doi:10.3969/j.issn.1000-436x.2012.z2.016

基于 Windows 日志的电子证据获取与分析方法研究

董晓梅[1]，刘旭东[1]，李晓华[1]，费雅洁[2]
(1. 东北大学 信息科学与工程学院，辽宁 沈阳 110004；2. 沈阳工程学院 信息工程系，辽宁 沈阳 110136)

摘 要：为解决 Windows 日志的实时获取问题，针对 2 种日志文件格式，分别提出了相应的日志实时获取方法。在实时获取日志的基础上，提出了将日志文件与原子攻击功能关联的方法，将对日志文件的分析转换成对原子攻击功能的分析，大大减少了日志文件分析的时间。提出了一种基于时间的日志关联分析和事件重构方法，实现对计算机犯罪场景的还原。实验结果表明，提出的方法可以有效获取日志证据，重构犯罪过程。

关键词：计算机取证；Windows 日志；获取；分析；事件重构
中图分类号：TP 309 **文献标识码**：A **文章编号**：1000-436X(2012)Z2-0125-10

Study on electronic evidence acquisition and analysis method over Windows logs

DONG Xiao-mei[1], LIU Xu-dong[1], LI Xiao-hua[1], FEI Ya-jie[2]
(1. College of Information Science and Engineering, Northeastern University, Shenyang 110004, China;
2. Department of Information Engineering, Shenyang Institute of Engineering, Shenyang 110136, China)

Abstract: In order to collect logs in real time, two methods to acquire Windows logs in real time were proposed respectively according to the two types of log file formats. Based on acquiring logs, an approach for correlating log files with atomic attack functions was proposed. After the correlation, atomic attack functions can be analyzed instead of log files, which can greatly decrease the time of analysis. A time based log correlation and event reconstruction method was proposed to reconstruct the computer criminal scenarios. Experimental results show that log evidences can be acquired and the crime process can be reconstructed effectively.

Key words: computer forensics; Windows logs; acquisition; analysis; event reconstruction

1 引言

计算机取证技术的研究，对于打击计算机犯罪，保障网络和计算机系统的正常运行具有重要意义。日志是电子证据的一个重要来源，由计算机系统内部运行的程序产生，能够详细记录系统内部发生的各种事件和一些系统状态。通过分析日志，可以发现入侵者的操作行为，从而再现入侵场景，为打击计算机犯罪提供重要线索。然而，通过实时获取和分析日志进行取证的相关工作尚未见报道。

目前对系统日志进行分析，主要是为了帮助事件预测和错误诊断，可用于资源分配、任务调度和系统管理[1~3]。还有一些研究利用系统日志分析来挖掘分布式系统的依赖性，或者用于 IT 服务可用性建模[4,5]。这些分析方法都属于静态日志分析，不能提供实时服务，也不能捕获日志的动态变化[6,7]。一些论文中则使用基于规则的数据挖掘方法进行日志的

收稿日期：2012-11-05
基金项目：教育部中央高校基本科研业务费基金资助项目(N100404005)
Foundation Item: The Fundamental Research Funds for the Central Universities(N100404005)

动态分析[1,8,9]。

现有的系统往往没有采取有效措施来保护日志，因此入侵者在成功入侵计算机后，会迅速清除掉计算机中的日志记录。将计算机日志作为电子证据，必须能够证明日志的原始性；在对日志进行存储转移时，需要保证日志的完整性。因而，如何确保计算机日志文件的真实性、可靠性、完整性，已经成为亟需解决的问题。

此外，计算机系统中的日志数据量庞大，格式复杂多样，人工查找和分析非常耗费时间，而现有的计算机取证工具中，缺乏具有数据提炼能力的综合的日志搜索和分析系统，还没有专门为计算机取证目的而设计的日志保护和分析工具。

为此，本文提出了实时获取日志文件的方法，即使系统中原来的日志文件被破坏，仍有实时收集保存的日志文件可用；提出了一种将日志文件应用于计算机取证的日志规范化方法，将不同的日志文件转换成一种统一的日志文件格式，便于阅读和处理；提出了日志证据的关联分析和事件重构方法，将日志文件与原子攻击功能相关联，通过将日志事件与原子攻击相匹配来还原入侵的场景。实验结果表明，本文提出的方法可以有效获取相关的日志并通过分析对入侵过程进行重构。

2 基于 Windows 日志的取证框架

基于日志进行电子证据获取和分析，需要满足以下几个目标：1) 尽可能多地识别主机上的日志格式，最好能够有通用的日志处理能力；2) 大容量日志处理能力；3) 关联分析的能力；4) 保留现场信息的能力；5) 搜索查询能力。

针对以上需求，本文提出了一种基于 Windows 日志的电子证据获取及分析方法，总体框架如图 1 所示。在对 Windows 日志进行实时获取后，首先需要对日志规范化，进行分类和统一表示，存储到日志库中。然后对日志证据进行关联分析和事件重构，找出证据之间的联系及与攻击行为的对应关系，进而重构出攻击过程。最后，将相关的证据保存到证据库中，以备查询。

