基于渗透测试的抗攻击测试体系构建与渗透攻击系统设计

祝宁，陈性元，张永福
（解放军信息工程大学 电子技术学院，河南 郑州 450004）

摘 要：分析了当前渗透测试的研究与发展现状，基于渗透测试的基本理论方法，以弥补渗透测试的不足为目标，定义构建了抗攻击测试体系，形成了以渗透测试为核心的新的信息系统安全性与免疫能力分析与衡量方法。同时，对作为抗攻击测试实施的首要环节和基础保障的渗透攻击进行了详细的系统功能设计与模块划分，并实现了渗透攻击实施原型子系统。通过功能测试，验证了该系统实施功能的正确性、有效性与合理性。

关键词：渗透测试；抗攻击测试；原子攻击；渗透攻击系统
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2011)11A-0071-08

Construct of the attack resistance test and design of the penetration attack system based on penetration testing

ZHU Ning, CHEN Xing-yuan, ZHANG Yong-fu
（Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China）

Abstract: By analyzing the present condition of development & research for penetration testing, based on the basic theory of penetration testing, in order to fix the defect of penetration testing, defined and constructed attack resistance test(ART). It was a new method to analyze and measure the security and immunity of information system which used penetration testing as a kernel tool. Simultaneously, designed the penetration attack system detailedly which was the first step and important indemnification of ART, divided the function modules of the system, and realized the prototype system software, then checked and confirmed the correctness, effectively, and reasonableness of the system by building the test environment and carrying out function testing.

Key words: penetration testing; attack resistance test; atomic attack; penetration attack system

1 引言

由于计算机系统存在可以被渗透的脆弱性，在互联网飞速发展的今天，信息安全越来越为人们所关注，信息安全保障成为互联网时代的焦点问题。信息系统的使用前免疫程度分析与评估成为确保其安全可靠运行的关键，是信息安全保障的重要环节。中国在《2006-2020 年国家中长期科学和技术发展规划纲要》[1]中就提出了要建立“强免疫系统”的要求；美国 2006 年《联邦网络安全和信息保障研究发展计划》（Federal Plan for Cyber Security and Information Assurance Research and Development，简称“联邦计划”）[2]也提出构建“内在安全、高安全保障和可证明安全系统结构（Inherently Secure, High-Assurance, and Provably Secure Systems and Architectures）”，同时提出要求“网络或者系统的拥有者能够从破坏的通信或操作，或者从危及安全或安全恶化的信息中，采用技术实践，提高抵抗攻击

收稿日期：2011-08-24
基金项目：国防预研基金项目；国家重点基础研究发展计划（“973”计划）基金资助项目（2011CB311801）
Foundation Items: The National Defense Pre-Research Foundation Program; The National Basic Research Program of China (973 Program) (2011CB311801)

或者阻止攻击的能力”；美国《信息保障技术框架（IATF）》[3]也指出，在信息系统安全工程（ISSE）全过程中，均要进行“保护有效性”的评估。

综合上述分析，安全测评已成为信息安全保障的重要环节，安全保护的有效性分析是信息安全保障的重要支撑，而模拟真实攻击环境下安全程度测试与“保护的有效性”评估的渗透测试则成为一种新的有效方法。

2 渗透测试分析

目前，渗透测试在国内外尚处于理论研究和起步发展应用阶段，主要理论研究包括有：由 ISECOM 编纂的开源安全测试方法学手册(OSSTMM)[4]，德国联邦信息安全办公室发表的渗透测试模型[5]，美国国家标准和技术研究所(NIST)发表的信息安全测试技术指导方针(technical guide to information security testing，SP800-115)[6]及国内外利用攻击建模进行的相关研究[7~11]，包括中国航天二院 706 所张继业提出的基于攻击图的渗透测试模型、华中师范大学的周伟提出的一种基于树结构的网络渗透测试系统、广东工业大学的徐正强提出的网络信息安全渗透测试平台、北京大学陈国栋等人提出的基于网络攻击图的自动渗透测试系统、重庆大学的袁浩提出的新的改进渗透测试方法、中国科学技术大学宇佳提出的一种可扩展的分布式网络攻击测试系统、信息工程大学信息工程学院崔颖提出的基于攻击图的渗透测试方案自动生成方法等。然而，总结当前的渗透测试发展现状，还存有不足。

