第 36 卷 第 7 期 计 算 机 工 程 2010 年 4 月
Vol.36 No.7 Computer Engineering April 2010
·安全技术· 文章编号：1000—3428(2010)07—0129—03 文献标识码：A 中图分类号：TP309

网络攻防训练模拟系统的研究与实现

徐建军，单 懿，仇广煜，周 黎
(南京军区司令部指挥自动化工作站网络信息中心，南京 210016)

摘 要：为提高计算机网络对抗能力，研究和实现一种网络对抗训练模拟系统，讨论系统的组成、运行流程，阐述其中的关键技术，包括网络环境模拟、攻防过程数据采集、攻防工具库与知识集成以及网络对抗效能评估等技术。通过攻防演练实例说明了系统的有效性。
关键词：网络攻击；网络防御；网络对抗；训练模拟

Research and Implementation of Network Attack and Defence Training Simulation System

XU Jian-jun, SHAN Yi, QIU Guang-yu, ZHOU Li
(Network Information Center, C4I Workstation in Headquarters, Nanjing Military Zone, Nanjing 210016)

【Abstract】To improve the confrontation capability of computer network, a network confrontation training simulation system is studied and implemented and its architecture and running flow are discussed. The key technologies are demonstrated, including network environment simulation, data collection, attack and defence toolkit and knowledge integration, network confrontation effectiveness evaluation and so on. Example of network confrontation drilling proves the validity of the system.
【Key words】network attack; network defence; network confrontation; training simulation

1 概述

随着网络中心战成为未来信息战的核心样式，网络对抗已经成为信息对抗的主要作战方式。网络化战场的显著特点就是以计算机为中心，通过网络将各种人员、装备有机地组织为一个整体。如果失去了网络的支撑，也就失去了作战的优势。自美国提出信息战理论[1]以来，为了满足未来网络战的需求，国内外已经开展网络对抗的信息化和数字化训练，构建了各种有效的网络攻防训练和研究平台，其中包括：美国 IWSS16(InfoWorld Security Suite 16)系统[2]，西点军校信息保障作战实验室[3]；国内如上海交大的信息安全工程实践综合实验平台[4]，中科院的网络安全防护若干关键技术和防范实验平台[5]等。

网络对抗训练模拟系统是对网络对抗技术进行学习、研究和训练的平台，为网络攻击、网络防御等作战样式和网络战战法的运用提供对抗模拟、效果演示和攻防训练环境，还能够为研究人员提供可验证的网络对抗评估环境，为安全保障人员的态势感知、安全评估和决策提供客观的科学依据。

2 网络对抗训练模拟系统组成结构

2.1 网络对抗的概念

自 1994 年提出信息战、1997 年提出网络中心战构想以来，信息对抗、计算机网络对抗的研究已经成为一个热点。目前，美国给出的计算机网络对抗是计算机网络攻击、计算机网络防御以及探测。计算机网络对抗是采取各种手段摧毁、破坏和瘫痪对方的计算机网络系统，阻止对方对有效信息的获取、传递和处理流程；同时对自己的计算机网络实施整体防护，保证己方网络的信息畅通。

2.2 网络对抗训练模拟系统组成结构

网络对抗训练模拟系统的组成按照分层模块化的设计思想，从低到高分别由数据层、服务层及应用层构成，其中，数据层为服务层中的各个模块提供数据基础，服务层中的各个模块为训练模拟系统的正常运行提供各种服务。网络对抗训练模拟系统的组成结构如图 1 所示。

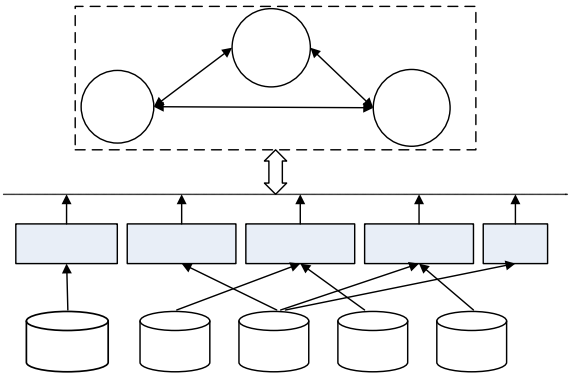


图 1 网络对抗训练模拟系统的组成结构

服务层包括网络环境模拟、攻防数据采集、攻防工具与知识集成、网络攻防效能综合评估、可视化等服务，是训练模拟系统的运行基础，攻防各方系统调用上述服务完成攻防训练模拟的整个过程。

