基于陷阱网络的入侵行为研究*)

郑秋生　邵奇峰　郭基凤　裴　斐
(中原工学院计算机科学系　郑州450007)

摘　要　介绍了陷阱网络的概念和体系结构,分析了陷阱网络的计算机取证技术,论述了基于陷阱网络的入侵行为研究。

关键词　网络安全,陷阱网络,入侵行为,计算机取证

Study of Intrusion Behavior Based on Honeynet

ZHENG Qiu-Sheng　SHAO Qi-Feng　GUO Ji-Feng　PEI Fei
(Zhongyuan Institute of Technology , Zhengzhou 450007)

Abstract　This paper introduces the conception and architecture of honeynet, analyzes its computer forensics, discusses the study of intrusion behavior based on honeynet.

Keywords　Network security,Honeynet,Intrusion behavior,Computer forensics

1　引言

信息和网络安全技术经过近十年来的应用已经证明:安全策略的制定、安全技术的应用和安全保障的获得很大程度上要取决于对安全威胁的了解。但当前我们对安全威胁的了解仅停留在各种攻击工具上,而对安全威胁制造者的行为却了解的非常有限。安全威胁的制造者也就是入侵者的行为包括:入侵者攻击系统的目的,入侵者是如何发现了易受攻击的系统,入侵者是如何攻击系统的,入侵者在控制了系统后又做了什么。同时作为正面防御者更需要了解的还有:如何提取入侵者攻击系统的证据,如何对入侵者进行定位追踪,如何取得最新的攻击技术并对未来的攻击趋势作出预测等,而陷阱网络[1](Honeynet)就为对以上入侵行为进行研究提供了环境。

2　陷阱网络的概念

陷阱网络最初是由 Sun Microsystems 公司的 Lance Spitzner 发起和主导的一个由30余名安全专业组织成员组成的,专门致力于了解 blackhat 团体使用的工具、策略和动机以及共享他们所掌握的知识的项目。其实际上是一个专门设计来让入侵者"攻陷"的网络,一旦被入侵者所攻破,入侵过程中所产生的网络数据包和系统日志等都将被用来对入侵行为进行分析研究。

传统意义上的信息安全一般都是建立在被动防御的基础上,比如防火墙、入侵检测系统、加密等,其基于规则和特征匹配的工作方式无法适应网络安全动态的、基于时间变化的特点,而陷阱网络可以给予组织主动权,即积极收集入侵特征信息,就可能将一场攻击或者防御中的失误扼杀在萌芽状态。

陷阱网络也可提供关于系统自身所存在的风险和薄弱环节的情报。它可以由相同于组织实际环境中所用的系统和应用构成,从而发现当前组织环境中存在的安全风险和薄弱环节,以主动提升组织自身的安全级别。例如,某公司想发布一个新的网上支付系统,但又担心可能会存在的风险,若其操作系统和应用程序如果能先在陷阱网络的中得到测试以识别任何未知的风险和薄弱环节,将会在很大程度上提高其安全性。

陷阱网络还可在网络攻防中提高组织的计算机取证和紧急响应能力。在实际网络系统中很难区分正常行为和入侵行为,但在陷阱网络中所有进出的数据包和新增的日志基本上就可以断定为入侵,从而也就更容易取得入侵证据和改善响应策略。

陷阱网络与传统蜜罐[2](Honeypot)系统是有区别的。传统蜜罐系统是一个故意设计为有虚假敏感信息或漏洞的单机系统,通常是用来对入侵者的行为进行诱骗或者警报,以降低正常系统被攻击的风险。而陷阱网络是一个网络系统,不需要刻意地模拟某种环境或者故意地使系统不安全,即须保证收集到的信息的真实性,以学习和研究真实环境中的入侵行为。陷阱网络有时也称其内部系统为陷阱机(Honeypot),但并非指传统的蜜罐系统。

