doi 10.3969/j.issn.1671-1122.2014.06.014

电力信息安全实验室攻防演练平台的设计与应用

么利中，文伟平
（北京大学软件与微电子学院，北京 102600）

摘 要：随着电力公司信息化快速发展，特别是SG-ERP的实施，信息系统的基础性、全局性作用越来越强。文章论述了信息安全攻防演练平台采用的基于Hook的主机监视技术、隐藏技术、虚拟机管理技术。文章通过对信息安全现状的需求分析，给出了信息安全攻防演练平台的总体架构和各部分功能描述，重点讲述了管理模块、攻防考试模块、培训演练模块和数据日志模块的构成及其设计与实现过程。通过对系统的运行进行测试，验证了各项功能的合理性和可用性。

关键词：电力；信息安全；培训；攻防演练平台
中图分类号：TP309 文献标识码：A 文章编号：1671-1122（2014）06-0078-06

Design and Implementation of Electric Power Information Security Attack and Defense Platform

YAO Li-zhong, WEN Wei-ping
(*School of Software & Microelectronics, Peking University, Beijing* 102600, *China*)

Abstract: With the fast development of informationization of electric power enterprises, especially after the implementation of SG-ERP, information system increasingly plays a basic and global role. In this paper, some techniques adopted in information security attack and defense platform are elaborated, including hook-based host computer monitoring technique, concealing technique, virtual machine management technique. Through analyzing the present information security situation, the overall framework of the platform is put forward and the functions of each part are described, the constitution, design and implementing procedure of management module, attack and defense examination module, training and drilling module and data daily record module are demonstrated with focus. By testing the system operation, the rationality and feasibility of each function are verified.

Key words: electric power; information security; training; attack and defense platform

0 引言

随着电力公司信息化快速发展，特别是SG-ERP的实施，信息系统的基础性、全局性作用越来越强。信息化在带来效能的同时，病毒感染、黑客攻击也极大威胁着电力公司的网络安全与应用安全[1,2]。

为了进一步提升安全人员的攻防技能，并能利用常见的攻击方式对测试系统进行模拟攻击，测试出应用系统自身的抗攻击能力和安全配置的实效性[3]，进而能够提出安全策略修订和相关加固方案，确保应用系统的安全性，需要进行信息安全攻防演练平台的建设。

通过搭建信息安全攻防演练平台，可进行主流操作系统、数据库系统、中间件系统等的漏洞攻击防护测试，提供培训、演练、测试的平台，培养信息安全专家队伍，进行系统上线前安全评估、在运系统安全测试工作，不断提升公司人员信息安全技术水平[4,5]。

本项目主要以安全攻防技能培训与模拟考试为出发点，通过专业化的攻防演练和考试系统加深对攻防过程的理解，全面提升技术人员的安全技能，保障公司信息安全。

收稿日期：2014-05-13
基金项目：国家自然科学基金[61170282]
作者简介：么利中（1972-），男，河北，高级工程师，硕士，主要研究方向：系统与网络安全、软件安全漏洞分析；文伟平（1976-），男，湖南，副教授，博士，主要研究方向：网络攻击与防范、恶意代码研究、信息系统逆向工程和可信计算技术等。

1 电力信息安全攻防演练平台关键技术分析

1.1 基于hook技术的主机行为监视技术

系统在目标虚拟主机上内置主机行为监视模块，实时捕获主机数据生成主机行为日志。主机行为监视模块基于Hook 技术，使用无进程运行的方式工作。

Hook 技术品种繁多，如 IAT hook、EAT hook、SSDT hook、Shadow SSDT hook、IDT hook、IRP hook、SPI hook、TDI hook、NDIS hook 和 Inline hook，总结归纳为如下两点[6]：

1）拦截特定的操作，做特定处理（如过滤、记录或关联分析）。

2）改变原来的函数调用流程，使其执行被 Hook 函数之前，先执行某个第三方函数，再在第三方函数做特殊处理。

基于 Hook 技术的主机行为监视模块可以在无进程状态下运行，为自身隐藏提供了有利条件。

1.2 隐藏技术

主机行为监视模块的隐藏技术包括自我隐藏和通讯隐藏两部分，不管是自我隐藏还是通讯隐藏，归根结底还是通过应用 Hook 技术实现[7]。

1）自我隐藏。通过 Hook 对应函数实现文件表项隐藏，避免被 dir/ls 之类的命令查看到主机行为监视模块的相关文件；实现注册表隐藏，防止使用 regedit 之类的工具看到相关注册表项；运行时和系统双链表断开，实现驱动本身的动态隐藏。

