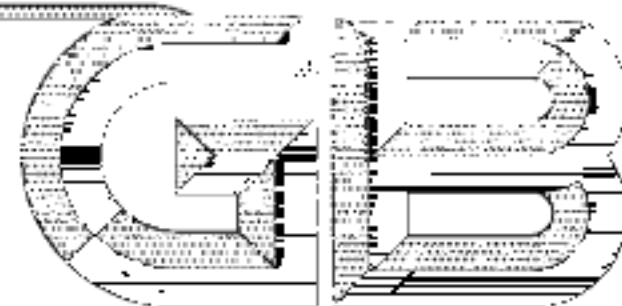




中华人民共和国国家标准

GB/T 36627—2018

信息安全技术 网络安全等级保护测试评估技术指南

Information security technology—
Testing and evaluation technical guide for classified cybersecurity protection

2018-09-17 发布

2019-04-01 实施

国家市场监督管理总局
中国国家标准化管理委员会 发布

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义、缩略语	1
3.1 术语和定义	1
3.2 缩略语	2
4 概述	2
4.1 技术分类	2
4.2 技术选择	2
5 等级测评要求	2
5.1 测评准备	2.2
5.1.1 文档检查	2
5.1.2 日志检查	3
5.1.3 规则集检查	3
5.1.4 配置检查	4
5.1.5 文档完整性检查	4
5.1.6 硬件设备	5
5.1.7 识别和分析设备	5
5.2 网络扫描	5
5.2.1 网络扫描	5
5.2.2 网络扫描和性能测试	5
5.2.3 漏洞扫描	5
5.2.4 无线扫描	6
5.3 漏洞验证技术	6
5.3.1 口令破解	6
5.3.2 渗透测试	6
5.3.3 远程访问测试	7
附录A (资料性附录) 测评后活动	8
附录B (资料性附录) 渗透测试的有关概念	9
附录C (资料性附录) 参考文献	13

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

引言

网络安全等级保护测评过程包括测评准备活动、方案编制活动、现场测评活动、报告编制活动四个

信息安全技术
网络安全等级保护测试评估技术指南

1 范围

2 规范性引用文件

于本文 下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用

[illegible]

Figure 6

转人三

G5069-2018-信通安

3 术语和定义、缩略语

3.1 术语和定义

69—2010 界定的以及下列术语和定义适用于本文件。

GB 17859—1999 及 GB/T 250

3.1.1

字典式攻击 **dictionary attack**

目定义词典中的单词或短语的攻击方式。

在破解口令时,逐一尝试用户自

✓ checking

算、存储每一个保留文件的校验,将已存储的校验重新计算以比较当

文件完整性检查 file integrity

通过建立文件校验数据库,计算

支修改。

直和存储值,从而识别文件是否被

3.1.3

网络嗅探 network sniffer

一种监视网络通信、解码协议,并对关注的信息头部和有效载荷进行检查的被动技术,同时也是—

3.1.4

规则集 rule set

$\text{Pr}(\text{A}|\text{B}) = \frac{\text{Pr}(\text{A} \cap \text{B})}{\text{Pr}(\text{B})}$

© 2012 Pearson Education, Inc. or its affiliate(s). All rights reserved.  Pearson Education, Inc.

511

valuation

测评对象 target of testing and ev

的因素, 主要涉及相关信息系统、资金制度文档、设备设施及人

等级测评过程的不同测评方法作

3.2 缩略语

下列缩略语适用于本文件。

CNVD:国家信息安全漏洞共享平台(China National Vulnerability Database)

DNS:域名系统(Domain Name System)

DDoS:分布式拒绝服务(Distributed Denial of Service)

ICMP:Internet 控制报文协议(Internet Control Message Protocol)

IDS:入侵检测系统(Intrusion Detection Systems)

IPS:入侵防御系统(Intrusion Prevention System)

MAC:介质访问控制(Media Access Control)

SSH:安全外壳协议(Secure Shell)

SSID:服务集标识(Service Set Identifier)

SQL:结构化查询语言(Structured Query Language)

VPN:虚拟专用网络(Virtual Private Network)

