渗透测试技术浅析

王晓聪 张 冉 黄赫东
(63892部队 洛阳 471003)

摘 要 渗透测试亦即以一个攻击者的身份对网络系统进行安全检查和审核,是对安全评估的一种有益补充。根据当前各类渗透测试技术,简单分析研究总结了渗透测试的对象、方法、基本步骤,并设计了一种渗透测试系统的模型,概括介绍了该模型的架构设计、主要节点和测试流程。

关键词 渗透测试技术,渗透测试模型,渗透测试方法
中图法分类号 TP393.08 **文献标识码** A

Penetration Test Techniques Shallow

WANG Xiao-cong ZHANG Ran HUANG Cheng-dong
(Unit 63892, PLA, Luoyang 471003, China)

Abstract Penetration testing is security check and audit for the network system, by an attacker identity and is a useful supplement of the safety assessment. According to the various types of penetration test, this paper summarized the penetration testing object, method, basic procedure, and designed a penetration testing system model, introduced the model of architecture design, main node and test process.

Keywords Penetration test techniques, Penetration test model, Penetration testing method

渗透测试(Penetration Test)具体来说,就是要求测试人员在客户允许下的范围内,采取可控的黑客入侵手法,尽可能真实地模拟攻击者使用各种方法和技术对目标系统实施的攻击,以检验系统在真实应用环境中的安全性[1,2]。

渗透测试亦即以一个攻击者的身份对网络系统进行安全检查和审核,是对安全评估的一种有益补充。它可以协助客户发现其管理的网络系统中存在的潜在安全漏洞,并能直观、动态地将攻击过程展示给客户,以帮助客户充分了解目前其管理的网络系统的安全状况,让客户意识到其管理的网络系统存在着一定的安全风险,进而提高客户对信息安全的认知水平和重视程度。

渗透测试软件系统是渗透测试的实现平台,为渗透测试人员提供渗透测试工具、使用说明和测试范例等,并具有渗透测试的相关功能。而渗透测试系统模型是建立渗透测试软件系统的基础。[3]

1 渗透测试目标和技术分类

1.1 渗透测试实施目标

如图1所示,渗透测试的目标一般可以划分为3种:

1)网络硬件设备:主要包括各类防火墙、入侵检测系统、网络设备等。

2)主机操作系统:主要包括 Windows、Unix、Linux、Solaris、AIX 等各类操作系统(包含操作系统提供的服务:拨号服务、DNS 服务、E-mail 服务和由 ASP、JSP、PHP 等组成的 Web 站点的服务等)。

3)主机应用软件:主要包括 Oracle、MySQL、DB2 等数据库应用软件和 Word、Adobe Reader、Powerpoint 等其他应用软件。

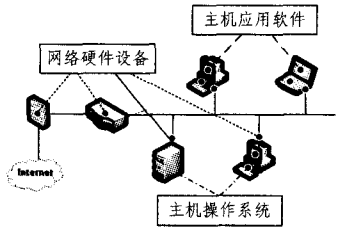

图1 渗透测试目标

1.2 渗透测试方法分类

(1)根据测试执行人员对目标系统环境相关信息掌握程度的不同,可以分为两种类型:黑盒测试和白盒测试。

· 黑盒测试

黑盒测试又被称为"Zero-Knowledge Testing"。它指的是测试人员事先完全不了解被测系统的任何信息,就像面对一个"黑盒子",对目标系统进行渗透测试。有关目标系统的所有信息都需要测试人员自行去搜集分析。黑盒测试主要是真实地模拟外来攻击者攻击被测系统的行为方式。

· 白盒测试

白盒测试正好和黑盒测试相反,它指的是测试人员事先已经了解被测系统一定的相关信息(包括网络地址段、使用的网络协议、网络拓扑结构甚至内部人员资料等),对目标系统进行渗透测试。白盒测试主要是模拟熟知目标系统环境的攻击者(包括系统内部人员)攻击被测系统的操作行为。

王晓聪(1985-),男,助理工程师,主要研究方向为网络攻防,E-mail:www.wxcong1985@sina.com;张 冉 男,硕士,工程师,主要研究方向为指控系统;黄赫东 男,硕士,工程师,主要研究方向为网络攻防。