2）通讯隐藏。通过NDIS hook直接操纵网卡传输数据，解决通讯隐藏问题，防止蜜罐 sniffer 自身和其他蜜罐发送报文。

1.3 数据监视与捕获范围

目标虚拟机作为系统的基础数据来源，能够捕获到什么数据直接决定了系统的作用。本平台综合国内外科研机构多年来在漏洞挖掘与恶意代码分析上的研究经验，对如下操作系统行为进行监视形成日志[8]：

1）操作系统用户的登录和登出事件。通过审计操作系统用户的登录和登出事件，发现未经授权的交互式或非交互式登录会话。

2）操作系统用户和用户组的变更事件。用户增加、用户删除、用户密码更改等。

3）进程的创建、消亡、被杀事件。攻击者的行为是由一系列进程来完成的，在攻击的各个阶段都伴随着进程的创建和消亡。如果攻击者通过远程溢出进入系统，一般需要创建一个 shell 进程。攻击者进入系统后，对系统状况进行检测、留下后门都会创建特殊的进程，甚至杀掉安全防护软件的进程以利于自己的操作。因此对进程的生命周期进行审计可以追踪攻击者的行为。

4）网络连接变化事件。外部攻击必然伴随着网络连接的变化。

5）文件变化事件。针对文件创建、修改、删除等的行为进行审计，可以发现植入后门的行为。

6）注册表变化事件。记录注册表项变化、注册表值变化等信息，以还原攻击者的操作对主机注册表的影响。

7）驱动程序的加载事件。攻击者获得系统最高权限后，可以通过加载驱动的简单办法在内核层自由进行各种操作，如对击键进行记录。因此对加载驱动事件进行审计可以发现攻击行为。

8）远程注入线程事件。远程注入线程是一种常见的攻击手段，通过这种手段可以在目标进程中执行指定的代码。木马可以将自身代码嵌入到系统进程中，然后删除自身的程序文件从而实现隐身。因此对远程注入线程事件进行审计可以发现攻击行为。

9）消息钩子加载事件。消息钩子机制使得攻击代码能够得到执行机会并可以监视系统键盘等操作，所以也很常用。

10）跨进程操作内存事件。操作系统提供的跨进程操作内存的能力往往被攻击者用来修改系统进程而嵌入恶意代码，对这种行为的审计非常有必要。

11）应用层直接操作物理内存事件。攻击者在获得系统最高权限后，可以在应用层直接操作物理内存区域和植入恶意代码而无需借助高层的驱动程序，所以需要审计这类危险操作。

除产生上述日志之外，系统在 Hook 文件变化时对新增或修改过的文件进行判断，提取文件，形成样本，供后续进一步分析用。

1.4 虚拟机管理相关技术

本攻防平台的演练和考试环境通过虚拟机环境实现。不同课程及考试所需的操作系统环境及应用环境并不相

同，本平台提供方便的环境部署方法。

在虚拟机环境中预置多个虚拟机母镜像，每个镜像提供不同的操作系统及应用环境。通过生成多个快照的方式提供统一的环境部署[9]。

在虚拟机网络结构设计中，基于虚拟化技术，把攻击链路及管理链路分别映射到不同的物理网卡。虚拟机网络与管理链路隔离，在目标虚拟机上无法感知到管理链路的存在。

对目标虚拟机的管理不在虚拟机操作系统上进行，而是通过 WebServices 等远程接口连接目标宿主机系统，在宿主机上对目标虚拟机进行管理，包括启动停止、升级、修改及获取性能数据。

