虚拟蜜网核心功能剖析与实例部署

易秀双[1] 马世伟[2] 王卫东[1]
(东北大学计算中心 沈阳 110004)[1] (东北大学信息科学与工程学院 沈阳 110004)[2]

摘 要 传统蜜网硬件利用率低、配置复杂、管理难度大等缺点日渐凸显,如何解决这些问题越来越受到研究人员的关注。针对蜜网当前面临的问题,提出了使用虚拟技术构建蜜网的必要性。通过对蜜网关键技术的研究,分析并给出蜜网核心功能在虚拟系统中的工作流程,在此基础上设计并实现了一种虚拟蜜网的解决方案。实验结果表明,建立的虚拟蜜网工作良好,并在一定程度上解决了传统蜜网在硬件利用率、配置和管理等方面存在的问题。

关键词 蜜网,虚拟技术,功能分析,解决方案
中图法分类号 TP393.08 **文献标识码** A

Core Functions Analysis and Example Deployment of Virtual Honeynet

YI Xiu-shuang[1] MA Shi-wei[2] WANG Wei-dong[1]
(Computing Center, Northeastern University, Shenyang 110004, China)[1]
(College of Information Science and Engineering, Northeastern University, Shenyang 110004, China)[2]

Abstract As conventional honeynet's low hardware utilization, complex configuration and difficult management are increasingly appearing, how to solve these problems has been getting more and more researcher's attention. Aiming at the problems that honeynet currently is facing, the paper proposed the necessity of using virtual technology to construct honeynet. Through the studying on core functions of honeynet, the paper analyzed and provided the workflow of core functions in virtual systerm. Based on that, we designed and implemented a proposal of the virtual honeynet. The results show that the established virtual honeynet works well and solves the shortcomings of conventional honeynet in a certain extent.

Keywords Honeynet, Virtual technology, Functions analysis, Proposal

1 引言

随着蜜网技术[1]的不断发展,蜜网的体系结构和核心功能也在不断完善,但有两个问题一直没有得到有效解决[2]。问题一,在传统物理网络上部署蜜网,硬件利用率低。由于蜜网中每台蜜罐都是一台物理主机,且该主机一般只充当蜜罐,没有其他用途,因此硬件资源的利用率很低。问题二,由于蜜罐在物理位置上分散,导致对蜜网的配置和管理比较繁琐和耗时。

然而,硬件性能的不断改善和虚拟技术的不断发展,为解决这两方面问题提供了强有力的技术支持。一方面,虚拟技术使我们能够在一台物理主机上部署一个完整的网络,最大限度降低硬件的花费,同时使得对整个网络的配置和管理变得相对简单。另一方面,硬件性能的不断提高可以解决因在一台物理主机上部署过多的虚拟设备而带来的性能下降问题。因此,虚拟蜜网可以很好地解决传统蜜网面临的问题。

所谓虚拟蜜网,就是指通过应用虚拟操作系统软件(如VMware和User Mode Linux等)在单一的主机上实现整个蜜网的体系架构。虚拟蜜网的引入使得架设蜜网的代价大幅降低,同时对蜜网部署和管理也变得容易。

2 核心功能分析

蜜网有3大核心功能[1]:数据捕获、数据控制和数据分析。数据捕获能够检测并审计黑客攻击的所有行为数据;数据控制能够确保黑客不能利用蜜网危害第三方网络的安全,以减轻蜜网架设的风险;数据分析能够从捕获的数据中分析出黑客的攻击行为、使用的工具及其意图。

使用Honeywall Roo[3]和VMware软件部署虚拟蜜网,是Windows操作系统下最常见的虚拟蜜网解决方案[4]。本文的分析、研究也基于此方案。该方案中,最核心的部分是一个称为Honeywall的蜜网网关。它有3个接口:Eth0,采用桥接模式与主机的一块网卡相连,并通过该网卡与外部网络通信;Eth1,采用仅主机模式与虚拟蜜罐网络相连;Eth2,采用桥接模式与主机另一块网卡相连,并通过该网卡与管理网络通信。

