

基于协议分析的网络入侵动态取证系统设计

杨卫平^{1,2}, 黄烟波¹, 段丹青^{1,2}, 黄伟平¹

(1. 中南大学 信息科学与工程学院, 湖南 长沙 410083;

2 湖南公安高等专科学校, 湖南 长沙 410006)

摘要: 计算机取证技术分为静态取证和动态取证两种。静态取证技术由于采用事后分析的方法提取证据, 因而证据的采集不够全面, 同时恢复的数据可能是已经被篡改的数据, 因而法律效力低。文中将计算机取证技术与入侵检测技术结合, 提出一种基于协议分析的网络入侵动态取证系统。该系统采用基于协议分析的入侵检测方法, 提高了入侵检测效率及数据分析能力, 有助于解决动态取证的实时性; 同时系统采取了较全面的安全机制, 确保收集的电子证据的真实性、有效性、不可篡改性, 是动态计算机取证的一种较好解决方案。

关键词: 计算机取证; 电子证据; 入侵检测; 证据提取

中图分类号: TP393.08

文献标识码: A

文章编号: 1005-3751(2006)04-0215-03

Design of Protocol Analysis Based IDS and Dynamic Computer Forensic System

YANG Wei-ping^{1,2}, HUANG Yan-bo¹, DUAN Dan-qing^{1,2}, HUANG Wei-ping¹

(1. College of Information Science and Engineering, Central South University, Changsha 410083, China;

2. Hunan Public Security College, Changsha 410006, China)

Abstract: The computer forensic mainly consists of two techniques: the static forensic and dynamic forensic. The static computer forensic collects electronic evidences after the intrusion has happened, so it's difficult to collect the evidences entirely and even the recovered files may has been modified, the collected electronic evidences are not so available in law. The paper provides a dynamic computer forensic system combined computer forensic technology and intrusion detection system based on protocol analysis. The system can improve the efficiency of intrusion detection and the ability of data analysis by using the protocol analysis method. It's helpful to realize collecting electronic evidences dynamically in real-time. The system also uses several kinds of network safe mechanisms to ensure the accuracy, validity, immutability of the electronic evidences. It's a good solution of dynamic computer forensic.

Key words: computer forensic; electronic evidence; intrusion detection; evidences collection

0 引言

随着社会信息化程度的不断推进, 计算机网络的不断普及, 国家事务、政府事务网站的不断建立, 利用计算机或网络窃取商业秘密、国家机密, 从事渗透、颠覆以及破坏祖国统一等犯罪活动也日渐猖獗, 网络入侵事件呈指数级增长, 由此带来的损失难以估量。

为了遏制计算机犯罪数量日益增长的趋势, 世界许多国家都制订了相应的法律来惩治计算机犯罪, 然而由于电子证据具有隐蔽性、可篡改性、可复制性、可伪造性、可删除性等独特的特点, 如何完整地从中提取电子证据, 并对其进行固定和保全, 以确认犯罪, 在计算机犯罪案

件的侦查过程中显得尤为重要。计算机取证学已经成为人们研究与关注的焦点。计算机取证是指对能够为法庭接受的、足够可靠和有说服性的、存在于计算机和相关外设中的电子证据的确认、保护、提取和归档的过程^[1], 即针对计算机入侵与犯罪, 进行证据获取、保存、分析和出示。从技术上讲, 计算机取证是一个对受侵计算机系统进行扫描和破解, 以对入侵事件进行重建的过程^[2]。

计算机取证分为静态取证和动态取证。传统的取证方法一般是采用静态取证, 它是在事发后对数据进行提取、分析、抽取有效证据, 但是这种取证方法主要是对文件系统的恢复, 这种恢复不可能达到 100% 的还原; 而且由于计算机犯罪专业性强, 大部分入侵者会在入侵后掩盖、删除或篡改证据, 因而即使文件被恢复了, 恢复的数据也有可能是已经被修改过的数据, 不能作为法庭证据, 因而这种取证方法存在一定的缺陷。动态取证是将入侵检测系统、防火墙、HoneyPot 等网络安全技术紧密结合起来, 实时获取数据并采用智能分析技术, 实时检测入侵, 分析

