

中国传媒大学 2017-2018 学年第 二 学期

课程编码 113008

课程名称 信息安全管理

题 目 信息系统安全审计在计算机
取证方面的应用分析

学生姓名 郭韵婷

学 号 201511123021

班 级 2015 级信息安全班

学生所属学部、学院 计算机学院

任课教师 曹刚

教师所属学部、学院 计算机学院

平时成绩

结课论文成绩

总评成绩

信息系统安全审计在计算机取证方面的应用分析

郭韵婷

学号: 201511123021, 班级: 信息安全 2015 级

摘要: 维护信息系统安全的第一步即发现安全风险和系统脆弱点, 这需要我们能熟练运用信息系统安全审计的相关流程与方法。而安全审计的主要应用之一就是进行计算机取证, 当犯罪分子利用计算机进行违法犯罪时, 安全专家可以采取多种方式分析采集到的信息, 将统计得出的结果以电子证据的形式提交给法庭, 作为审判的依据给犯罪者应有的制裁。虽然计算机取证有很好的应用前景, 但是目前我国取证相关法律方面的建设仍不健全, 随着技术的快速发展, 计算机犯罪手段的不断提高, 我们需要健全规范的计算机取证流程, 加强计算机取证技术研究, 制定和完善相关的法律法规。

Abstract: The first step in maintaining the security of information systems is to identify security risks, that is, system vulnerabilities. This requires us to be proficient in the related processes and methods of information system security auditing. One of the main applications of security auditing is computer forensics. When criminals use computers to commit crimes, security experts can use various methods to analyze the collected information and submit the statistical results to the court in the form of electronic evidence. As a basis for the trial, the offender should be given sanctions. Although computer forensics has good application prospects, the construction of related laws for evidence collection in China is still unsound. With the rapid development of technology and continuous improvement of computer crime methods, we need a sound and standardized computer forensics process. Research on computer forensics technology, formulate and improve relevant laws and regulations.

关键词: 安全审计; 计算机取证; 计算机犯罪; 信息安全

Keywords: Security Audit; Computer Forensics; Computer Crime; Information Security

1 研究背景

如今信息系统各项技术快速发展, 为个人与社会带来巨大利益的同时, 一些风险也随之而来。互联网技术使用户可以快速、廉价的访问网站、数字图书馆或其他数据来源提供的大量信息[1]。但如果控制不当, 可能会使信息系统受到欺诈、破坏等恶意的行为的影响。据安永会计师事务所的调查显示, 安全事件每次发生时可能使公司花费 17 至 28 百万美元[2]。另一项持续 13 年的调查显示[3], 病毒事件发生频率最高 (占答复者组织的 49%), 次发生频率最高的事件是内部滥用网络 (44%), 其次是盗窃笔记本电脑和其他移动设备 (42%)。此外, 除了外部威胁外, 还有很大一部分风险 (有时超过风险总数的 50%) 来自合法网络用户。

虽然很多的安全技术可应用于阻止系统入侵、防止数据泄露或越权访问等，但具体措施的选择应根据当前信息系统所面临的潜在风险所决定，因此，进行系统安全维护的第一项工作就是识别风险，即进行系统安全审计。系统管理员根据一定的安全策略，通过记录和分析历史操作事件及数据，发现系统脆弱点而后进行对应的系统安全维护与措施的改进，能够大大提升信息系统安全维护的有效性。

综上，安全审计是揭示信息安全风险的首要工作和最佳手段。同时，进行计算机取证是安全审计的主要功能之一。通过利用审计工具对系统活动进行监视与记录，可为已发生的系统破坏性行为提供追究的重要证据。据统计，计算机取证技术已经得到了广泛应用，现在美国至少有 70% 的法律部门拥有自己的计算机取证实验室，取证专家在实验室内分析从犯罪现场获取的计算机，试图找出犯罪者和犯罪行为的相关信息[4]。

