

基于蜜罐技术的计算机动态取证系统研究

鄢喜爱^{1,2}, 杨金民¹, 常卫东²

(1 湖南大学 软件学院, 湖南 长沙 410082; 2 湖南公安高等专科学校 计算机系, 湖南 长沙 410138)

摘 要: 提出了一种基于蜜罐的计算机动态取证方法. 该方法通过蜜罐技术将入侵转移到一个虚拟的环境, 不仅可以保护网络或主机不受攻击, 而且还可以为证据的提取争取到更长的时间, 从而获得更为真实的电子证据. 实验结果表明: 基于蜜罐的动态取证系统具有检测率高、误报率低、取证能力强的特性.

关键词: 网络安全; 计算机犯罪; 动态取证; 蜜罐

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2010)01-0135-03

Research of Dynamic Computer Forensics System Based on Honeypot

YAN Xi-ai^{1,2}, YANG Jin-min¹, CHANG Wei-dong²

(1 Software College, Hunan University, Changsha 410082, China;

2 Department of Computer, Hunan Public Security College, Changsha 410138, China)

Abstract: A dynamic computer forensics method based on honeypot is presented in this paper. This method can transfer the intrusion to a virtual environments with honeypot. It can not only protect the network or host, but also gain the more time for gathering evidence, so that the more authentic evidence can be achieved. Experimental result shows that the system remains higher detection rate and lower false alarm rate and better forensics ability.

Key words: network security; computer crime; dynamic forensics; honeypot

1 引言

随着信息技术的不断发展, 计算机网络越来越多地参与到人们的工作和生活中. 与此同时, 网络安全事件也呈上升趋势, 计算机犯罪逐渐增加. 当今主流的信息安全技术如防火墙、数据加密、入侵检测等可以从一定程度上预防入侵事件的发生, 但并不能够防止所有入侵^[1]. 为此, 借助法律来对入侵者实施惩罚和威慑已成为重要的手段, 此手段的关键是找到真实、可靠、具有法律效力的电子证据, 计算机取证技术也就应运而生.

2 对现有取证技术的观察和启发

通过仔细分析现有取证技术的研究, 主要有以下两点观察和启发:

观察 1: 现有计算机取证技术的研究多为静态

分析方法, 不能够在入侵的同时或者一定的时限内自动获取合法的证据. 这种静态的取证模式对于新兴的反取证技术(如数据隐藏技术、数据擦除技术等)则显得无能为力.

启发 1: 取证系统必须采用实时的动态方式对电子证据进行提取和保存, 能在网络攻击行为发生的时候自动地收集网络攻击证据并对攻击行为做出反应.

观察 2: 现有计算机取证方式多为被动方式, 证据获取的主动性不足, 加之防御系统可能会在遭到网络攻击时立即切断网络连接或整个系统处于瘫痪, 证据的完整性也会受到影响.

启发 2: 蜜罐(Honeypot)是一种主动防御的网络安全技术, 可以吸引入侵者的攻击, 保护工作网络免于攻击, 还可以模仿提供一些服务, 从而有比较长的时间监视和跟踪入侵者的行为并以日志形式记录

收稿日期: 2008-12-30; 修回日期: 2009-02-08

基金项目: 国家自然科学基金项目(60473031); 公安部应用创新计划项目(2006YYCXHNST024)

下来进行分析,从而学习入侵者的工具、策略和方法[2].

基于以上两点观察和启发,文中设计了一种基于蜜罐技术的计算机动态取证系统,该系统能及时主动获取完整的电子证据,并在遭到网络攻击时利用重定向技术保护被取证端免受攻击.

3 基于蜜罐技术的计算机动态取证系统

基于蜜罐技术的计算机动态取证系统的拓扑结构如图 1 所示.

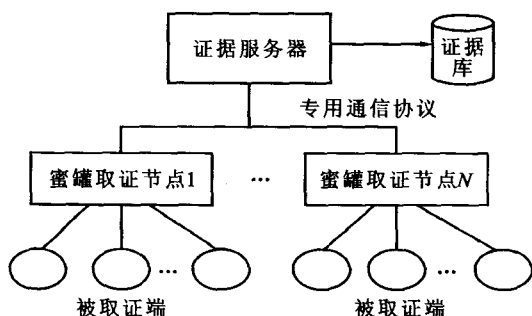


图 1 系统的整体拓扑结构图

系统采用具有蜜罐特性的取证节点组成三层分布式体系结构. 证据服务器是全局事务的控制中心, 负责取证任务的发起, 接收来自蜜罐取证节点的取证结果, 在进行数字签名验证之后, 将取证结果进行筛选、组合和重构, 使之能再现整个事件的攻击过程, 并生成完整的报告, 在加盖时间戳之后保存到证据服务器的证据库中[3]. 蜜罐取证节点层是本系统的关键层, 负责某逻辑网段中被取证端证据的实时采集、分析、保存, 并将取证结果通过专用的通信协议提交给服务器.

