Sandboxie-style Offense and Defense Laboratory Environment for Computer Network Security

LIN Xing-zhi
Guangxi Economic Management Cadre College，Nanning，Guangxi，530007，China
lxz4562509@139.com

Abstract: Through the analysis on the status of offensive and defensive experimental teaching in computer network security, the existing problems in technological transformation and the innovation of network experimental, according to features of computer Sandboxie technology and virtual technology, combined with the requirements of experiment construction and vocational ability cultivation in offensive and defensive of computer network security, the author proposed a innovative methods and realization approach, which based on the virtual technology, virtual no-disk technology, Shortest Path Dijkstra Routing Algorithm, network experiment sandboxie and virtual hardware network device to build sandboxie-style offensive and defensive computer network security laboratory environment. Sandboxie-style security offensive and defensive laboratory is a cross-platform, fusion, reconfigurable experimental teaching system of offensive and defensive in computer network security with the virtual intelligence flexible technology and load balancing. The system used virtualization equipment and technology such as VPN, 802.1x, BAS, DCBI, UTM, IDS and firewall to achieve a virtual reality environment of sandboxie-style security attack and defense. Construction of offensive and defensive experimental teaching of computer network security is proof to be feasible both in experiment mode and in experiment methods.

Keywords: Sandboxie; Computer Network; Security Attack and Defense Laboratory Environment

沙盘式计算机网络安全攻防实验室环境构建

林兴志
广西经济管理干部学院，广西南宁，中国，530007
Lxz4562509@139.com

【摘要】通过对计算机网络安全攻防实验教学现状、技术等存在问题的分析，根据计算机沙盘技术、虚拟化技术和职业能力培养的特点与要求，提出了融合构建沙盘式计算机网络安全攻防实验室环境的创新模式与实现方法。沙盘式安全攻防实验室是运用虚拟化智能弹性技术、虚拟化无盘技术、最短路径路由算法和负载均衡等技术组建的多环境、融合式、可重构的网络安全攻防实验教学系统，系统运用 VPN、802.1x、IDS 和防火墙等虚拟化设备和技术实现了虚拟化现实环境的沙盘式安全攻防演练，在实验模式和实现方法上证明了构建沙盘式计算机网络安全攻防实验室可行。

【关键词】沙盘；计算机网络；安全攻防实验室环境

1 引言

安全攻防实验室是沙盘式计算机网络（Sandboxie-style of Computer Network Course）教学的组成部分，是虚拟化技术（Virtualization）、虚拟化智能弹性技术与网络技术融合发展的产物，是实现计算机网络安全教学与实验的重要途径，起着培养人才与促进安全技术进步的重要作用[1]。随着信息技术的发展，网络安全问题日益突出，网络系统与数据被大量黑客或病毒软件入侵，软硬件遭到不同程度破坏，系统漏洞、配置和口令等问题对计算机信息安全构成严重威胁，如何识别网络主机的脆弱性与安全性变得越来越重要。安全攻防实验室的构建是计算机安全技术教学与安全技术

基金资助：广西教育科学“十一五”规划课题《基于虚拟化技术的沙盘式计算机网络课程教学研究》(2010C186)阶段性成果。
Fund: Guangxi Education and Science "Eleventh Five-Year Plan" subject "based on virtualization technology sandbox-style teaching of computer networks" (2010C186) initial results.

提升的关键所在，通过沙盘系统环境攻防实验，使学生与科研人员充分掌握网络安全技术与开发出新的安全应用程序，在系统实验的同时不破坏系统与网络，达到即时重构与虚拟化现实实验的目的[2]。

安全攻防实验室是采用智能重构技术构建的聚合式与分布式系统为一体的沙盘式实验平台，实验以权限和信任为两大对立实验核心，有针对性地制定安全机制和攻防实验机制，以提高实验的真实性[3]。