(2)根据执行渗透测试的范围的不同,可以分为3种类型:内网测试、外网测试和不同网段/Vlan之间的渗透测试。

• 内网测试

内网测试指的是渗透测试人员从内网对目标系统进行渗透攻击。测试人员可以避开边界防火墙的"保护机制",通过对一个或多个主机进行渗透来发现整个被测系统的安全隐患。

• 外网测试

外网测试指的是渗透测试人员完全从外部网络(例如拨号、ADSL或外部光纤)对目标系统进行渗透攻击。测试人员所模拟的外部攻击者既可能对内部状态一无所知,也可能对目标系统环境有一定的了解(甚至是熟知)。

• 不同网段/Vlan之间的渗透测试

不同网段/Vlan之间的渗透测试指的是渗透测试人员从某内/外部网段,尝试对另一网段/Vlan进行渗透。

2 渗透测试基本过程

根据被测目标、测试环境和测试要求等因素的不同,渗透测试具体过程也各不相同,但一次比较完整的渗透测试基本上可以划分为以下4个步骤:

1)目标搜索

无论是哪种渗透测试,首先必须尽快搜索并发现目标。这是进行渗透测试的先决步骤。测试者需要广泛搜索各种与目标可能相关的有用信息(如域名、IP地址等),以获得目标的"踪迹"。同时,可以利用Ping扫描来决定潜在目标或判断目标机器是否在网络中存活。

2)信息挖掘

在搜索到目标后,渗透测试人员需要对目标信息进行进一步的挖掘并加以整理。测试人员需要进行各种信息攫取工作,如采用社交工程、物理闯入等方式从外围收集各类被测目标的基本信息(如目标系统用户的个人相关资料等),利用各种扫描工具(如TK2006、X-Scan和sss扫描器等)对目标机器进行端口扫描来获取端口开放信息,对目标机器的操作系统进行识别,对目标机器运行的服务及服务软件的版本信息进行识别,设法获取目标机器的防火墙规则等。测试人员甚至还需要设法搜集被测系统网络的网络拓扑结构信息、路由设备信息等。

3)漏洞关联

漏洞关联指的是测试人员根据经过挖掘、整理的被测目标的关键信息,将被测目标与众所周知的安全漏洞关联起来(有时也会与未知漏洞相关联)。这是渗透测试中最为重要的一步。实现漏洞关联的一种方法是将被测目标的一些特殊信息和已开放的安全漏洞的相关信息作对比,以此推断目标是否具有某种漏洞。比如,测试者已经检测出被测目标用的apache版本是1.3.27,根据漏洞Apache chunking integer overflow vulnerability的存在环境是apache 1.3.24和早期的版本,那么测试人员可以判断出被测目标不存在与漏洞Apache chunking integer overflow vulnerability相关联的可能性。

4)入侵攻击

在完成漏洞关联后,渗透测试人员可以进入到入侵攻击测试阶段。测试者可以根据通过漏洞关联发现的目标安全漏洞,有针对性地利用相应的漏洞工具进行渗透,获取、提高、维持权限,并在攻击结束后清除攻击痕迹。测试人员也可以根据具体情况,采用其他方式进行攻击。总之,无论测试者如何入侵攻击目标,其最终目的是为了检验目标系统的脆弱性。

3 渗透测试系统模型

目前,一些安全服务商不仅提供形式多样的渗透测试服务,还专门开发了独有的渗透工具集成化的渗透测试系统。结合目前几种现有的专业渗透测试系统的体系架构,本文设计了一种新的渗透测试系统的模型。