3 日志证据的实时获取与规范化

Windows 系统中，日志的种类繁多，各种日志之间没有统一的日志格式标准。此外，为了防止日志文件遭到破坏，也不能直接从日志文件中获取数据，一般需要第三方的日志获取工具。然而，常用的工具软件中，对 Windows 日志获取的类型有限，多数工具只能获取某一类型的 Windows 日志文件，难以满足取证分析的需要。为此，本文提出了一种实时的日志监控获取方法，能够实时监控日志文件的变化，收集 Windows 系统中的大部分日志文件。

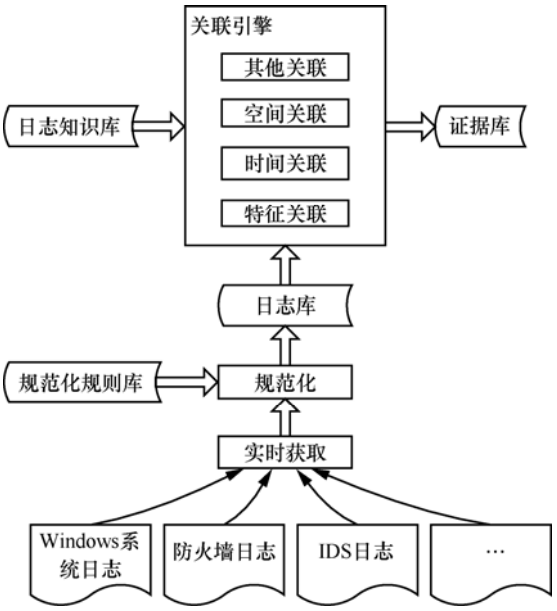


图 1 基于 Windows 日志的取证框架

3.1 Windows 日志格式及存储路径

从 Windows 2000 开始，Windows 系统日志都以二进制的方式保存。Windows 系统中常见的日志文件包括：系统日志、应用程序日志和安全日志。其中，安全日志默认不开启，需要系统管理员开启。除了以上系统日志文件，根据系统的配置和应用，可能还有文件目录服务日志、DNS 日志、PC 厂家定制的日志文件、FTP 日志、WWW 日志和 Internet 防火墙（ICF）日志等。这些日志文件，都受到 EventLog（日志记录）的保护，不能被删除，但是其中的日志记录可以被清空。

系统日志文件，可以通过系统提供的事件查看器进行查看，以统一的日志格式进行描述，如表 1 所示。这些常见的日志，都有一个默认的存放路径，如表 2 所示。

表 1 系统日志格式

记录头	事件描述	附加数据
日期、时间、主体标识、计算机名、事件编号、事件来源、事件等级、事件类别	事件所描述的内容，取决于该事件的名称、对事件的说明、事件产生的原因、对该事件提供的建议	可选数据区，通常包括能用十六进制方式显示的二进制数，具体内容由相应的应用程序的记录格式来决定

表 2　Windows 常见日志默认位置

日志	日志文件默认位置
系统日志	%systemroot%\system32\config\SysEvent.evt
应用日志	%systemroot%\system32\config\AppEvent.evt
安全日志	%systemroot%\system32\config\SecEvent.evt
DNS 日志	%systemroot%\system32\config
文件目录日志	%systemroot%\system32\config
FTP 日志	%systemroot%\system32\logfiles\msftpsvc1\
WWW 日志	%systemroot%\system32\logfiles\w3svc1\
防火墙日志	%systemroot%\
Scheduler 服务日志	%systemroot%\schedlgu.txt
…	…

3.2　日志实时获取方法

Windows 日志中，有一部分日志文件是以文本的方式存储的，比如 FTP 日志、WWW 日志以及计划任务日志等等，访问比较简单。另一些应用程序或者系统日志是受保护的，以二进制方式存储，只有采用系统或软件本身提供的方法才能获取。

3.2.1　二进制日志文件的实时获取方法

本文主要探讨 Eventlog 产生的二进制日志文件的获取方法。微软公司为 Eventlog 日志的访问提供了相应函数。在微软的.NET 平台下提供了一个 EventLog 类，这个类提供了对 Eventlog 日志文件的读取、删除等一系列操作的方法。如表 3 所示是其中的一部分方法介绍。

表 3　EventLog 类的方法

API	功能
EventLog.Exists	判断指定的日志是否存在
EventLog.clear	把事件日志中的所有项全部清除
EventLog.CreateEventSource	建立一个能够将事件写入到日志中的事件源
EventLog. WriteEntry	将有关事件记录写入日志
EventLog. SourceExists	判断是否存在某个事件源
EventLog. GetEventLogs	获取某一个事件的日志数组
…	…