蜜罐取证节点的结构如图 2 所示. 当有可疑行为发生时, 虚线上部分的模块提供蜜罐服务, 虚线下部分的模块完成取证任务. 蜜罐服务运行在用户空间, 名义上是一个真实的服务, 其实是一个诱饵, 受到取证模块的监控, 取证模块运行在内核空间. 整个蜜罐取证节点的取证流程包括证据的检测、提供蜜罐服务、证据的分析提取、证据的签名传送等 5 个部分.

3.1 证据检测

为了方便检测, 在证据服务器上设置了一个初始的特征知识库, 初始知识库收集了常见攻击行为的特征记录, 并通过系统的自学习不断的更新, 实时发布到蜜罐取证节点. 经过检测模块的外网数据流的流向如图 3 所示.

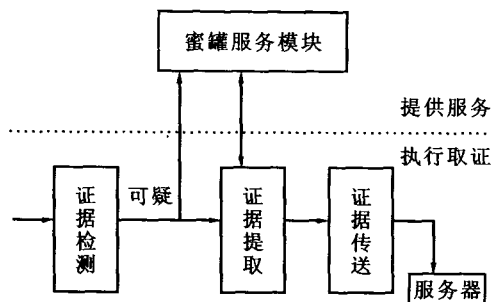


图 2 蜜罐取证节点的功能模块及流程

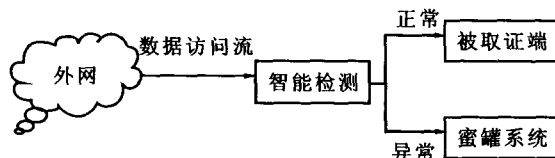


图 3 经过智能检测模块的外网数据流向

智能检测模块通过对网络数据流的捕捉和分析, 对网络的运行情况进行实时监控. 正常情况下, 检测模块连接的是被取证端, 当发现有可疑入侵行为时, 检测模块将攻击行为实时漂移到蜜罐服务系统中, 整个漂移过程对于攻击者来说是透明的, 被取证端仍旧对正常访问者提供服务. 在漂移的同时, 发送一个取证请求消息给取证模块开始取证.

3.2 蜜罐服务系统

蜜罐服务模块通过检测模块的漂移功能来改变攻击者的攻击目标. 它向攻击者展示一个虚拟的仿真环境, 故意设置一些虚假的敏感信息和常见的网络服务对攻击者进行跟踪分析, 并保证对入侵行为有一定的控制能力[4-5]. 为了降低系统资源的开销, 本系统的蜜罐服务模块采用开放源代码的低交互虚拟蜜罐框架 Honeyd 来搭建. Honeyd 可以自动收集日志信息, 记录黑客使用某服务的痕迹[6]. 在搭建蜜罐过程中, 通过模拟操作系统的部分 TCP/IP 栈来建立蜜罐, 即在网络级模拟虚拟蜜罐系统(含操作系统及设备), 其方法是使用与 Nmap 或 Xprobe 相同的指纹数据库来模拟操作系统, 以响应入侵者对虚拟蜜罐的网络请求.

3.3 证据提取

证据提取的来源主要是检测模块对数据包的分析情况和蜜罐系统的日志审计信息. 证据提取的内容主要包括两大部分[7]: 一部分是入侵发生时的主机运行参数, 例如系统内存信息、CPU 使用率、进程运行状况、缓冲区信息、磁盘文件的读写等, 获得这些数据实际上是对整个攻击现场的快照, 是还原入侵犯罪场景不可缺少的因素. 另外一部分是网络通

讯情况,如网络数据包大小、数据流量、攻击方源地址、目的地址、端口、使用协议、网络连接数量、连接时间、连接类型等。

3.4 证据传送

证据获取之后,最终要存到服务器的证据库。为了保证原始的电子证据安全有效的传送到证据服务器,在证据传输时设置了专用的通信协议对证据进行数字签名,其实现流程如下:

(1) 通过增量备份的方式从本地证据库中找到将要传输的证据信息 M 。

(2) 利用 SHA 安全散列函数计算出要传输信息的散列码,记为 $h = H(M)$ 。

(3) 发送方用其私钥 K_{Ra} 对散列码进行加密,形成数字签名,然后用一个对称密钥 K 对附加了数字签名(加密的散列码)的消息进行加密,得密文信息 $C = E_k[M \parallel E_{kRa}[H(M)]]$