2 信息安全攻防演练平台的总体设计

2.1 系统的设计原则

在规划和设计时，系统应遵循以下几项设计原则[10]：

1）稳定性。保证 7×24 小时不间断稳定运行。

2）可靠性。系统运行平均无故障时间超过 100,000 小时；系统平均无故障率 >99.96%；具备手动恢复措施。

3）扩展性。基于现有虚拟系统环境，应具有二次开发能力模块。

4）先进性。系统基于蜜罐和蜜网研究技术，开发稳定可靠的攻防平台宿主机系统，同时保证系统的多样性和异构性。

2.2 总体架构设计

信息安全攻防平台总体架构如图 1 所示。

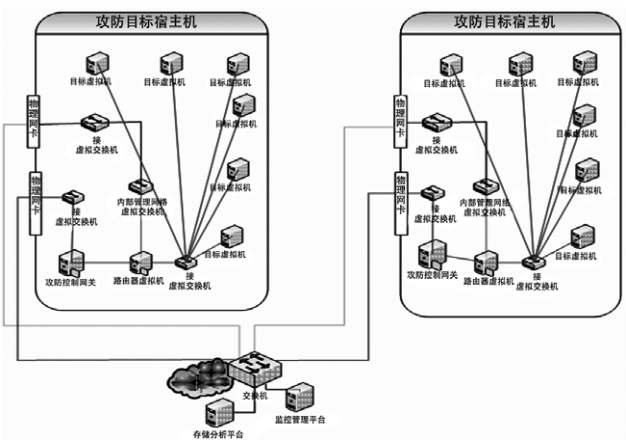

图1 信息安全攻防平台总体架构

信息安全攻防平台主要硬件构成包含 3 个部分：

1）系统管理引擎

系统管理引擎仅系统管理员可见。系统管理员可在此对平台进行运行配置、数据管理、用户与权限管理、维护管理等操作。

2）数据库引擎

主要配置系统后台数据文件的存储时限。系统已经默认配置了后台数据文件的存储策略，系统管理员可以对其进行重新编辑。

3）蜜罐宿主机引擎

蜜罐宿主机引擎包含虚拟蜜网网关、虚拟路由器和 8 台虚拟主机，通过虚拟网关、虚拟路由器的连接，使用户可以从设备接入交换机并联通到虚拟主机进行攻防演练。

2.3 系统功能结构设计

系统功能结构如图 2 所示。

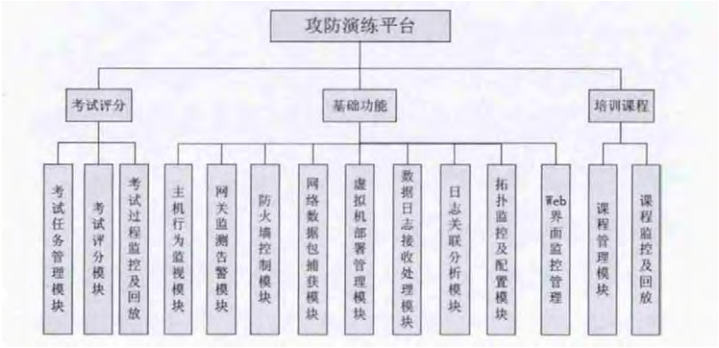

图2 系统功能结构

信息安全攻防演练平台由 4 个主要功能模块组成，分别是系统管理模块、攻防考试模块、培训演练模块和数据日志模块，各个功能模块又由若干子模块组成。

1）系统管理模块。系统管理模块由运行配置、数据管理和用户与权限管理 3 个子模块组成。

2）攻防考试模块。攻防考试模块由考题模板、考试计划、待评考试和历史考试记录 4 个子模块组成。

3）培训演练模块。培训演练模块由课程管理和培训计划两个功能模块组成。

4）数据日志模块。数据日志模块由实时日志、分类日志和日志下载 3 个子模块组成。

系统管理模块用于管理员对系统设备、用户及权限进行设置，后3个模块实现攻防演练平台教学培训的主要业务功能。

2.4 系统运行环境

应用服务器操作系统：Linux 64 位。

应用服务器 Web 服务 ：Tomcat

软件运行平台 ：gcc version 4.5.3

数据库服务器 ：10.2.0（非商用版本）

客户端 ：FireFox，显示器最佳效果 1024×768 像素

3 信息安全攻防演练平台关键模块设计

3.1 系统管理模块设计

3.1.1 运行配置设计

为了保证攻防演练平台的正常运行，需要在运行配置页面进行如下操作 ：

1）目标虚拟机。管理目标虚拟机及其所属目标宿主机。

2）目标网络。配置被攻击的目标网络。

3）网络设备管理。配置网络设备地址以接收该设备的 syslog 日志。

4）本机网络配置。配置攻防演练平台的网络接口和路由。

5）NTP 服务器。配置 NTP 服务器，以便同步攻防演练平台的时间。

3.1.2 数据管理设计

为更好地进行数据管理，需要对数据文件存储策略进行配置。数据文件存储策略主要配置系统后台数据文件的存储时限。系统管理员可以对最大文件大小、超时时间、存储过期时间进行编辑。数据文件存储策略如图 3 所示。

