网络对抗训练模拟系统的设计与实现

甘 刚，陈 运，李 飞

(成都信息工程学院网络工程系 成都 610225)

【摘要】提高计算机网络对抗能力，是夺取信息优势和控制网络权的必要手段和途径；网络对抗训练模拟系统的建立有利于网络对抗人才的培养。研究和设计了一种网络对抗训练模拟系统，并从关键技术及其实现的角度讨论了相关子系统，包括交互式对抗训练模拟系统、对抗训练模拟支持软件系统、对抗训练模拟评估系统和对抗训练模拟信息库。该系统能够为网络对抗理论研究与对网络抗训练模拟提供一个良好的环境，具有十分重要的意义。

关 键 词 攻击; 防御; 网络对抗; 训练模拟
中图分类号 TP393.01 文献标识码 A

Design and Implementation of Network Confrontation Training Simulation System

GAN Gang，CHEN Yun，LI Fei

(Network Engineering Department, Chengdu University of Information and Technology Chengdu 610225)

Abstract To study and develop the confrontation capability of computer network is necessary to gain information superiority and network domination. Network confrontation training simulation system helps cultivate confrontation persons with ability and increase confrontation standards. This paper presents a network confrontation training simulation system, and discusses the related subsystems including interactive confrontation training simulation system, support software system, evaluation system, and information data base. The system can provide a favorable environment for confrontation theory research and confrontation training. It is of great significance and benefits in practice.

Key words attack; defense; network confrontation; training simulation

随着网络中心战[1]成为未来信息战的核心战场，网络对抗已经成为信息对抗的主要作战方式。无论是作为军事重要基础设施的战术互联网，还是国家永久性民用基础设施的Internet，都有可能受到各种各样的网络入侵和攻击。在未来的网络对抗中，谁掌握过硬的网络对抗技术，谁就将赢得未来信息战争的主动权。自20世纪80年代美国提出信息战理论[2]以来，为了满足未来网络战和信息战的需求，世界各国亟需开展网络对抗的信息化和数字化训练，建立网络对抗训练模拟系统，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。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，通过对网络对抗技术的研究，把网络对抗机制和攻防方法引入网络基础设施和环境，根据对抗双方的设想开展网络对抗、模拟进攻和防御演习，通过攻防实践使防御方和攻击方获得更多的应用技能，从而提高参训人员的攻防水平。网络对抗训练模拟系统的建立还能够为研究人员提供可验证的网络对抗评估环境，为网络管理人员和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。

1 网络对抗训练模拟系统的组成结构

1.1 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。网络对抗是信息对抗在计算机网络中的表现形式，其内涵和外延的定义也不尽相同，体系结构也尚在探索中。目前，美国给出了计算机网络对抗[3]的概念，并指出网络对抗包括计算机网络攻击、计算机网络防御以及探测(Exploitation)。计算机网络对抗就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、传递与处理流程；同时对自己的计算机网络实

收稿日期：2007 – 03 – 25
基金项目：四川省科研基金资助项目(2006C033)
作者简介：甘 刚(1974 –)，男，硕士，讲师，主要从事信息安全方面的研究.

施整体防护，保证自己网络的信息畅通[4]。网络对抗的基本特征是以计算机网络空间为战场、以计算机为主要武器、以信息和软件为作战手段、以计算机网络系统为主要目标进行信息网络进攻与防御。网络对抗包括攻击性网络对抗活动、防护性网络对抗活动和支持性网络对抗活动。

1.2　网络对抗训练模拟系统的设计

根据以上对网络对抗概念的分析，可以看出网络对抗在未来信息化社会中的重要作用，特别是在军事领域，网络对抗在某种程度上改变着传统的作战观念、思想和方法。因此，需要建设网络对抗训练模拟系统，加强信息安全、网络安全与对抗技术人才的培养。通过培养和训练，使参训人员掌握网络对抗的基本战术和技能，适应未来网络战的需要。针对网络对抗人才培养的特点和需要，本文研究和设计了一种网络对抗训练模拟系统，该系统由交互式对抗训练模拟系统、对抗训练模拟支持软件系统、对抗训练模拟评估系统和对抗训练模拟信息库四个部分组成，框架结构如图1所示。四个部分联动融合，互相配合，形成体系，构建以对抗训练模拟信息库为基础，交互式对抗训练模拟系统为框架的分布式、全方位、多层次的网上训练和考核体系，可以实现网络对抗训练和考核评估等功能。