4 概述

4.1 技术分类

可用于等级测评的测评技术分成以下三类。

- a) 漏洞扫描技术:对目标资产进行扫描,发现资产中存在的漏洞,并生成漏洞扫描报告。
- b) 漏洞识别技术:对目标资产进行扫描,发现资产中存在的漏洞,并生成漏洞识别报告。
- c) 漏洞验证技术:验证漏洞存在性的测评技术。基于检查、手动执行或使用自动化的工具,主要包括口令破解、渗透测试、安全漏洞进行验证确认,获得证据。

4.2 技术选择

当选择和确定用于等级测评活动的技术方法时,考虑的因素主要包括但不限于适用性、测评技术对测评对象可能引入的安全风险,以选择合适的技术方法。

当所选定的技术方法在实施过程中可能影响被测对象正常业务运行时,应采取适当措施,如选择非业务高峰期进行测试,或在业务系统冗余架构下进行测试,以减少对被测对象业务的影响。

当所选定的技术方法可能影响被测对象数据安全时,应采取适当措施,如选择非业务高峰期进行测试,或在业务系统冗余架构下进行测试,以减少对被测对象数据的影响。

5 等级测评要求

5.1 检查技术

5.1.1 文档检查

对对象运营单位提供的文档,评价其策略和规程的技术准确性。

文档检查的主要功能是满足等级测评要求。

和完整性。进行文档检查时,可考虑以下评估要素:

- a) 检查对象包括安全策略、体系结构和要求、标准作业程序、系统安全计划和授权许可、系统互连

品技术规范和系统实施计划等,确保技术方案的完整性和准确性;

系统互连的技术规
划和安全措施的实

- b) 检查安全策略、体系结构和要求、标准作业程序、系统安全计划和授权许可范、事件响应计划等文档的完整性,通过检查执行记录和相应表单,确认措施与制度文档的一致性;

江原的工

- c) 发现可能导致遗漏或不恰当实施安全控制措施的缺陷和弱点,验证测试对象的技术是否符网络安全等级保护国家标准和相关法规符合,存在有缺陷或策略;

长度和复

- d) 文档检查的结果可用于调整其他的测试技术,例如,当口令管理策略规定了最小口令复杂度要求的时候,该信息应可用于配置口令破解工具,以提高口令破解效率。

5.1.2 日志检查

应用、配置

日志检查的主要功能是验证安全控制措施是否记录了测评对象的信息系统、设备设施的使

能够发现

和修改的历史记录等关键信息,确保保护对象的运营使用单位是否建立了日志管理策略,并且

安全策略中要求安全策略应明确记录日志,记录内容应包括系统设备、网络设备、数据库、操作系统、应用系统、安全设备、安全策略、安全策略变更、账

- 户变更(例如账户创建和删除、账户权限分配)以及权限使用等信息;

- 操作系统的日志应包括系统和服务的启动、关闭、主要软件的安装、文档访问、安全策略变更、账

户变更(例如账户创建和删除、账户权限分配)以及权限使用等信息;

- IDS/IPS 日志,包括恶意行为和异常事件记录;

查

5.1.3 规则集检

的主要功能是发现基于规则集的安全控制措施的漏洞,检查对象包括网络设备、安全设

规则集检查

系统及应用系统的访问控制列表、策略集,三级及以上等级保护对象还应包括强制访问

设备、数据库、操作

规则集检查时,可考虑以下评估要素和评估原则:

控制机制,进行

访问控制列表;

- a) 路由访

三条规则都应是有效的(例如,因临时需求而设定的规则,在不需要的时候应及时移除);

- 1) 每

检查对象的安全策略应明确记录日志,记录内容应包括系统设备、网络设备、数据库、操作系统、应用系统、安全设备、安全策略、安全策略变更、账

设备、数据库、操作

设备、数据库、操作

设备、数据库、操作

设备、数据库、操作

设备、数据库、操作

设备、数据库、操作

设备、数据库、操作

设备、数据库、操作

设备、数据库、操作

设备、数据库、操作

设备、数据库、操作

设备、数据库、操作

设备、数据库、操作

设备、数据库、操作

设备、数据库、操作

相同的访问规则；

- 3) 以数据库形式存储和操作的用户数据,在操作系统的支持下,应实现主体级粒度的强制访问控制;
- 4) 检查强制访问控制的范围,应限定在已定义的主体与客体中。