为了保证被获取的日志信息的真实性，需要保证日志没有被修改，因此，本文对日志进行实时监控，在有事件记录被写入到日志的同时，就将相应的事件记录另外保存到日志库，以保证获取到的日志信息的完整性和真实性。在.NET 组件中，提供了 EntryWritten 事件。当有数据写入 Eventlog 日志的时候，触发该事件。此时可以通过一些方法，获取将要写入到 Eventlog 日志中的事件记录，将事件记录同时保存到日志库中。

3.2.2　文本日志文件的实时获取方法

对于文本方式存储的日志文件，本文以监视文本文件改变的方法来实现实时监控与获取。在微软的.NET 平台下，提供了一个 FileSystemWatcher 类，能够侦听系统中文件发生的改变，在文件目录或者文件目录中的文件发生改变时给予通知。只需用到其中监听文件变化的相关 API 就可以实现对 Windows 日志文件的监控。FileSystemWatcher 类中的一些方法如表 4 所示。

表 4　FileSystemWatcher 类的方法

方法	功能
FileSystemWatcher	对 FileSystemWatcher 类初始化为对指定目录的指定文件类型进行监控
OnChanged	引发 Changed 事件，即目录文件发生改变时调用该方法
OnRenamed	引发 Renamed 事件，当文件目录或者文件重命名时调用该方法
OnDeleted	引发 Deleted 事件，当文件目录或者文件发生被删除时调用该方法
WaitForChanged	返回包含有关所发生更改的特定信息的结构
…	…

首先对需要监控的 Windows 日志文件创建事件对象，然后通过 Changed 事件来捕获日志文件的修改，记录写入日志的信息。当有事件记录写入相关日志中时，调用日志获取函数。在日志获取函数中，需要用到 FileSystemEventArgs 类，其中保存有事件记录的相关内容。通过对 FileSystemEventArgs 数据的获取，就可以得到相应的事件记录信息。

3.3　日志格式的规范化处理方法

在获取到日志证据后，需要对证据进行关联分析和事件重构。但是 Windows 日志文件中包含的信息比较多，且格式复杂多样，显然不利于对日志证据的关联分析。因此，本文提出了将日志格式进行规范化处理的方法。

对 Windows 日志规范化处理的过程如下。

1) 对系统中的 Windows 日志文件进行分类，

在数据库中建立相应的表，指出该类日志文件的存储方式，存储格式等信息。

2) 对同类 Windows 日志文件，建立统一的存储格式表，描述这些日志文件的名称、存放路径以及对 Windows 日志文件的描述。

3) 对所有的日志文件，设计一个统一的描述格式。

本文根据需要，在进行日志电子证据的关联分析前，将所有需要分析的日志证据转换成如图 2 所示的格式。

Type	Signature	Exists	Timestamp	IP_address	Logfile

图 2 日志规范化格式

规范化格式中每一个属性的含义如下。

1) Type 属性是对日志类型的描述；

2) Signature 属性描述了记录在 Windows 日志文件里的日志信息，这个属性在进行 Windows 日志关联时使用；

3) Exists 属性是表示该日志记录是否为某一个原子攻击功能的一部分的标志位；

4) Timestamp 属性用来描述 Windows 日志产生的时间；

5) IP_address 是从相应的 Windows 日志记录中提取出来的入侵者的 IP 地址；

6) Logfile 用来记录 Windows 日志文件的来源。

类型和特征属性在日志与原子攻击功能的关联过程中使用，其他属性则用来存储有关日志的一些信息。在日志关联分析过程中，当某一条日志记录的特征与某一原子攻击功能中的一条日志记录的特征相同时，Exists 标志位被置为 TRUE，并把相应的其他属性信息填入相对应的属性字段。

如图 3 所示是一条第三方根目录序列号更新检索成功的日志，这是一条应用程序日志，将其进行日志规范化之后如图 4 所示。规范化后的日志，存储到日志库中。

图 3 一条日志的详情

“更新”，“自动更新检索第三方根目录序列号成功”，FALSE，“2012-5-19 10:49:28”，0，“Application Event Log”}

图 4 规范化后的日志

4 日志证据的关联分析与事件重构

证据的关联分析和事件重构，是取证中的重要步骤。对证据进行关联分析，可以从中找到有关犯罪的线索。文献[10]和文献[11]分别提出了基于入侵检测系统报警的证据分析方法，对入侵检测系统发出的报警进行关联分析和事件重构。本文针对获取的 Windows 日志，提出了一种基于日志的关联分析和事件重构方法，将计算机取证人员对日志分析的经验，转换成知识库；将 Windows 日志与原子攻击功能关联，在分析的时候，把相应日志与有关知识进行匹配，并进一步重构入侵过程。

4.1 原子攻击功能定义

原子攻击功能定义为攻击行为集合中不可分割的、独立的、具有明确含义的最小攻击行为。该行为在攻击的效果和操作上都是单一的，它不需要与其他的攻击操作交互而能够独立完成攻击操作，是攻击行为中的最小的行为序列。对于原子攻击功能的提取，需要注意以下原则。