收稿日期: 2005-08-14

基金项目: 湖南省教育厅青年项目(03B009); 湖南省公安厅科研项目资助(湘公科[2003]14号)

作者简介: 杨卫平(1969-), 男, 湖南益阳人, 硕士, 讲师, 研究方向为网络技术; 黄烟波, 教授, 研究方向为网络技术。

入侵企图,采取相应的响应措施,在确保安全的情况下,获取入侵者的大量证据,同时将这些证据进行保全、提交的过程。可以看出,动态取证技术能全面、及时地获取入侵证据,通过及时分析入侵者的企图,采取相应的防御措施,切断或追踪入侵途径,从而将损失降到最小。

文中提出一种基于协议分析的网络入侵动态取证系统,系统通过入侵检测系统记录系统工作及黑客入侵的全过程,及时分析入侵企图,通过入侵响应模块对入侵行为及时采取相应的响应措施,同时入侵检测系统将记录的入侵证据传送给证据库作证据保全。

1 系统体系结构

系统的体系结构如图 1 所示。

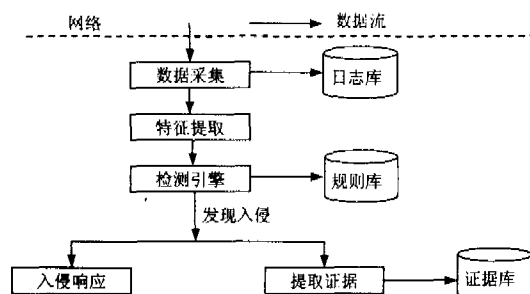


图 1 系统总体结构图

数据采集模块通过将网卡设置成混杂模式,收集流经网络的数据包。网络数据包的截获采用基于 BSD 数据包过滤器的数据过滤机制,收集到的网络数据存入日志库,供相关模块调用,同时也可作为计算机取证提供原始数据。

由于流经网络的数据量非常庞大,为了提高入侵检测的速度,特征提取模块先将收集到的网络数据包进行精简,提取与网络连接相关的特征,这些特征最能体现出该连接的类型,如源 IP 地址、源端口地址、目标 IP 地址、目标端口地址等,通过特征提取可以减小数据匹配量,提高检测效率。

检测引擎通过分析流经网络的数据包,检查其是否与规则库中已知的攻击特征相匹配来判断是否存在攻击事件。若检测到入侵,检测引擎将检测结果通知入侵响应模块和证据提取模块,以便采取相应措施保障网络安全,并提取相关入侵证据。

响应模块根据入侵类型决定采取何种响应方式。入侵响应包括主动响应和被动响应,主动响应是指系统在发现入侵行为后,采取某种响应手段或措施阻塞攻击的进程或改变受攻击的网络环境配置,从而达到阻止入侵危害性后果的发生或尽可能减少危害性后果的目的;主动响应采取的措施主要有:切断攻击发起主机或网络的网络连接、反向攻击入侵主机系统、切断当前异常网络 TCP 连接等,更为先进的主动响应手段包括自动修补目标系统的安全漏洞、动态更改检测规则集合等方法。被动响应是系统在检测到入侵行为后,仅仅报告和记录所检测到的异常活动信息,被动响应的手段通常包括如下类型:告警、日志记

录、发送网管信息等^[3]。

证据提取模块对网络中发生的攻击过程及攻击行为进行记录和分析,并确保记录信息的真实性、完整性、安全性及独立性等^[4]。为了妥善保存获取的证据,不使它发生任何损失、更改,以免失去法律效力,应将提取的证据传送到证据库进行证据保全。证据在传送前应先进行认证,采用加密方式进行传送,送达证据库后应将数据加上数字签名,以确保信息的完整性、真实性、不被篡改性。

2 检测引擎

检测引擎是整个系统的核心,由于目前的网络速度快,要实现实时检测,则要求检测引擎能快速、高效、准确地对截获的网络数据包进行检测,检测引擎采用的检测方法将直接影响系统性能。目前大部分入侵检测系统(IDS)采用基于模式匹配的入侵检测方法,该方法是由 Kumar 在 1995 年提出的^[5],主要是用一定的模式描述来提取攻击的主要特征,通过判别网络中搜集到的数据特征或从主机审计数据中提取的数据特征是否在入侵库中出现来检测入侵行为。模式匹配的特点是原理简单、扩展性好、检测效率高,可以实现实时检测,因而已经成为入侵领域中应用最为广泛的检测手段和机制之一。