3　陷阱网络的体系结构

陷阱网络体系结构的发展已经历了两个阶段:陷阱网络一代(GenI Honeynet)和陷阱网络二代(GenII Honeynet)。

3.1　陷阱网络一代

陷阱网络一代的体系结构如图1所示,防火墙将整个系统分隔离为陷阱网络、管理网络和 Internet 三个部分,其中陷阱网络是由用于被攻击的代表各种系统和应用的陷阱机的集合,管理网络是进行入侵数据收集和对整个系统进行管理的区域,Internet 通常是入侵者发起攻击的不可信的外部网络。防火墙用于隔离网络和对外出流量进行数据控制。路由器用于隐藏防火墙,并作为防火墙的补充进行数据控制。IDS 以隐藏 IP 地址的方式接入陷阱网络,并捕获陷阱网络中传送的数据包。陷阱网络中的 log server 用于实时收集所有陷阱机的日志数据。管理网络中的 Log/Alert server 用于实时收集 IDS 和防火墙的预警和日志数据。

*)基金项目:河南省自然科学基金资助项目(0111061200)。郑秋生　副教授,硕士,主要研究方向:计算机网络安全、软件复用技术。

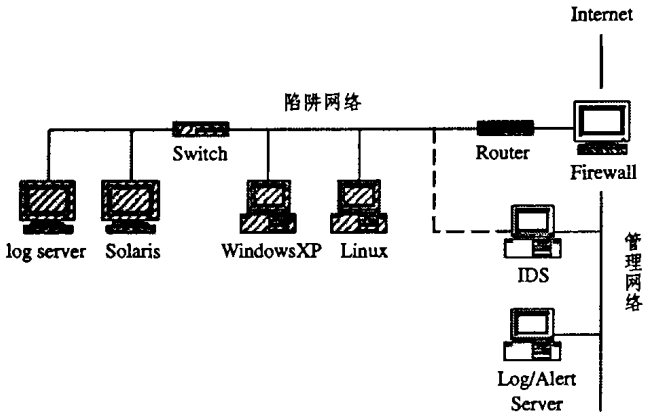

图1 陷阱网络一代的体系结构

陷阱网络是一个高度受控的网络，无论创建和维护哪一代陷阱网络，都要依赖于两大关键因素：数据控制和数据捕获。

(1)*数据控制* 就是对进出陷阱网络中的数据进行规则上的控制，假若某陷阱网络被攻破以后，应首先确保其决不会被用于攻击陷阱网络以外的其他网络。数据控制的关键之处就在于访问控制设备防火墙，可用它将陷阱网络、管理网络和Internet等严格地隔离，并对所有外出的数据包进行过滤。因此防火墙必须定义三条控制数据流向的规则：1)任何人都可发起从Internet到陷阱网络的连接，这样就允许入侵者扫描、探测并攻入陷阱网络；2)严格控制由陷阱网络发往Internet的对外连接数量，确保其决不会被用于攻击陷阱网络以外的其他网络。通常会让防火墙记录陷阱网络向Internet发起连接的次数，若一旦达到某个阈值，防火墙就会自动阻断其以后所有的连接；3) 陷阱网络与管理网络之间不可有任何的直接的连接，确保管理网络不会被攻破和管理网络中收集到的入侵数据的完整性。

对于防火墙规则的定义，用户可根据自身的实际环境和希望研究的内容进行适当的修改和调整，要保证给入侵者足够的空间不至引起他们的怀疑，以便捕获尽可能多的入侵数据，又要保证陷阱网络不会被用于攻击别人的网络系统，即所能获得的入侵数据的数量是与所承担的风险成正比的。

(2)*数据捕获* 是对入侵行为进行研究的依据，对数据进行全面和正确的捕获是整个项目成功的关键。因此不能依赖于单独的某个层次，而是要尽可能地进行多层次的数据捕获，这样就可以综合各层次的信息，并能够对入侵行为有更深层次的研究。陷阱网络中有以下几个数据层次：1)防火墙和路由器的日志文件；2)IDS或Sniffer捕获的网络数据包；3)陷阱机操作系统和应用程序产生的日志文件和击键信息；4)入侵者修改和删除的文件。