1) 渗透测试尚未形成体系化，目前渗透测试大多作为现有漏洞发现与分析的支撑技术而使用，作为对扫描与探测结果的一种正确性验证，多用于“辨认技术系统弱点和管理失误”，没有形成体独立的测试实施体系和专用的评估标准。

2) 渗透测试不具备标准化的执行流程，不具有共享性，其评估结果无法可再生。

3) 渗透测试操作实施过程复杂，对操作人员技术水平要求高，需要能够“对组件、系统功能和行为深入理解”，具有“很好的能力和资质”。

4) 操作过程依赖于人员对相关攻击工具的使用，工具的可信程度与可靠性受质疑。

5) 渗透测试尚属于粗粒度测试，其结果的分析与评判仅关注于对脆弱点存在与否的验证，对信息系统免疫能力的程度衡量与分析无法实现。

因此，具有一定先进性的渗透测试还尚无法达到作为一项普通测试而广为接受和使用的程度。为此，本文基于渗透测试提出了抗攻击测试的概念，并构建抗攻击测试体系，以有效弥补渗透测试的缺陷。

3 抗攻击测试体系

3.1 抗攻击测试定义

构建抗攻击测试体系，需明确如下定义。

定义 1 抗攻击能力（AR, attack resistance），是指系统在实际受到攻击的情况下维持其安全功能的能力，系统的安全功能通常通过保密性、完整性和可用性等方面来度量。

定义 2 抗攻击测试（ART, attack resistance test），即是对目标系统抗攻击能力的测试衡量与评估。它是一种通过模拟系统在实际运行环境中可能出现的网络攻击，结合检测目标所遭受的实际受损情况，对系统抵御攻击的能力与免疫程度进行度量的安全测评方法。抗攻击测试的最终目的不是完全消除脆弱性，而是提供一种目标系统安全程度的合理度量，意在帮助决策者在“提供服务”和“保证安全”之间找到平衡。

抗攻击测试，从本质上来说就是一种渗透测试，但其关注与侧重点却又有所区别。

总体上看，抗攻击测试更关注于对攻击造成的后果进行程度分析，给出符合逻辑的科学衡量，而非渗透测试的对发现漏洞的验证及找出可利用漏洞的攻击方法。

抗攻击测试侧重于分析每种原子攻击操作对目标信息系统造成的实际损伤，并通过评估原子攻击操作的免疫程度，判断整个攻击的效果，发现新的攻击实施组织形式，进而综合评价信息系统总体安全程度。其中，所谓原子攻击，如定义 3 所述。

定义 3 原子攻击（atomic attack），只为实现全部攻击流程中一个目的，对目标单一脆弱性的一次利用，实现一种基本攻击效果的基础、结构完整的攻击功能实现。原子攻击是攻击实现的最小结构单元，不能够再进行拆分，否则将不具有攻击的性质。

3.2 抗攻击测试体系构成

基于抗攻击测试的要求与目标，建立抗攻击测试体系由渗透攻击、攻击效果检测、抗攻击能力综合评价和抗攻击测试标准 4 部分构成，如图 1 所示。

其中，抗攻击测试标准是整个抗攻击测试体系的基础，它是实施抗攻击测试，确保测试过程标准化的

重要依据；渗透攻击与攻击效果检测是抗攻击测试顺利实施的保障；对信息系统安全性的抗攻击能力综合评价则是整个抗攻击测试体系的核心与目标。

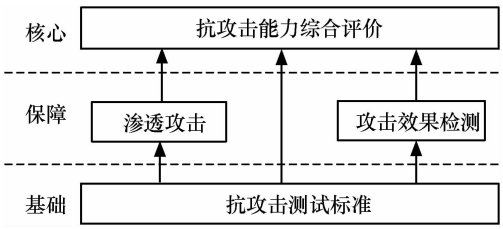

图 1　抗攻击测试体系组成

1) 渗透攻击：负责依据测试要求，构建测试方案，统一组织调度攻击实施，完成模拟实际环境下的对测试目标的攻击。同时，还负责建立抗攻击测试中所需的攻击工具储备。

2) 攻击效果检测：包括外部服务提供性能检测及目标内部工作性能检测两部分，负责针对攻击具体类型特点，检测目标在攻击下的反映攻击效果的指标数据，分析评估攻击下目标的受损情况，形成对单一攻击下的目标受损程度，即攻击的效果的评估结果。