准确性和快速性是衡量一个入侵检测系统性能的重要指标。采用模式匹配的 IDS 能否准确地识别出入侵行为,一方面依赖于入侵模式库的完备性,另一方面也取决于能否对网络上的全部数据包进行监听和分析。在 IDS 中,截获网络的每一个数据包,并分析、匹配其中是否具有某种攻击的特征需要花费大量的时间和系统资源,由于新的攻击方法层出不穷,新的漏洞不断被发现,入侵模式库若不能及时更新则会造成系统漏报;但入侵模式库的不断更新必将使其变得越来越庞大,对整个模式库中的模式进行一次匹配耗费的时间也就越多,因而不可避免地会降低检测效率。

可以看出,随着网络规模的不断扩大及攻击手段的不断翻新,网络传送的网络包数量不断增加,入侵模式库不断膨胀,采用传统模式匹配方法的 IDS,其性能将呈线性下降。为了有效地提高 IDS 的检测效率,在不断改进模式匹配算法、提高模式匹配速度的同时,还应尽量减少模式特征库中的模式匹配数量,以缩短模式匹配时间。

基于以上考虑,本系统采用基于协议分析的网络入侵检测方法,系统在进行模式匹配之前,先对捕获的数据包进行分析,捕获的数据包是链路层的帧,因此需要从链路层协议开始进行分析,一直到应用层的协议。在网络通信中,网络协议定义了标准的、层次化、结构化的网络数据包。利用这种层次性对网络协议逐层分析,可以大幅度减少模式匹配数量,提高分析效率,得到更准确的检测结果。图 2 为一个以太网数据包的封包格式。

以太网头	IP	TCP/UDP 头	应用协议及数据
------	----	-----------	---------

图 2 以太网封包格式

一个以太网的帧结构中,头 14 个字节为以太网头,分别由 6 字节的以太网地址(MAC)地址、6 字节的源以太网地址及 2 字节的帧类型组成,帧类型给出上层(网络层)所包含的协议类型,如 IP、IPX 等,它们对应的协议号分别为(十六进制):0800、8137。没有选择项时,IP 包头的长度为 20 字节,主要包含以下内容:源 IP 地址、目的 IP 地址、分片标志和偏移、及 IP 负载的协议类型(长度为 1 字节),IP 负载的协议类型指明传输层协议类型,如 TCP、UDP 等,其协议号分别为 6、17;TCP 包头在没有选择项时,也为 20 字节,主要包含源端口、目的端口、标志位、包序列号及 ACK 等域。根据 TCP 包的源和目的端口号可以得到该包的应用类型,比如 80 为 HTTP 协议,21 为 FTP 协议,23 为 Telnet 协议等。如果把所有的协议构成一棵协议树(如图 3 所示),则采用基于协议分析的方法,对一个网络数据包的分析就是一条从根到某个叶子的路径。

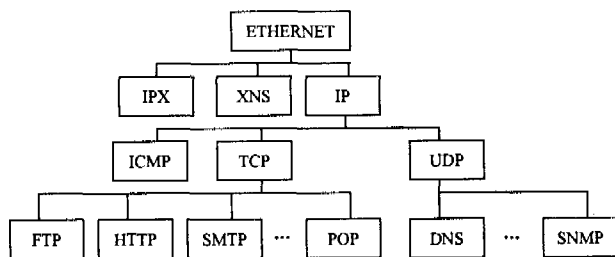


图 3 协议树

传统的模式匹配方法,在对网络数据进行协议分析时,基本上不涉及到应用层。由于没有对应用层协议进行分析,因而系统在进行模式匹配时只能将应用协议看成没有结构的比特流,进行盲目匹配,很可能将 Telnet 的攻击模式用来匹配 HTTP 包;而且需进行匹配的模式数量多,计算量较大。

基于协议分析的入侵检测方法,在对网络数据包进行协议分析时,一直分析到应用层,与传统的模式匹配方法相比,该方法具有以下优点:

