网络取证系统及工具分析

徐晓琴,龚 俭,周 鹏
(东南大学 计算机科学与工程系 江苏省计算机网络技术重点实验室,江苏 南京 210096)

摘 要:随着网络技术的发展,计算机网络犯罪总量持续上升,计算机取证工作显得越来越重要。计算机取证分为事后取证和实时取证。早期的实时取证所利用的网络安全工具在取证学角度都存在一定的局限性,它们所产生的数据不能成为法律意义上的证据。由此,网络取证系统应运而生,它对网络入侵事件、网络犯罪活动进行证据获取、保存、分析和还原,弥补了传统安全工具在实时取证中的不足。文中对网络取证系统进行了详细分析,并对目前的一些网络取证工具进行了比较。

关键词:网络取证系统;网络取证工具;网络安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1005-3751(2005)05-0139-03

Analysis of Network Forensics System and Its Tools

XU Xiao-qin, GONG Jian, ZHOU Peng
(Jiangsu Key Lab. of Computer Network Techn., Dept. of Computer Sci. & Eng.,
Southeast University Nanjing 210096, China)

Abstract: With the development of Web, the quantities of computer crimes are increasing and computer forensics is becoming more and more important. Computer forensics is divided into post-event investigation and real-time investigation. In the early days, network security tools were used in network forensics. But it is limited and the data that they produced can't be regarded as the evidence in the legal meaning. Network forensics system has made up these deficiencies in real-time investigation. It involves capturing, recording, analyzing and reconstructing network audit trails. The paper discusses the network forensics system and a detailed comparison has been made to these tools.

Key words: network forensics system; network forensics analysis tool; network security

0 引 言

随着互联网的飞速发展,计算机网络犯罪的总量持续上升。据有关部门统计,1999 年国内各类计算机违法犯罪案件共立案 908 起,2000 年共立案 2670 起,2001 年则达 2741 起。作为破获网络犯罪的重要环节——计算机取证引起了各界高度注视。计算机取证技术是防范黑客入侵的有效途径。它采取主动出击的方法,搜集入侵证据,重现入侵过程,分析攻击手段,有效地阻止黑客入侵[1]。电子证据同传统证据一样,必须是真实的、准确的、完整的、符合法律法规和可为法庭所接受的[2]。

计算机取证可分为事后取证和实时取证。事后取证,也称静态取证,是指计算机在已遭受入侵的情况下,运用各种技术手段对其进行分析取证工作。随着网络犯罪技术的提高,事后取证已无法适应要求,解决方案是进行实时取证。实时取证,也称动态取证,是指利用相关的网络安全工具,实时获取网络数据并以此分析攻击者的企图和获得攻击者的行为证据[3]。

收稿日期:2004-08-19
作者简介:徐晓琴(1979—),女,江苏苏州人,硕士研究生,研究方向为网络安全。

早期的实时取证主要利用 NIDS、Honeypot 等传统网络安全工具来实时分析网络数据流,然而,这些工具从取证学角度看都存在着一定的局限性。NIDS 存在误报和漏报,其检测结论往往是不全面或不完全准确的;另外,NIDS 对网络数据的处理并没有按照法律规定的程序(例如,在对网络数据进行分析时改变了原始数据),因此,其产生的数据是不符合证据要求的。Honeypot 模拟脆弱性主机,提供攻击目标,可以为追踪和分析攻击者的行为提供证据信息。但由于其相关技术还不成熟,主观上有引诱犯罪的可能,因此 Honeypot 所收集的信息目前还不能成为法律意义上的证据。

网络取证系统弥补了 NIDS、Honeypot 在实时取证中的不足,能给执法机关提供准确的、完整的、合法的电子证据。文中在对该系统进行详细分析的基础上,对现有的网络取证工具进行了功能比较。

1 网络取证系统分析

网络取证系统对网络入侵事件、网络犯罪活动进行证据获取、保存、分析和还原,它能够真实、连续地获取网络上发生的各种行为;能够完整地保存获取到的数据,并且防篡改;对保存的原始证据进行网络行为还原,重现入侵

现场[4]。

尽管网络取证系统与NIDS有许多类似之处,都是在监听模式下,使用协议解析技术和入侵分析技术对网络进行监控,但在设计重点上,两者存在着较大的差异。NIDS的设计重点是准确有效地发现受监控网络中的攻击行为,从而进行响应;而网络取证系统旨在获取黑客入侵时的法律证据,其设计重点在于有效证据的获取。网络取证系统的总体结构如图1所示。

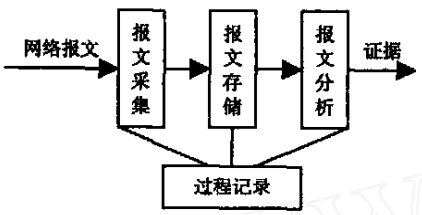

图1 网络取证系统总体结构图

1.1 报文采集

报文采集是实时取证的基本前提。基于证据的准确性和完整性,在获取报文的过程中,网络取证系统必须满足以下3个条件:

(1)数据获取的完整性,即不能对获取的网络数据进行修改或破坏;

(2)系统性能的可伸缩性,即网络流量对系统性能产生影响较小;

(3)工作方式的透明性,即不能影响到被测网络。

1.2 报文存储

对于获取的网络报文,NIDS只需对含有攻击特征的报文进行摘录,而网络取证系统出于证据获取完整性的原因,要求记录的报文必须是完整的,以便借助数据分析模块对报文进行基于应用协议的还原,追查到具体内容。

目前有两种记录报文的方式[4]。一种是将这些报文全部保存下来,形成一个完整的网络流量记录,采用这种方式的网络取证系统被称为"尽量获取"系统("Catch - it - as - you - can"system)。这种方式能保证系统不丢失任何潜在的信息,能最大限度地恢复黑客攻击时的现场,这对于研究新的攻击技术,进行安全风险评估都有很大的价值;但这种方式对系统存储容量的要求非常高。另一种是采用某种过滤机制排除不相关的网络报文,保存需要的网络报文。采用这种方式的网络取证系统被称为"停下来,观察并监听"系统("Stop,look and listen"system)。这种方式可以减少系统的存储容量需求,但有可能丢失一些潜在的信息,同时过滤进程还会增加系统负荷。这两种方式都需要引入淘汰机制来控制存储空间的增长。同时,系统还应采用诸如计算校验和的方式来检验数据的完整性。

1.3 报文分析

报文分析是网络取证关键,目的是识别入侵企图,并尽可能地以最小损失还原和重建网络中发生过的事情。

对报文的分析可以分为基本分析和深入分析两个阶段。基本分析能解决一般性的取证问题,同时为深入分析做准备,它包括对报文进行查询、分类、解码、简化等操作,其中,解码包括解密和协议分析。虽然NIDS也采用了协议分析等技术,但该技术在NIDS中仅作为一种模式匹配的加速手段,并没有进行深层次的利用;而网路取证系统中,协议分析则是作为一种重要的现场重现手段存在的。深入分析则包括对报文进行重组、寻找报文的来源、报文间的关联性分析、重建网络事件、图形化网络关系等。

与NIDS一样,网络取证系统也会有误报和漏报,但原始数据的存在,提供了充分、完全的现场资料,允许人们对之进行更深层次的分析和验证。

1.4 过程记录

为了保证"证据的连续性"——计算机取证中的一个重要原则,网络取证系统还应该具有贯穿全过程的记录功能,记录内容包括以下3项:

(1)网络取证系统当时的状态及性能情况,这样有利于对获取的数据及相关的分析进行正确评价;

(2)报文丢失情况,例如,丢失的时间,由哪个组件丢失的;

(3)操作人员在使用网络取证系统过程中的所有动作。

有的网络取证系统还具备报警功能,能及时通知安全人员进行事件处理,从而防止入侵事件的发生或减少相应损失。

2 网络取证工具的比较

这里从报文采集、报文存储和报文分析这3个方面对以下5个网络取证工具进行比较:NetWitness,InfiniStream,NetIntercept,NetDetector,SilentRunner。其中,除了NetIntercept属于"Catch - it - as - you - can"system外,其他4个工具均属于"Stop,look and listen"system[5]。

2.1 报文采集功能比较

文中以这些工具所支持的网络接口及报文采集速度来比较它们的报文采集功能,如表1所示。其中,NetDe-

表1 网络取证工具报文采集能力分析

工具	报文采集功能分析
NetWitness	一般
InfiniStream	工作于G比特Ethernet SX,报文采集速度较快,可达1,200Mbps
NetIntercepter	功能较强,它能在10/100/1000 BaseT局域网上或高速的交换机的某个端口上进行报文采集。实验表明,NetIntercept在满负荷的100Base - T网络中的报文采集率达99.9%,而在非满负荷情况下,其报文采集率达99.99%
NetDetector	功能强大,几乎支持所有网络接口,如T1/E1,以太网,X.21,V.35,ATM/POS - OC - 3/OC - 12,T3/E3,HSSIFDDI,PPP等
SilentRunner	支持10/100MB以太网,T1,T3等

tector 以其强大的网络报文采集功能著称,它几乎支持各种网络接口。

2.2 报文存储功能比较

文中以这些工具的存储容量来比较它们的报文存储功能。NetDetector 的内部存储容量可达 1.46TB 外部存储容量是无限的,因为它采用了 SAN;Infinistream 的存储容量达 2.9TB;Net Intercepter 则采用 CD - RW 来保存大量数据;NetWitness 则利用数据库来保存数据。