2 沙盘式攻防安全实验室构概述

在传统安全设备中，硬件与软件设备包括防火墙、UTM 统一威胁管理、入侵检测引擎、认证计费、日志系统等，可以组建完整的网络进行设备安装调试实验，但却不能满足学生多重重构产品配置、无限制的攻防实验；缺乏可扩展的实验环境教学体系，缺乏全新的计算机安全教学系统要求的不断扩容实验能力[4]。沙盘式安全攻防实验室在系统的构建上主要是对传统实验室的技术改造与转型，以及以虚拟化技术和硬件沙盒为核心的构建新型沙盘实验室问题。

在沙盘式实验室构建中，主要采用虚拟化技术和安全沙盒融合实验室的现有设备进行构建。安全沙盒是一种使实验室具有攻防教学功能的独特产品，如神州数码的 DigitalChina Secure SandBox（DCSS）等；虚拟化技术是一个广阔的概念，包括智能弹性虚拟化技术、虚拟机技术和硬件沙盒技术，它提供一种融合式实验，在沙盘式的安全攻防教学中起着主导地位作用，为计算机安全教学提供实验课程以及实验环境[5]。系统环境部署如“Figure 1”（图 1）所示：

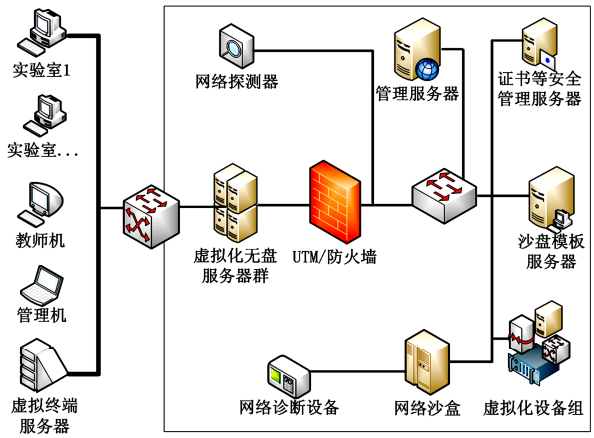

Figure 1. Laboratory system environment deployment

图 1.实验室系统环境部署

沙盘式实验环境构建中，主流虚拟机软件有 VMware 和 VirtualBox 等，均能在 Windows 系统上虚拟出多个操作系统、网络系统等，且可在同一桌面系统上同时兼容安装 Linux、Windows、OS/2、FreeBSD 等操作系统和网络组件。沙盘式实验系统是一套具备完整虚拟硬件与现实软件的实验系统，各个操作平台中均有自己独立的 CPU、硬盘、内存、网络设备等，与现实系统环境一模一样，提供的是一个真实的实验环境。实验中网络安全攻击和防御是在沙盘环境中真实进行，没有仿真的痕迹，对锻炼学生网络安全维护能力与创造性思维有着很大的促进作用。

3 沙盘式安全攻防实验室环境构建

3.1 系统设计的目标与思路

沙盘式安全攻防实验室不仅仅是计算机网络安全教学实验室，它把攻防演练技术和实际操作技能带进了课堂实验教学，把实验室升级到运维和攻防级别。采用虚拟化技术与安全沙盒进行融合构建，使独有的安全攻防平台在需要增加新的教学内容时，不需要添加其他服务器和设备就可以在管理端构建出全新的实验环境，以系统模板的方式服务于各教学终端[6]。在沙盘式的计算机网络安全攻防实验室的构建中，为了保证系统的正常运行和网络的高效吞吐量，我们采用了负载均衡算法和 Dijkstra 的最短路径的算法。

