

基于插件的网络攻防训练模拟系统设计与实现

汪 渊, 杨 槐, 朱安国

(解放军炮兵学院, 安徽 合肥 230031)

摘 要:网络中心战是信息战中一种重要的作战方式, 网络在现代战争中发挥着不可替代的作用。通过分析网络攻防训练系统功能要素, 构建网络攻防训练模拟平台以实现网络攻防相关技术的实战训练。利用网络安全漏洞量化方法、网络安全漏洞信息案例推理及网络安全攻防分类方法, 平台可以实现网络攻防训练模拟中辅助决策功能, 最后给出训练模拟平台的实现原型框架。通过网络攻防训练模拟系统, 可以较好地掌握网络攻防原理与技巧, 达到较好的网络攻防模拟训练效果。

关键词:网络攻防; 训练模拟; 安全分类; 漏洞量化

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2010)07-0172-03

Plug-in Based Network Attack-Defense Training Simulation System Design and Implementation

WANG Yuan, YANG Huai, ZHU An-guo

(PLA Artillery Academy, Hefei 230031, China)

Abstract: The network-centric warfare is an important operation mode. The network is playing an important role in the modern war. By analyzing the function elements in an actual network attack-defense training system, a complete network attack-defense training system is constructed to realize the simulated training of the network attack-defense technology. By classifying the network attack-defense means, reasoning the network vulnerabilities and quantifying the network security vulnerability, the assisted decision function can be provided in the network attack-defense training system. Finally gives the implementation framework of the network attack-defense training simulation platform. This system can make the training persons better grasp the network attack-defense principle and skills and realize a better training effect.

Key words: network attack/defense; training simulation; security classification; vulnerability quantification

0 引 言

“网络中心战”就是利用计算机网络对部队实施统一的作战指挥, 其核心是利用网络将地理上分散的各部队、各种武器联系起来, 实现信息共享, 实时掌握战场动态, 缩短决策时间, 减少决策失误, 以便对敌人实施快速、精确、连续的打击^[1,2]。因此, 战争胜负的关键在于作战双方谁取得了制信息权, 而计算机网络是信息对抗的物质基础, 它在现代信息战中扮演着神经中枢的角色。计算机网络是战争中各种指挥控制信息流动的通道, 一旦它遭到致命性的破坏则后果可想而知, 所谓“知己知彼, 百战不殆”, 要解决自身的安全问

题, 首先必须要了解自己的系统目前究竟存在哪些安全隐患^[3], 因此, 建立一个仿真的网络攻防软件系统对网络知识的学习与未来网络环境的备战都十分必要。

1 系统设计

在实际网络对抗过程中, 网络攻防是密不可分的。攻击方随时可能转换为防守方, 防守方也可抓住机会转换为攻击方。作为训练模拟手段, 可以将这两个过程分开训练, 即我方防御敌方进攻样式和我方进攻敌方防御样式。训练一方被指定为敌方(相当于演习中的蓝方), 另一方被指定为我方(相当于演习中的红方)。攻击方通过熟练运用网络刺探工具及网络攻击工具, 辅以掌握的网络安全相关知识, 可以进行相关攻击。防守方通过熟练运用网络检测与防御工具, 辅以掌握的网络安全知识, 可以进行积极防御。整个网络攻防模拟训练平台结构如图1所示^[4,5]。

收稿日期: 2009-11-01; 修回日期: 2010-02-28

基金项目: 国防预研基金资助项目(200109)

作者简介: 汪 渊(1973-), 男, 安徽安庆人, 博士, 研究方向为网络安全及辅助决策; 杨 槐, 副教授, 研究方向为数据库系统、辅助决策; 朱安国, 副教授, 研究方向为指挥自动化、辅助决策。