2.3 报文分析功能比较

NetWitness、Infinistream 的分析方式较其他 3 个少,分析功能也没有其他 3 个强。

Net Intercepter、NetDetector 具有很强的基本分析能力,它们自带网页浏览功能,能对网络流量进行重现并进行趋势分析,它们都还具有报警功能。Net Intercepter 最大的特点是能解密 SSH - 2 会话,而 NetDetector 则以较强的报警功能著称,可以手工配置其报警种类,包括:主机扫描,端口扫描,主机泛洪,TCP 计数等。

Silent Runner 以分析和图形化功能的强大而著称[5]。它采用 N - gram 分析方法对流量进行关联性分析(N - gram 分析法是将大规模的文本数据分解成 n 个较小的片断,然后对这些片断进行统计分析,寻找片断间的相同点,从而找出这些大规模数据间的联系),它能绘制出网络的三维图像,重现网络中发生的事件,有助于管理员对发生的事件作出更准确的判断。

总的来说,Net Intercepter 和 NetDetector 具有最好的基本分析能力,对于一般的取证分析已经足够了;而 Silent Runner 的 N - gram 分析方法和三维图形化功能更利于进一步的数据分析。

3 结　论

通过对现有的网络取证工具进行比较可以看出,这些工具大多侧重于对事件的分析,而对数据的安全性方面考虑的不是很多,因此,现阶段的网络取证工具还是不成熟的。今后的工作可以朝以下几个方面发展。

对于存储的网络流量,需要对它们进行完整性检查,这可以在系统中或系统外实现。为了保证"证据的连续性",网络取证系统应具有记录功能,记录包括数据丢失源、系统状态及性能、操作人员的行为。最后,还应将数据的输入输出格式进行统一,这样有利于工具间互相协作。

参考文献:

[1] 余晓雯,高　强,丁　杰. 一种入侵检测取证系统模型的设计[J]. 微机发展,2004,14(8):117 - 119.

[2] 许榕生,吴海燕,刘宝旭. 计算机取证概述[J]. 计算机工程与应用,2001,21:7 - 8.

[3] 梁锦华,蒋建春,戴飞雁,等. 计算机取证技术研究[J]. 计算机工程,2002,28(8):12 - 14.

[4] Corey V,Peterman C. Network Forensics Analysis[EB/OL]. http://www.sandstorm.net/downloads/netintercept/ni - ieee.pdf,2002 - 10.

[5] Sira R. Network Forensics Analysis Tools:An Overview of an Emerging Technology [EB/OL]. http://www.giac.org/practical/GSEC/Rommel_Sira_GSEC.pdf,2003.

(上接第 138 页)

况,对于内存分区中内存块数大于 64 的情况可以建立两个或几个内存块大小相同的内存分区来实现。但是也可以用三级内存管理(把上面的方法称为二级内存管理,因为是先通过在 OSMemGrp 中找到在 OSMemTbl[ ]中对应的组,再在对应的组中分配和释放相应内存块)。即在 OSMemTbl[ ]中每一位对应相应的 8 个为一组的内存块,这样一次就可以在一个内存分区中管理 512(8^3)个内存块,不过这样将增加算法的难度,同时分配和释放内存块的时延也将增加。因此在应用中应避免用三级内存管理。另外,对于内存分区的内存块数不超过 8 的情况,用一级内存管理就可实现,其分配和释放内存块的速度较二级内存管理要快,实现也很简单。

3 结束语

文中分析了 μC/OSII 中的内存管理方法后,再提出了一种改进的内存管理方法。其实,μC/OSII 的内存管理还有需要改进的地方,例如,现在的内存管理只支持固定大小的分区,而实际应用中有动态分配非固定分区的需求。这就要求 μC/OSII 有实现该功能的软件结构和内存分配、回收算法[4,5]。在嵌入式应用中,应针对具体的应用采用合适的内存管理方法,这样对提高开发系统的性能和节约资源都有很大的作用。

参考文献:

[1] 彭良清. μC/OS - II 任务栈处理的一种改进方法[J]. 单片机及嵌入式系统应用,2003(1):106 - 108.

[2] Labrose J J. μC/OS - II ——嵌入式实时操作系统(第 2 版)[M]. 邵贝贝译. 北京:北京航空航天大学出版社,2003.

[3] 封　斌,龚　灼,杨学军. 实时操作系统保护模式下的内存管理策略[J]. 武汉:华中科技大学学报(自然科学版),2002,30(3):94 - 96.

[4] Noble J,Weir C. Small Memory Software Patterns For System With Limited Memory[M]. 侯　捷,王　飞,罗　伟,译. 武汉:华中科技大学出版社,2003.

[5] 王保进,王志刚,刘恒禹. μC/OS - II 实时操作系统内存管理的改进[J]. 电子技术应用,2002(5):19 - 21.