2.1 数据捕获流程

数据捕获的目的是监控并且记录蜜网中入侵者的活动,隐秘地捕捉属于入侵者的所有流量,包括其发送、接收的所有

到稿日期:2011-04-07 返修日期:2011-06-22 本文受国家科技支撑计划项目(2008BAH37B05),国家自然科学基金项目(61070162),国家863计划项目(2007AA041201),国家CNGI专项(CNGI2008-123)资助。
易秀双(1969—),男,博士,副教授,主要研究方向为计算机网络、下一代互联网、网络与信息安全、高性能计算,E-mail:xsyi@mail.neu.edu.cn。

信息，这是进一步分析入侵的基础。

虚拟系统中数据捕获功能[5]的实现流程如图 1 所示。从图中可以看出，虚拟蜜网对数据的捕获分为 3 个层次：

(1) 基于防火墙日志。入侵者的数据包首先经过虚拟交换机 WMnet0，从 Eth0 流入蜜网网关后将通过 Iptables 防火墙，防火墙则会在 IP 层根据预先设定的规则对流入的连接进行记录。需要注意的是，无需对流入的攻击进行过滤，可以直接跳过 Snort_inline(入侵防御系统)。

(2) 在数据包从 Eth1 流出并进入虚拟蜜罐区域前，Snort(入侵检测系统)会在链路层对所有的流量进行监控、分析并记录，以用于后续的攻击分析。

(3) 此外，虚拟蜜网中每个蜜罐除了操作系统自带的日志功能外，还都安装有 Sebek 的客户端，能够记录蜜罐上的活动；同时通过隐秘通道(图 1 中的点状虚线)将收集到的信息传送到位于 Honeywall 中的 Sebek 服务器上。

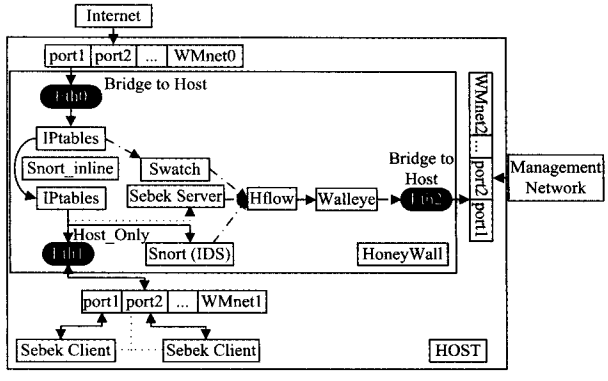

图 1　数据捕获功能流程图

2.2　数据控制流程

数据控制的主要目的是确保被攻陷的蜜罐主机不会被入侵者用来攻击蜜网之外的第三方主机。数据控制可以减少蜜网被入侵者利用的危险，因为一旦攻击者攻陷了蜜网中的一台主机，攻击者就可以利用该主机攻击其它的非蜜罐主机，所以必须对入侵者进行控制。

虚拟蜜网中数据控制功能的实现流程[5]如图 2 所示。Honeywall 虽然对流入的数据包不进行任何限制，使入侵者能够进入蜜网，但会对入侵者使用蜜网向外网发起的连接进行严格控制。数据控制功能是通过对连接数进行限制和对攻击包进行抑制两种手段相结合来实现的。

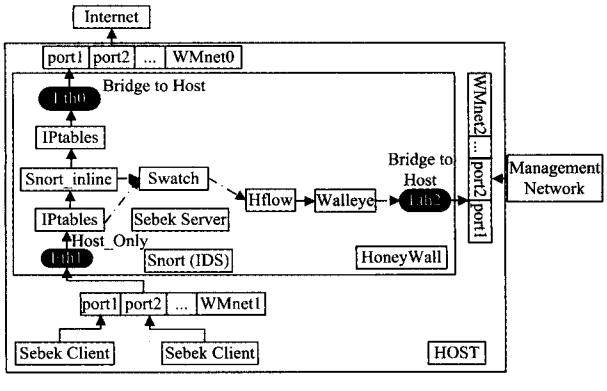

图 2　数据控制功能流程图

(1) 对外连接限制，主要用于网络探测和拒绝服务。管理者可以预先在 Iptables 中设置特定的规则，当从 Honeypots 向外发起的连接数超过预先设定的阈值时，Iptables 会将其记录到日志中，并断开后续连接，从而可以避免蜜网中被攻击的蜜罐主机作为入侵者的跳板，对第三方进行网络探测或拒绝服务攻击。