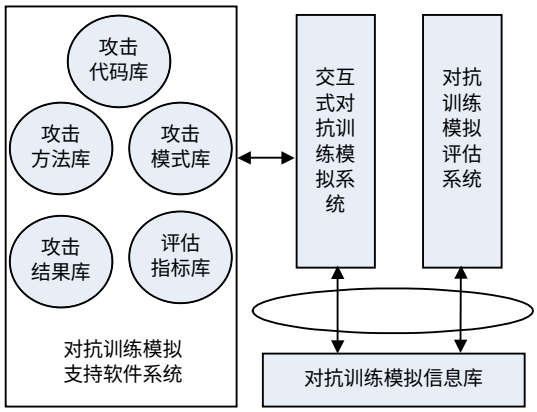

图1　网络对抗训练模拟系统的组成结构

(1) 交互式对抗训练模拟系统模拟网络对抗演练环境，理论结合实际，将对抗训练模拟信息库中的安全知识与实战技能结合，为参训人员提供实践环境，进行交互式网络对抗训练和对抗。对抗双方采取交互与独立相结合的方式进行对抗方法和对抗过程的演练。

(2) 对抗训练模拟支持软件系统由攻击代码库、攻击方法库、攻击模式库、攻击结果库和评估指标库等部分组成，为参训人员提供实施对抗训练的全套工具、方法和模式。

(3) 对抗训练模拟评估系统采取自动评判模式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判模式，对攻防对抗过程中具体操作的方法、步骤由人工干预进行测评，能够实现训练评估系统的标准化和训练效果反馈的自动化。

(4) 对抗训练模拟信息库通过对大量原始数据的分析、统计、归纳，建立以网络对抗为主题的信息库体系，主要包括与训练有关的信息的知识库、漏洞主机库和漏洞列表库，内容涵盖了网络安全、网络攻击技术和防御技术、应用方案、系统漏洞和系统补丁等大量信息，该信息库是其他三个部分的基础和信息提供平台。

2　系统关键技术及其实现

2.1　交互式对抗训练模拟系统

交互式对抗训练模拟系统包括对抗训练区、集成仿真环境区和综合演示区三个环境，如图2所示。

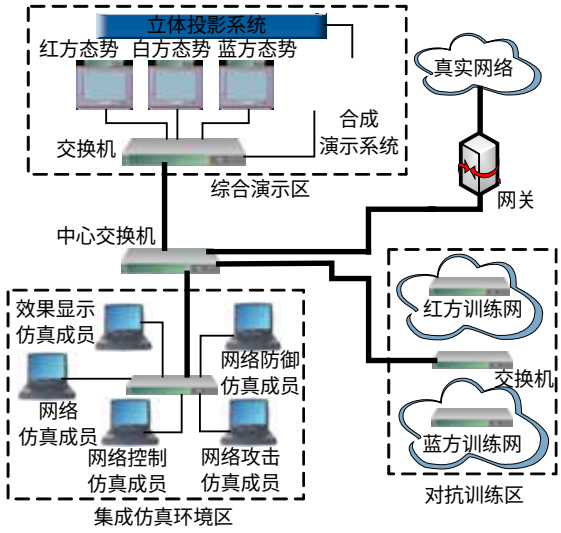

图2　交互式对抗训练模拟系统

为了降低真实网络的硬件规模、网络结构和网络应用对网络探测、攻击和防御过程的影响和限制，真正达到网络对抗训练和能力评估的目的，网络对抗训练模拟系统采用HLA/RTI仿真[5]技术，对网络对抗训练模拟进行研究。该系统采用TCP/IP网络的标准通信协议，底层链路通过仿真交互的方法传输数据；该系统使用Iris、Ethereal和Sniffer等工具，能够捕获真实网络的数据包，作为数据源导入仿真系统进行仿真；该系统还可通过网关与真实网络进行通信，实现仿真过程中交互数据与外界网络数据的互通，最终达到“虚拟和真实”相结合的网络攻防训练效果；该系统能够对一些预期系统、实际系统的攻防预案进行网络对抗演练和评估。

