附 录 B
（资料性附录）
渗透测试的有关概念说明

B.1 综述

渗透测试是一种安全性测试，在该类测试中，测试人员将模拟攻击者，利用攻击者常用的工具和技术对应用程序、信息系统或者网络的安全功能发动真实的攻击。相对于单一的漏洞，大多数渗透测试试图寻找一组安全漏洞，从而获得更多能够进入系统的机会。渗透测试也可用于确定：

a） 系统对现实世界的攻击模式的容忍度如何；

b） 攻击者需要成功破坏系统所面对的大体复杂程度；

c） 可减少系统威胁的其他对策；

d） 防御者能够检测攻击并且做出正确反应的能力。

渗透测试是一种非常重要的安全测试，测试人员需要丰富的专业知识和技能。尽管有经验的测试人员可降低这种风险，但不能完全避免风险，因此渗透测试宜经过深思熟虑和认真规划。

渗透测试通常包括非技术攻击方法。例如，一个渗透测试人员可以通过破坏物理安全控制机制的手段连接到网络，以窃取设备、捕获敏感信息（可能是通过安装键盘记录设备）或者破坏网络通信。在执行物理安全渗透测试时宜谨慎行事，明确如何验证测试人员入侵活动的有效性，如通过接入点或者文档。另一种非技术攻击手段是通过社会工程学，如伪装成客服坐席人员打电话询问用户的密码，或者伪装成用户打电话给客服坐席人员要求重置密码。更多关于物理安全测试、社会工程学技术以及其他非技术手段的渗透攻击测试，不在本标准的讨论范围。

