日志检测技术在计算机取证中的应用

林 英[1],张 雁[2],欧阳佳[1]
(1.云南大学 软件学院,云南 昆明 650091;
2.西南林学院 计算机科学系,云南 昆明 650224)

摘 要:计算机取证是指对计算机入侵、破坏、欺诈、攻击等犯罪行为,利用计算机软硬件技术,按照符合法律规范的方式进行识别、保存、分析和提交数字证据的过程。作为日常安全检测的重要内容和维持系统正常运行不可缺少的工具,日志分析与检测被广泛应用于计算机取证,是评估系统运行状况,检验网络安全策略有效性的必要手段。从日志预解码、日志解码以及日志分析三个方面设计并实现了一个根据日志进行监控及取证的系统。实验结果表明该方法是有效的,能够帮助管理人员及时发现入侵,动态取证。

关键词:计算机取证;入侵检测;日志检测
中图分类号:TP391 **文献标识码**:A **文章编号**:1673-629X(2010)06-0254-03

Application of Log Testing Technology in Computer Forensics

LIN Ying[1],ZHANG Yan[2],OU Yang-jia[1]
(1.School of Software,Yunnan University,Kunming 650091,China;
2.Computer Science Department,Southwest Forestry University,Kunming 650224,China)

Abstract:Computer forensics refers to the process of identification, preservation, analysis and preservation of digital evidence, which use of computer hardware and software technologies and should be in accordance with laws and regulations. As an indispensable tool for maintenance of the running of computer system, log analysis and testing technology is widely used in computer forensics and it is an effective way to assess the status of system operation, to test the effectiveness of network security policy. In this paper, designed and implemented a log monitor system from three aspects of log pre-decoding, decoding, and analysis. The experimental results show that the method is effective and can help administrator to detect system intrusion.

Key words:computer forensics;intrusion detection;log testing

0 引 言

随着信息技术的不断发展,计算机越来越多地参与到人们的工作与生活中,与计算机相关的法庭案例(如电子商务纠纷,计算机犯罪等)也不断出现。一种新的证据形式——存在于计算机及相关外围设备(包括网络介质)中的电子证据逐渐成为新的诉讼证据之一。电子证据本身和取证过程的许多有别于传统物证和取证的特点,对司法和计算机科学领域都提出了新的挑战。作为计算机领域和法学领域的一门交叉科学,计算机取证[1~3](Computer Forensics)正逐渐成为人们研究与关注的焦点,连续几年成为FIRST(forum of incident response and security teams)安全年会的热点。

从技术角度看,目前计算机取证最大的障碍就是证据的真实性、有效性和及时性。因为一方面黑客在攻击目标时,一般都会采用各种手段伪造身份,尽可能销毁各种证据;另一方面犯罪的证据很容易被更改,而有些人可以借此故意扩大自己的损失。因此如何确保收集到的证据是真实的、有效的和及时的,是计算机取证的关键所在,这也正是目前计算机取证面临的主要问题。

在获取证据阶段,日志是一个首要的选择。许多入侵检测系统,也是采取日志作为主要的分析数据源[4~6]。根据产生日志的计算机的不同,通常日志数据被覆盖重写的时间间隔短则几分钟,长则数月。在获取证据阶段,取证人员必须尽快采取行动,否则这些日志可能会永远消失。文中设计并实现了一个根据日志进行监控及取证的系统,希望能够帮助管理人员及时发现入侵,动态取证。

收稿日期:2009-10-19;**修回日期**:2010-01-15
基金项目:云南省教育科研基金(07Y41295)
作者简介:林 英(1973-),女,讲师,研究方向为信息安全、软件工程;张 雁,副教授,研究方向为软件工程。

1　日志分析机制

日志是计算机系统运行轨迹的真实写照,它被广泛用于系统调试、监控和安全检测中。日志管理和分析是系统管理和入侵检测的基础设施,是评估系统运行状况,检验网络安全策略有效性的必要手段,日志分析工具已经成为日常安全检测的重要内容和维持系统正常运行不可缺少的工具[7~9]。

在文中所讨论的系统中,日志分析包含以下三个步骤:

1)日志预解码;2)日志解码;3)日志分析。

日志预解码的目的是从日志中提取一般信息,例如从系统日志头中获取主机名、程序名和时间等信息。

例如,假设 SSHD 日志中新产生了一条 SSHD 消息:

Apr 14 17:32:06 linying sshd[1025]: Accepted password for root from 172.16.29.26 port 1618 ssh2

经解码后,消息中的日期 Apr 14 17:32:06,主机名 linying 以及程序名称 sshd 将被提取出来。

日志解码是为了获得比预解码阶段更为丰富的信息,它是从日志内容中用正则表达式(Regular Expression)标识出某些关键字。在日志解码阶段,一般需要提取源 IP 地址、用户名、ID 号等有用的信息。

