入侵检测系统的探讨

江 嘉
(昆明理工大学 计算中心, 云南 昆明　650051)

摘要: 将论述入侵检测系统的概念及原理, 并探讨怎样利用 UNIX 操作系统自身的日志功能及系统管理员自己编写的软件/脚本进行入侵检测. 为预防和阻止黑客攻击提出了技术建议, 使我们的计算机网络更加安全可靠.

关键词: 入侵检测; 网络; 黑客; 安全
中图分类号:TP393.08　　文献标识码:A　　文章编号: 1007-855X(2003)04-0062-05

Discussion about the Intrusion Detection System

JIANG Jia
(Computer Center, Kunming University of Science and Technology, Kunming 650051, China)

Abstract: The concept and principle of the intrusion detection system are discussed, and the exploration is made into the ways to make use of the built-in journal function of UNIX operating system and the software or script programmed by the system administrators to carry out intrusion detection. In order to prevent hackers from invading the system, the technology suggestions are put forward to make our computer network more reliable.

Key words: intrusion detection; network; hacker; security

0 引 言

虽然计算机网络系统从各方面逐渐完善, 减少非法者的入侵, 但系统难免有缺陷或漏洞. 系统安全是一个连续的过程, 随着新漏洞的出现和服务器应用的变化, 系统的安全状况也在不断变化着. 因此, 再高明的系统管理员也不能保证提供服务的服务器绝对不被入侵.

如今各种黑客资料、入侵工具泛滥成灾, 被攻击的案例也越来越多. 仅仅是被动地防御已经不足以保证自身的安全了. 我们需要一种对潜在的入侵动作作出记录、并预测攻击后果的系统, 入侵检测系统就是这样一种软件. 入侵检测是一种比较新的、还有待增强和完善的技术. 入侵检测技术属于积极主动地安全防护技术, 它提供了对内、外攻击和误操作的实时保护, 在系统受到危害之前拦截入侵.

1 概念及功能

1.1 概 念

入侵检测系统(Intrusion Detection System) 是通过收集系统中的若干关键点信息并进行分析, 达到发现系统中是否有违反安全策略的行为和被攻击的迹象. 入侵检测作为放火墙之后的第二道安全防线, 在不影响系统性能的情况下能对系统进行监测, 从而提供对内部攻击、外部攻击和误操作的实时保护.

1.2 功 能

入侵检测系统可以实现以下功能:

(1) 监控和分析用户以及系统的活动; (2) 核查系统配置和漏洞; (3) 评估关键系统和数据文件的完整性; (4) 识别攻击的活动模式并向网管人员报警. (5) 统计分析异常活动, 识别违反政策的用户活动.

收稿日期: 2002-03-19.

作者简介: 江　嘉(1966.8~), 男, 实验师; 主要研究方向: 计算机网安全. **E-mail:** jianjiaem@163.com

2 功能分类

按照检测的功能不同, 入侵检测系统可以分为以下几类:

1) 网络入侵检测系统(NIDS)

这类入侵检测系统通过对网络中传输的数据包进行分析, 从而发现可能的恶意攻击企图. 例如在不同的端口检查大量的TCP 连接请求, 以此来发现TCP 端口扫描的攻击企图. 网络入侵检测系统既可以运行在监视自己的端口的主机上, 也可以运行在监视整个网络状态的处于混杂模式的 sniffer 主机上.

2) 系统完整性校验系统(SIV)

这类入侵检测系统用来校验系统文件, 查看系统是否被黑客攻破而且更改了系统原文件并留下后门. 系统完整性校验系统不仅可以校验文件的完整性, 也可以对其他组件, 例如 Windows 注册表, 进行校验. 这类软件的缺点是它需要使用者有系统的最高权限, 并且一般没有实时报警功能. 这样, 入侵者既然可以修改系统文件, 也就可以修改系统完整性校验软件, 因此无法保证检测的可靠性.

3) 日志文件分析系统(LFM)

通过分析网络服务产生的日志文件来获得潜在的恶意攻击企图. 和网络入侵检测系统类似, 这类软件寻找回日志中的暗示攻击企图的模式来发现入侵行为. 例如“Swatch”, 它就是通过分析 HTTP 服务器日志文件来寻找黑客扫描 CGI 漏洞的行为.