为了实现对入侵行为的实时追踪，也可以利用防火墙或IDS的E-mail预警功能，当有和定义的规则相匹配的入侵行为出现时，可以及时地获得通知，同时预警也可作为一种补充的数据捕获手段。另外还需注意的是：捕获的数据一定要存储在可信的、入侵者无法察觉的地方，以免数据被入侵者破坏或修改。可以将所有陷阱机中的日志信息另存在远程的日志服务器中，即使日志服务器被攻破，IDS也会捕获当初通过网络发往远程日志服务器的日志数据包。

3.2 陷阱网络二代

陷阱网络二代具有创建更易、觉察更难且风险更低的特点，其体系结构如图2所示。陷阱墙(Honeywall)是整个体系结构的核心，进出陷阱网络的所有流量都必须经过它，所以数据控制和数据捕获全都被集成在陷阱墙中。陷阱墙共包含了三个接口：eth0、eth1和eth2。接口eth0用于连接处理正常业务的真实网络，这表示在陷阱网络二代中，引入了对内部入侵行为的研究。接口eth1用于连接由陷阱机集合构成的陷阱网络。接口eth2直接连接至路由器，用于远程管理陷阱墙和远程传送捕获数据。陷阱墙实际上是一个工作在第二层的网桥，接口eth0和接口eth1并没有IP地址，所以通过陷阱墙的数据包不存在路由步跳和TTL减数问题，其实接口eth0和接口eth1连MAC地址都没有设置，也就是说陷阱墙对入侵者是透明的。接口eth2是用于远程管理的，所以需要设置IP地址。

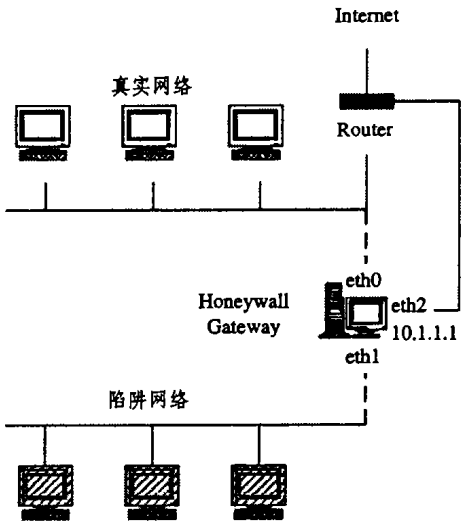

图2 陷阱网络二代的体系结构

为了在对外连接上给入侵者更大的空间，以至能收集更多的入侵行为，陷阱网络二代在数据控制中引入了NIPS(Network Intrusion Prevention System)，NIPS就是在提高对外连接阈值的基础上，对由陷阱网络向外发出的所有数据包进行入侵特征检测，如果发现有攻击性的行为，就将该连接阻断或修改数据包内容后放行。修改数据包使其对Internet上的网络的威胁丧失的同时，入侵者仍可接受到入侵失败的响应，也就不会觉察到陷阱网络的存在。计算阈值与NIPS的结合，能以较低的风险收集更多的入侵信息。

虚拟陷阱网络(Virtual Honeynet)是利用VMware或User-Mode Linux[3]等虚拟软件将陷阱机集合、数据控制和数据捕获全部在一台主机上实现。该方案的优点是创建廉价、维护简单和移动灵活，缺点是风险集中和功能有限。

4 陷阱网络的计算机取证

对陷阱网络中的捕获数据进行计算机取证，是对入侵行为进行研究过程中最关键、最耗时和最具挑战性的部分。根据经验表明：入侵者30分钟的攻击，需要研究者30到40小时的分析。另外也很少有研究者能通晓所有领域中的分析取证技术，这就需要依靠组织的力量来分工解决问题。