(4) 发送密文信息 C 至证据服务器。

4 实验分析评价

根据上述设计的模型,文中开发了一个加载蜜罐 Honeyd 的动态取证原型系统(简称 HCF),并在操作系统为 Redhat Linux 9.0、硬件为 2.4GHz 奔腾 IV 处理器、512MB 内存环境下,进行了检测效率、取证能力两个方面的测试。为了更好地说明各个类别的检测情况,与没有加载蜜罐的取证系统(简称 NHCF)进行了比较。

(1) 检测率和误报的测试:检测率和误报是检测系统最重要的指标。检测率可定义为发生入侵行为时系统发出报警的概率;误报率 False Alarm 定义为没有发生入侵行为时,系统发出报警的概率。实验的数据取自 KDDCUP99 数据集。该数据集中包含的攻击类型有 4 种: DOS 类、PROBE 类、U2R 类、R2L 类。由于训练数据集数据量巨大,从 10% 训练集中随机抽取 20000 条记录作为训练集,从 10% 测试集中随机抽取 10000 条记录数据作为测试集。实验结果如图 4 所示。

从图 4 可以看出,基于蜜罐技术的取证系统的性能要明显优于无蜜罐的取证系统。在所有的入侵中 DOS 攻击的检测准确率最高误报率最低,而 R2L 攻击的检测准确率最低误报率最高,出现这种现象的原因主要是 R2L 类攻击的数目很少,导致训练过程中得出的条件概率误差较大。

(2) 取证能力测试:利用 VC6.0 编写一个

SYNFLOOD 攻击的程序,对某一被取证机进行攻击。在无蜜罐时,由于被取证端在几秒钟之内就陷入瘫痪状态,所以取证节点仅能获取 IP 地址和端口号。在加载蜜罐之后,证据检测模块成功将连接漂移到虚拟蜜罐,由于蜜罐提供的是一个虚假服务,所以整个系统并未受影响。取证节点还可获取到进程运行状况、网络数据包大小、数据流量使用协议、网络连接数量、连接时间、连接类型等信息。

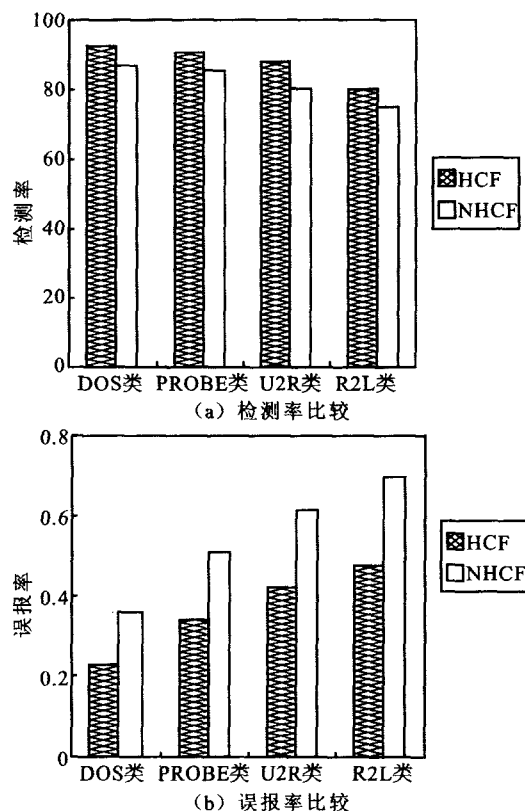


图4 有无蜜罐时检测率与误报率的比较

5 结束语

文中提出了将蜜罐技术应用到计算机取证当中,所设计的动态取证原型系统具有检测率高、误报率低、取证能力强的特性。此外,蜜罐取证节点自治地完成取证任务,有效减轻了证据服务器的负载和网络通信的瓶颈问题。如何更加逼真地模拟被取证端的真实环境又不暴露敏感信息,即可更为隐蔽地将入侵者诱惑至蜜罐中,是下一步工作的重点。

参考文献:

- [1] Marcus K, Kate S. The future of computer forensics: a needs analysis survey[J]. Computers & Security, 2004, 23(1): 12-16. (下转第 140 页)

$(D'_0, D'_1 = D'_0)$ 是不同的. 但是, 以后签名者在需要时还可以证明签名 $\delta(m)$ 和 $\delta'(m)$ 是同一个人产生的环签名, 因为只有签名者本人能够证明这两个签名的参数 a 是相同的.