4) 欺骗系统(DS)

通过模拟一些漏洞并提供虚假服务来设计欺骗入侵者. 这类软件中比较著名的是 Deception ToolKit. 也可以不使用任何软件就达到欺骗黑客的目的, 例如重命名 NT 上的 administrator 账号, 然后设立一个没有权限的虚假账号让黑客来攻击, 一旦他中计, 他的行为就会被记录下来.

3 实现的途径

入侵检测首先要收集各种必要的信息, 然后分析这些信息, 进而发现问题并及时处理.

3.1 收集信息

收集的信息包括系统、网络、数据、用户活动的状态和行为. 信息来自于计算机网络系统中的若干个不同关键点, 并对来自几个信息源的信息进行比较, 将它们的不一致性看作是可疑行为或入侵标识, 从而进一步分析处理.

入侵检测利用的信息一般来自 4 个方面:

1) 系统日志

黑客经常会在系统日志中留下踪迹, 我们可以充分利用系统日志进行入侵检测. 日志文件中记录了各种行为类型, 每种类型又包含不同的信息. 对于不正常的或不期望的行为, 日志中记录的用户活动表现为重复登录失败、登录到不期望的位置以及非授权的企图访问重要文件等等.

2) 目录以及文件中的异常改变

网络环境的文件系统中包含很多软件和数据文件, 其中的一些文件和私有数据文件中包含重要信息, 它们经常是黑客修改或破坏的目标. 检查目录和文件中不期望的改变(如修改, 创建和删除等, 特别是那些正常情况下被限制访问的), 可以判断是否有入侵行为, 至少可能就是一种入侵产生的指示和信号.

3) 程序执行中的异常行为

网络系统上的程序执行用途包括操作系统、网络服务以及一些特定目的, 例如数据库服务器等. 每个执行程序会包括一个以至多个进程, 每个进程执行于具有不同权限的环境中, 这种环境控制着进程可访问的系统资源、程序和数据文件等. 当一个进程出现了不期望的行为时, 这就可能表明黑客正在入侵你的系统.

4) 物理形式的入侵信息

物理形式的入侵包括两个方面内容,一是未授权的对网络硬件连接,二是对物理资源的未授权访问.黑客会设法突破网络的周边防卫,如果他们能够在物理上访问内部网,就能安装他们自己的设备和软件.依此,黑客就知道网上的由用户加上去的不安全(未授权)的设备,然后利用这些设备访问网络.

3.2 数据分析

一般通过3种技术手段进行数据分析,包括模式匹配、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.

1) 模式匹配

将收集到的信息与已知的入侵模式数据进行对比匹配,如果发现有相配信息,就能准确发现违背安全策略的行为(即非法入侵).这就是模式匹配方法,它的一大优点就是只需收集、分析相关的数据集合,能显著减少系统负担,此项技术已相当成熟.

这种技术手段与病毒防火墙采用的方法一样,检测准确率和效率都相当高.但也存在明显的缺点:需要不断的升级以对付不断出现的黑客攻击手段,不能检测到未出现过的黑客攻击手段.因此,对于经常改变攻击手段的黑客来说,模式匹配手段就显得力不从心.

2) 统计分析

首先给系统对象(如用户、文件、目录和设备等)创建一个统计描述,然后统计正常使用时的一些测量属性值(如访问次数、操作失败次数和延时等),将测量的平均值作为参考,与网络系统的行为测量值进行比较,任何系统测量值在参考值范围(可以设定一个上下限值)之外时,就可认为是有入侵发生.

这种统计分析的手段优点是可检测到未知的、更为复杂的入侵.但误报、漏报率比较高,并且不适应用户正常行为的突然改变.

现今主要有基于专家系统的、基于模型推理的和基于神经网络的统计分析方法,它们都属于智能型手段,正处于研究热点并得以迅速发展

3) 完整性分析

完整性分析主要关注某个文件或对象是否被更改,包括文件和目录的内容及属性,它在发现被更改的、被特络伊化的应用程序方面特别有效.其优点是不管模式匹配方法和统计分析方法能否发现入侵,只要是成功的攻击导致了文件或其它对象的任何改变,它都能够发现.但不能实时响应,通常以批处理方式实现.