(2) 攻击包抑制，主要用于一些使用少量连接就能够奏效的攻击(如权限提升等)。在图 2 中，Snort_inline 可以检测出从蜜网向外发出的含有攻击特征的数据包，从而发出警报，同时对攻击包进行修改或丢弃，使其不能对第三方造成危害。

2.3　数据分析流程

数据分析是对捕捉到的探测、攻击或其他一些恶意行为活动进行理解、分析并跟踪。

Honeywall 中的分析软件通过与防火墙(Iptables)、入侵防御系统(Snort_inline)、入侵检测系统(Snort)等安全设备相结合，可以对进出蜜网的流量进行详尽分析，并以可视化的方式给出分析后的结果。从图 1 和图 2(图中虚线部分)中可以看出，数据分析主要分为以下 3 个层面：

(1) Swatch 软件收集来自 Iptables 和 Snort_inline 的报警和日志信息，并预处理这些数据和信息。Sebek 服务器端收集并处理 Sebek 客户端发送的信息。Snort 记录并统计流入蜜网的流量。

(2) Hflow2 软件接收经过 Swatch，Snort_inline 和 Sebek_Server 预处理后的数据，并将这些信息进行整合、归纳，处理之后再输出到 Walleye。

(3) Walleye 的主要功能是提供给管理者一个可以远程登录的 Web 控制界面。在这个控制界面上，管理者可以对整个蜜网进行监控、配置和管理，并且 Walleye 具有实时更新功能，因此管理者可以实时掌握蜜网最新动态。

除此之外，Honeywall 还包含一些其它的辅助分析工具，如 Argue，Tcpdump，P0f[6]等。

3　虚拟蜜网部署

"Honeynet Project(蜜网项目组)"提供了一些关于部署 Gen III[1](第三代蜜网)的一般性文件，对任何想使用 Honeywall Roo 和 VMware 构建虚拟蜜网的个人或组织提供了一个可参考的模板。

"Pakistan Honeynet Project"于 2008 年在其网站上给出了一种虚拟蜜网的解决方案[4]，本文实验参考的结构体系正是来自于该方案。图 3 是本文虚拟蜜网的详细部署图[7]。

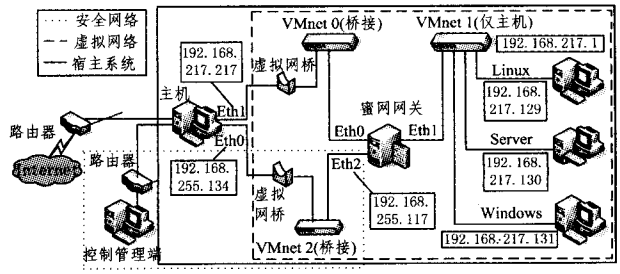

图 3　虚拟蜜网的结构图

3.1　部署与配置

图 3 中，VMnet 0，VMnet 1 和 VMnet 2 是 VMware 软件提供的虚拟交换机，而网桥实际上也是 VMware 软件提供的一种虚拟服务。这些虚拟设备和服务稍作配置即可以直接使用[10]。以下是虚拟蜜网中的主要设备和模块，更多的细节和信息请查看表 1。

(1) 宿主主机:本文实验所使用的主机只有一块网卡,因此 Eth1 实际上是在真实的物理网卡上添加的一个 IP 地址。实验所处环境是局域网,所以 Eth0 的 IP 地址是局域网地址。

(2)Honeywall:集成在一个精简内核版的 CentOS 系统中。该系统部署在一台虚拟主机上,并添加 3 块虚拟网卡:

1)Eth0:采用虚拟桥接(Bridge)模式,桥接到宿主主机网卡上,用于接入外网或不安全的网络。

2)Eth1:采用仅主机(Host-Only)模式,用于连接蜜罐区域。

3)Eth2:采用虚拟桥接(Bridge)模式,仅用于管理者对蜜网进行远程登录管理,该接口对外界透明。

(3) Honeypots:本文试验中,部署了 3 台不同类型的蜜罐主机,分别是 Windows-Server-2003,Windows-2000,Ubuntu-10.04,以便模拟真实网络中主机操作系统的多样性。