例如,依然假设 SSHD 日志中新产生了一条 SSHD 消息:

Apr 14 17:32:06 linying sshd[1025]: Accepted password for root from 172.16.29.26 port 1618 ssh2

经解码后,除了预解码阶段提取的日期、主机名和程序名称外,日志的实质内容 Accepted password for root from 172.16.29.26 port 1618 ssh2,源 IP 地址 172.16.29.26 以及相关联的用户名 root 都将被提取出来。

在日志经过预解码、解码两个阶段后,所有的规则被读入到规则树中。在文中,基于 OSSEC[10,11]的全部 400 多条规则来构造规则树,规则树的大体结构如图 1 所示,图中标号表示节点号。

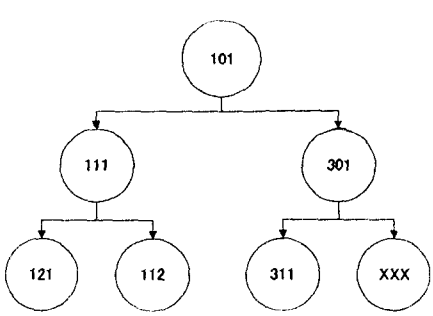

图 1　规则树

规则树构造完毕后,下一步便是匹配的过程。将解码后的事件依次遍历所有的规则,该过程可以看为是对一个树状结构进行查找的过程,例如,有如图 1 所示的规则树,现需要对事件 IF 进行匹配,那么匹配过程可以描述如下:

首先,将事件 IF 与 101 节点比较,若匹配成功,则进入 101 的左节点 111,否则进入其右节点 301。同理,IF 与规则树中的每一个节点进行比较时,匹配成功则进入规则树当前节点的左节点,否则进入其右节点。

倘若找到与之匹配的规则,那么先判断是否要进行忽略操作,若不忽略,那么就执行审计,以有效地追踪攻击,最后判断应该执行何种指令。

2　系统设计

系统的实现,包括系统的初始化,日志的监控,以及日志的分析和匹配。

日志首先要收集才能进行分析,日志收集流程用自然语言描述如下:

1) 从配置文件中读取要监控的日志名及所在路径,并将它们读入一个链表;

2) 遍历链表中的日志,检查当前遍历的日志是否有变动,一旦有变动,则执行 3,否则重复 2;

3) 将日志中新增加的事件发送到事件分析器;

4) 返回 2。

日志分析流程用自然语言描述如下:

(1)初始化规则集,将规则读入一个树状结构中;

(2)初始化解码器,将解码规则也读入一个树状结构中;

(3)等待接收事件,一旦接收到事件,则执行 4;

(4)将接收到的事件用解码器进行解码;

(5)对解码后的事件进行分析,并进行相应处理;

(6)返回 3。

日志分析机制的关键在于日志的匹配与检测,在文中,借鉴了 OSSEC 的框架和利用了 TCT[12](The Coroner's Toolkit)工具包,在 OSSEC 规则库的基础上进行扩展。该规则库由 XML 撰写,用户可以自行对规则进行添加、修改、删除。日志匹配与检测流程用自然语言描述如下:

a. 遍历当前节点,如果匹配则进入其右子树,执行 2,否则进入其左子树,重复 1。如果 2 执行完毕,也进入其左子树,重复 1。

b. 遍历当前节点,如果匹配则记录下当前规则,否则进入其右子树,重复 2。当该子树被遍历完时,返回 1,继续匹配过程。

c. 以上过程进行到整棵规则树被遍历完为止。

3 系统实现

3.1 系统初始化

首先,系统要进行初始化,载入用户之前设置的配置信息,读取入侵规则、解码规则等信息。系统分为两个端:一个是Agent端,一个是Server端。Agent端是分析日志信息的,Server是收集日志信息的。因此,初始化分为两个部分:Server初始化和Agent初始化。

Server初始化分为五个步骤:第一步,读取配置文件;第二步,读取规则文件;第三步,遍历所有规则,初始化规则树;第四步,初始化事件链表;第五步,创建Socket,开始监听。Agent初始化分为二个步骤:第一步,读取本地日志信息;第二步,连接服务器端的Socket。

3.2 记录到日志

Agent和Server都启动之后,系统就会从所监控的日志文件中提取信息进行分析,一旦发现入侵行为就会报警,并写入到入侵日志中。图2是系统从日志信息中分析出来的入侵行为。