B.2 渗透测试阶段

B.2.1 概述

渗透测试通常包括规划、发现、攻击、报告四个阶段，如图 B.1 所示。

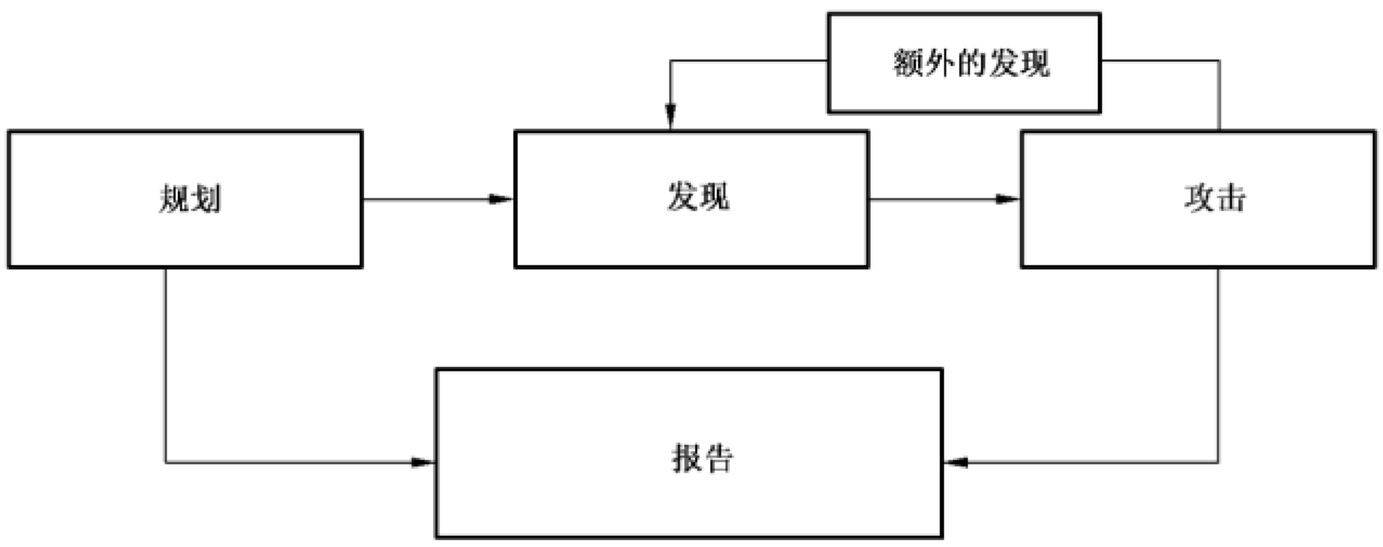

图 B.1 渗透测试的四个阶段

B.2.2 规划阶段

在规划阶段，确定规则，管理层审批定稿，记录在案，并设定测试目标。规划阶段为一个成功的渗透测试奠定基础，在该阶段不发生实际的测试。

B.2.3 发现阶段

渗透测试的发现阶段包括两个部分：

第一部分是实际测试的开始，包括信息收集和扫描。网络端口和服务标识用于进行潜在目标的确定。除端口及服务标识外，还有以下技术也被用于收集网络信息目标：

a) 通过 DNS、InterNIC(WHOIS)查询和网络监听等多种方法获取主机名和 IP 地址信息；

b) 通过搜索系统 Web 服务器或目录服务器来获得系统内部用户姓名、联系方式等；

c) 通过诸如 NetBIOS 枚举方法和网络信息系统获取系统名称、共享目录等系统信息；

d) 通过标识提取得到应用程序和服务的相关信息，如版本号。

第二部分是脆弱性分析，其中包括将被扫描主机开放的服务、应用程序、操作系统和漏洞数据库进行比对。测试人员可以使用他们自己的数据库，或者 CNVD 等公共数据库来手动找出漏洞。

B.2.4 攻击阶段

执行攻击是渗透测试的核心。攻击阶段是一个通过对原先确定的漏洞进一步探查，进而核实潜在漏洞的过程。如果攻击成功，说明漏洞得到验证，确定相应的保障措施就能够减轻相关的安全风险。在大多数情况下，执行探查并不能让攻击者获得潜在的最大入口，反而会使测试人员了解更多目标网络和其潜在漏洞的内容，或诱发对目标网络的安全状态的改变。一些漏洞可能会使测试人员能够提升对于系统或网络的权限，从而获得更多的资源；若发生上述情况，则需要额外的分析和测试来确定网络安全情况和实际的风险级别。比如说，识别可从系统上被搜集、改变或删除的信息的类型。倘若利用一个特定漏洞的攻击被证明行不通，测试人员可尝试利用另一个已发现的漏洞。如果测试人员能够利用漏洞，可在目标系统或网络中安装部署更多的工具，以方便测试。这些工具用于访问网络上的其他系统或资源，并获得有关网络或组织的信息。在进行渗透测试的过程中，需要对多个系统实施测试和分析，以确定攻击者可能获得的访问级别。虽然漏洞扫描器仅对可能存在的漏洞进行检查，但渗透测试的攻击阶段会利用这些漏洞来确认其存在性。

B.2.5 报告阶段

渗透测试的报告阶段与其他三个阶段同时进行(见图 B.1)。在规划阶段，将编写测试计划；在发现和攻击阶段，通常是保存测试记录并定期向系统管理员和/或管理部门报告。在测试结束后，报告通常是用来描述被发现的漏洞、目前的风险等级，并就如何弥补发现的薄弱环节提供建议和指导。

B.3 渗透测试方案

渗透测试方案宜侧重于在应用程序、系统或网络中的设计和实现中，定位和挖掘出可利用的漏洞缺陷。渗透测试重现最可能的和最具破坏性的攻击模式，包括最坏的情况，诸如管理员的恶意行为。由于渗透测试场景可以设计以模拟内部攻击、外部攻击，或两者兼而有之，因此外部和内部安全测试方法均要考虑到。如果内部和外部测试都要执行，则通常优先执行外部测试。

外部攻击是模拟从组织外部发起的攻击行为，可能来自于对组织内部信息一无所知的攻击者。模拟一个外部攻击，测试人员不知道任何关于目标环境以外的信息，特别是 IP 地址或地址范围情况的真实信息。测试人员可通过公共网页、新闻页面以及类似的网站收集目标信息，进行综合分析；使用端口扫描器和漏洞扫描器，以识别目标主机。由于测试人员的流量往往需要穿越防火墙，因此通过扫描获取的信息量远远少于内部角度测试所获得的信息。从外部控制该组织网络上的主机后，测试人员可尝试将其作为跳板机，并使用此访问权限去危及那些通常不能从外部网络访问的其他主机。模拟外部攻击的渗透测试是一个迭代的过程，利用最小的访问权限取得更大的访问。

内部攻击是模拟组织内部违规操作者的行为。除了测试人员位于内部网络(即防火墙后面),并已授予对网络或特定系统一定程度的访问权限(通常是作为一个用户,但有时层次更高)之外,内部渗透测试与外部测试类似。测试人员可以通过权限提升获得更大程度的网络及系统的访问权限。