3.2 实验室负载均衡环境构建

负载均衡(Outbound Load Balancing)技术在安全攻防实验室中主要提供的是聚合式并发访问或数据流量分担到多台节点设备上分别处理，减少用户等待响应的时间，每个节点设备处理结束后，将结果汇总，返回给用户，使系统处理能力得到大幅度提高。实验室采用负载均衡自适应算法（Auto Mode）的对称启动算法，算法中分为发送者（Sender）、接收者（Receiver）和中立者（Neutral）三个节点机。算法的 Sender 和 Receiver 的启动由节点机决定，节点机就绪队列长度超过上限时转化为 Sender，启动 Sender 算法；节点机成为 Receiver 时启动 Receiver 算法。实验室系统中引入负载、动态阈值等进行动态构建，打破定式技术的缺点，为系统动态地提供各种优化组合。节点的负载值计算公式：

$$P_i = \sqrt{\sum_{i=1}^{n} (S_i \bullet Q_i^2)} \qquad (1)$$

978-1-935068-31-0 © 2010 SciRes.

P_i：本地节点 S_i 的负载值；Q_i：选定的负载分量；S_i：分量权重。

动态阈值作为判断主机节点负载状态的度量值，分为上限（H）和下限（L）。根据主机节点的负载 P_k，将节点分为：

超载：$P_k \geq H$ （节点负载大于 H，判断为超载，启动负载分配）

中载：$L \leq P_k \leq H$ （H 与 L 的差值较大，表示各节点间存在较大的负载差异）

轻载：$P_k \leq L$ （节点负载小于 H，判断为轻载，启动负载分配）

为改变以上负载分配，引入上限偏移量 R_h 改变阈值上限和下限偏移量 R_l 改变阈值下限。设 P_s 为节点负载的均值和方差，根据沙盘式安全攻防网络的实际情况修改 R_h、R_l 值达到改变阈值的目的，使适中负载区间为$(H+R_h, L+R_l)$。

当 $L \leq P_k \leq H$ 负载区间的中点与负载均值相差较大时，阈值上下限满足以下条件：

$$P_s = \frac{(H + R_h) - (L + R_l)}{2} \qquad (2)$$

当负载的 P_s 较大时，说明各节点负载差异大，这时应增大 R_l 而减小 R_h，适中负载区间变小，从而提高启动负载分配的频率。当负载的 P_s 较小时，说明各节点负载趋于平均，这时应减小 R_l 而增大 R_h，使适中负载区间扩大，从而降低启动负载分配的频率。

3.3 实验室最短路径路由环境构建

沙盘教学环境现有网络的各个核心部分随着任务量高、访问量和数据流量大的特点，其处理能力和计算强度也相应地增大，引入迪杰斯特拉（Dijkstra）按路径长度递增的次序产生最短路径路由算法，以适应系统的大量实验要求。

Dijkstra 算法中，设定带权有向图 G 和源点 v，求从 v 到 G 中其余各顶点的最短路径，实现路由路径的最优化。Dijkstra 算法是求出一个连通加权简单图中从结点 a 到结点 z 的最短路。边{i,j}的权 w（i,j）＞0，且结点 x 的 标号为 L（x），结束时，L（z）是从 a 到 z 的最短路的长度。Dijkstra 算法流程：

G 带有顶点 $a=v0,v_1,\ldots,v_n=z$ 和权 $w(v_i,v_j)$,若（v_i,v_j）不是 G 中的边，则 w（v_i,v_j）=∞;

For i:=1 to n

$L(v_i)$:= ∞

L(a):=0

S:=ø

初始化标记：a（1）的标记为 0，其它标记为∞，S 是空集。如“Figure 2”（图 2）所示：

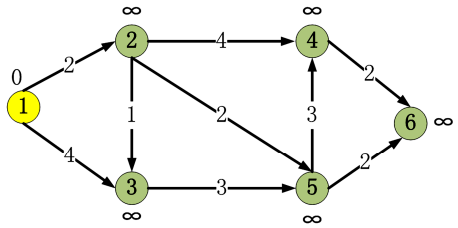

Figure 2. Initialize Schemes
图 2. 初始化示意图

While z ∉ S

Begin

U:=不属于 W 的 L(u)最小的一个顶点

S：=SU{u}

For 所有不属于 S 的顶点 v

If L(u)+w(u,v)<L(v)