在应用层中将攻防训练模拟系统抽象描述为 3 方：导演方，攻击方以及防守方，其中，导演方是总控制中心，通过它控制系统的运行，具有攻防态势感知、信息传输、分析判

作者简介：徐建军(1979－)，男，工程师、博士，主研方向：网络安全，多媒体信息系统；单 懿，高级工程师、博士；仇广煜、周 黎，工程师、硕士
收稿日期：2009-12-10 **E-mail：**jjunxu@126.com

断、指挥调理和实时判断等能力。

3 系统运行流程

网络攻防训练模拟系统的具体运行流程如下：

步骤 1 制定某次攻防训练的想定预案。

步骤 2 根据想定预案对网络环境进行部署，对导演方、攻击方和防守方的席位进行设定，推送各种数据采集探针以及对各方的约束条件。

步骤 3 导演部下达演练开始命令，演练开始。

步骤 4 攻防双方根据此次攻防训练的想定从攻防工具数据库中选择相应的攻防工具进行网络攻防对抗。

步骤 5 导演部根据双方的攻防情况判断是否需要干预，如需要，则进行干预，转步骤 4，否则继续。

步骤 6 导演部根据数据采集数据和态势判断是否满足演练结束条件，如满足，则继续，否则转步骤 4。

步骤 7 演练结束，导演方宣布演戏结束命令。根据双方的攻防行为以及数据采集的结果对此次演练过程进行攻防效能评估，并给出评估结论。

4 系统关键技术设计与实现

4.1 网络环境模拟

考虑到降低网络的硬件规模，网络环境模拟采用了半实物仿真(Hardware-In-Loop, HIL)的方式，即实际网络设备与虚拟网络交错连接的形式，其中部分用与实际系统相同或相近的实物代替，仿真网络能从实际物体获得真实的输入输出，比纯软件仿真更接近实际情况，节约了基础环境搭建的成本。

半实物仿真采用 OPNET[6]技术，并在其中嵌入了蜜罐技术进行开发，实现虚拟网络与真实网络连接。半实物网络完整性与包转发机制，仿真控制和同步机制的功能，可进行网络模拟、主机系统模拟和漏洞模拟，如图 2 所示。在底层环境的搭建中，除了模拟仿真的网络外，还部署了具有高交互特性的蜜罐，采用比较流行的虚拟机技术实现，提供的各种服务都是真实并可控的。

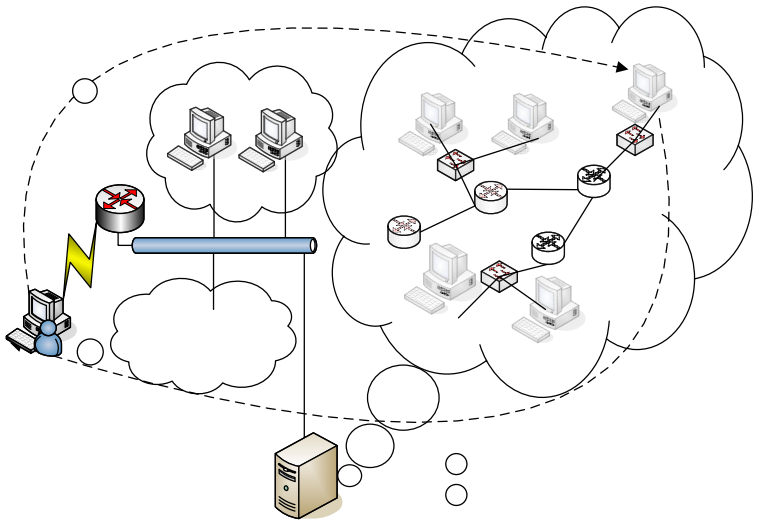


图 2 基于半实物的网络环境仿真

虚拟网络仿真原理示意图如图 3 所示。其中，数据包分发器对虚拟网络接收到的数据包进行处理。查询现有配置以查找到一个符合目标地址的虚拟网络配置，根据 IP 数据包中的协议字段，数据包和相应的配置被转交给相应的协议处理器处理；ICMP, TCP, UDP 协议处理器分别对各种报文进行处理。

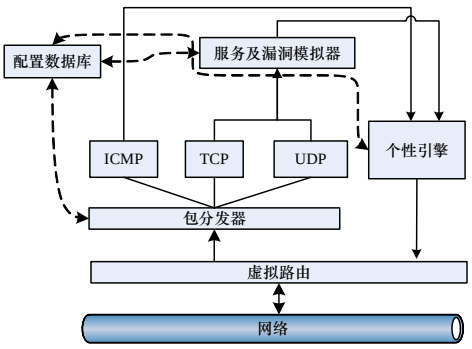


图 3 网络模拟仿真原理

服务及漏洞模拟器是网络环境模拟中蜜罐技术运用的关键部分，针对访问者所发出的数据构造出相应的响应，随后经个性引擎处理后发回给访问者，使其误认为存在一个真实的服务，同时可以用脚本来编制各种服务可能存在的各种漏洞，提高了模拟的灵活性。