4 利用系统日志做入侵检测

虽然功能单一的入侵检测系统是系统本身的日志无法替代的,但如果能够充分地利用系统日志,也可以最大程度地对潜在的恶意攻击迹象作出记录和预测.

Unix系统中的重要日志文件

/var/adm是Unix的日志目录(在LLinux下是/var/log).有相当多的ASCII文本格式的日志保存在这里,焦点首先集中在mess%es这个文件,它记录了来自系统级别的信息.但其中大量的日志记录对于我们是无用的.

比如:

Feb 2 14:25:30 1999 unix: Copyrigh(c) 1983~ 1997, Sun Microsystems, Inc.

Feb 2 14:25:30 1999 unix: mem= 262 144K(0×10 000 000)

显示此版权或者硬件信息的记录,而:

Jul 19 23:56:47 www login [28845]: FAILED LOGIN 1 FROM 202.106.111.25,

User not known to the underlying authentication module

则是登录失败的记录.而如果有以下信息:

Jul 19 23: 52: 45 game PAM_pwdb [29509]: (login) session opened for user test by (uid= 0)

则 99% 以上的可能是系统已经被入侵了, 首先应该是 Kill- HUP cat '/var/run/syslogd. ppid'. 但有可能入侵者已经做了, 那样我们将得不到任何有用的信息.

在/var/adm, /var/log, /etc 目录里可以找到名为 wtmp 和 utmp 的文件, 它记录着用户何时, 何地用 telnet 程序连接过主机. 在黑客中流行着一种可抹掉这两个文件中用户登录信息的程序, 但很多入侵者并没有上载或编译这个文件, 管理员要做的就是使用 lastlog 这个命令来获得入侵者上次连接的源地址. 当然, 这个地址有可能是伪造的.

ftp 日志一般是 /var/log/xferlog, 该文本形式的文件详细地记录了以 FTP 方式上传文件的时间、来源、文件名等. 不过由于该日志太明显, 所以稍微高明一些的入侵者就不会使用该方法来传文件, 取而代之的是使用 rep. 你可以用 # cat /var/log/xferlog | grep - v202. 这种方式来查看那些不应该出现的地址.

在获得 root 权限后, 入侵者可以建立他们自己的入侵账号, 更高级的做法是给类似 uucp, lp 等不常使用的系统用户名加上密码. 在遭受入侵后, 即使入侵者删除了. sh_history 或者. bash_hi- story 这样的文件, 只要执行 kill- HUP 'cat/var/rnu/inetd. conf', 即可将保留在内存页中的 bash 命令记录重新写回到磁盘, 然后执行 find / - name. sh_historyprint, 仔细查看每个可疑的 shell 命令日志. 尤其是在 /usr/spool/lp(lp home dir), /usr/lib/uucp/(uucp home dir) 这样的目录下找到. sh_history 文件时.

入侵者在目标机和工作机之间传送文件时为了避免被 syslog, 可能会使用从目标机 ftp 到工作机的方法, 因此在. sh_history 中你有可能发现类似 ftp 111. 222. 333. 444 或者 rep someone@ 111. 222. 333. 444: /tmp/ .../tmp/ ..的显示入侵者的 IP 或域名的命令.

还有一个重要的日志是 http 服务器日志. 这有可能是确定入侵者真实攻击发源地的最有效工具. 以最流行的 apache 服务器为例, 在${prefix}/logs/ 目录下可以发现 access. log 文件, 该文件记载了访问者的 IP, 访问的时间以及请求访问的内容. 在遭受入侵后, 可以在该文件中发现类似下面的语句:

record: 111. 222. 333. 444- - [28/Apr/2000: 00: 28: 05- 0800]"GET/cgi- bin/rguest. exe"404- 111. 222. 333. 444, - - [28/Apr/2000: 00: 28: 57- 0800] "GET/msade/Samples/SELECTOR/showcode. asp" 404-

它表示来自 IP 为 111. 222. 333. 444 的某人在 2000 年 4 月 28 号的 0 点 28 分试图访问/msads/Samples/SELECTOR/showcode. asp 文件, 这是在使用 Web cgi 扫描器后遗留下的日志. 大部分的 Web 扫描器都是基于 MS 操作系统的, 而为了更快的速度, 使用基于* nix 扫描器的入侵者常选择离自己最近的服务器件进行扫描. 结合攻击的时间和 IP, 我们可以知道入侵者的大量信息.