3) 抗攻击能力综合评价：面向单一攻击建立结合攻击特点量化（攻击危害、复杂程度、实施代价等）与攻击实施效果的抗攻击能力评估；形成针对全部测试项目中的评估结果建立对测试目标整体测试要求下的综合抗攻击能力评价。

4) 抗攻击测试标准：是抗攻击测试体系的基准，它贯穿并指导着整个抗攻击测试过程，是进行测试需求确定、攻击实施、受损采集与分析及综合抗攻击能力评价的参照。

在抗攻击测试体系中，渗透攻击是实施抗攻击测试的首要环节，是整个体系得以正常运转的起始点与重要保障。同时，该部分也是继承渗透测试并完成了渗透攻击过程的标准化、结构化和自动化，是对渗透测试的有益修正。为此，下面详细阐述渗透攻击系统的功能与设计。

4　渗透攻击系统设计

渗透攻击是抗攻击测试的首要环节，是整个测试体系得以顺利实施的基础保障。据此，对渗透攻击系统进行需求分析与功能设计。

4.1　功能需求

根据抗攻击测试体系及其实施要求，渗透攻击系统主要用来依据测试需求，组织和实施渗透攻击。因此，该系统应具有主要功能如下：

1) 满足精确测试的要求，提供多角度、多层面可供选择的测试要求；

2) 能够依据选择测试要求与条件，查找并确认所需实施的原子攻击操作；

3) 能够自动组织符合实际的原子攻击操作顺序关系并建立描述原子攻击操作实施的渗透攻方案；

4) 依据渗透攻击方案，实现调度相应原子攻击操作，执行对目标信息系统的渗透攻击；

5) 收集攻击过程特征信息与攻击反馈信息，结合原子攻击自身的特征属性信息，形成对攻击结果的全面详细描述，结合检测的攻击效果，供抗攻击能力综合评价使用。

4.2　理论基础

上述功能要求中，最为复杂的即是自动组织建立渗透攻击方案，它涉及到攻击特征描述、攻击间的关联组织关系分析、建立合理有效符合实际的攻击执行顺序等攻击本质，是具有难度的理论研究。对此，作者通过对攻击模型的研究，基于攻击树模型，定义并设计建立了面向抗攻击测试的渗透攻击模型，利用模型建立基于攻击需求的具体实例构建了渗透攻击方案，并提出了利用方案的攻击调度与执行算法。具体参见文献[12]。

同时，为保证抗攻击测试过程中，渗透攻击实施过程的可信、可控、有效，设计了面向抗攻击测试的攻击描述语言（AASL, attack script language for ART），及语言专用解释器，并构建了 DoS 攻击和溢出攻击的通用描述模板，用于开发各类测试使用的原子攻击。关于该方面的理论研究，参见文献[13]。

4.3　系统架构设计

系统设计采用模块化思想，本着模块间的功能耦合度尽量小的原则，渗透攻击系统划分为两大子系统，分别为渗透攻击实施子系统和攻击生成子系统。其中，渗透攻击实施子系统负责完成对目标信息系统的渗透攻击工作；渗透攻击生成子系统负责相关原子攻击的开发。该系统的组成结构如图 2 所示。