①数据匹配量小:由于采用基于应用层的协议分析方法,如果在对数据包的协议进行分析时,检测到应用层使用的是 HTTP 协议,则系统在进行模式匹配时,FTP、Telnet 等高层协议相关的攻击模式就没有必要进行匹配,大大减少了匹配数量。

②提高准确性:基于应用层协议分析之后,协议分析器采用的是命令解析方式,而这就意味着“/.”、“/phf”及所有其它类似的“/.”变形,通过分析器都被看作同一攻击,即“/phf”攻击,在入侵模式库中,同一攻击只需一种模式特征即可检测到,因而可以大量减少模式特征库的规模。

3 证据提取

证据提取模块实现对入侵过程及入侵行为进行记录和分析,同时将鉴定出来的证据传送到证据库进行保全,

该模块主要实现以下功能:

①从截获的网络数据包中提取出反映客观事实的、具有法律效力的、与入侵事件相关的电子证据;

②从 IDS 接受报警数据;

③采用关联规则、聚类分析等智能分析技术,通过分析入侵来源、入侵方法,取得新的攻击技术资料,以实现系统规则库的更新;

④为用户提供信息资源的查询功能;

⑤将提取的证据、分析结果进行加密或数字签名;

⑥将经过安全处理后的证据通过 VPN 送至服务器上的证据库;

⑦形成分析报告,提供给法庭。

在取证过程中应注意:证据在提取前应做好备份,证据分析、提取时应针对备份数据进行分析,而不是对原始数据进行分析,要保证原始数据不被破坏。

4 安全机制

由于网络入侵取证系统的某些模块本身存在于被攻击系统中,因此系统本身的安全性应是首先要考虑的问题,只有保证了整个取证系统的完整性才能依据此系统所取得的数据进行后续的取证分析工作。

4.1 日志文件的安全性

入侵者在进行入侵活动之后,都会想方设法清除入侵留下的痕迹,日志文件能够很好地反应系统的安全状况,它能告知我们已经发生的事情。因而日志文件经常成为入侵者首要的攻击目标,一旦攻击者获得 root 权限,就可以轻而易举地修改、破坏或删除系统所保存的日志记录,从而掩盖他们入侵的踪迹,因而日志文件的安全性在系统中极为重要。

为了保护日志文件不被修改或破坏,除了将日志文件设置成只读属性、改变其默认目录等常规手段外,给日志文件加密是增加其安全性的必要手段,本系统采用 DES 加密算法对日志文件进行加密。

为防止日志文件被破坏,应对其进行备份。备份时要尽量避免在原盘进行,因为攻击者一旦获取 root 权限,便与系统管理员一样拥有着对这台机器的控制权,因此更加安全的办法是及时将日志文件数据传送到其它机器上。在本系统中,采用第三方存储策略。该策略主要有如下优点:攻击者对基于操作系统的漏洞非常熟悉,但很少有人入侵第三方日志的知识;第三方日志可以被隔离保护,免受入侵者攻击^[6]。

4.2 数据传输的安全性

被备份的日志文件及经过分析后收集的入侵证据应传送到证据库妥善保管起来,只有这样,才能保证在今后的诉讼中,司法机关有据可查,不至于影响原来提供的证言、物证等的证明作用,保证诉讼的顺利进行。因而保证这些数据在传送过程中的真实性、完整性及不被篡改性就

(下转第 220 页)

登录,如果用户在某个时间段,每访问一次受保护资源都要登录一次会使用户感到非常厌倦,而且系统运行的效率也不高。第二个 cookie 作用在于减少对服务器通过用户 ID 查找用户角色的次数,提高运行效率。

3 关键技术

Web 应用通过 HTTP 协议进行通信,而 HTTP 协议是无连接的应用层协议,因此要在 Web 上实现应用程序的访问控制,如何让服务器知道用户的身份就成了一个需要解决的问题。而在上文的实现过程中使用了 cookie,通过 cookie 存放用户身份并保持用户和服务器之间的联系。但使用 cookie 传递信息安全性很差,主要表现在 3 个方面^[5]:

* 如果 cookie 明文传递,那么就有可能在传输过程中被其他人窃听;

* cookie 一般存放在用户的硬盘上,容易被非法用户进行拷贝;