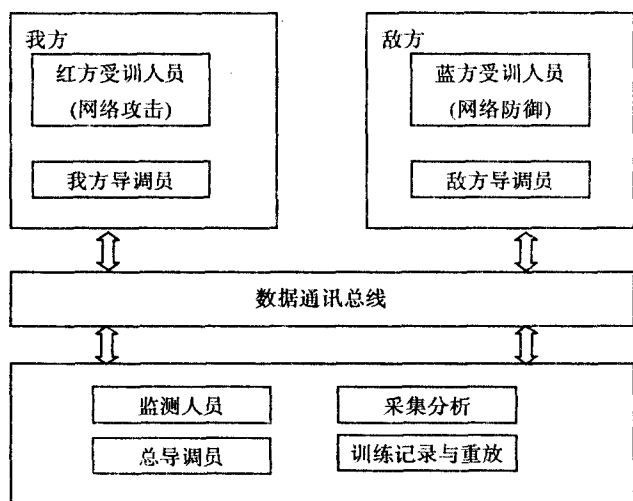


图 1 网络攻防训练模拟平台

在整个平台中,敌方导调人员可以指导敌方参训人员进行网络攻击准备与实施,我方人员可以指导我方参训人员进行网络检测与主动防守。敌我双方的所有攻击行为都通过数据通讯总线进行传输。控制台的监测人员可以对敌我双方的计算机屏幕及通讯流量进行实时监控,并且可以通过总导调员对双方进行预定科目考核,为了成绩考核及评定,控制台可以对敌方双方模拟训练过程中的流量进行采集分析,并且可以对所有训练结果进行记录和回放。

实际实现过程中,可以将训练模拟系统设计成多客户端和单服务器端模式。客户端主要完成结果显示、连接建立、配置及执行等功能,服务器端是运行多种服务的后台,可以为客户端提供实际的各种插件应用程序、各种辅助数据库、训练评估、训练模拟数据采集与记录等。后台可以控制前台的行为,并且可以与前台通过软件进行交互。系统功能结构如图 2 所示。

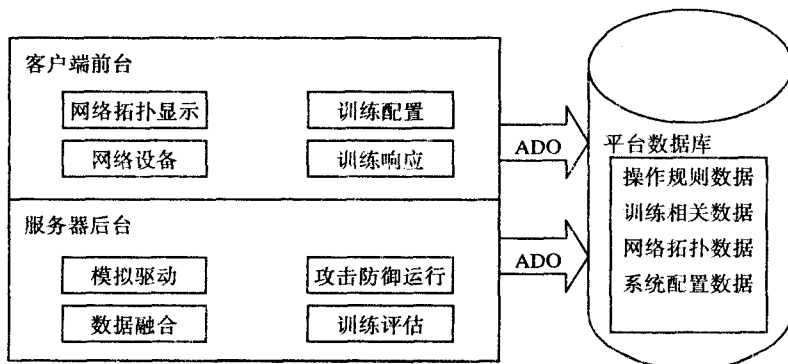


图 2 平台系统功能模块结构

2 关键技术

2.1 网络攻防分类技术

网络攻防模拟的基础是对各种攻防手段进行分类,这样才能进行针对性训练。训练模拟平台中采用

的分类机制如表 1 所示^[6,7]。

表 1 网络安全攻防手段分类

网络攻击 - 防护技术	网络攻击	扫描	网络拓扑检测
			OS 指纹识别
			端口扫描
			漏洞扫描
		嗅探器	ARP 欺骗
			线路截取识别
			重定向攻击
		密码	操作系统密码
			应用程序密码
			文档密码
			密钥
		SQL 注入	
		漏洞	操作系统漏洞
			数据库漏洞
			应用程序漏洞
		社会工程	网络钓鱼
			网络欺骗
			网络假冒
		木马	键盘记录
			远程控制
			网络摆渡
			集成功能
		后门	
网络防护	网络防护	安全策略	
		加密	数据加密
			识别
			认证
		蜜罐	
		防火墙	软件防火墙
			硬件防火墙
			虚拟专用网
			网络代理服务器
		入侵检测	

2.2 网络攻击漏洞威胁量化

在训练模拟中,当刺探工具得到多个可利用漏洞时,参训人员可以利用漏洞威胁量化库对漏洞威胁程度进行量化与选择。主要漏洞量化指标体系解释如下^[8~10]:

* 条件关联性:指某些攻击是多条件的,且有的条件外部扫描是无法确定判别的。

* 攻击可检测性:指有些攻击手段具有隐蔽性,对其检测误警率高。

* 攻击可处理性:指对攻击事件的处理所消耗资源多。

* 攻击条件存在的普遍性:指攻击条件在实际中存在可能性的统计分析。

* 攻击条件存在时间:指攻击所利用的漏洞已存在的时间。

- * 攻击可操作性:指攻击所需的技术要求难度。
- * 攻击的持续性:指攻击在达到目的的持续时间。

2.3 基于案例的安全攻击情景推理

整个网络的多点脆弱性的产生与传播机理用图论来描述形象且直观,但在软件的具体实现上,用案例推理则较为容易。因为对网络脆弱性的推理分析是基于知识的推理过程,而案例推理对知识的表达比较直观且比较有效,且案例库容易更新,所以在实际问题的解决中应用非常广泛。由于脆弱性的直观表示形式也是由多种属性及相应的后果所组成,其与案例表达方式非常相似,且案例可以表达那些不易分解为单个规则的推理关系,所以用 CBR(case-based reasoning)作为脆弱性分析的推理机制是合适的^[11,12]。案例推理作为一种有效地解决问题的方法,具体推理流如图 3 所示。

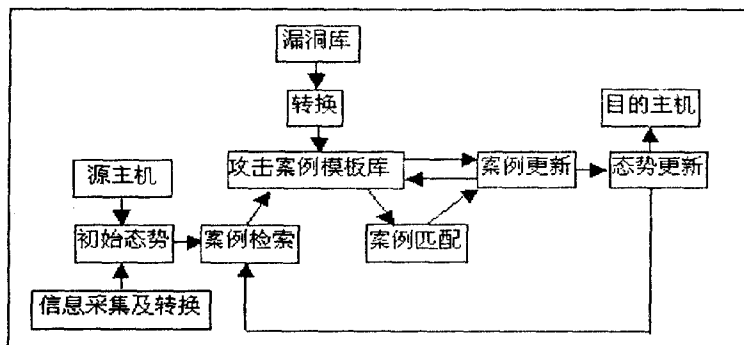


图 3 基于案例推理的脆弱性检测

3 系统实现

整个网络攻防训练模拟系统(Network Attack - Defense Training Simulation System,简称 NADTSS 系统)是建立在一个实际的网络环境中,系统由客户端和服务端两部分组成。服务器端提供多种安全攻击与防御程序服务,客户端主要是用于操作、配置和显示。在服务端还采用了 plug-in 的体系,允许用户加入执行特定功能的插件,通过插件,可以即时更新和扩展安全攻防训练。网络攻防训练模拟流程如图 4 所示。