其中，测试需求选择模块主要用于依据目标的安全需求，用户要求及脆弱性检测与分析结果，建立整体的测试要求，并将结果传递给攻击方案生成模块，以用于建立测试方案。

攻击方案生成模块依据测试要求，结合攻击知识库中的与测试要求相关的攻击知识信息，组织建立抗攻击测试中的渗透攻击的实施方案。

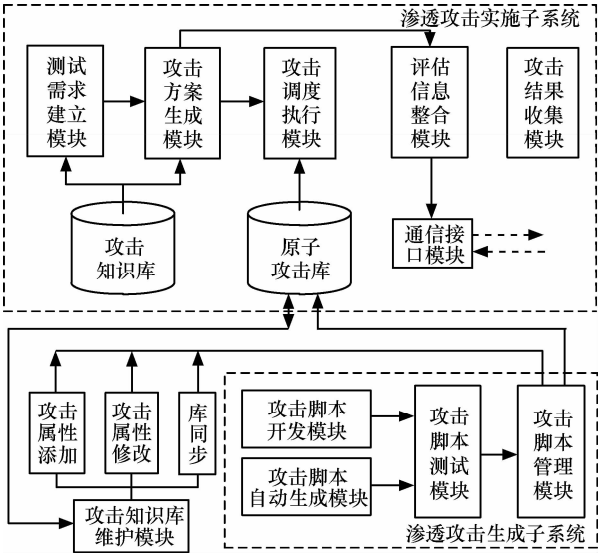

图 2　渗透攻击系统架构

渗透攻击调度与执行模块的功能为依据方案描述所原子攻击间的关系，建立可行的攻击执行序列，并从攻击脚本库中调用相应的攻击操作脚本，完成对测试目标进行渗透攻击。

攻击结果收集模块主要用于收集攻击实施过程中和作用后目标系统的返回结果，并将返回结果传递给评估信息整合模块。

评估信息整合模块主要用于整合所采用的渗透攻击自身的相关属性信息和攻击结果反馈信息，提交抗攻击能力综合评估，作为综合抗攻击能力评价的依据。

攻击脚本开发模块提供攻击脚本的开发环境，用于编写各类以 AASL 语言描述的具体渗透攻击脚本，形成攻击测试用例。

攻击脚本自动生成模块的功能为自动解析 SNORT 规则，提取相应的攻击特征，利用脚本模板自动构建渗透攻击脚本，形成测试用例[15]。

攻击脚本测试模块用于对编写的攻击脚本或翻译转换而生成的攻击脚本进行功能正确性及攻击有效性测试。

攻击脚本管理模块用于将建立的攻击脚本存入攻击工具库（脚本库），同时调用攻击知识库维护功能将相关攻击信息存储于攻击知识库，提供攻击相关知识信息供攻击方案建立使用。

库维护模块主要用于实施对 2 个支持库的维护与管理。包括向攻击知识库中添加、修改和删除攻击行为相关信息、向攻击知识库中添加、删除相关攻击行为等操作。其中的库同步操作主要用于保证攻击知识库中攻击的信息与攻击脚本库中具体的攻击脚本相对应。

通信接口模块是渗透攻击平台与抗攻击测试体系的其他平台交互通信的通道，主要用于实现向综合评价平台传递渗透攻击信息，即由评估信息整合模块整理的攻击代价信息。

对渗透攻击系统功能的全面支持主要由 2 个库结构实现。

1) 攻击知识库：用来对攻击进行分类、标识与管理。它基于本体的思想，依据面向攻击原子，采用多属性分类方法[14]对攻击的描述进行分类存储，保存与攻击相关的属性信息、攻击间的相互关系信息及攻击的存储位置信息等相关内容。利用攻击知识库，可以方便的分析某种攻击的属性，详细了解攻击的特征，掌握攻击间的条件与关联关系。

2) 原子攻击库：即攻击工具库，它以统一形式对测试用例进行存储管理，存储渗透攻击所需要的各类攻击。

4.4　渗透攻击实施子系统工作流程

攻击实施子系统是抗攻击测试顺利实施的保障，是渗透攻击系统的关键核心组成。其科学、有效、准确的实施是保障整个抗攻击测试的基础。该子系统的基本工作过程如图 3 所示，具体实施过程可划分为以下 6 个步骤。