Then L(v):=L(u)+w(u,v)

给 S 中添加带最小标记的顶点，并且更新不在 S 中的顶点标记。

End L（z）＝从 a 到 z 的最短路的长度。

算法具体实现步骤：步骤一，初始时，L 只包含源点，即 L＝，v 的距离为 0，U 包含除 v 外的其他顶点，U 中顶点 u 距离为边上的权（若 v 与 u 有边）或（若 u 不是 v 的出边邻接点）；步骤二，从 U 中选取一个距离 v 最小的顶点 k，把 k，加入 L 中（该选定的距离就是 v 到 k 的最短路径长度）；步骤三，以 k 为新考虑的中间点，修改 U 中各顶点的距离；若从源点 v 到顶点 u 的距离（经过顶点 k）比原来距离（不经过顶点 k）短，则修改顶点 u 的距离值，修改后的距离值的顶点 k 的距离加上边上的权；步骤四，重复步骤二和三直到所有顶点都包含在 L 中。最终结果如“Figure 3”（图 3）所示：

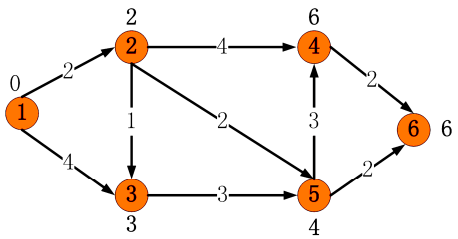

Figure 3. Consequence Schemes
图 3. 结果示意图

每次一个顶点为源点，重复执行 Dijkstra 算法一次。这样，便可以求得每一对顶点之间的最短距离。在计算机网络安全攻防实验室网络中，建立一个子网，网中的每个节点为一台虚拟化路由器，每个节点由各通信线路相连接。为了在一对给定的路由器之间选择一条路由路径，路由算法只需在网络中找到这对节点之间的最短路径即可。

3.4 系统实验环境实现

沙盘式计算机网络安全攻防实验室使用主流的虚拟化安全设备，如网络安全实验沙盒虚拟化软件、虚拟化无盘服务器、WINDOWS/LIUNX 等操作系统、虚拟化防火墙、入侵检测与防御系统、统一威胁管理系统、终端安全系统、安全准入认证系统等硬件与软件设备运用虚拟化技术融合组成实验环境，将典型安全漏洞、主机系统攻防等实验案例构建成沙盘式安全攻防实验平台。网络沙盘与所有设备组合部署成一个强大的网络测试环境，学生和研究人员可以直观、有效、方便地体验设备中安全技术的部署，记录并攻击沙盘中定制服务器常见的操作系统漏洞和网络应用服务漏洞等。实验室环境架构如“Figure 4”（图 4）所示：

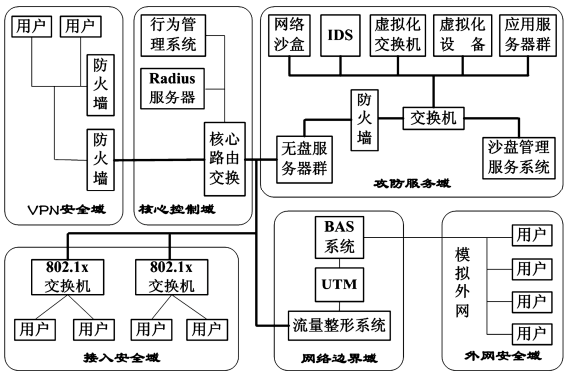

Figure 4. Security defense laboratory environment

图 4.安全攻防实验室环境架构

在沙盘式计算机网络安全攻防实验室的各个实验环境与区域中实现以下各种实验：网络 VPN 实验，使用防火墙进行 VPN 技术的组网和配置，让学生了解 VPN 技术的特点、适用范围以及安装调试；网络接入实验，使用 802.1x 技术、Web 接入技术或者 PPPoE 接入技术管理接入安全，也可以利用虚拟化技术构建内网安全管理系统进行病毒检查和资产评估；内网核心安全实验，部署日志系统和 Radius 服务器进行安全审计；网络边界域，具有支持虚拟化技术的流量整形网关设备、UTM 和 BAS 设备，可以很完整的管理边界安全；模拟外网实验，主要进行远程接入的安全设置以及模拟外网产生的恶意扫描和攻击。