通用性：原子攻击功能需要能够对大多数的攻击行为有一个攻击描述，而且，需要能够在所有的攻击场景中都能使用，并且对攻击原子功能的划分是一致的，不会因为攻击场景不同而有不同的原子攻击功能提取。

独立性：提取出来的原子攻击功能，不能与其他的操作上有交互，要保证原子攻击功能是能够自身独立完成这个攻击操作。

明确性：对于提取出来的原子攻击功能，不能在语义上有模糊含义，对于攻击的描述需要目标明确。

表 5 是对原子攻击功能的描述。

表 5 原子攻击功能描述

攻击类别	提取的相关原子攻击功能
目标探测	Ping 扫描、端口扫描、操作系统识别
隐藏踪迹	修改日志、文件隐藏
预留后门	远程控制、特洛伊木马
权限提升	缓冲区溢出、字符串格式化
权限获取	口令破解、会话劫持

...	...

在获取了足够多的日志证据之后，就可以进行事件重构，对整个计算机犯罪的场景进行还原。本文采用了层级描述的方法，来描述整个犯罪场景。

计算机犯罪的过程是十分复杂的，犯罪分子在进行相关计算机入侵活动的时候，往往是分为多个步骤多个阶段实施，通过一系列的攻击行为组合，才能实现对计算机入侵，并达到入侵目的。攻击过程的每一阶段的攻击行为，都具有一定的目的性。例如，对操作系统进行端口扫描或者操作系统识别，是为了下一步能够从系统中找出可以利用的操作系统漏洞。

按照攻击目的，可以将攻击过程分为若干个攻击阶段，每一个攻击阶段由若干个原子攻击序列组成。一个攻击阶段对应多个攻击行为，每个攻击行为都可以看作一个原子攻击功能。因此，按照层次的方法，将攻击过程从上到下细化到原子攻击功能，就可以表示出整个攻击过程。

下面以 DDoS 攻击场景来举例说明。DDoS 攻击的攻击者首先在网络上搜索一些活动的主机，并对主机的端口开放情况和系统信息进行探测；然后，扫描主机上可以利用的主机漏洞；在获得相关漏洞之后，利用漏洞进行缓冲区溢出；然后通过一些方法，将分布式拒绝服务攻击的代理软件安装到该主机上，使其成为分布式拒绝服务的代理系统；最后，多个这样的分布式拒绝服务的代理系统一起向目标发起 DDoS 攻击。对 DDoS 攻击场景的描述如图 5 所示。

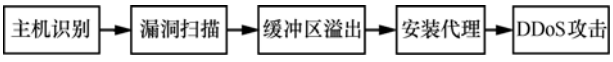


图 5　DDoS 攻击场景描述

上述的攻击过程，是从各个阶段进行描述，比如主机识别，就有好几种方法，比如 ping 方法，ipsweep 方法等等，其他各个阶段也有相似的情况，因此，对整个场景的详细描述，就有可能是如图 6 所示的情况。

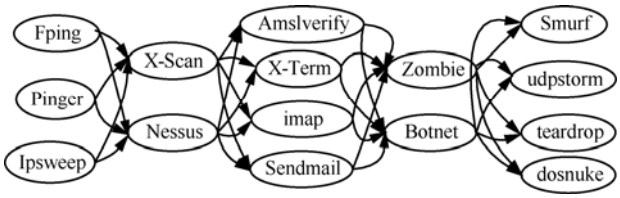


图 6　DDoS 攻击场景详细描述

4.2　Windows 日志与原子攻击功能关联

对 Windows 日志文件记录进行上述的规范化处理之后，就可以将系统中的所有日志与原子攻击进行关联。原子攻击功能与日志的关联表示如图 7 所示。

Attack={

[$type_1$, $signature_1$, $exists_1$, $timestamp_1$, $ip\_address_1$, $logfile_1$]

[$type_2$, $signature_2$, $exists_2$, $timestamp_2$, $ip\_address_2$, $logfile_2$]

...

[$type_n$, $signature_n$, $exists_n$, $timestamp_n$, $ip\_address_n$, $logfile_n$]

}

图 7　原子攻击功能与日志的关联表示

在规范化的日志文件中，时间戳属性所表示的时间，是经过时间同步处理之后的时间。这样，就可以按照时间顺序对日志进行关联分析，重构计算机犯罪入侵场景。

在进行 Windows 日志与原子攻击功能关联的过程中，需要使用到攻击知识库，该攻击知识库由原子攻击功能组成，知识库中的每一个原子攻击功能都由系统中的若干个日志文件记录构成。攻击知识库的建立，相当于是把计算机取证人员相关的取证经验转换成可以被相应程序理解的规则或者定义，从而可以在日志关联中使用。

将日志与原子攻击功能关联的大体思想是：将获取的日志文件，与原子攻击功能中的日志文件匹配，当某一日志文件的 Signature 属性匹配成功时，将相应的原子功能中的日志记录的 Exists 属性设置为 TRUE，并记录相应信息；当原子攻击功能中所有的日志记录的 Exists 属性都为真的时候，证明该攻击发生，把其记录下来，方便后续分析。此外，还需要将该攻击记录保存。