个性引擎在发送数据到外部网络前，对数据包进行修改，使得数据包看上去和从指定配置的操作系统网络栈发出的一样从而符合指纹识别软件预期的 OS 特征。虚拟路由模块用于模拟虚拟网络的拓扑结构和网络连接的时延和丢包现象。

4.2 攻防过程数据采集

攻防过程数据采集要实现的功能是实时记录攻防双方的行为、网络主机系统相关事件、网络系统在攻防过程中的状态变化，监控的对象包括攻防双方所在的真实网络设备和计算机系统以及虚拟网络设备和虚拟主机，采集内容涵盖了各种底层网络数据包的采集(IP, ICMP, TCP, UCP 等数据包)，将这些底层采集来的数据与高层攻击行为进行相关联和分析，并统计出各种网络性能指标。其中，虚拟网络设备的采集可直接通过网络环境模拟引擎将包截获存储在服务器中。

真实主机的数据采集包括高交互的蜜罐和攻防双方的主机系统，采集的内容包括：计算机运行状态(包括硬件资源使用，系统服务和当前进程)，用户键盘记录，文件系统事件采集，注册表变更事件采集，屏幕快照采集，进程变更事件采集，端口访问采集等。此时在真实机器上部署探针已完成数据的采集。探针的部署如图 4 所示。

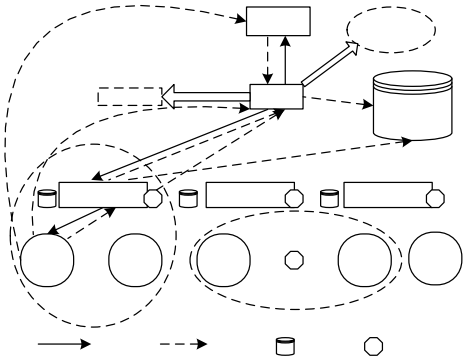


图 4 数据采集探针部署

4.3 攻防工具库与知识集成

攻防知识库和知识集成中的漏洞库采用与国际流行的 CVE 标准相兼容，漏洞库中的结构字段包括漏洞名称、漏洞描述、漏洞危害等级、受影响的系统、补丁下载途径等相关信息。同时，将攻防工具库与漏洞库关联起来，攻击工具库

中设立一个字段 CrisisDegreeToTool 来标明某个工具对某个漏洞的攻击效果指数，该指数是在攻击工具收集和分析时通过人工分析得到的一种经验值，范围为 0~1。当在对网络主机完成扫描和漏洞检测后，针对网络设备的某个漏洞，从数据库中检索出攻击效果指数，从高到底地对攻击工具排列，用户从列表中选择攻击效果指数最高的攻击工具进行攻击。

4.4 网络对抗效能综合评估

网络对抗效能评估是为了评估演练双方对抗效果，是系统不可或缺的重要组成部分。网络对抗效能综合评估采取自动评判和人工干预模式相结合的方法评估训练效果，对客观部分采用自动评估模式，对攻防对抗过程具体操作方法、步骤由人工干预进行评判。在本系统中主要考虑到以下 2 个方面的评估：

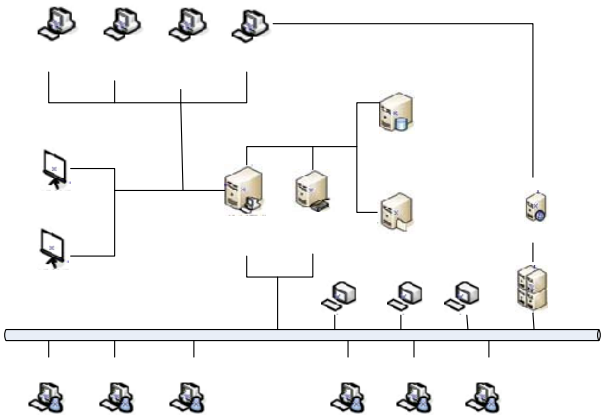
(1)可量化的网络性能指标。根据网络性能指标(包括网络平均时延、网络防御开销、网络吞吐量、链路误码率、链路丢包率、链路利用率等统计数据，通过网络监控数据分析获得)评估各种攻击方法对网络性能的影响程度，对于上述可量化的网络性能指标，本文采用“网络熵”[7]对受攻击网络前后性能进行评估。网络熵越小，表明网络信息系统的安全性越好。对于网络的某一项性能指标来说，其熵值可以定义为 $H_i=-\mathrm{lb}v_i$，V_i 为该项指标的归一化参数，显然，网络信息系统受到攻击后，其服务性能下降，系统稳定性变差，熵值应增加。因此，可用“熵差” $\Delta H=-\mathrm{lb}(V_2/V_1)$ 对攻击效果进行描述，其中，V_1 为网络系统原来的归一化性能参数(如吞吐量、响应时间等)；V_2 为网络受攻击后的归一化性能参数。