(1)*防火墙日志* 在实际网络系统中，很难区分防火墙日志中的合法流量和可疑流量，但在陷阱网络中，所有的流量全都是可疑的。因此陷阱网络中的防火墙设计为：对所有流入和流出的流量都应发出预警，流入的预警表明入侵者正在探测和攻击系统，而流出的预警表明入侵者已经攻破了系统。若预警采用E-mail或短信的方式就不必去手动查看防火墙日志，从而可简化分析取证工程。

(2)IDS 分析　IDS 提供了 IDS 预警、报文载荷和会话文件三种信息。IDS 预警的优点在于通过其特征匹配功能，能识别出具体的行为(如缓冲区溢出)。报文载荷提供了有关入侵行为的详细信息。会话文件非常有利于对 FTP、TELNET 和 IRC 等明文会话的迅速分析。

(3)系统日志　详细记录了入侵者是如何攻破系统和攻破系统后的行为，但它也是入侵者攻破系统后最先修改和删除的部分。所以系统日志应保存在三个地方：本地系统、远程 syslog 服务器和发往 syslog 服务器的全部信息的 IDS 报文载荷。通过三者的比较就可判别出入侵者是否对系统日志进行过修改。

(4)被动指纹[4](Passive Fingerprinting)　主动指纹(Active Fingerprinting)是通过使用工具(例如 Nump 或 Queso)主动检测远程主机以判断其操作系统，而被动指纹只是被动地嗅探远程主机的数据包来判断其操作系统。其可通过检查 TCP/IP 报文首部中的四个部分(TTL、窗口大小、DF 和 TOS)和 ICMP 回应请求来判断远程主机的操作系统、服务和应用。显然被动指纹不易被入侵者觉察，但是仍要防范入侵者的签名欺骗。

(5)取证[5](Forensic)　入侵者攻破系统以后，通常修改或删除了入侵的攻击程序、系统的日志文件、管理程序、配置文件甚至内核等，取证技术就是在被攻破系统的映像上，尽可能地恢复被入侵者破坏的数据，以重构入侵行为和提取入侵证据。The Coroner's Toolkit[6](TCT)包是取证过程中最常用的工具。

(6)统计(Statistics)　统计是指在陷阱网络长时间和多地域运行后，采集其所有的攻击数据，然后利用统计学原理对攻击数据进行分析，并对未来的攻击趋势作出预测。例如：可以统计某类探测特征与其攻击成功的时间间隔，以便将来此类特征重现时能够准确预测攻击将发起的时间。

(7)Sebek2[7]　入侵者目前也大量地使用了 SSH 或 3DES 等加密信道与被攻破的系统通信，这就给数据捕获工作带来了难度。不论是否使用加密信道，Sebek2是运行在陷阱机上直接捕获入侵者击键信息和上传文件的内核模块，其不断地将捕获的本地数据发向远程日志服务器，但这些数据包不会被入侵者的 Sniffer 捕获，因为所有陷阱机的内核都基于本地 MAC 地址做了相应的隐藏。

5　陷阱网络的风险

陷阱网络的确可以帮助研究入侵行为，但是同时它也包含着风险。尽管使用了防火墙、路由器和其他技术对入侵行为进行数据控制以降低风险，但是数据控制仍然可能会被入侵者躲过。另外，利用加密和反 IDS 技术也可躲过基于 Sniffer 的数据捕获。所以要真正地降低风险，就需要对陷阱网络进行持续的管理和维护。

结束语　陷阱网络的成功应归功于其简捷性：一个仿真实际系统的高度受控网络。所有进出陷阱网络的流量都会被捕获和分析，根据分析就可以了解入侵者的行为，对入侵者的行为了解的越多，对所面临威胁的觉悟和知识就会越高。但是入侵者的行为是不断变化的，这就需要陷阱网络的体系结构和计算机取证技术也要不断地动态变化。