4 安全性分析

(1) 强匿名性

即使攻击者知道了环成员的所有私钥和随机数 $a = \log_{D_0} D_1$, 攻击者也不能判断出签名者的身份. 因为, 对于消息 m 的环签名 $\delta(m) = (D_0, D_1, c_1, \dots, c_n, s_1, \dots, s_n, s_A)$, 对于 $1 \leq i \leq n$, 都有 $s_i = \log_g R_i - x_i c_i \bmod q$, 所以, 攻击者不能判断出谁是真正的签名者.

(2) 可选择联接性

签名者既可以产生可关联的环签名, 也可以产生不可关联的环签名: 如果签名者 P_π 用相同的参数 (D_0, a) 产生了两个环签名, 则联接标签 (D_0, D_1) 在这两个签名中是相同的, 因此, 这两个环签名是可联接的; 如果两个环签名中, 签名者 P_π 用不相同的参数 (D_0, a) 和 (D'_0, a') , 则, 联接标签 $(D_0, D_1 = D'_0)$ 和 $(D'_0, D'_1 = D'_0)$ 是不同的, 因此, 这两个环签名是不可联接的.

签名者可以选择产生不可联接的环签名, 以后签名者在需要时还可以将签名转换成可联接的环签名: 签名者 P_π 用参数 (D_0, a) 和 (D'_0, a') 产生了两个环签名, 因为联接标签 $(D_0, D_1 = D'_0)$ 和 $(D'_0, D'_1 = D'_0)$ 是不同的, 因此验证者不能确定 $\delta(m)$ 和 $\delta'(m)$ 是同一个人产生的环签名. 但是, 以后签名者在需要时还可以证明签名 $\delta(m)$ 和 $\delta'(m)$ 是同一个人产生的环签名, 因为只有签名者本人能够证明这两个签名的参数 a 是相同的.

5 结束语

文中提出的环签名框架采用随机数作为可关联标签, 设计了一种具有强匿名性和可选择关联的环签名框架, 并对环签名框架进行了强匿名性和可选择联接性分析.

参考文献:

- [1] Liu J K, Wei V K, Wong D S. Linkable spontaneous anonymous group signature for ad hoc groups[C]//Proc ACISP'04. Berlin: Springer-Verlag, 2004: 325-335.
- [2] Mh A U, Chow S S M, Susilo W. Short linkable ring signatures revisited[C]//EuroPKI 2006. Berlin: Springer-Verlag, 2006: 101-115.
- [3] Tsang P P, Wei V K. Short linkable ring signatures for E-voting, E cash and attestation[C]//Proc. First Information Security Practice and Experience Conf. (ISPEC'05). Berlin: Springer-Verlag, 2002: 48-60.
- [4] Au M H, Liu J K, Susilo W, et al. Constant-size ID-based linkable and revocable - iff - linked ring signature [C]//Proc. Int'l Conf. Cryptology in (INDOCRYPT'06). India, 2006: 364-378.
- [5] Liu J K, Wong D S. Enhanced security models and a generic construction approach for linkable ring signature [J]. Foundations of Computer Science, 2006, 17(6): 1403-1422.
- [6] Zheng D, Wei V K, Chen K F. GDH group-based signature scheme with linkability [J]. IEE Proc. Comm., 2006, 153(5): 639-644.

作者简介:

李德荣 女, (1964-), 硕士, 副教授. 研究方向为通信与信息安全.

(上接第 137 页)

- [2] 胡蓓, 李俊, 郁伟, 等. 对未知攻击进行检测的蜜罐系统的实现[J]. 计算机应用, 2006, 26(10): 2336-2337.
- [3] 王丹, 蔡皖东, 蔡俊朝. 分布式网络行为审计系统设计与实现[J]. 微电子学与计算机, 2008, 25(5): 80-83.
- [4] Moran D B. Tapping and tracking hackers [EB/OL]. (2000-07-15) [2008-09-10]. www.recourse.com.
- [5] 李平均, 刘权, 李天. 基于主被动结合的网络入侵检测系统的设计与实现[J]. 微电子学与计算机, 2007, 24(7): 50-52.

- [6] 连红, 连立祥. 虚拟蜜罐系统的设计[J]. 兵工自动化, 2007, 26(1): 54-55.
- [7] 林果园, 黄皓. 入侵检测动态取证模型[J]. 计算机工程与应用, 2006, 42(27): 140-143.

作者简介:

鄢喜爱 男, (1972-), 硕士, 副教授. 研究方向为信息安全.
杨金民 男, (1967-), 博士, 副教授. 研究方向为系统容错.
常卫东 男, (1967-), 硕士, 副教授. 研究方向为信息安全.