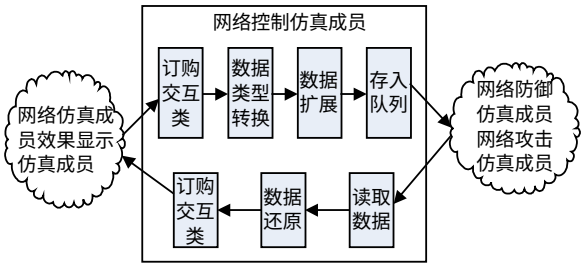

图3 仿真成员工作示意图

集成仿真环境中的网络仿真成员和效果显示仿真成员从系统中订购要实施攻防的交互类，网络防御仿真成员和网络攻击仿真成员根据需要对数据进行处理，将防护或攻击过的数据包以交互类的形式公布到联邦中去，网络控制仿真成员控制整个数据的处理、订购和公布过程。整个集成仿真环境中仿真成员的工作流程如图3所示。

2.2 对抗训练模拟支持软件系统

在对抗训练模拟支持软件系统的实现过程中，关键是对各数据库字段(包括攻击代码库、攻击方法库、攻击模式库、攻击结果库和评估指标库)的设计，各数据库的结构字段如表1所示。

表1 对抗训练模拟支持软件系统中各数据库的结构字段

攻击代码库	攻击方法库	攻击模式库	攻击结果库	评估指标库
攻击代码_ID	攻击方法_ID	攻击模式_ID	攻击结果_ID	索引_ID
攻击代码_名称	攻击方法_名称	攻击模式_名称	攻击结果_类型	索引_名称
系统	系统	索引_ID	标识符	索引_类型
版本	攻击能够达到的目标	…	指向下一步操作指针	根数
攻击要求达到的目标	攻击代码_ID	…	…	层数
攻击能够达到的目标	攻击代码_ID	…	…	权数
攻击代码	…	…	…	…

2.3 对抗训练模拟评估系统

网络对抗的综合效能主要反映在信息的机密性、完整性和可用性等方面，这些安全属性与网络的可靠性、抗毁性等因素密切相关，但这些性能指标很难从仿真结果的数据分析中得出。因此，对网络攻防训练效果的评估应当着眼于可量化的网络性能指标或系统安全事件，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、网络连通度、链路利用率等统计数据，以及对系统安全属性损害事件的捕获，如是否存在被篡改的程序和文件，是否存在非法增加的帐户和软件，是否存在不明的端口和服务等安全事件等。整个评价过程主要包括两个方面：

(1) 评估所采取的防御方法和技术能否保证信息的机密性、完整性、可用性等安全指标上的要求，并计算各种安全防御措施在时间上的开销，统计不同防御方案的运行效率；

(2) 根据网络性能指标评估各种攻击方法对网络性能的影响程度，根据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。

网络攻击流程如图4所示，相应的攻击方法包括信息截断、信息欺骗、内容篡改、数据伪造和拒绝服务等。

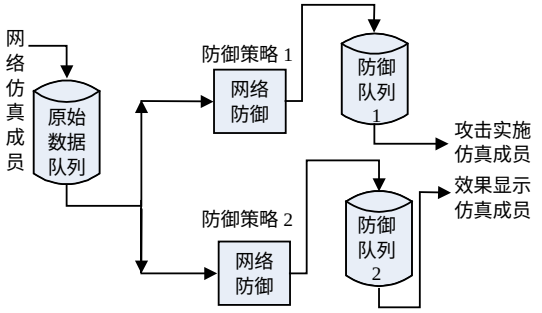

图4 网络攻击流程图

网络防御过程如图5所示，相应的防御方法包括对称加密、密钥信封、数字签名和消息认证等。按照不同防御策略实施保护后的数据分别存入防御队列1和防御队列2中，供攻击实施仿真成员和效果显示仿真成员调用。