本文第 1 节介绍该课题的研究背景，第 2 节介绍信息系统安全审计的基本理论，第 3 节介绍该理论在计算机取证方面的应用，第 4 节给出一个完整的取证案例，第 5 节从个人理解的角度，分析现有技术的局限性和难点。第 6 节对计算机取证技术的发展做出总结与展望。

2 信息系统安全审计概述

2.1 安全审计的概念

信息系统安全审计是计算机技术与法学、审计学等多门学科交叉发展的产物，主要在信息安全领域针对用户行为进行事件采集与事件分析，以方便接下来的事件响应工作。ISO/IEC15408-2:1999《信息技术安全性评估准则》中对信息系统安全审计（ISSA, Information System Security Audit）给出了明确定义[5]：安全审计涉及识别，记录，存储和分析与之相关的信息安全相关活动；由此产生的审计记录可以检查以确定哪些安全相关活动发生以及谁（哪个用户）对他们负责。其具有的对系统事件的记录功能，能够为网络违法犯罪最行为及非法泄密等恶意操作提供取证重要依据。通过对大量安全事件与用户行为的收集和分析，对特定高嫌疑对象进行追踪，能够提高事后分析和取证的效率和准确度，进而有效保护信息系统的安全。

2.2 安全审计的系统模型及流程

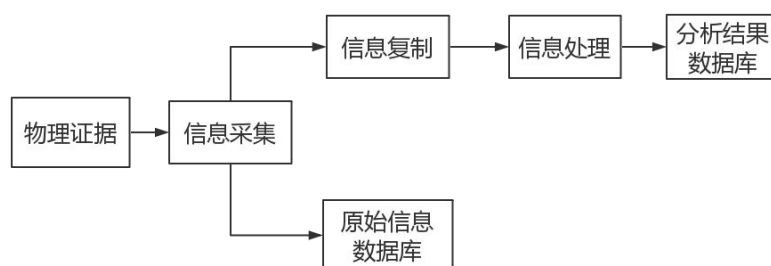


图 1 信息系统安全审计流程

安全审计模型主要由三部分组成：

1) 信息采集单元

按预定审计策略对除入侵检测系统外的其他客体进行相关审计事件采集，将结果传递给后续各组件。

2) 信息处理单元

对事件进行分析，将分析结果形成审计报告，交由响应单元。

3) 系统响应单元

对事件分析的结果采取对应行动,生成审计记录存入审计数据库并进行备份。

3 信息系统安全审计在计算机取证方面的应用

3.1 计算机取证的概念

二十世纪八十年代初,个人电脑渐渐被消费者所接受,其中有一些被用于犯罪活动(例如实施欺诈行为、冒名顶替、逻辑炸弹等),该类犯罪具有隐蔽性高、手段智能化、复杂度高、损失大且发展迅速等特点。计算机取证学科在此期间出现,作为恢复和调查数字证据以供法庭使用的一种方法。今天该方法用于调查各种各样的犯罪,包括儿童色情、间谍活动、谋杀和强奸等。这门学科在民事诉讼中也具有信息收集的功能。取证技术分析的范围可以从简单的信息检索到重构一系列事件。在2002年出版的计算机取证书中,作者 Kruse 和 Heiser 将计算机取证定义为涉及“保存,识别,提取,记录和解释计算机数据”[6]。

通俗地讲,当有与计算机技术相关的犯罪发生时,计算机中会留下大量与犯罪有关的数据。计算机取证就是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。取证的目的是找出入侵者,并解释入侵过程。与其他证据一样,电子证据必须是真实、可靠、完整和符合法律规定的。