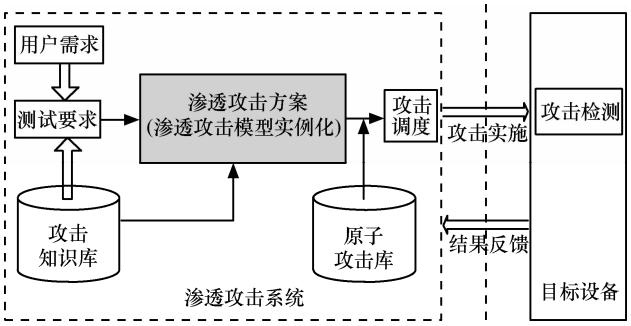

图 3　渗透攻击实施子系统工作过程

1) 攻击知识库依据其对攻击属性特征的存储管理，提供对目标信息系统进行渗透测试的可选测试需求。

2) 用户按照自己的安全防御需求，从中选取所要测试的内容，形成抗攻击测试的总体需求。

3) 基于对目标信息系统的测试需求，结合攻击知识库中存储的攻击属性特征和具体攻击行为的特征，以面向抗攻击测试的渗透攻击模型为依据，建立模型的具体实例，即渗透攻击方案。

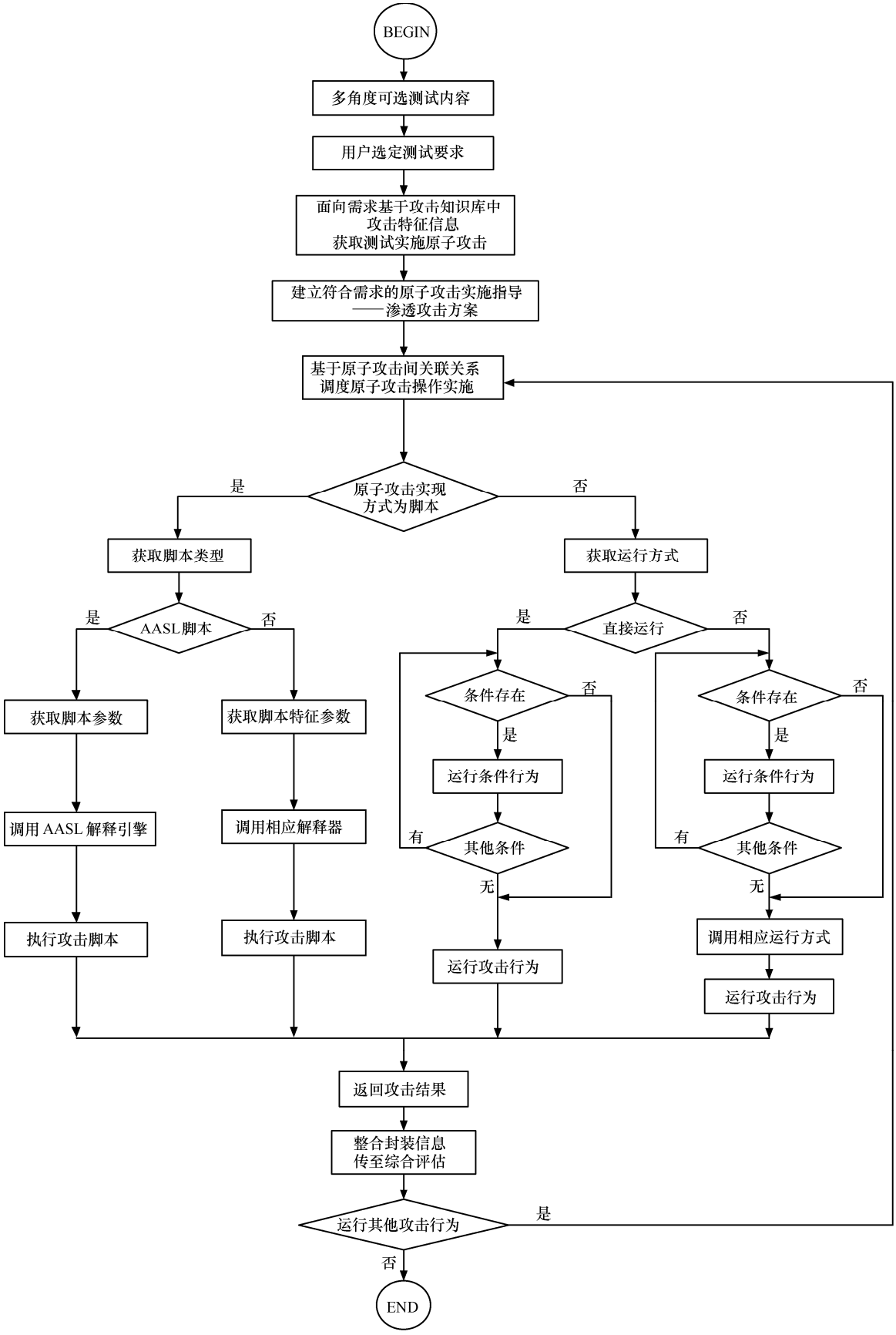

图 4　渗透攻击实施子系统攻击测试流程

4) 遵照渗透攻击方案，从原子攻击工具库中调用相应的攻击行为，依据攻击方案描述形成攻击间的执行顺序关系，组织调度攻击按照符合实际的顺序执行。

5) 基于攻击实例的具体类型，采用适当的运行方式，实现攻击对目标信息系统的渗透攻击操作。

6) 收集目标信息系统对实施攻击的响应数据，整合攻击相关信息，封装形成评估主机对目标设备的抗攻击能力进行评估的具体参考指标效果数据，并将其传送至评估平台以供使用。

至此，一个完整的渗透攻击过程结束。图 4 以流程图的方式描述了该渗透攻击系统对目标设备进行渗透攻击测试的整个流程。

5　原型系统实现与实例分析

基于上述系统结构设计，开发实现了渗透攻击原型系统（图 5），并利用该系统进行了服务器的抗 DoS 攻击能力的验证测试。

以对服务器的抗 DoS 攻击能力进行测评，判断安装防火墙前后服务器抗 DoS 攻击能力的变化情况为例，搭建测试环境。测试环境设备包括：Windows NT 服务器一台（开启 RTX 服务和 Server-U v5.1FTP 服务）、百兆交换机一台、评估主机一台（评估服务质量）、渗透攻击主机一台（建立攻击方案、组织攻击序列，对服务器实施攻击），另外在服务器上还装有相关检测代理，如图 6 所示。