系统管理 ▸ 数据管理 ▸ 数据文件存储策略

	最大文件大小(KB)tes)	超时时间(分)	存储过期时间(天)
原始数据包文件	100	5	2
Netflow数据文件	10	10	365

编辑

图3 数据文件存储策略

3.1.3 用户与权限设计

攻防演练平台中，通过该模块可以配置具有不同权限的用户组，允许拥有不同权限的用户登录系统，用户登录后只能在自身权限范围内进行操作。用户主要包括教官、学员和系统管理组，其权限划分如下所示 ：

1）教官。实时监控当前系统的运行状况，制定培训计划、进行培训课件管理、分配学员任务、制定考试计划、监控考试现场、进行考试评分等。

2）学员。参与攻防培训课程、了解课程状况、进行操作演练、按考试计划进行考试。

3）系统管理员。除具备教官的权限外，还具有用户管理、系统资源管理等权限。

3.2 攻防考试模块设计

攻防考试模块是系统管理员或教官用来评判学员攻击或防护能力的平台。该模块包括考题模板、考试计划、待评考试、历史考试记录 4 个子模块。教官和系统管理员可以查看并操作全部 4 个子模块内容，学员只能查看考试计划、待评考试和历史考试记录。

1）考题模板

考题模板旨在规范考试环境、考试目标及时间要求，可以重复使用。系统管理员 / 教官在下发考试计划之前必须制定相应的考题模板，但其操作权限略有不同 ：

（1）教官。可以查看授权给自己的考题模板，添加考题模板及对自己所创建的考题模板进行修改或删除。

（2）系统管理员。可以查看所有考题模板，添加、删除或修改考题模板内容。

在考题模板中可以实现添加、修改、删除考题模板，修改目标网络、修改拓扑图等功能。

2）考试计划

系统管理员 / 教官可以在考试计划中，利用已有的模板创建考试任务，指定需要参与考试的人员名单及所对应考试的客户端机器和目标虚拟主机。考试开始前，学员只能看到自己的考试名称及倒计时信息，看不到其他考试的具体内容及目标，以免提前操作产生影响。考试开始后，学员可以看到自己的考试任务及目标主机，按照考试任务要求自行完成考试。该子模块主要实现 ：系统管理员、教官制定考试计划、部署环境、启动考试以及查看考试监控信息等 ；学员查看授权给自身的考试计划、考试目标，查看考试监控信息和日志信息。

考试计划制定完成后，必须先通过部署环境启动目标 IP 对应的目标虚拟机类型，然后才能够启动考试。

3）待评考试

待评考试模块对于系统管理员、教官、学员均可见，但他们拥有的权限不同 ：系统管理员、教官可查看待评考试的考试目标、攻击目标的基本信息，回放考试过程，以及对答卷进行评分 ；学员可查看待评考试的考试目标和日志信息，回放整个考试过程。

评分过程首先是系统自动评分，然后系统管理员、教官根据考试目标，回放考试过程，针对目标达到情况确认

系统的自动评分。

4) 历史考试记录

系统管理员 / 教官评分结束后，此次考试进入“ 历史考试记录 ” 页面，供系统管理员、教官、学员查询。

(1) 教官。可以查看自己所负责的已经结束的考试记录。打开该考试记录后，可以查看所有学员的该次考试的考试结果，可以对考试得分进行修订，同时可以回放基于拓扑展示的考试过程以及考试过程的日志信息。

(2) 系统管理员。可以查看全部已经结束的考试记录。打开该考试记录后，可以查看所有学员的该次考试的考试结果，可以对考试得分进行修订，同时可以回放基于拓扑展示的考试过程以及考试过程的日志信息，并对不需要的考试记录进行删除。

(3) 学员。可以查看自己所参与的已经结束的考试记录。打开该考试记录后，可以查看自己该次考试的考试结果，可以回放本次考试过程和考试目标、本次考试的基本信息和目标完成情况，以及考试过程的日志信息。