为了提高匹配的效率，本文将一些发生频率非常高的原子攻击功能放在一个初始化队列中。这些原子攻击可以通过历史的统计数据获得，或者是由管理员人工设定。设置了初始化原子攻击功能队列

后，能在其中快速找到很大一部分日志记录对应的匹配项，从而减少日志搜索匹配的时间，加快日志关联的进程。此外，还可以将原子攻击功能按照所组成的日志记录进行分类，比如，某一些原子攻击功能只涉及到某一类日志，而另外的一些原子攻击功能则涉及到多类日志。

经过关联分析以后，所有日志都与原子攻击功能关联起来。经过关联的日志，已经转换成了原子攻击功能。通过将原子攻击功能按照时间进行排序和关联分析，就可以重构入侵事件过程。

日志与原子攻击功能的关联算法如算法 1 所示。其中 L 为规范化后形成的日志库，A 表示攻击数据库，I 为初始攻击队列，P 为待匹配的临时原子攻击队列，Q 为最终形成的原子攻击队列。

算法 1 日志与原子攻击功能关联算法

输入：日志库 L，攻击数据库 A，初始攻击队列 I

输出：原子攻击队列 Q

$Q = \varnothing$

$P = \varnothing$

for each $l \in L$:

if $\exists a \in P$，l.signature=a.signature$_i$:

a.exists$_i$ ← TRUE

a.type$_i$ ← event type from A

a.ip_address$_i$ ← l.ip_address

a.timestamp$_i$ ← l.timestamp

a.logfile$_i$ ← l.logfile

end if

if $\forall a \in P$, for all $i \in \{1,2, \cdots, n\}$, a.exsits$_i$ = TRUE:

Append a to Q

Remove a from P

else if $\exists a \in I$，l.signature=a.signature$_i$:

create a new attack s

s.exists$_i$ ← TRUE

s.type$_i$ ← event type from A

s.ip_address$_i$ ← l.ip_address

s.timestamp$_i$ ← l.timestamp

s.logfile$_i$ ← l.logfile

Append s to P

else if $\exists a \in A$，l.signature=a.signature$_i$:

Create a new attack s

s.exists$_i$ ← TRUE

s.type$_i$ ← event type from A

s.ip_address$_i$ ← l.ip_address

s.timestamp$_i$ ← l.timestamp

s.logfile$_i$ ← l.logfile

Append s to P

else drop l

end if

end for

设日志库 L 的大小为 N，则在算法 1 中，每条日志都要与临时原子攻击队列 P 中的每个攻击进行 signature 属性的匹配。最坏情况下，当前第 i 条日志与 P 中最多 i−1 个原子攻击进行匹配，共进行 $\sum_{i=1}^{N}(i-1)=\frac{N(N-1)}{2}$ 次匹配，由于 I 和 A 的大小为常数，对 signature 属性的匹配操作也是常数时间的，因此算法 1 的时间复杂度为 $O(N^2)$。

4.3 事件重构

关联后的 Windows 日志文件，就转化成了攻击行为的证据。如果在日志收集足够多的情况下，就有可能对整个计算机犯罪场景进行重构。由于入侵计算机的犯罪是一种十分隐蔽的事件，保留在计算机上的电子证据具有异构性，而且计算机犯罪采用的技术手段往往都不一样，因此到目前为止，还没有有关学者或者机构提出具有通用性的犯罪场景重构方法。

本文采用的是时间线的分析方法，对已经发生的原子攻击功能，按照时间先后顺序进行排序，然后根据入侵 IP，重构出计算机犯罪的现场。重构算法如算法 2 所示。其中，Sort()是一个排序函数，将关联后的攻击队列按照时间戳进行排序。

算法 2 入侵场景重构算法

输入：关联后的原子攻击队列 Q

输出：入侵场景队列 S

$S = \varnothing$

Sort(Q) by timestamp

for each $a \in Q$

if $\exists s \in S$，s.ip_address=a.ip_address

Append a to s

else

Create a new scenario m

m. ip_address ← a.ip_address

Append a to m

Append m to S

end if

end for

类似地，设 Q 中共有 N 个原子攻击，则每个原子攻击与 S 中的每个入侵场景进行 IP 地址的比较。最坏情况下，S 中有 $N-1$ 个入侵场景，因而算法 2 的时间复杂度也是 $O(N^2)$。

该算法还存在一定的局限性：1) 并非所有的 Windows 日志都能将入侵者的 IP 地址记录下来，若是有些日志没有记录 IP 地址，就无法用该算法重构出完整的入侵事件；2) 有些入侵者入侵时采用的是动态 IP 技术，多步入侵操作在日志中记录的 IP 地址可能不一样。这样对于同一个场景的原子攻击功能，可能无法通过 IP 地址将其关联起来，也就无法把入侵场景完整重构出来。