图 5　渗透攻击实施子系统原型系统

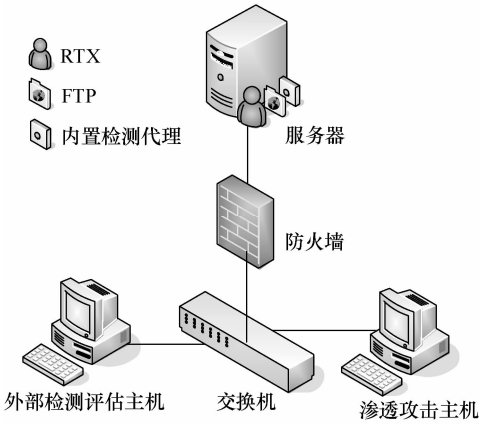

图 6　抗攻击测试实验环境

基于需求建立的渗透攻击方案如图 7 所示，图 8 则给出了基于方案的攻击调度执行序列。依据该攻

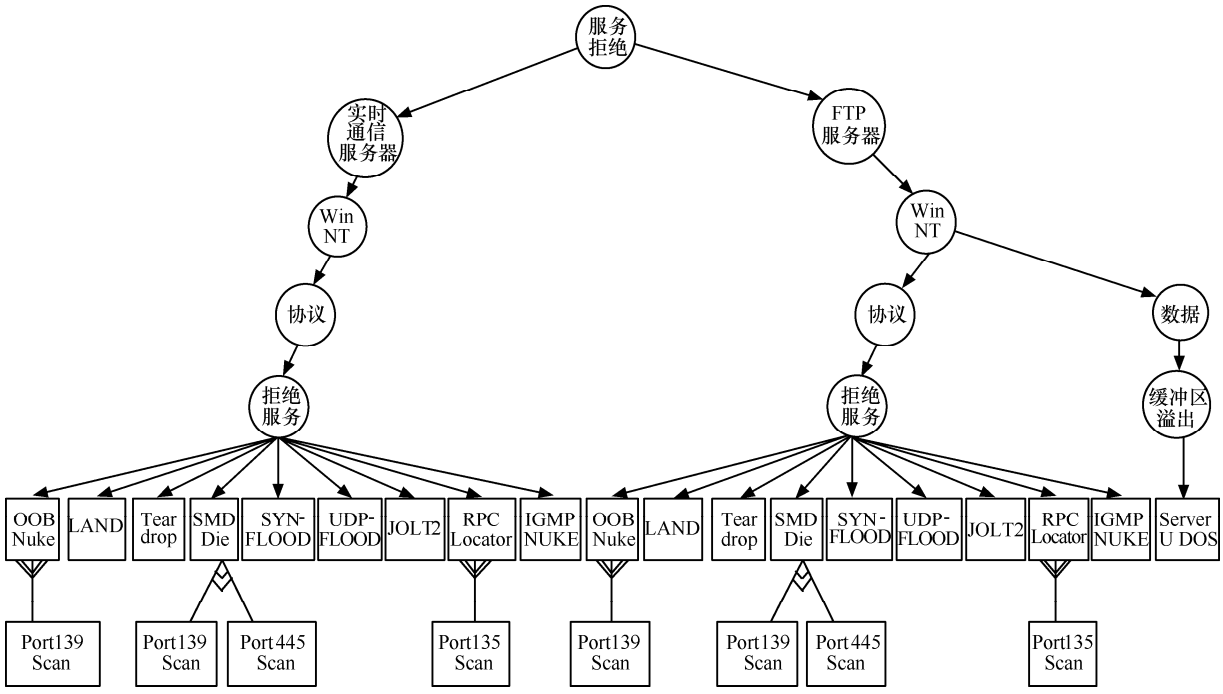

图 7　模型生成渗透攻击方案

击序列实施攻击，检测端检测分析服务器正常服务的提供情况及防火墙工作前后提供功能的变化情况，进而分析评估目标系统自身的抗拒绝服务攻击能力及增加防火墙后抗攻击能力的变化。表 1 系符合测试要求的 SYN-FLOOD 用例攻击下，基于 3GPP QoS 标准[16]测得的服务器的抗攻击能力数据。

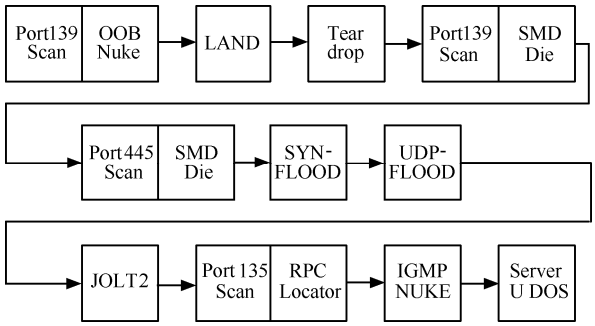

图 8　基于方案的攻击调度执行序列

表 1　　SYN-FLOOD 攻击测试数据

服务	指标项	QoS 指标阈值	未安装防火墙		安装并使用防火墙	
			攻击测试指标值	拒绝服务程度	攻击测试指标值	拒绝服务程度
FTP	单向延迟	10s	20s	35.4%	3s	0
	分组丢失率	Zero	Zero		Zero	
即时通信	单向延迟	400ms	5s	79.4%	200ms	0
	抖动	1ms	1s		1ms	
	分组丢失率	3%	0%		0%	

6　结束语

本文通过对渗透测试的论证与分析，基于渗透测试建立了抗攻击测试体系，并对其中的渗透攻击进行了详细的系统设计。该渗透攻击系统能够合理组织渗透攻击，建立标准化、可重现、可共享的执行流程。同时，自动建立方案与执行调度也降低了测试对操作人员的能力要求，使测试更具普遍意义。抗攻击测试的建立，使渗透测试的组织实施摆脱对人的依赖，避免了测试过程的因人而异。下一阶段，将以完善效果检测系统、综合评价系统为目标，最终建立起系统全面的抗攻击测试的标准体系。

参考文献：

[1] 《2006-2020 年国家中长期科学和技术发展规划纲要》[EB/OL]. http://www.gov.cn. 2010.

《The outline plan of national long-term scientific and technological development during 2006-2020》[EB/OL]. http://www.gov.cn. 2010.