3.3 培训演练模块设计

培训演练模块主要针对攻防培训课程的管理、监控及回放。为了使学员能够迅速掌握攻防知识，系统管理员、教官通过制定培训计划并录制培训课程供学员自主学习。

教官及系统管理员可以查看自己所能看到的课程列表以及课程详细信息，查看及编写课程提纲，上传及下载课件，工具，设定课程需要的演示环境，录制及查看课程记录等。学员可以查看到自己所能看的课程列表以及课程详细信息，查看课程提纲，下载课件及工具，查看课程记录等。

1) 课程管理

课程管理模块仅对系统管理员和教官可见。系统管理员、教官在制定培训计划之前，必须添加培训课程。在该模块中可以按需求添加培训课程，修改培训课程基本信息（包括培训课程的名称、课程简介、录制培训课程的教官、课程权限类型、用来显示目标宿主机和目标虚拟机及其使用的操作系统的拓扑图），编辑目标网络、编辑拓扑图、上传资料、删除上传资料、删除培训课程等。

2) 培训计划

培训课程添加完成后，系统管理员、教官首先需要添加培训计划，然后在指定时间内自动开始或结束录制培训课程，或者在任意时间手动开始或结束录制培训课程。学员可以通过回放授权给自己的培训课程、查看课程笔记、下载资料等来进行学习。培训计划配置完成后，可以部署培训环境，正式开始录制培训课程。为了便于学员理解和学习培训课程，系统管理员、教官可以在录制前、录制过程中和录制完成后编写培训笔记，以便列出培训要点或注意事项等信息。

3.4 数据日志模块设计

数据日志模块仅对系统管理员和教官可见。该模块通过不同的日志类型、数据类型在统一层面展示系统的变化状况，起到整体系统的审计作用。

该模块主要包括以下功能 ：

1) 实时日志。实时日志节点包括 3 部分 ：目标网关日志、主机监视日志和网络设备日志。实时日志实时展示最近 15 分钟的日志。目标网关日志来源于目标网关，包括网络告警日志、数据控制日志 ；主机监视日志来源于目标虚拟机，包括主机变化日志、主机状态日志、系统性能日志、URL 捕获日志和样本捕获日志 ；网络设备日志来源于向攻防演练平台发送 syslog 日志的网络设备 [11,12]。

2) 分类日志。分类日志主要包括网络告警日志，数据控制日志，主机变化日志（进程变化日志、文件变化日志、连接变化日志、注册表变化日志、服务变化日志、登录变化日志、账号变化日志、时间变化日志、驱动变化日志、钩子变化日志、线程注入日志、跨进程内存日志、写物理内存日志、文件保护日志），主机状态日志（主机进程日志、网络连接日志、CPU 监视日志、内存监视日志），系统性能日志，样本捕获日志，URL 捕获日志和网络设备日志 [13]。

3) 数据下载。系统管理员、教官可以查看、下载的数据文件包括 ：

(1) 原始抓包数据。指由目标网关捕获，经过目标网关的所有数据包。

(2) 网络告警数据。指由目标网关生成，触发网络攻击告警的数据包。

4 系统测试与应用

攻防平台上线后，为保证系统能够正常使用，我们对系统进行了基本功能测试与实际攻防演练。

4.1 基本功能测试

1) 实验室系统的负载能力。即系统所能容忍的最大用户数量，也就是在正常响应时间中，系统能够支持的最多的客户端数量。

2) 实验室系统的课程管理功能。即对实验课程的加载、删除，相关工具下载、课程文档下载等功能是否具备。

3) 虚拟机系统环境管理功能。即对虚拟主机的启停管理、快照还原、环境加载删除等功能是否具备。

4) 教官管理功能。可以查看自己所负责的正在进行和尚未启动的考试计划列表并点击查看详细信息。对于正在进行的考试，可以单击“监控”实现对考试过程基于拓扑图的状况监控；对于未启动的考试计划，可以进行修改、删除以及启动等操作：(1) 学员。可以查看自己参与的正在进行的和尚未启动的考试计划列表。对于自己正在参与的考试，单击考试名称可以查看考试要求、自己在考试中的角色（攻击者还是防护者），以及自己在考试过程中产生的攻击日志输出。对于尚未启动的考试，只能看到考试名称和计划启动时间。(2) 系统管理员。可以查看到所有正在进行的和尚未启动的考试计划列表并单击查看详细信息。对于正在进行的考试，可以单击“监控”实现对考试过程基于拓扑图的状况监控。对于未启动的考试计划，可以进行修改、删除以及启动等操作。