3.2 安全审计模型在计算机取证中的运用

在信息采集阶段,要尽早采集数据,保证证据的连续性,最重要的是保证其没有被破坏。在不对原有物证进行任何改动或损坏的前提下获取证据。

信息的采集一般包括物理证据的获取和数字信息的发现两个阶段[4]。物理证据的获取是指调查人员来到计算机犯罪现场,寻找并扣留相关的计算机硬件,而信息发现是指从原始数据(文件,日志等)中寻找可以利用的信息。在物理证据收集阶段,调查者应遵循的原则有[7]:

- 1) 不要改变原始记录;
- 2) 不要在作为证据的计算机上执行无关的程序;
- 3) 利用反销毁技术,不要给犯罪者销毁证据的机会;
- 4) 详细记录所有的取证活动;
- 5) 妥善保存得到的物证。

取得物理证据后进行关键信息的发掘,通常情况下,考虑从系统日志、数据文件、缓存、网络数据等多方面获取信息[7],常采用的技术有备份技术以及恢复技术。专家通常将原信息文件妥善存储,基于数据备份去进行下一步的分析。该步骤可采用的硬件包括硬盘拷贝机以及硬盘拷贝光盘[8]。

在信息处理阶段,取证专家依靠恢复的数据进行分析。主要进行的工作包括:关键字查询、文件属性分析、数字摘要比对、对加密文件进行解密、鉴定设别来源、鉴定软件来源、鉴定 IP 地址来源以及对内容进行分析等。对得到的数据进行统计,进而分析攻击者的身份、攻击意图、攻击方法等可攻监察机构使用的电子证据。目前有一些以开发好的网络取证分析(NFA)平台,主要功能即包括数据恢复、数据识别、信息检索和信息鉴别[8]。

在响应阶段,法庭通过参考得到的相关明确且符合法律规范的电子证据和相应说明文档对事件进行评估,做出合理的判决结果。

整个过程中所有的电子数据和文档会在保证完整性、真实性、机密性等的基础上以 xml 形式存入检方数据库。专家应确保完整的记录下所采取的每一个步骤以及采取该步骤的原因。

4 案例分析

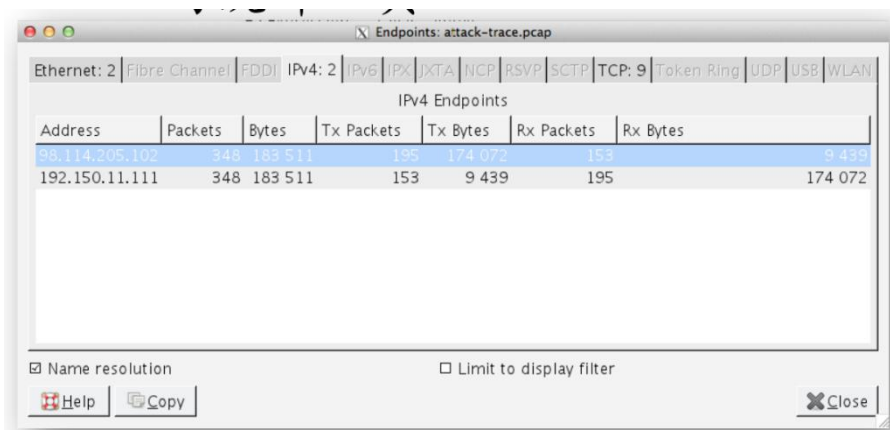
上一节介绍了安全审计及计算机取证的主要原理与技术，接下来对一个具体案例进行分析，该实例为对在受害者主机上抓取的 pcap 包进行分析，得到攻击者相关信息，该案例仅作为实验分析使用[9]：

1) 已掌握的原始证据

wireshark 抓包捕获的数据 (.pcap 格式)。

2) 分析攻击者主机信息

使用 tshark 或 wireshark 统计工具，对报文的 ip_host 字段进行统计，获取可能的所有数据包来源的 IP 地址和发包数量等基本信息，见图 2。



IPv4 Endpoints						
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
98.114.205.102	348	183 511	195	174 072	153	9 439
192.150.11.111	348	183 511	153	9 439	195	174 072