[2] The Interagency Working Group on Cyber Security and Information Assurance. Federal Plan For Cyber Security And Information Assurance Research And Development[R]. USA 2006.4

[3] National Security Agency, Information Assurance Solutions, Technical Directors. Information Assurance Technical Framework[R]. USA, 2002.

[4] OSSTMM2.2[EB/OL]. http://www.iseco -m.org. 2011.

[5] 渗透测试模型[EB/OL]. http://download.csdn.net/source/2501647. 2006.

Penetration testing mode[EB/OL]. http://download.csdn.net/source/2501647. 2006.

[6] NIST SP800-115 信息安全测试和评估指南[EB/OL]. http://wk.baidu.com/ view/997d8d15abe23482f4dfb?pcf=2#1. 2011.

NIST SP800-115 Information security testing and evaluation guidelines[EB/OL].http://wk.baidu.com/view/997d8d15abe23482f4dfb?pcf=2#1. 2011.

[7] 张继业, 谢小权. 基于攻击图的渗透测试模型的设计[J]. 计算机工程与设计, 2005, 26(6): 1516-1518.

ZHANG J Y, XIE X Q. Penetration testing model based on attack graph[J]. Computer Engineering and Design, 2005, 26(6): 1516-1518.

[8] 周伟, 王丽娜, 张焕国. 一种基于树结构的网络渗透测试系统[J]. 计算机与数字工程, 2006, 34(12)：15-18.

ZHOU W, WANG L N, ZHANG H G. A network penetration testing system based on tree[J]. Computer & Digital Engineering, 2006, 34(12): 15-18.

[9] 徐正强. 网络信息安全渗透测试平台研究[D]. 广州：广东工业大学, 2008.

XU Z Q. Study on the Penetration Platform of Network In-formation Security[D]. Guangzhou: Guangdong University of Technology, 2008.

[10] 李勻. 网络渗透测试——保护网络安全的技术、工具和过程[M]. 北京：电子工业出版社，2007.

LI Y. Network Penetration Testing - Technology, Tools and Processes to Protect Network Security[M]. Beijing: Electronics Industry, 2007.

[11] 崔颖, 章丽娟, 吴灏. 基于攻击图的渗透测试方案自动生成方法[J]. 计算机应用, 2010, 30(8): 2146-2150.

CUI Y, ZHANG L J, WU H. Automatic generation method for penetration test programs based on attack graph[J]. Journal of Computer Applications, 2010, 30(8): 2146-2150.

[12] ZHU N, CHEN X Y, ZHANG Y F. Design and application of penetra-

tion attack tree model oriented to attack resistance test[A]. Proceedings of the 2008 International Conference on Computer Science and Software Engineering (CSSE 2008)[C]. Wuhan: IEEE, 2008.

[13] ZHU N, CHEN X Y, ZHANG Y F. A new method to construct DoS attack oriented to attack resistance test[A]. Proceedings of 2010 IEEE International Conference on Information Theory and Information Security (ICITIS 2010)[C]. Beijing, 2010.

[14] 刘欣然. 网络攻击分类技术综述[J]. 通信学报, 2004, 25(7)：30-36.
LIU X R. Survey of network attack classification[J]. Journal on Communications, 2004, 25(7)：30-36.

[15] 王江涛, 陈性元, 唐慧林等. 面向渗透测试的攻击代码生成方法[J]. 计算机工程与设计, 2010, 31(2):249-251.
WANG J T, CHEN X Y, TANG H L, *et al*. Attack code generation approach oriented to penetration test[J]. Computer Engineering and Design, 2010, 31(2)：249-251.

[16] SU P, CHEN X Y, TANG H L, *et al*. DoS attack impact assessment based on 3GPP QoS indexes[A]. 3rd International Conference on Innovative Computing, Information and Control (ICICIC'08)[C]. Dalian, 2008.

作者简介：

祝宁（1981-），男，河南安阳人，解放军信息工程大学博士生，主要研究方向为信息安全和网络攻防。

陈性元（1963-），男，安徽无为人，解放军信息工程大学教授、博士生导师，主要研究方向为信息安全、分布式系统和软件工程。

张永福（1942-），男，河北昌黎人，解放军信息工程大学教授、博士生导师，国家信息化专家咨询委员会委员，主要研究方向为信息安全。