其中训练模拟平台运行扫描任务时的软件界面如图 5 所示。

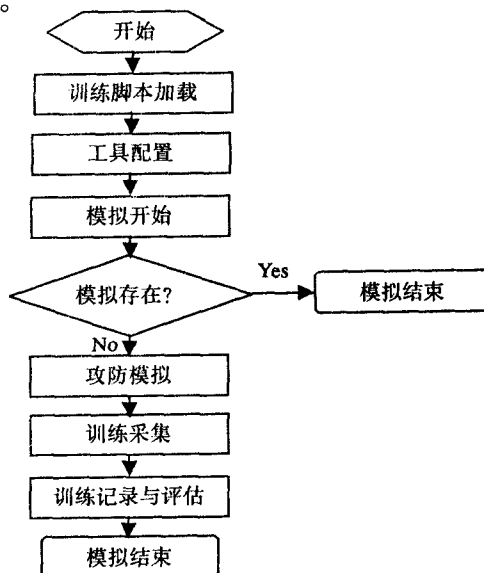


图 4 网络训练模拟系统流程

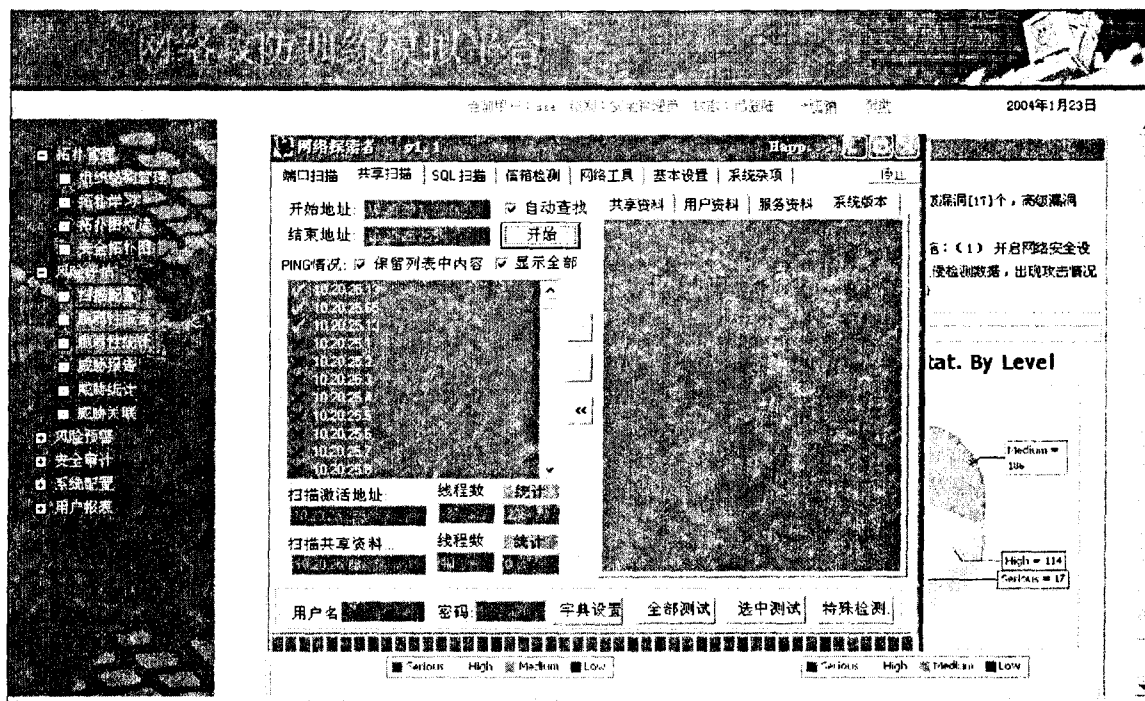


图 5 网络攻防训练模拟平台界面

<return_type>:函数返回的结果类型;

<method_body>:方法体(程序代码);

<language>:方法体所使用的程序语言

代理类的定义包括定义类名、代理类型、扩展属性和方法,以及代理规则。通过删除类的命令,用户可以将任何类从数据库中删除。

4 结束语

分析并指出了地理信息的存储和管理是当前地理信息系统发展的重点和难点。通过对地理信息系统空间数据建模的阐述,分析了混合数据库模型、扩展结构模型、全关系模型、面向对象模型和对象关系模型解决的问题和依然存在的不足,引出了使用对象代理机制建立地理信息系统模型的思想,并提出了对象代理空间数据模型。

文中的创新之处在于把对象代理机制引入到空间数据库的建模以及地理信息的组织和显示中,完成了地理信息系统中的空间数据存储和管理的新形式,更大程度地满足了用户的操作需求。虽然文中的研究取得一些成果,但很多地方仍需要进一步研究和改进。

参考文献:

- [1] 许捍卫,冯学智.空间数据存储机制研究[J].计算机应用研究,2003,20(2):39-40.