4.2 病毒与恶意软件分析实验

在本攻防平台上，安全人员通过研究、测试企业网内经常遭遇的病毒、木马、蠕虫、恶意程序等，学习如何利用杀毒软件、工具软件或以手工方式来发现、采样、分析和处理病毒和恶意软件，甚至对内部病毒源头进行追踪[14]。

4.3 系统层的攻防实验

安全专责人员在实验室环境内学习针对主流操作系统、数据库的攻击及防御技术，学习如何从攻击角度发现和利用系统漏洞、猜测账号及口令、利用系统后门，如何从防御角度去防范漏洞、迷惑和诱骗，进行攻击事件发生后的定位、修补、追踪和取证。

4.4 针对应用的攻防实验

在实验室系统基础平台上，建设一套应用系统，专业测评人员在该应用系统上进行模拟演练，学习对常见应用系统的漏洞发现和利用，以及对这些应用系统的防护及加固，这些工作为今后安全实验室内部开展应用系统级的安全评测做好了技术、知识和人员的储备。

5 结束语

本文介绍了某电力信息安全攻防演练平台的总体结构设计和功能，总结该平台具有以下特点：系统结构合理、功能基本完整、功能易用性较好、系统具有较好的扩展性以及较强的实用性，能够较好地满足公司实际的业务需要[15,16]。然而，该平台也存在一些不足，主要体现在操作复杂、智能化程度低等方面。设计和实现一款更加通用、便捷的攻防演练平台是下一步努力的方向。（责编 马珂）

参考文献

[1]Yuan E, Tong Jing. Attribute Based Access Control(ABAC) for Web Services[C].Proc. of the IEEE International Conference on Web Services. Piscataway, USA: IEEE Computer Society, 2005:561-569.

[2]Perlman R. An Overview of PKI Trust Models[J]. IEEE Network, 1999, 13(6): 38-43.

[3]Lang Bo, Foster I, Siebenlist F, et al. Attribute Based Access Control for Grid Computing[EB/OL].ftp://info.mcs.anl.gov/ pub/tech_reports/reports/P1367.pdf, 2006-04-25.

[4]Park J S, Sandhu R. Smart Certificates: Extending X.509 for Secure Attribute Service on the Web[C].Proc. of National InformationSystems Security Conference. Arlington, USA: [s. n.], 1999:340-346.

[5]OASIS. eXtensible Access Control Markup Language(XACML) Version 2.0[EB/OL].docs.oasis-open.org/xacml/2.0/ access_control-xacml-2.0-core-spec-os.pdf. 2005-02-01.

[6]Ragsdale D J, Surdu J R, Carver C A.Information assurance education through active learning[R].The IWAR Laboratory, 2002.

[7]de Vivo M, de Vivo G O, Isern G.Internet security attacks at the basic levels[J].Operating Systems Review, 2002, 32(2):111-116 .

[8]Teo L, Zheng Y, Ahn G.Intrusion detection force: an infrastructure for internet- scale intrusion detection[C].Proceedings of the First IEEE International Workshop on Information Assurance(IWIA'03) , Darmstadt, Germany, 2003:73- 91.

[9]BJORLIN M.A study of modeling and simulation for computer and network security[R].Stockholm: University of Stockholm / Royal Instituteof Technology，2005.

[10] 董辉，马建 . 基于虚拟蜜网的网络攻防实验平台的构建 [J]. 齐齐哈尔大学学报 ：自然科学版，2012，28（02）：67-72.

[11] 李玉超 . 网络攻防对抗平台（NADP）研究与实现 [D]. 长沙 ：国防科技大学，2008.

[12] 孔红山，唐俊，张明清 . 基于 SITL 的网络攻防仿真平台的设计与实现 [J]. 计算机应用研究，2011，28（07）：2715-2718.

[13] 谢杰，张明清 . 基于 OPNET 的拒绝服务攻击建模与仿真 [J]. 系统仿真学报，2008，20(10）：2736-2739.

[14] 刘芸，顾晓鸣，匡晓 . 一种基于 OPNET 的网络半实物仿真方法研究 [J]. 软件导刊，2009，8（02）：125-127.

[15] 郝杲旻，殷肖川，王燊燊 . 网络攻防平台节点连通性研究 [J]. 福建电脑 ，2009，(02）：67-68.

[16] 孔轶艳 . 网络攻防模拟实验平台的设计与实现 [J]. 通信技术，2012 ，45（11）：37-39.