图 2 使用 wireshark 工具统计的该 pcap 包内所有数据包基本信息

接下来通过根据 tcp 标示字段 (tcp.flags==0x02) 进行过滤，发现进行网络连接的发起者，其对应 IP (即图 3 中的 98.114.205.102) 很大可能为攻击者主机 IP。

```

1 0.000000 98.114.205.102 -> 192.150.11.111 TCP 1821 > 445 [SYN] Seq=0
Win=64240 Len=0 MSS=1460
5 0.134550 98.114.205.102 -> 192.150.11.111 TCP 1828 > 445 [SYN] Seq=0
Win=64240 Len=0 MSS=1460

```

图 3 统计网络连接的发起者信息

3) 分析攻击持续时间

```

File name:          attack-trace.pcap
File type:          Wireshark/tcpdump/... - libpcap
File encapsulation: Ethernet
Number of packets:  348
File size:          189103 bytes
Data size:          183511 bytes
Capture duration:   16 seconds
Start time:         Mon Apr 20 11:28:28 2009
End time:           Mon Apr 20 11:28:44 2009
Data byte rate:     11314.42 bytes/sec
Data bit rate:      90515.34 bits/sec
Average packet size: 527.33 bytes
Average packet rate: 21.46 packets/sec

```

图 4 capinfos 统计的 pcap 包信息

通常攻击的持续时间小于捕获到的攻击者发送的数据包的起止时间。使用 capinfos 命令统计所需

(3) 执行攻击指令阶段

追踪对应包的 TCP 流，发现此次攻击目的为建立 ftp 远程连接后下载远程恶意代码，见图 8。



图 8 攻击指令

(4) 建立 FTP 会话，见图 9



图 9 FTP 会话信息

(5) 下载恶意程序

图 10 中为恶意程序 ssme.exe。



图 10 恶意程序 ssme.exe

6) 将所得计算机证据收集并进行文档记录，而后交由司法机关，相应所有文件存档。

至此，我们完成了一次计算机取证工作。获得了攻击者的 IP 及攻击行为，对攻击程序进一步分析可得到攻击目的。

上述案例为日常实验案例，流程与方法上还存在一些局限性和不合理性，分析如下：

1) 取证分析不合理

该实例直接在原始介质上进行分析，破坏了证据的原始性并且可能导致证据被有意或无意破坏，同时可能导致数据的丢失。

2) 判定依据不合理

单依据 IP 来判定网络行为可靠性较低，应辅助以其他手段。

3) 局限性

(1) 为方便实验, 该 pcap 包中截获的报文数量有限, 但实际取证过程中涉及的数据包数量很多, 但依靠可疑 IP 的筛选效率和可靠性都比较低。

(2) 本实例大量依靠手工分析及专家的经验, 效率较低, 应考虑引入自动化分析平台及工具, 应用大数据挖掘技术对电子证据进行分析归类。

(3) 本实例中的攻击指令及恶意代码都为明文形式传输, 而现实生活中犯罪者往往应用数据擦除和数据隐藏等技术, 通过对文件类型进行伪装以及对可执行文件进行加密来给工作人员的分析带来困难, 因此真正分析时还应考虑是否需要数据进行解密、文件还原、攻击过程重构等操作。

(4) 只针对于获取的 pcap 包分析, 证据不够充分。若能追踪到攻击者主机位置, 可以通过收集磁盘上的辅助信息和现场的其他存储介质等, 获取更多数字证据。

5 计算机取证技术局限性分析

目前我国还很难找到能对计算机上所有数据进行综合分析的可靠软件, 信息的发现与分析还主要依靠手工方式, 这对相应工作人员的知识掌握情况具有很高的要求, 而且, 对各式各样的电子证据的收集方式与可靠性分析以及如何证明它们和犯罪相关还没有一个统一的标准, 因此, 计算机取证技术还存在着一些应用局限性。