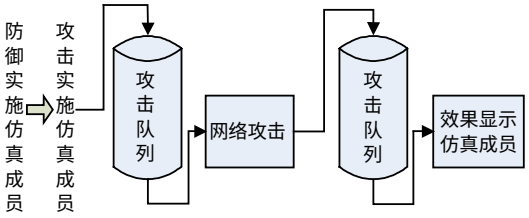

图5 数据完整性保护过程

在每次的仿真过程中实时显示每个数据包的概要信息，包括该数据包的序列号、防御方式、可能遭受的攻击以及防御开销等，如图6所示。

图6　数据包信息

仿真过程中实时统计并显示各种防御方式的平均时间开销，如图7所示。

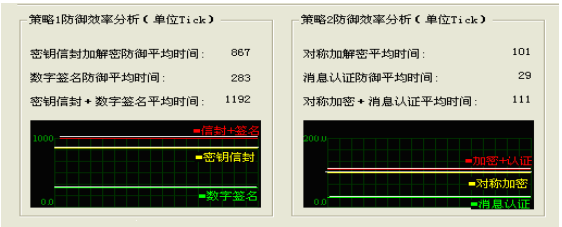

图7　防御开销对比分析

通过图6和图7可以看出，从保护机密性的角度分析，密钥信封的防御开销要远大于数字签名的开销；从保护完整性的角度分析，对称加密防御效率要高于消息认证；而如果既保护机密性又保护完整性，则采用对称加密＋消息认证的方式效率要好一些。同时在仿真过程中可以发现，对多条链路同时实施防御时，各种防御方式的时间开销都会不同程度的增大。

2.4　对抗训练模拟信息库

对抗训练模拟信息库包括知识库和漏洞数据库。知识库是对抗训练模拟信息库中的重要部分，它通过与相关领域专家进行交流，总结专家的经验，并通过一定的知识表示方法组织而成。知识库的表示方法有很多种。根据网络对抗训练模拟系统的特点，本文采用产生式规则与过程表示结合的方式，并给出知识库规则的一个实例：

If system[X] is Unix AND Version[Y] is Sendmail8.8.* AND

Level_s[Z] is RS AND Level_l[Z] is 6 AND Level_a[Z] is W AND

Hack(d0_v8-BOF,X) THEN Level_a[Z] is [LS,L3,W]

漏洞数据库包括漏洞主机库和漏洞列表库。(1) 在对网络主机完成扫描和漏洞检测后，可将存在漏洞的主机的信息存放到漏洞主机库中，作为下一步攻击的可利用主机的信息。漏洞主机库的结构字段主要包括主机IP地址(IP address)、操作系统(OS)、拓扑结构(Topology)和存在的漏洞(Vulnerability)等。(2) 漏洞列表库存储漏洞本身的相关信息，可实现对漏洞信息的查询、更新。漏洞列表库的结构字段主要包括漏洞名称(Name)、漏洞描述(Description)、记录修改时间(Time)、漏洞引起的危害等级(Level)等。整个漏洞数据库的结构字段如表2所示。

表2　信息库中各数据库的结构字段

漏洞主机库	漏洞列表库
IP 地址	名称
操作系统	漏洞描述
拓扑结构	修改时间
漏洞	危害等级

3　结　论

随着计算机网络技术和模拟仿真技术的逐渐成熟，运用高技术进行网络对抗训练模拟已经成为网络战人才培养和训练的重要方式。通过构建网络对抗训练模拟系统：(1) 能够模拟网络攻击的各个主要步骤，实现目标侦测、信息窃取、网络入侵、信息窃取、信息或服务破坏等攻击方法；(2) 能够观察和检测各种网络攻击行为，正确评估攻击效果；(3) 能够通过采取有效防护措施控制安全风险，并根据防御训练后的评测结果比较攻防效果；(4) 能够提高参训人员的信息安全意识，增强网络对抗的实践技能。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测评，使训练人员利用该系统进行自主实验、自我训练和不断改进，为培养一支掌握网络对抗技术、打赢未来网络战的高素质人才队伍提供良好的教学支持。

参　考　文　献

[1] 费爱国, 王新辉. 网络中心战的效能度量[M]. 北京: 军事科学出版社, 2004.
[2] 胡晓峰. 作战模拟术语导读[M]. 北京: 国防大学出版社, 2004.
[3] WILSON C. Information warfare and cyberwar: Capabilities and related policy issues[EB/OL]. http://www. fas.org/irp/crs/, 2007-01-28.
[4] 卢　昱. 协同式网络对抗[M]. 北京: 国防工业出版社, 2003.
[5] DMSO. High level architecture object model template specification[EB/OL]. http://www.dmso.mil., 2007-01- 30.
[6] 景　旭, 唐晶磊, 韩永国. 基于信息对抗的网络集成防御系统[J]. 微计算机信息 2006, 8(3): 99-100.

编　辑　熊思亮