3.2 虚拟蜜网工作流程

外部网络和虚拟蜜罐主机可以通过宿主主机 Eth1 接口、虚拟交换机 VMnet 0、蜜网网关、VMnet 1 这条虚拟链路进行通信。管理网络则可以通过宿主主机 Eth0 接口、虚拟交换机 VMnet 2 这条虚拟链路与蜜网网关进行通信。

蜜网网关对流经它的数据进行监听、记录和控制,并通过数据分析软件进一步分析处理得到的信息。管理者可以登录到蜜网网关上查看这些信息,并依据这些信息进一步对蜜网进行管理和配置。

由图 3 可以看出,整个蜜网部署在一台物理主机上,因此相对于传统蜜网,虚拟蜜网可以充分利用硬件资源,使硬件的利用率达到最大。此外,由于虚拟蜜网中所有的网络设备都集中在一台物理主机上,因此对蜜网的配置和管理也变得相对简单。

4 实验结果分析

本文为了对虚拟蜜网进行有效的测试,设计了一个用例。要注意的是在进行测试之前,应该使用 VMware 软件的快照功能为蜜网网关和每台蜜罐主机设置一个还原点,以便在测试结束后可以将蜜网网关和蜜罐主机恢复到测试之前的状态。这样做一方面是防止测试数据污染蜜网网关和蜜网捕获到的数据,另一方面可以使被入侵或攻陷的蜜罐主机恢复到原始状态。

4.1 数据捕获和分析功能

该测试模拟黑客(192.168.217.217)通过扫描或其它途径获得了一台蜜罐主机(Windows 主机)的用户名和密码,并利用 telnet 工具远程登录到蜜罐主机 192.168.217.131 上,随后在蜜罐主机上使用反向 Shell 连接,利用 FTP 工具登录到黑客自己的主机,下载木马程序到蜜罐主机上并运行。

图 4 是蜜网网关对这次连接的记录,包括源 IP 地址和端口、源主机操作系统类型;目的 IP 地址和端口;连接持续的时间、发送的数据包数、字节数和触发的 IDS 规则等。

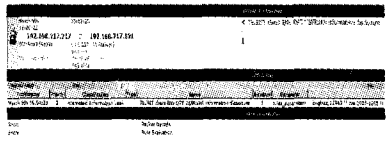

图 4 数据捕获功能的截图

Snort 软件记录了经过蜜网网关的数据包,可以点击图中的"Packet Decode"查看详细内容,并还原整个攻击过程。图 5 是 Sonrt 记录的相关信息。

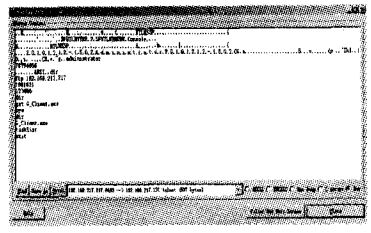

图 5 数据分析功能的截图

从图 5 中可以清晰地看出这个连接的整个攻击过程:攻击者首先使用用户名 administrator 和密码 78794656 登录到蜜网主机上,用 dir 命令查看主机文件目录后,又使用 FTP 工具反向登录到自己的主机上(192.168.217.217),并下载了木马客户端程序 G_Client.exe;最后返回到蜜罐主机并运行木马客户端。在使用 tasklist 命令确定木马程序运行后,攻击者离开了蜜罐主机。

需要说明的是,由于篇幅有限,本文使用了 Wireshark 来代替 Snort 进行解码(Snort 解码:点击 Packet Decode),使用 Snort 可以得出相同的分析结果。

4.2 数据控制功能

将蜜网部署一段时间,查看蜜网网关/etc/log 目录下的 iptables 文件,得到以下信息:

Mar 9 16:35:15 localhost kernel:Drop udp>20 attempts-IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT =eth0 SRC=192.168.217.131 DST=192.168.217.255 LEN=202 TOS=0x00 PREC=0x00 TTL=128 ID=6 6624 PROTO=UDP SPT=138 DPT=138 LEN=182