渗透测试对确定一个信息系统的脆弱性以及如果网络受到破坏所可能发生的损害程度非常重要。由于渗透测试使用真正的资源并对生产系统和数据进行攻击,可能对网络和系统引入额外的风险,因此测试人员宜制订测试方案,明确测试策略,限制可能使用的特定工具或技术,在可能造成危害之前停止测试。测试人员宜重视渗透测试过程及结果的交流,帮助系统管理员和/或管理部门及时了解测试进度以及攻击者可能利用的攻击方法和攻击途径。

B.4 渗透测试风险

在渗透测试过程中,测试人员通常会利用攻击者常用的工具和技术来对被测系统和数据发动真实的攻击,必然会对被测系统带来安全风险,在极端情况或应用系统存在某些特定安全漏洞时可能会产生如下安全风险:

a) 在使用 Web 漏洞扫描工具进行漏洞扫描时,可能会对 Web 服务器及 Web 应用程序带来一定的负载,占用一定的资源,在极端情况下可能会造成 Web 服务器宕机或服务停止;

b) 如 Web 应用程序某功能模块提供对数据库、文件写操作的功能(包括执行 Insert、Delete、Update 等命令),且未对该功能模块实施数据有效性校验、验证码机制、访问控制等措施,则在进行 Web 漏洞扫描时有可能会对数据库、文件产生误操作,如在数据库中插入垃圾数据、删除记录/文件、修改数据/文件等;

c) 在进行特定漏洞验证时,可能会根据该漏洞的特性对主机或 Web 应用程序造成宕机、服务停止等风险;

d) 在对 Web 应用程序/操作系统/数据库等进行口令暴力破解时,可能触发其设置的安全机制,导致 Web 应用程序/操作系统/数据库的账号被锁定,暂时无法使用;

e) 在进行主机远程漏洞扫描及进行主机/数据库溢出类攻击测试,极端情况下可能导致被测试服务器操作系统/数据库出现死机或重启现象。

B.5 渗透测试风险规避

针对渗透测试过程中可能出现的测试风险,测评人员宜向用户详细介绍渗透测试方案中的内容,并对测试过程中可能出现的风险进行提示,并与用户就如下内容进行协商,做好渗透测试的风险管控:

a) 测试时间:为减轻渗透测试造成的压力和预备风险排除时间,宜尽可能选择访问量不大、业务不繁忙的时间窗口,测试前可在应用系统上发布相应的公告;

b) 测试策略:为了防范测试导致业务的中断,测试人员宜在进行带有渗透、破坏、不可控性质的高风险测试前(如主机/数据库溢出类验证测试、DDoS 等),与应用系统管理人员进行充分沟通,在应用系统管理人员确认后方可进行测试;宜优先考虑对与生产系统相同配置的非生产系统进行测试,在非业务运营时间进行测试或在业务运营时间使用非限制技术,以尽量减少对生产系统业务的影响;对于非常重要的生产系统,不建议进行拒绝服务等风险不可控的测试,以避免意外崩溃而造成不可挽回的损失;

c) 备份策略:为防范渗透过程中的异常问题,建议在测试前管理员对系统进行备份(包括网页文件、数据库等),以便在出现误操作时能及时恢复;如果条件允许,也可以采取对目标副本进行渗透的方式加以实施;

d) 应急策略:测试过程中,如果被测系统出现无响应、中断或者崩溃等异常情况,测试人员宜立即

中止渗透测试，并配合用户进行修复处理；在确认问题并恢复系统后，经用户同意方可继续进行其余的测试；

e) 沟通机制：在测试前，宜确定测试人员和用户配合人员的联系方式，用户方宜在测试期间安排专人职守，与测试人员保持沟通，如发生异常情况，可及时响应；测试人员宜在测试结束后要求用户检查系统是否正常，以确保系统的正常运行。

参 考 文 献

[1] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[2] GB/T 20270—2006 信息安全技术 网络基础安全技术要求
[3] GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求
[4] GB/T 22239 信息安全技术 信息系统安全等级保护基本要求
[5] GB/T 28448 信息安全技术 信息系统安全等级保护测评要求
[6] GB/T 28449 信息安全技术 信息系统安全等级保护测评过程指南

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
网络安全等级保护测试评估技术指南
GB/T 36627—2018
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2018 年 9 月第一版
*
书号:155066·1-61231

GB/T 36627-2018