系统攻防演练设计：演练是一个计算机网络安全攻防教学与实验的重要手段，运用虚拟化技术形成一个多任务的实验系统，学生在沙盘环境上进行系统的攻击和防御，IDS 等入侵检测引擎负责网络安全的嗅探和威胁发现。为了保证安全攻防实验室不对网络的其他区域造成危害，需要使用防火墙和三层交换机进行安全配置，以便对其它计算机实验教学区域隔离，使用内网沙盘安全管理系统对这些工具和软件进行资产管理。

4 结论

沙盘式计算机网络安全攻防实验室在教学中把每一个实验内容标签成为一个小的沙盘，并运用虚拟化技术扩展网络与系统的异构功能，从而使用户在实验时大大地提高实验室的安全系数和实验的成功概率，提高了学生的动手操作能力，解决了一般学校因资金与技术而无法解决的实验室建设问题。在服务器等网络设备与系统的访问与攻防控制上，沙盘式实验可以防范一些针对服务器权限的攻击，保护了系统的内核和关键组件不会被病毒、恶意程序、或者程序开发过程中发生的失误或者意外所破坏，这样可以极大地降低系统所面临的风险，实现了实验室的即时重构。沙盘式计算机网络安全攻防教学技术给信息技术带来了一种新的思维，在进一步的研究与实验中，我们需要细化沙盘模型的一些细节，重新定义安全策略的组织形式及重构策略，定义更详尽的实验元素和模式来描述沙盘实验的角色信息，使沙盘式实验教学更具可持续发展的趋势。

致谢

本文为广西教育科学“十一五”规划课题《基于虚拟化技术的沙盘式计算机网络课程教学研究》（项目编号：2010C186）阶段性成果，在撰写与研究时得到了项目组成员的大力支持与帮助，在此深表感谢。

References (参考文献)

[1] WU Jun-qiang. Building a Computer Network Training Room with Integration of the Virtual and Actual[J]. Research and Exploration in Laboratory. 2009,(11):245-247.
吴俊强.构建虚实结合的计算机网络实训室[J].实验室研究与探索.2009,(11):245-247.

[2] WANG Xiao-zhong.Practice and Exploration of Sand Table Simulation Teaching[J].Journal of Changzhou Vocational Col-

lege of Information Technology.2009,(1):41-43.

[3] LIN Xiong; LIN Yuan-guai; DU Yan.Research on Application of Virtual Machine in Computer Network Course Teaching[J].Computer Era.2010,(5):58-59.
林雄,林元乖,杜岩.虚拟机在计算机网络课程教学中的应用研究.计算机时代[J].2010,(5):58-59.

[4] LIN Xing-zhi.Integration Application of NGN and Universities and Colleges Unified Messaging System.[J]Journal of Guangxi Economic Management Cadre College.2010,(2):99-104,109.
林兴志. NGN 与高校统一信息系统融合应用[J].广西经济管理干部学院学报.2010,(2):99-104,109.

[5] CHEN Bing.An Improvement on Enterprise's Strategic Management of Sand Table System for Teaching Application[J]. Research and Exploration in Laboratory. 2010, (1):174-177.

[6] LIN Xing-zhi1,WEI Ying1,LUO Hai-peng.Unified Messaging Service of Information System in Next Generation Network Environment[J].Journal of Guangxi Academy of Sciences. 2010, 26(2): 167-170.
林兴志,魏鹰,罗海鹏.下一代网络环境下信息系统的统一信息服务构建[J].广西科学院学报.2010,26(2):167-170.