还有就是利用 CoreDump, 这是一种相对较复杂也很有效的方法. 一个安全稳定的守护进程在正常运行的时候不会 dump 出系统的核心. 当入侵者利用远程漏洞攻击时, 许多服务正在执行一个 getpeername 的 socket 函数调用, 因此入侵者的 IP 也保存在内存中, 此时服务溢出, 系统内存页文件被 dump 到 core 文件中, 你可以在一大段杂乱无章的字符中(事实上是一个全局数据库中的进程变量) 去找一个包含有执行此 expoloit 的 IP. 有时也只能找到入侵者远程攻击的部分命令, 而无法找到攻击者的 IP 地址.

代理是大中型企业网常用来作为内外信息交换的一个接口, 它忠实地记录着每一个用户所访问的内容, 当然, 也包括入侵者的访问内容. 以最常用的叫 squid 代理为例, 通常可以在 /usr/local/squid/logs/ 下找到 access. log 这个庞大的日志文件. 由于日志记录添加得很快, 在出现安全问题之前就应该及时备份它, 并通过日志分析脚本对敏感文件访问日志的分析, 知道何人在何时访问了这些本该保密的内容.

默认方式下路由器不会记录任何扫描和登录, 因此入侵者常用它做跳板来进行攻击. 添加路由器的日志记录将有助于日后追踪入侵者. 对于管理员来说, 这样的路由器设置能确定攻击者到底是内贼还是外盗. 同时你需要一台额外的服务器来放置 router. log 文件.

在 Cisco 路由器上:

router (config) # logging faclity syslog

router (config) # logging trap informational

router (config) # logging[服务器名]

在 log server 上:

Ⅰ.在 /etc/syslog.conf 中加入一行:

*.info /var/log/router.log

Ⅱ.生成文件日志文件:

touch /var/log/router.log

Ⅲ.重启 syslogd 进程;

kill- HUP' cat /var/run/syslogd.pid'

对于入侵者来说,在实施攻击的整个过程中不与目标机试图建立 tcp 连接是不可能的,这有许多入侵者的主观原因和一些客观原因,而且在实施攻击时不留下日志也是相当困难的. 如果花上足够的时间和精力,就可以从大量的日志中分析出一些信息. 就入侵者的心理而言,他们在目标机上取得的权限越大,他们就越倾向于以保守的方式来建立与目标机的连接. 仔细分析早期的日志,尤其是包含有扫描的部分,就能有更大的收获.

5 结束语

在实际运用中,系统管理员对专业知识掌握的情况直接关系到他的安全敏感度,只有身经百战而又知识丰富、仔细小心的系统管理员才能从一点点的蛛丝马迹中发现入侵者的影子,扼杀入侵的行动.

参考文献:

[1] http://ciac.llnl.gov/ciac/toolsunixnetmon.html[OL].

[2] ftp://coast.cs.purdue.edu/pub/tools/unix/[OL].

[3] ftp://ftp.cert.dfn.de/pub/tools/audit/logsurfer/[OL].

[4] 赵斌斌. 网络安全与黑客工具防范[M]. 北京: 科技出版社, 2001. 19~116.

[5] [美] 安尼姆斯. 最高安全机密[M]. 朱鲁华译. 北京: 机械工业出版社, 2002. 10.

[6] [美] 安德森. UNIX 技术内幕[M]. 周靖译. 北京: 机械工业出版社, 2002. 10.

[7] [美] 匿名. 网络安全技术内幕[M]. 北京: 机械工业出版社, 1999. 188~196, 235~272.

[8] [美] Ogletree, t. 防火墙原理与实施[M]. 李之棠译. 北京: 电子工业出版社, 2001. 73~115.

[9] Berr Nance. Introduction to Networking, 3rd Edition, 1996.

[10] 王杰红, 李闻天. Win2K Internet Serrer 安全管理系统策略初探[J]. 昆明理工大学学报(理工版), 2002, 27(4): 90.