密和解密技术上。比如现在网上发布的许多软件源码都会带上自己的 MD5信息摘要，下载后经校验确认它没被更改或传输正确。MD5被普遍地应用到系统完整性校验系统中，查看系统是否已经被黑客攻破并修改了系统源文件和留下后门。

5 高级入侵检测环境 AIDE

AIDE（Adevanced Intrusion Detection Environment，高级入侵检测环境）是一个基于主机的入侵检测工具，主要通过校验系统文件的完整性，查看系统是否被黑客攻破而且更改了系统源文件和留下后门。这类系统完整性校验系统软件中，最著名的是 Tripwire。AIDE 不仅扩展了 Tripwire 的功能，而且是一个开放的、不断完善的免费软件。

用 AIDE 能够构造一个指定文件的校验数据库，并且是一个可压缩加密的数据库文件。在 AIDE 的配置文件 aide.conf 中指定系统中哪些目录、文件需要生成校验码，最后生成校验码数据库文件。AIDE 数据库能够保存指定文件的各种属性，包括：权限（permission）、索引节点序号（inode number）、所属用户（user）、所属用户组（group）、文件大小（size）、最后修改时间（mtime）、创建时间（ctime）、最后访问时间（atime）、增加的大小以及连接数。AIDE 除了前面所提的 MD5算法还能够使用 SHA1、RMD160、TIGER 等算法，并以密文形式建立每个文件的校验码或散列号。

在系统安装完毕，要连接到网络上之前，系统管理员应该建立新系统的 AIDE 数据库。这第一个 AIDE 数据库是系统的一个快照和以后系统升级的准绳。数据库应该包含一些关键信息：系统的二进制可执行程序、动态连接库、头文件以及其它稳定的文件，比如/dev。这个数据库不应该保存那些经常变动的文件信息，例如：日志文件、邮件 spool、/proc 文件系统、用户起始目录以及临时目录。

系统管理员可以设置系统定期检验系统的一致性，即使用 AIDE 按同一个 aide.conf 配置生成当前的验证码库并与一开始建立的验证码库相比较，产生多等级的比较报告，并通过系统地分析报告来判断系统是否正常。

6 广西大学校园网服务器的主要安全设置

广西大学校园网建设从自身的规模、用户数量以及安全性等角度出发，一开始就选择了

通信处理性能较高、安全性较好的SUN公司的中小型服务器，如SUN Enterprise 250和SUN Ultra 10等。SUN的服务器均配备了自己的Solaris操作系统。根据服务器的应用划分，我们把服务器主要分成2个部分，一部分是对外开放的，如提供DNS、WWW的服务器，另一部分是主要对内服务的，如校园OA、FTP、VOD、出国代理等的服务器。在这两部分之间使用了硬件防火墙进行隔离。

对于对外开放的服务器，由于没有硬件防火墙的保护，其基于主机自身的安全保护更显得极为重要。除了上述提到的最基本的安全措施外，我们为服务器加设了软件放火墙IP－Filter，并根据服务器提供的服务来设置IP包进、出过滤规则。比如DNS服务器，除必须对内外开放的DNS协议外，有选择的对其他协议和端口进行阻塞。如针对TELNET协议和ICMP协议，除网管中心地址段外，其余地址一律被阻止进入服务器。

虽然已经安装了基于网络的入侵检测系统，但由于必须分析处理的信息量太大，分析报告并不能马上产生。并且这种基于网络的入侵检测系统对网络内部发生的所有类型的异常都进行报告，系统管理员的工作并不轻松。广西教科网省网的FTP服务器曾经被黑客盗用用户密码入侵。黑客使用ROOTKIT进行系统入侵，一般会将一些系统工具，比如ls、ps、netstat以及who等替换掉，使入侵的文件、进程等信息都被掩藏起来，甚至修改系统日志，使系统管理员不能通过日常的工具发现自己的系统异常或已经被开了后门。对于用户密码被盗用的问题，基于网络的入侵检测系统也较难发现。所以有必要对于主要服务器安装完整性校验系统。

安装了AIDE，设置系统定期检验系统的一致性，运行AIDE检查，并使用邮件形式把分析比较的报告发送给系统管理员。根据前面所提MD5算法的特点，假冒某个文件的一个加密校验码将非常的困难了，更不要说假冒所有AIDE支持的校验码了。如果系统被侵入，系统管理员只要通过运行AIDE检查，就能够很快判断并识别出哪些关键文件被攻击者修改过。把黑客较有可能修改的系统可执行程序文件，比如供系统管理员用来检查系统进程（ps）、使用空间（df）、用户登陆情况（who）等命令文件做一个专门的校验码数据库，可以减少校验码库比较时的服务器的开销，同时也可以增加检查的次数。

为防范入侵者修改AIDE的执行文件和校验码数据库，把AIDE的数据库放到有硬件放火墙保护的其他服务器上，这样在进行检查时也确保AIDE的执行文件没有被修改。

7　结束语

由于网络技术的不断进步，网络攻击者攻击的角度、攻击能力也不断的发展变化，必然要求各种网络安全技术不断发展和不断完善。不论是网络服务器的日常安全维护，还是以网络入侵检测系统进行辅助，也必然要求系统管理员的工作更加小心谨慎，并综合多种方法，从各个方向把好安全大门。

参考文献

1　王　锐. 网络最高安全技术指南. 北京：机械工业出版社，1998.

2　Terry Escamilla［美］. 入侵者检测. 吴　焱等译. 北京：电子工业出版社，1999. 3.

3　斯海飞，赵国庆. 入侵检测技术分析概述. 电子对抗技术，2002，17(2)：31～35.

（责任编辑：黎贞崇）