虽然在日志收集不够全面的情况下，无法把整个计算机犯罪场景重构出来，但是 Windows 日志文件经过关联后，可以向计算机取证人员提供原子攻击功能查询，或者由计算机取证人员定义一个由原子攻击功能组成的攻击序列，在由匹配成功产生的原子攻击功能中，按照时间的先后顺序进行查找。最后，还可以对原子攻击功能向上进行归纳，进一步减少取证人员的工作量。

5　实验结果及分析

本文设计了一系列实验，来分别对 Windows 日志文件的获取方法以及日志与原子攻击功能的关联进行验证，然后通过一个例子来实现对事件重构方法的验证。

5.1　实验设置

实验用的硬件环境为：Intel(R) Core(TM)2 Duo CPU E8500 3.16GHz，内存为 4G。由于现有的数据集中，没有专门针对 Windows 系统收集的日志数据的数据集，所以，需要自己模拟一些入侵行为，把相应的日志记录下来，并将这些日志数据应用于取证分析中。所以需要模拟犯罪场景，本文采用的是在虚拟机下实现模拟。

本文实验使用的虚拟机是 VMware WorkStation 6.0，编程采用的是 Microsoft Visual Studio 2008 编程环境，数据库使用的是微软的 SQL Server 2005，主机操作系统是 Windows XP 系统。

5.2　实验结果及分析

本文设计了日志实时获取和关联分析的实验，验证了 Windows 日志文件的实时获取功能和对日志的关联分析功能。

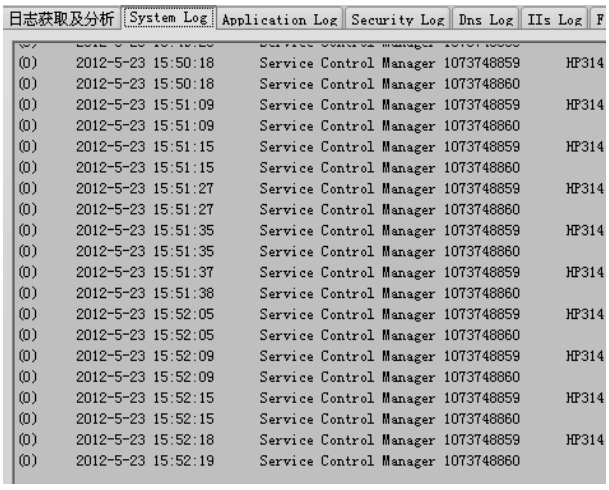
5.2.1　日志的实时获取实验

为了验证 Windows 日志文件的实时获取方法，进行了 2 种实验：一种是实时获取 Event Log 日志的实验，一种是实时获取文本日志文件的实验（实验中选取的是 IIS 日志）。

在 Event Log 日志的实时获取实验中，通过对 hpqwmiex 服务的启动和关闭来验证。首先运行监控程序，监控程序完成对日志读取的初始化工作，然后启动 hpqwmiex 服务，实验结果如图 8 所示。

图 8(a)是日志初始化并进行监控时的截图，图 8(b)是对 hpqwmiex 服务启动和关闭后截获的日志记录的截图。图 8 表明，本文提出的方法能够及时地获取和记录相关的 hpqwmiex 服务启动和关闭的日志记录。