可以看到,在 16:35:15 时丢弃了一个连接,触发的规则是 UDP 的连接数大于每小时 20 个,该连接企图从 eth1 进入并从 eth0 发出;源 IP 地址为 192.168.217.131,端口为 138;目的 IP 地址为 192.168.217.255,端口为 138;连接使用的协议是 UDP。

由以上分析可以看出,虚拟蜜网的 3 大核心功能(数据捕获、数据分析和数据控制)工作良好。实验结果表明,使用虚拟技术构建蜜网(见表 1)可以很好地实现蜜网的各项功能。

表 1 虚拟蜜网配置列表

设备	系统/软件	型号/版本
宿主主机 操作系统	Windows XP SP3	型号:ThinkCentre m6100 RAM:3G
虚拟机 1 (Honeywall)	Honeywall-Roo -1.4.hw-2008	处理器:1 RAM:256M
虚拟机 2 (Linux 系统)	Ubuntu 7.10	处理器:1 RAM:512M
虚拟机 3 (服务器)	Windows Server 2003	处理器:1 RAM:512M
虚拟机 4 (Windows 系统)	Windows XP SP2	处理器:1 RAM:512M
虚拟机软件	VMware server	vmware-workstation-7.1.2
内核级 捕获工具	Sebek	Sebek-win32-3.0.5 Sebek-linux26-3.2.0b
防火墙	Iptables	Iptables-1.3.5
入侵检测系统	Snort	Snort 2.6.1.5
入侵防御系统	Snort_inline	Snort_inline 0.6

结束语 虚拟蜜网技术是网络安全中的一个新兴领域,

(下转第 109 页)

4 仿真分析与性能评估

为了验证本文提出的节点跳数与距离关系的分析方法，在 Matlab 上进行仿真对比分析，取 $N=400$，$R_b=200$，$d_{max}=50$，$\sigma_s=4.0$ 和 $n_p=3.0$。参数 $\xi(h)$ 的值如表 1 所列，概率分布密度如图 3 所示，直线表示式(11)的理论推导数据，'▽'表示实验统计值。虽然当 $h=6$ 时受到边界效应的影响，结果略有差异，但图 3 的实验仿真数据和理论分析值表现出很好的一致性。给定任意两节点间的跳数，本文提出的方法可以有效地估计出距离的概率分布情况。

表 1 $\varepsilon(h)$的取值

h	1	2	3	4	5	6
ω(h)	1	1	0.82	0.78	0.63	0.54

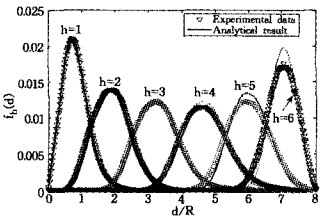

图 3 概率密度函数 $f_H(d)$实验数据与理论推导对比

结束语 传感节点的跳数与距离的关系信息对物联网的协议设计有着重要的意义。然而，目前大多数的研究集中在 UDG 模型，与实际网络环境不符。本文基于对数阴影衰落模型重新分析物联网框架下传感器节点间跳数与距离的关系，给出相应的概率分布表达式，并充分考虑多跳节点依赖问题。仿真结果表明，本文提出的计算表达式与实际仿真结果具有很好的一致性，增强了物联网应用的"实用性"和"可靠性"。

参 考 文 献

[1] Presser M, et al. The SENSEI project: integrating the physical world with the digital world of the network of the future[J]. Communications Magazine, IEEE, 2009, 47: 1-4

[2] Zorzi M, Rao R R. Geographic random forwarding (GeRaF) for ad hoc and sensor networks: multihop performance[J]. IEEE Transactions on Mobile Computing, 2003, 2(4): 337-348

[3] Sheu Jang-ping, Chen Pei-chun, Hsu C-S. A Distributed Localization Scheme for Wireless Sensor Networks with Improved Grid-Scan and Vector-Based Refinement[J]. IEEE Transactions on Mobile Computing, 2008, 7(9): 1110-1123