参 考 文 献

1 Honeynet Project. Know Your Enemy: Honeynets [EB/OL]. http://project.honeynet.org,2003
2 Spitzne L. Honeypots: Tracking Hackers[EB/OL]. http://www.tracking-hackers.com
3 Dike J. User-Mode Linux [EB/OL]. http://user-mode-linux.sourceforge.net
4 Dittrich D. Computer Forensics[EB/OL]. http://staff.washington.edu/dittrich/forensics.html
5 Farmer D. Venema W. The Coroner's Toolkit (TCT)[EB/OL]. http://www.porcupine.org/forensics
6 Spitzer L. Passive Fingerprinting[EB/OL]. http://www.enter-,act.com/~lspitz/finger.htm
7 Honeynet Project. Know Your Enemy: Sebek2[EB/OL]. http://project.honeynet.org,2003

(上接第86页)

根结点进行一次签字，与路经主机的数目无关。虽然增加了一些 *hash* 函数的计算，但它们所占用的时间与签字相比是微不足道的。因此，该协议在保证了安全性的同时，大大降低了代理主人的计算量。

结论　本文给出了一个基于 Merkle 树的安全移动代理路由协议。它在满足路由安全性质 P1～P5的基础上，利用二元 Merkle 树结合 *Hash* 函数，使得在计算路由信息时仅需移动代理主人进行一次签字，相比原有的嵌套加密方案，该协议大大降低了代理主人计算路由信息所需的计算量。

该协议也可以很方便地推广到可变路由协议[9]。在可变路由协议中，对于二元 Merkle 树来说，不必改变结构；只是对随机数异或结果进行 Hash 运算时，在可变路由阶段，保证随机数异或结果相一致即可。

参 考 文 献

1 Das A, Gongxuan Y. A Secure Payment Protocol Using Mobile Agents in an Untrusted Host Environment[A]. ISEC 2001, LNCS 2040[C], Springer-Verlag Berlin Heidelberg, 2001. 33～41
2 Hohl F. Time limited blackbox security: Protecting mobile agents from malicious host[A]. Mobile agent and security, LNCS 1419 [C], Berlin: Springer-Verlag, 1998. 92～113
3 Perry M, Zhang Q. SITA: Protecting Trade Agents from Malicious Host[A]. Mobile Agents for Telecommunication Applications, LNCS 2164[C], Berlin: Springer-Verlag, 2001. 173～183
4 Domingo-Ferrer J. Mobile Agent Route Protection through Hash-Based Mechanisms[A]. LNCS 2247[C], Springer-Verlag, Berlin Heidelberg, 2001. 17～29
5 Belmon S G, Yee B S. Mobile Agent and Intellectual Property Protection[A]. Mobile Agents, LNCS 1477[C], Springer 1998. 172～183
6 Westhoff D, Schneider M, Unger C, Kaderali F. Methods for Protecting a Mobile Agent's Route[A], ISW'99 LNCS 1729[C], Springer-Verlag, Berlin Heidelberg, 1999. 57～71
7 Westhoff D, Schneider M, Unger C, Kaderali F. Protecting a Mobile Agents Route Against Collusions[A]. LNCS 1758[C], Springer-Verlag Berlin Heidelberg, 2000. 215～225
8 Sander T, Tschudin C F. Protecting Mobile agents Against Malicious Hosts[J]. Mobile agent and security, LNCS 1419[C], Berlin: Springer-Verlag, 1998. 44～60
9 Mir J, Borrell J. Protecting General Flexible Itineraries of Mobile Agents[A]. ICICS 2001, LNCS 2288[C], Springer-Verlag, Berlin Heidelberg, 2002. 382～396
10 Sander T, Tschudin C. Protecting Mobile Agents Against Malicious Hosts[A]. In Mobile Agents and Security[19], pp. 137～153
11 Gassko I, Gemmell P S, MacKenzie P. Efficient and fresh certification[A]. LNCS 1751, Berlin: Springer-Verlag, 2000. 342～353
12 Karnik G, Asokan N, Gülcü C. Protecting the Computation Results of Free-Roaming Agents[A]. LNCS 1477, Springer-Verlag, 1998. 194～207
13 王育民，刘建伟. 通信网的安全——理论与技术[M]. 西安：西安电子科技大学出版社，1999