(a)　开启服务前



(b)　开启服务后日志监控情况

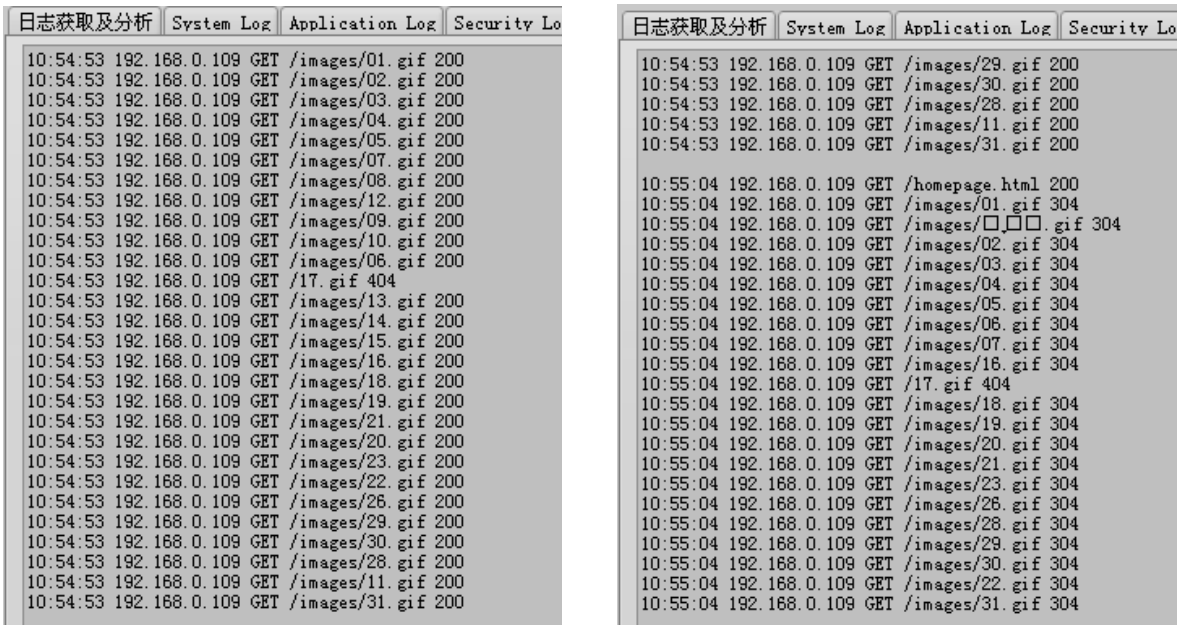
图 8　Event Log 监控情况

在文本日志的实时获取实验中，先运行实时日

志监控程序，然后再访问网页，对 IIS 日志记录进行实时监控，来验证相关的日志文件记录是否被实时捕获。实验结果图 9 所示。

图 9(a)是日志初始化并进行监控时的截图，图 9(b)是访问网站后截获的日志记录的截图。在对网站进行访问时，在网站的 IIS 中记录的有关访问记录，都通过实时监控程序捕获下来，进行了相应的记录。

安装系统之后，没有给管理员设置密码，或者是管理员密码设置得很简单，而且开放了 3389 端口，因此入侵者可以利用该漏洞入侵计算机。该实验的具体过程如下：在虚拟机中安装 2 个操作系统，并把操作系统连接在一个局域网中；然后通过远程登录进入系统中，并且在系统中添加一个用户 hack，给该用户分配管理员权限；最后退出系统。对于该过程，可以通过实时监控得到的日志文件，进行原



(a)　访问网站前　　(b)　访问网站后

图 9　文本日志监控情况

图 10　日志关联结果

5.2.2　日志的关联分析实验

为了验证日志与原子攻击功能的关联以及在此基础上的日志分析方法，本文通过实验，查看是否有相关的原子攻击功能关联。很多计算机用户在

子攻击功能关联，然后尝试进行事件重构。日志与原子攻击功能关联的结果如图 10 所示。

从图 10 中可以看到 3 条原子攻击，分别是成功登录、登录尝试以及退出登录。而每一条原子攻

击下边，有相对应的日志文件记录。

图 11 是对上述攻击场景进行事件重构之后的结果，从中可以看出用户首先由于密码等原因，有 2 次失败的登录尝试；在那之后，成功地登录了系统。在重构出的事件描述中，按照时间的先后顺序，描述出入侵者入侵计算机时所做的每一个动作。以上实验结果表明，将日志与原子攻击功能关联以及

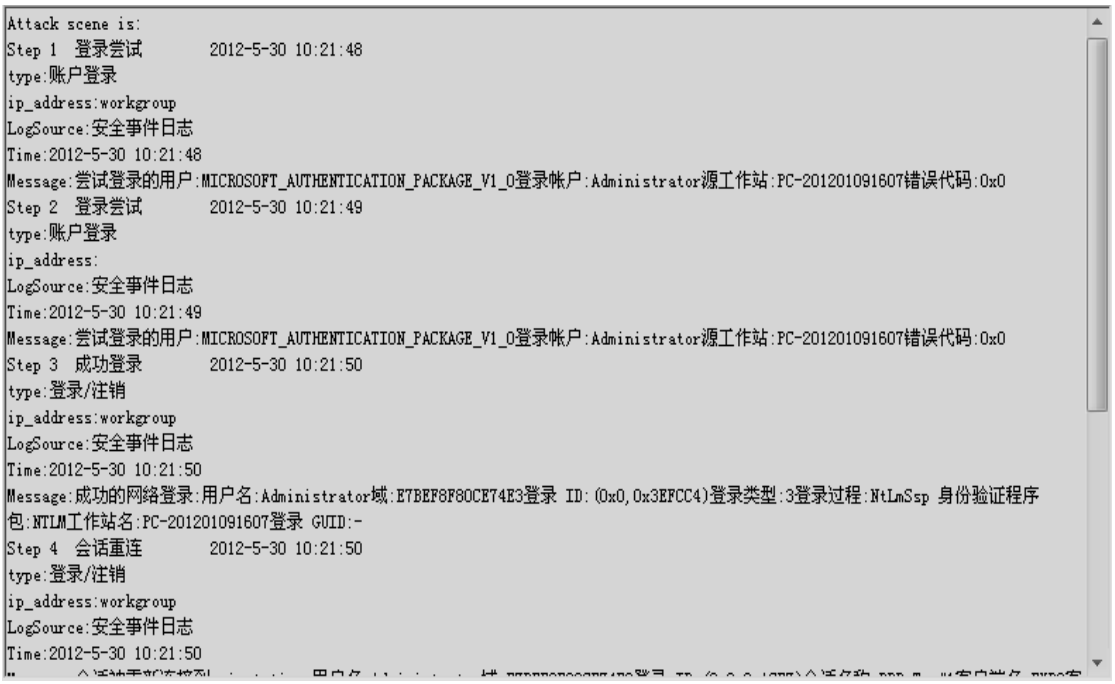


图 11　事件重构结果

Windows 日志文件的关联分析。提出了一种基于时间关联的事件重构方法，实现了对计算机犯罪场景的重构。通过实验，验证了本文提出的基于 Windows 日志文件的电子证据获取和分析方法是有效的。