[4] Chen Jia-ner, Jiang An-xiao, Kanj I A, et al. Separability and Topology Control of Quasi Unit Disk Graphs[C]// INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, 2007: 2225-2233

[5] Bettstetter C, Eberspacher J. Hop distances in homogeneous ad hoc networks[C]// Vehicular Technology Conference, 2003. VTC 2003-Spring, The 57th IEEE Semiannual, volume 4, 2003: 2286-2290

[6] Li Z, Trappe W, Zhang Y, et al. Robust statistical methods for securing wireless localization in sensor networks[C]// Proc. of the Int'l Symp. on Information Processing in Sensor Networks. Washington: IEEE Computer Society Press, 2005: 91-98

[7] Ta Xiao-yuan, Mao Guo-qiang, Anderson B D O. Evaluation of the probability of k-hop connection in homogeneous wireless sensor networks[C]// Global Telecommuniations Conference, 2007. GLOBECOM '07. IEEE, 2007: 1279-1284

[8] Dulman S, Rossi M, Havinga P, et al. On the hop count statistics for randomly deployed wireless sensor networks[J]. Int. J. Sen. Netw., 2006, 1(1/2): 89-102

[9] Zhao Liang, Liang Qi-lian. Hop-distance estimation in wireless sensor networks with applications to resources allocation[J]. EURASIP Journal on Wireless Communications and Networking, 2007: 8

[10] Bettstetter C, Hartmann C. Connectivity of wireless multihop networks in a shadow fading environment[J]. Wireless Networks, 2005, 11(5): 571-579

(上接第 103 页)

是对传统蜜网体系结构的重要扩充。研究分析蜜网核心功能在虚拟系统中的具体实现，对提高蜜网的安全性，改善蜜网的体系结构起着十分重要的作用。本文首先对虚拟蜜网中的核心功能进行分析，在此基础上给出了具体实现模型，并设计了测试用例，对建立的虚拟蜜网进行测试。实验及其结果表明，使用虚拟技术构建蜜网，不仅可以较好地实现蜜网的各项功能，而且可以最大程度地利用硬件资源并降低管理和配置难度。今后的工作是进一步研究和分析虚拟蜜网的核心功能，完善虚拟蜜网中的不足之处，并在规模更大、结构更复杂的网络环境下进行测试。

参 考 文 献

[1] Project H. Know Your Enemy: Honeynets [EB/OL]. http://old.honeynet.org/papers/honeynet/, 2006-05-31

[2] Jason Chang C-H, Tsai Y-L. Design of Virtual Honeynet Collaboration System in Existing Security Research Networks[C]// Communications and Information Technologies. Tokyo, 2010: 798-803

[3] Project H, Alliance R. Know Your Enemy: Honeywall CDROM Roo[EB/OL]. http://old.honeynet.org/papers/cdrom/roo, 2005-08-17

[4] Shuja F A. Virtual Honeynet: Deploying Honeywall Using Vmware[EB/OL]. http://www.honeynet.pk/honeywall/index.html, 2008-06

[5] 诸葛建伟. 蜜罐及蜜网技术简介[EB/OL]. http://www.honeynet.org.cn/reports, 2004-10-15

[6] Abbasi F H, Harris R J. Experiences with a Generation III Virtual Honeynet[C]// Telecommunication Networks and Applications Conference. Canberra, 2009: 1-6

[7] 北京大学计算机科学技术研究所 Artemis 项目组. 基于 Vmware-Workstation 的虚拟 Honeynet 的部署实例[EB/OL]. http://www.icst.pku.edu.cn/honeynetweb/, 2005-04-18

[8] Dornseif M, Freiling F C, Gedicke N, et al. Design and Implementation of the Honey-DVD[C]// Information Assurance Workshop. New York, 2006: 231-238

[9] 孙印杰，王敏，陈智芳. 解析蜜罐技术在网络安全方面的应用[J]. 计算机技术与发展, 2008, 18(7): 130-131

[10] Mware V. Workstation User's Manual[EB/OL]. http://communities.vmware.com/docs/DOC-12156/version. 2010-05

[11] 冯朝晖，范锐军，张彤. Honeynet 技术研究与实例配置[J]. 计算机工程, 2007, 33(5): 132-134