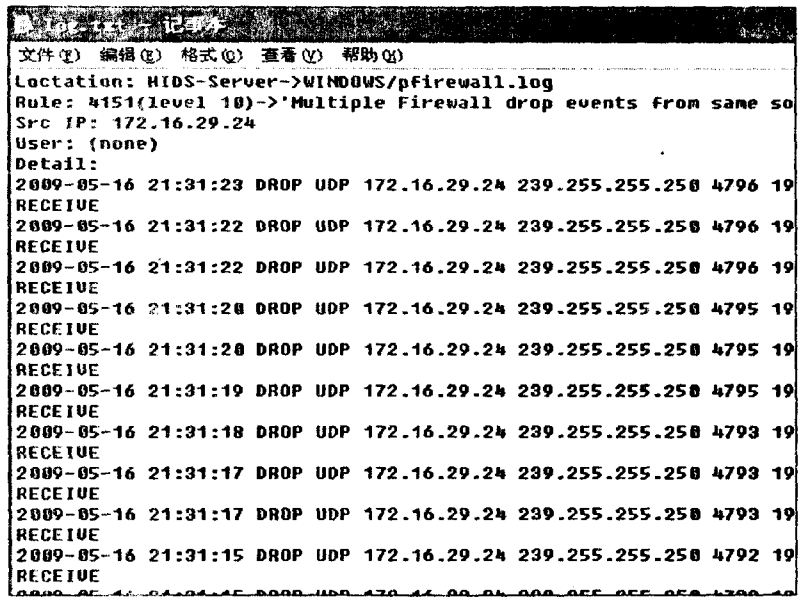

图2 入侵日志

3.3 响应到UI

将警告信息写入到警告日志之后,UI将会通知用户(如图3所示)。

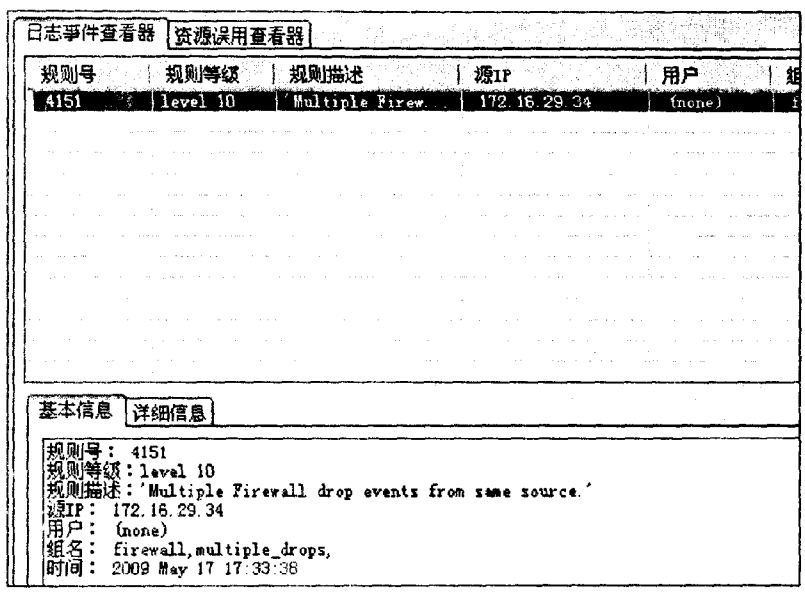

图3 UI通知用户有告警信息

4 结束语

日志分析检测作为计算机取证的一个重要组成部分,主要根据日志的收集和分析,将反映犯罪者犯罪的信息作为有效的诉讼证据提供给法庭。文中设计并实现了一个日志分析检测系统,并通过实例证明该方法是有效的。在日志分析过程中,一个主要技术就是对规则库的维护,规则库的更新速度和是否全面将成为检测成功率的瓶颈。下一步的工作是加大对规则库的维护,保证规则库的全面性和更新速度,这样可以在一定程度上弥补其漏报率较高的缺点。

参考文献:

[1] Kruse W G. 计算机取证:应急响应精要[M]. 段海新,等译. 北京:人民邮电出版社,2003.

[2] 殷联甫,任 静,王志欣. 计算机取证技术[M]. 北京:科学出版社,2008.

[3] 王 玲,钱华林. 计算机取证技术及其发展趋势[J]. 软件学报,2003,14(9):1635-1644.

[4] 曹元大. 入侵检测技术[M]. 北京:人民邮电出版社,2007.

[5] 薛静锋. 入侵检测技术[M]. 北京:机械工业出版社,2004.

[6] 田新广. 基于主机的入侵检测方法研究[D]. 长沙:国防科技大学研究生院,2005.

[7] 高丽婷,温秀梅. 日志检测系统的应用研究[J]. 河北建筑工程学院学报,2004,22(2):103-105.

[8] 林晓东,刘心松. 文件系统中日志技术的研究[J]. 计算机应用,1998,18(1):28-29.

[9] 国光明,洪晓光. 基于日志挖掘的计算机取证系统的分析与设计[J]. 计算机科学,2007,34(12):299-303.

[10] Daniel B. Cid. OSSEC[EB/OL]. 2008. http://www.ossec.net.

[11] Hay A, Cid D, Bray R. Log Analysis using OSSEC[M]. [s. l.]:Syngress,2007.

[12] Farmer D, Venema W. TCT[EB/OL]. 2009. http://www.porcupine.org/forensics.