(上接第174页)

4 结束语

整个系统主要在Windows系列平台上运行,采用的开发工具为MICROSOFT VC6.0。通过网络攻防训练模拟平台,可以较好地进行攻防理论及技巧的训练,增强受训人员的训练效果。整个平台以插件式实现,功能可以根据网络攻防相关技术的发展而扩展,具有可扩展性、低成本性和易用性。同时,通过在网络训练模拟平台中加入辅助决策功能,可以增强受训人员的决策能力。

参考文献:

- [1] Department of Defense, USA. Network Centric Warfare, DoD Report to Congress[R]. Washington DC: DoD, 2001.
- [2] SAlberts D, Garstka J J, Stein F P. Network centric warfare: developing and leveraging information superiority[M]. Washington DC: DoD Command and Control Research Program, 1999.
- [3] 王慧强,赖积保,朱亮,等.网络态势感知系统研究综述[J].计算机科学,2006,33(10):5210-5215.
- [4] 景旭,唐磊,韩永国.基于信息对抗的网络集成防御系

- [2] 张成才,孙喜梅,黄慧. SDE的实体关系模型空间数据管理方式研究[J]. 计算机工程与应用, 2003, 39(2): 199-201.
- [3] 罗忠文. 应用对象关系型数据库存储GIS数据[J]. 中国地质大学学报: 地球科学版, 2002, 27(3): 267-270.
- [4] 彭智勇, 彭煜玮, 翟博. 一个基于对象代理模型的多表现地理信息系统[J]. 计算机应用, 2006, 26(9): 2016-2019.
- [5] 谢卫平. 基于对象代理模型的地理信息建模和存储管理[D]. 武汉: 武汉大学, 2006.
- [6] 周迪民, 段国云. 地理信息系统属性数据不确定性的研究[J]. 计算机技术与发展, 2009, 19(12): 174-177.
- [7] 蔡正林, 韩金华, 李梦琪. 网格GIS体系结构研究及应用[J]. 计算机技术与发展, 2006, 16(7): 221-223.
- [8] 朱光, 季晓燕, 戎兵. 地理信息系统基本原理及应用[M]. 北京: 北京测绘出版社, 1997: 253-324.
- [9] Tang A, Adams T, Usery E. A Spatial Data Model Design for Feature Based Geographical Information Systems[J]. Geographical Information Systems, 1996, 10(5): 643-659.
- [10] Borges K, Davis J, Laender A. OMT-G: An Object-Oriented Data Model for Geographic Applications[J]. GeoInformatic, 2001, 5(3): 221-260.
- [11] Kosters G, Pagel B, Six H. GIS-Application Development with GeoOOA[J]. Geographical Information Science, 1997, 11(4): 307-335.
- [12] Shekhar S, Coyle M, Goyal B, et al. Data Models in Geographic Information Systems[J]. Commun ACM, 1997, 40(4): 103-111.

统[J]. 微计算机信息, 2006, 8(3): 99-100.

- [5] 卢昱. 协同式网络对抗[M]. 北京: 国防工业出版社, 2003.
- [6] Kumar S. Classification and Detection of Computer Intrusions[D]. West Lafayette, Indiana: Department of Computer Science, Purdue University, 1995.
- [7] Aslam T, Krsul I, Spafford E. Use of a Taxonomy of Security Faults[C]//Proceedings of the 19th NIST-NCSC National Information Systems Security Conference. [s.l.]: [s.n.], 1996: 551-560.
- [8] 肖道举, 杨素娟, 周开锋, 等. 网络安全评估模型研究[J]. 华中科技大学学报: 自然科学版, 2002, 30(4): 37-39.
- [9] 冯登国, 张阳, 张玉清. 信息安全风险评估综述[J]. 通信学报, 2004, 25(7): 10-18.
- [10] 郭亚军. 综合评价理论与方法[M]. 北京: 科学出版社, 2002.
- [11] 汪渊, 蒋凡, 陈国良. 基于图论的网络安全分析方法研究与应用[J]. 小型微型计算机系统, 2003, 24(10): 1865-1869.
- [12] 汪渊, 蒋凡, 陈国良. 一种基于安全案例推理的网络安全分析方法[J]. 小型微型计算机系统, 2003, 24(12): 2082-2085.