在取证流程方面, 具体的难点可能包括: 信息采集过程中和相关权利的冲突和协调, 在需要用到监听等收集方法的情况下, 如何保证相关人士的权利; 电子证据具有不稳定性, 收集人员也存在故意损毁或更改的可能性; 电子证据的分析过程必须遵守法律法规或法定流程, 如何降低办案人员不科学取证的概率, 增加电子证据的可信性等。可见不管哪一个环节出现问题, 都有极大的可能侵犯公民的隐私权。

在技术实现方面, 具体的难点包括: 计算机犯罪取证软件不够成熟, 对磁盘上的数据进行恢复与分析的难度很大; 随着计算机技术的发展, 很多反取证技术被攻击者利用, 包括数据擦除、数据隐藏、数据加密和操作痕迹的删除; 黑客还可以利用后门、木马病毒等手段获取目标系统的权限, 冒充合法用户进行相应的违法操作[10], 使计算机取证变得更为困难。

综上, 由于多方面的局限性和计算机犯罪手法的多样性, 计算机取证技术还需要进一步的发展以及与其他领域技术相融合, 才能满足实际大规模运用的需求。

6 总结与展望

信息系统安全审计的思想能很好的指导我们的计算机取证过程, 为打击基于计算机与网络的违法犯罪行为做出了卓越贡献, 在维护国家安全、保障消费者或公民权益等方面具有巨大的应用前景。然而我国的相关法律法规仍有待健全, 取证的技术也有待提高, 相信相关人员一定会加大对该方面的投入, 未来我国计算机取证的发展趋势可能包括:

- 1) 在系统的研究与设计阶段即考虑计算机取证的需求;
- 2) 利用数据挖掘、机器学习等方法, 时下取证工具的自动化与集成化;
- 3) 标准化工作将逐步展开, 我国针对计算机取证的法律法规将逐渐完善;
- 4) 国家将会培养更多专业技术人才。

相信随着技术的不断进步, 未来对计算机违法犯罪的打击将越来越有效与彻底。

参考文献

- [1] A. M. Suduc, M. Bizoi and F. G. Filip, “Ethical Aspects on Software Piracy and Information and Communication Technologies Misuse,” Preprints of IFAC SWIIS Conference, Bucharest, 2009.
- [2] A. Garg, J. Curtis and H. Halper, “Quantifying the Financial Impact of IT Security Breaches,” Information Management & Computer Security, Vol. 11, No. 2, 2004, pp. 74-83.
- [3] R. Richardson, CSI Computer Crime & Security Survey, 2008, Retrieved January 2010, from Department of Computer Science and Engineering, Available at: <http://www.cse.msstate.edu/~cse6243/readings/CSISurvey2008.pdf>
- [4] 王玲, 钱华林. 计算机取证技术及其发展趋势. 软件学报. 2003, 14(09): 1635-1644
- [5] ISO/IEC 15408-2: <http://www.comsec.spb.ru/materials/is/iso15408-2.pdf>
- [6] Computer forensics: https://en.wikipedia.org/wiki/Computer_forensics
- [7] Parra M. Computer forensics. 2002. http://www.giac.org/practical/Moroni_Parra_GSEC.doc.
- [8] 计算机取证与日志分析:
http://www.cert.org.cn/upload/2005AnnualConferenceCNCERT/5Product&ServicesTrack/CFKAT_YanZeming.pdf
- [9] 网络安全 第十二章 计算机取证: <http://sec.cuc.edu.cn/huangwei/course/2016/nsLecture0x12.pdf>
- [10] Grand J. pdd: memory imaging and forensic analysis of palm OS devices. In: Proceedings of the 14th Annual Computer Security Incident Handling Conference. Waikoloa, Hawaii: Forum of Incident Response and Security Teams, 2002. <http://www.mindspring.com/~jgrand/pdd/pdd-palm-forensics.pdf>.