(2)网络和主机安全事件。根据双方网络上部署的探针获取的数据分析对系统安全有损害的事件，如是否存在被篡改的程序和文件、是否存在非法增加的账户和软件、是否存在不明的端口和服务等，通过网络安全事件评估各种攻击方法对网络安全属性造成的影响程度。此部分目前采用人工判别的方法。

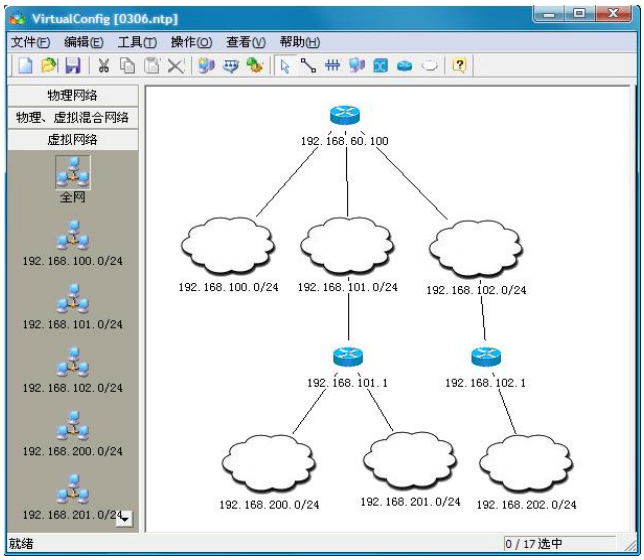
5 攻防演练实例

下面以一个攻防演练实例来说明系统的操作和运行。制定的预案内容包括席位、文书和网络环境，在演练实例中攻击方的 3 个席位的 IP 地址为：192.168.0.1, 192.168.0.2, 192.168.0.3，具体席位如图 5(a)所示。虚拟网络环境配置如图 5(b)所示，在虚拟网络中配置了 6 个子网，每个子网中包括了一些可以模拟各种操作系统漏洞的主机以达到欺骗攻击方的目的，每个子网通过虚拟的入口路由器与真实机器通信。预案通过文书下发给攻击方规定演练的攻击任务：窃取文件和种植木马。当攻防双方机器安装完数据采集探针并准备就绪后，导演部通知双方演练开始。

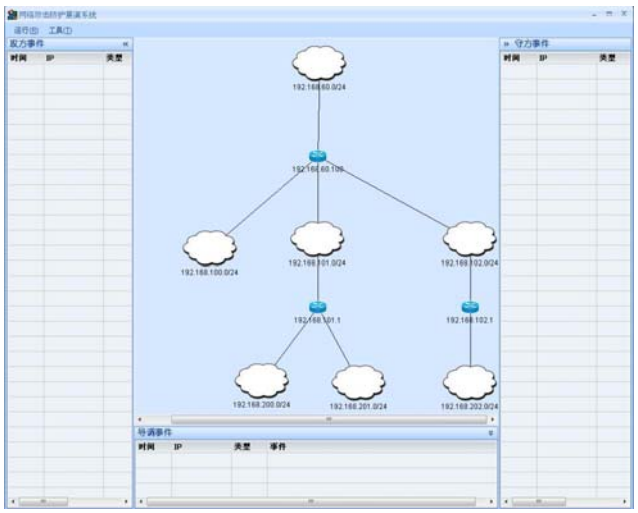
接收到演练开始命令后，攻击方调用扫描工具 X-Scan 在导演部指定的网络地址范围搜索防守方网络中的机器，通过 MS08-067 漏洞利用工具对目标主机进行溢出攻击成功后添加超级用户，用该超级用户登录目标机器进行文件窃取和木马种植操作。如果攻击方长时间扫描不到攻击目标，则导演部可进行导调，如开放防火墙或缩小地址空间等。攻击时部署在攻防双方上的探针将各种攻击事件显示到全屏可视化展示界面中，并将事件与图形中的主机和网络关联，受到攻击时该子网和子网中受攻击的主机的图标会变色，如图 5(c)所示。当演练结束后，导演部根据采集的数据和双方上报的事件进行综合评判。



(a)演练席位配置



(b)虚拟网络环境



(c)全屏可视化展示

图 5 攻防演练实例的配置界面

6 结束语

本文研究并实现一种网络对抗训练模拟系统，介绍实现的关键技术，通过一个实例说明系统的运用，该系统的建立可实现仿真环境下网络对抗训练以及网络攻防的效果评估，为网络对抗训练提供了良好的平台环境。

（下转第 135 页）