3.1 系统架构设计

本文所设计的系统主要分为6个模块:操作控制模块;任务管理模块;漏洞扫描模块;渗透验证模块;报告生成模块;数据传输模块。系统架构如图2所示。

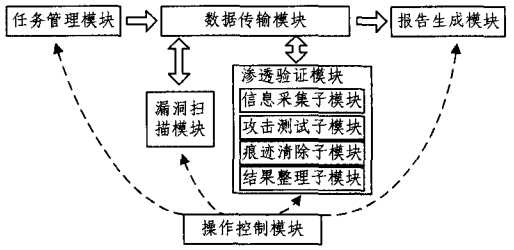

图2 系统架构

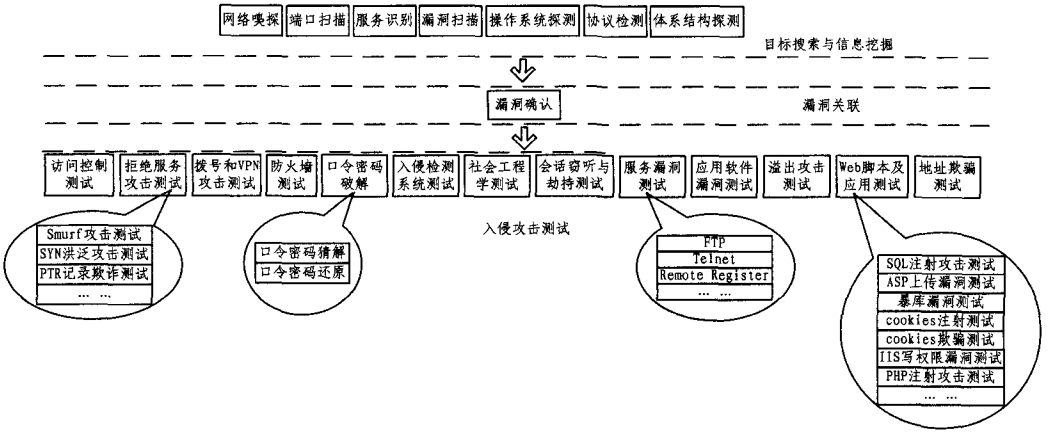

图3 渗透测试主要节点的相互关系

其中的操作控制模块负责全系统管理,对各模块功能进行集中控制。任务管理模块负责对渗透测试环境进行构建,

制定渗透测试任务并进行任务下达。漏洞扫描模块负责依托专业的网络安全扫描器，并加以人工辅助检测，对任务目标进行全面的漏洞扫描、识别。渗透验证模块由信息采集、攻击测试、结果整理和痕迹清除4个子模块组成，负责利用专用安全测试工具和各类测试手段，结合富有经验的安全工程师的人工经验，根据漏洞扫描结果和其他相关信息，进行验证性渗透测试。报告生成模块负责生成渗透测试报告。数据传输模块负责各模块之间的信息交互。

3.2 渗透测试主要节点

渗透测试主要有以下节点(见图3)：端口扫描、网络嗅探、体系结构探测、操作系统探测、服务识别、协议检测、漏洞扫描、漏洞确认、应用软件漏洞测试、拨号和VPN攻击测试、防火墙测试、访问控制测试、入侵检测系统测试、服务漏洞测试、社会工程学测试、口令密码破解、拒绝服务攻击测试、Web脚本及应用测试、会话窃听与劫持测试、溢出攻击测试、地址欺骗测试。

3.3 渗透测试流程

3.3.1 渗透测试的总流程

如图4所示，一次完整的渗透测试的总流程是：首先确认好目标，然后构设渗透测试环境，接着制定并下达渗透测试任务。在任务下达后，一方面利用专业的网络安全扫描器，辅以人工检测，对目标进行全面的漏洞扫描、识别，另一方面利用多种手段收集目标其他相关信息。根据漏扫结果和收集到的其他有用信息，进行验证性渗透攻击测试。在攻击结束后，进行痕迹清除，同时整理验证攻击结果，结合先前的漏洞扫描结果生成渗透测试报告。