在未来的工作中，将研究更多类型的日志文件的实时监控和收集方法，扩充原子攻击功能知识库，并对事件重构技术进行更深入的研究。

进行相关的事件重构的方法是可取的。

此外，以上是对安全审计日志分析得到了整个攻击过程，还存在一些其他的日志，也可以证明入侵者对计算机做了上述操作，例如防火墙日志就记录了入侵者建立的连接过程。因此，如果能够多收集日志，并且从多个方面加以证明，则使得相关的日志文件在法庭上作为证据使用时，更加具有说服力。

6　结束语

本文对 Windows 日志的实时获取和基于 Windows 日志证据的关联分析方法进行了研究，根据 Windows 日志文件的特点，分别提出了针对二进制日志文件和文本日志文件的 2 种实时获取方法。为了对日志进行关联分析，提出了一种将经验知识转换成知识库的方法，将计算机取证人员关于 Windows 日志取证的相关经验知识，转换成与之相对应的原子攻击功能，形成了原子攻击功能知识库。通过将原子攻击功能与日志记录进行关联，来实现

参考文献：

[1] SAHOO R K, OLINER A J, RISH I, *et al*. Critical event prediction for proactive management in large scale computer clusters[A]. Proceedings of KDD 2003[C]. Washington, DC, USA, 2003. 426-435.

[2] FU S, XU C. Exploring event correlation for event prediction in coalitions of clusters [A]. Proceedings of the International Conference for High Performance Computing, Networking, Storage, and Analysis[C]. Reno, USA, 2007. 1-12.

[3] FU S, XU C. Quantifying temporal and spatial correlation of failure events for proactive management[A]. Proceedings of 26th IEEE International Symposium on Reliable Distributed Systems (SRDS2007)[C]. Beijing, China, 2007. 175-184.

[4] SALFNER F, TSCHIRPKE S. Error log processing for accurate event prediction[A]. Proceedings of the USENIX Workshop on the Analysis of System Logs (WASL)[C]. San Diego, USA, 2008.

[5] LOU J G, FU Q, WANG Y, *et al*. Mining dependency in distributed systems through unstructured logs analysis [J]. ACM SIGOPS Operating Systems Review archive, 2010, 44(1): 91-96.

[6] OLINER A, STEARLEY J. What supercomputers say: a study of five

system logs[A]. Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07)[C]. Edinburgh, UK, 2007. 575-584.

[7] ROUILLARD J P. Real-time log file analysis using the simple event correlator (SEC)[A]. Proceedings of LISA '04: Eighteenth Systems Administration Conference[C]. Atlanta, USA, 2004. 233-150.

[8] TANG D, IYER R K. Analysis and modeling of correlated failures in multicomputer systems[J]. IEEE Transactions on Computers, 1992, 41(5): 567-577.

[9] OLINER A J, AIKEN A, STEARLEY J. Alert Detection in Logs[A]. Proceedings of Eighth IEEE International Conference on Data Mining (ICDM'08)[C]. Pisa, Italy, 2008. 959-964.

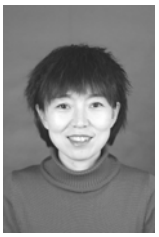
[10] 张有东, 曾庆凯, 王建东. 网络协同取证计算研究[J]. 计算机学报, 2010, 33(3): 504-513.
ZHANG Y D, ZENG Q K, WANG J D. Studies of network coordinative forensics computing[J]. Chinese Journal of Computers, 2010, 33(3): 504-513.

[11] 伏晓, 石进, 谢立. 用于自动证据分析的层次化入侵场景重构方法[J]. 软件学报, 2011, 22(5): 996-1008.
FU X, SHI J, XIE L. Layered intrusion scenario reconstruction method for automated evidence analysis[J]. Journal of Software, 2011, 22(5): 996-1008.

作者简介：

董晓梅（1970-），女，河南开封人，博士，东北大学副教授，主要研究方向为网络与信息安全、信息隐藏、计算机取证等。

刘旭东（1987-），男，湖南娄底人，东北大学硕士生，主要研究方向为网络与信息安全、计算机取证。



李晓华（1969-），女，蒙古族，辽宁凌源人，硕士，东北大学讲师，主要研究方向为网络与信息安全、信息隐藏、计算机取证等。

费雅洁（1968-），女，河北唐山人，硕士，沈阳工程学院教授，主要研究方向为网络与信息安全、智能信息处理、计算机取证等。