* 如果非法用户通过假冒某个服务器站点来接受用户的 cookies,以后他就可以使用这些收集到的 cookies 来对那些应该接收这些 cookies 的站点发动攻击。

由此可见,要在 Web 上实现基于角色的访问控制,其中一个必要的前提是所传递的 cookie 必须是安全的,因此为了保证上述过程的安全实现,需要做如下改进:

(1) 在 Web 服务器上安装 SSL,以防止他人在 cookie 传递过程中进行窃听。

(2) 将上述两个 cookie 加密后再发给客户端浏览器。

(3) 利用 ASP.NET 提供的功能,将 cookie 存放到浏

览器的内存中,这样可以防止他人从硬盘上拷贝 cookie。

以上改进很好地保证了 cookie 在客户端与服务器之间传递时的安全,其中(2)和(3)利用 ASP.NET 提供的类可以方便地实现。

4 结束语

基于角色的访问控制机制为管理用户与受保护资源提供了便利。文中从 Web 应用目前的发展状况与需求出发,分析了 Web 应用所需要的访问控制方式,并在此基础上采用 RBAC 模型,实现了在 .NET 环境下的 Web 应用程序访问控制。

参考文献:

- [1] Sandhu R S, Coyne E J, Feinstein H L, et al. Role - Based access models[J]. IEEE Computer, 1996, 29(2): 38 - 47.
- [2] Barkley J F, Cincotta A V, Ferraiolo D F, et al. Role Based Access Control for the World Wide Web[A]. Proc of 20th NIST - NCSC National Information Systems Security Conference, National Institute of Standards and Technology [C]. Baltimore, Maryland, U.S.A. :[s. n.], 1997.
- [3] 李敏波. ASP.NET 1.1 高级编程[M]. 北京:清华大学出版社, 2005.
- [4] Gaster B, Kent D, Sabbadin E, et al. ASP.NET 安全性高级编程[M]. 北京:清华大学出版社, 2003.
- [5] Park J S, Sandhu R, Gail - Joon Ahn. Role - Based Access Control on the Web[J]. ACM Transactions on Information and System Security, 2001, 4(1): 37 - 71.

(上接第 217 页)

显得极为重要。

本系统通过 VPN 实时地将这些数据写入到证据库中保存起来,被传送的数据一旦写入证据库,就使用 MD5 对存储的数据进行数字签名,使这些原始数据具有不可篡改性。

使用 VPN 通道提供强壮的认证和加密通信的优点在于:

①数据在传送前首先通过 VPN 认证,保证信息在传送过程中不被窃取;

②数据在传送前就已加密,因此没有任何明文数据在网络中传送;

③数据送达到证据库后,进行解密,以明文形式存储下来,同时使用 MD5 加密算法进行数字签名,以防数据被篡改。

5 结束语

计算机取证是网络诉讼的核心,是当前计算机犯罪案件侦查的关键技术。本系统将计算机取证与入侵检测结合起来,采用基于协议分析的入侵检测方法,提高了入侵

检测效率及数据分析能力,有助于解决动态取证的实时性;通过实时检测,根据入侵行为的类型,及时采取相应的响应措施,可以将入侵损失降到最低;同时系统采取了较全面的安全机制,以确保收集到的入侵证据的真实性、准确性及不可篡改性,使其成为有效的法庭证据。该系统是动态计算机取证的一种较好的解决方案。

参考文献:

- [1] 钟秀玉,凌捷. 计算机动态取证的数据分析与研究[J]. 计算机应用与软件, 2004(9): 26 - 27.
- [2] 张斌,李辉. 计算机取证——有效打击计算机犯罪[J]. 网络安全技术与应用, 2004(7): 59 - 61.
- [3] 唐正军,李建华. 入侵检测技术[M]. 北京:清华大学出版社, 2004. 208 - 211.
- [4] 丁菊玲,刘晓洁,李涛,等. 基于人工免疫的网络入侵动态取证[J]. 四川大学学报(工程科学版), 2004, 36(5): 108 - 111.
- [5] Kumar G. Classification and detection of computer intrusion [D]. Purdue University, 1995.
- [6] 黄文,文春生,欧红星. 分布式网络系统日志的安全性研究[J]. 零陵学院学报, 2004, 25(3): 66 - 68.