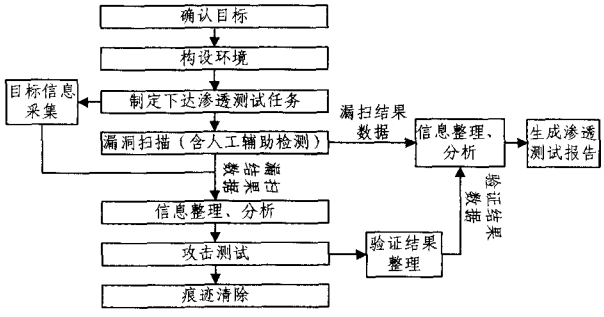

图4 渗透测试总流程

3.3.2 渗透验证流程

渗透验证模块进行渗透验证的流程如图5所示：首先对目标进行嗅探、扫描、ARP欺骗攻击，如果发现目标主机存在弱口令，则直接尝试远程连接主机，如果连接成功，则进行后门添加、日志清除，如果连接失败，则继续进行嗅探、扫描，判断目标主机是否存在漏洞。如果存在漏洞，则进行漏洞攻击，否则对目标进行DDoS攻击。在漏洞攻击成功后，如果得到的用户权限是普通用户权限，则尝试将其提升为管理员权限，若提权失败则对目标进行DDoS攻击。如果在漏洞攻击成功后得到的是管理员权限，则直接尝试利用该权限远程连接主机，若连接成功，则进行后门添加、日志清除，否则进行提权操作。如果提权成功，则直接尝试远程连接主机，若连接成功，则进行后门添加、日志清除，否则对目标进行DDoS攻击。

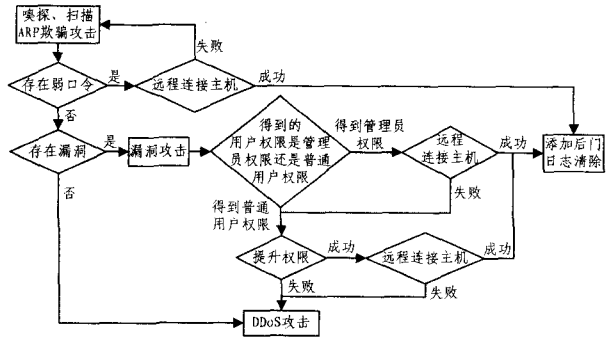

图5 渗透验证流程

结束语 随着社会信息化、网络化的不断发展和各类网络系统在商业和军事领域开发、应用的越发广泛，网络系统的安全问题日益被人们所重视。为了能较为有效地抵御各类黑客攻击，检验网络系统的安全性，提升网络系统的防御力，降低因网络系统被攻破而造成损失的风险，渗透测试作为一种能对网络系统中可能存在的安全漏洞进行全面检测的有效手段，已经越来越被人们所关注，其技术手段、方法机制也在不断发展并多种多样。本文对渗透测试的对象、方法、基本流程等进行了一定的探讨，并设计了一种渗透测试系统模型，给出了渗透测试中的系统架构、主要节点和测试流程，为渗透测试软件系统的开发和渗透测试的准确程度、专业水平的提高提供了一种可以借鉴的思路。

参 考 文 献

[1] 瑜文. 渗透测试：以攻击者的方式思考[J]. 软件世界，2006，(21)：84-85

[2] 吴鲁加. 渗透测试中的攻与守[J]. 软件世界，2007(05)：81-83

[3] 唐秀存，杜德慧. 渗透测试技术与模型研究[J]. 计算机与信息技术，2007(05)：33-35

[4] 楼芳，李亮，贺志强. 基于本体的渗透测试用例复用模型[J]. 计算机工程与科学，2011(02)：23-26

[5] 闻观行，张园超，张玉清. 基于数据格式支持机制的自动化渗透测试框架[J]. 中国科学院研究生院学报，2011(05)：676-683

[6] 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(08)：2146-2150

[7] 正理. 渗透测试揭秘[J]. 信息网络安全，2001(05)：18-19

[8] 白海涛，马惠铖. 浅谈企业网络安全之渗透测试[J]. 科技资讯，2010(30)：145

[9] 李亮，楼芳. 网络渗透测试流程、用例管理和风险控制研究[J]. 煤炭技术，2010(11)：175-176

[10] 李明. 浅谈渗透测试[J]. 信息网络安全，2008(08)：65

[11] 林炜. 利用渗透测试进行安全评估及效果检查[J]. 华南金融电脑，2009(06)：9-10

[12] 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(12)：14-18

[13] 张继业，谢小权. 基于攻击图的渗透测试模型[J]. 信息网络安全，2005(09)：72-74