5.1.4 配置检查

配置检查的主要功能是通过检查测评对象的安全策略设置和安全配置文件,评价测评对象安全策略配置的强度,以及验证测评对象安全策略配置与测评对象安全加固策略的符合程度。进行配置检查时,可考虑以下评估要素:

- a) 依据安全策略进行加固或配置;
- b) 仅开放必要的服务和应用;
- c) 禁用不必要的服务和应用;
- d) 实施最小权限原则;
- e) 检查配置文件的完整性;
- f) 检查配置文件的版本;
- g) 检查配置文件的权限;
- h) 检查配置文件的加密;
- i) 检查配置文件的备份;
- j) 检查配置文件的恢复;
- k) 检查配置文件的更新;
- l) 检查配置文件的删除;
- m) 检查配置文件的迁移;
- n) 检查配置文件的复制;
- o) 检查配置文件的粘贴;
- p) 检查配置文件的打印;
- q) 检查配置文件的删除;
- r) 检查配置文件的迁移;
- s) 检查配置文件的复制;
- t) 检查配置文件的粘贴;
- u) 检查配置文件的打印;
- v) 检查配置文件的删除;
- w) 检查配置文件的迁移;
- x) 检查配置文件的复制;
- y) 检查配置文件的粘贴;
- z) 检查配置文件的打印;

5.1.5 文件完整性检查

文件完整性检查的主要功能是通过检查测评对象的重要文件,评价测评对象重要文件的完整性。进行文件完整性检查时,可考虑以下评估要素:

- a) 采用哈希或数字签名等手段,保证重要文件的完整性;
- b) 采用哈希或数字签名等手段,保证重要文件的完整性;
- c) 采用哈希或数字签名等手段,保证重要文件的完整性;

5.1.6 密码检查

密码检查的主要功能是对测评对象中采用的密码技术或产品进行安全性检查。进行密码检查时,可考虑以下评估要素:

- a) 密码长度符合国家标准或行业标准的有关规定;
- b) 密码复杂度符合国家标准或行业标准的有关规定;
- c) 密码有效期符合国家标准或行业标准的有关规定;
- d) 密码复杂度符合国家标准或行业标准的有关规定;

5.2 识别和分析技术

5.2.1 网络嗅探

网络嗅探的主要功能是通过捕捉和重放网络流量,收集、识别网络中活动的设备、操作系统和协议、未授权和不恰当的行为等信息。进行网络嗅探时,可考虑以下评估要素和评估原则:

- a) 在网络流量中识别出活动的设备、操作系统和协议;
- b) 识别出网络流量的来源和去向;
- c) 识别出网络流量的类型;
- d) 识别出网络流量的大小;
- e) 识别出网络流量的速度;
- f) 识别出网络流量的方向;
- g) 识别出网络流量的时间;
- h) 识别出网络流量的地点;
- i) 识别出网络流量的内容;
- j) 识别出网络流量的元数据;
- k) 识别出网络流量的上下文;
- l) 识别出网络流量的上下文;
- m) 识别出网络流量的上下文;
- n) 识别出网络流量的上下文;
- o) 识别出网络流量的上下文;
- p) 识别出网络流量的上下文;
- q) 识别出网络流量的上下文;
- r) 识别出网络流量的上下文;
- s) 识别出网络流量的上下文;
- t) 识别出网络流量的上下文;
- u) 识别出网络流量的上下文;
- v) 识别出网络流量的上下文;
- w) 识别出网络流量的上下文;
- x) 识别出网络流量的上下文;
- y) 识别出网络流量的上下文;
- z) 识别出网络流量的上下文;

口及端口的状态。

- d) 在网络边界处部署网络嗅探器,用以评估进出网络的流量;

5.2.2 网络端口和服务识别

网络端口和服务识别的主要功能是识别活动设备上开放的端口、相关服务与应用程序。进行网络端口和服务识别时,可考虑以下评估要素和评估原则:

- 对主机及存在潜在漏洞的端口进行识别,并用于确定渗透性测试的目标;
- 在从网络边界外执行扫描时,应使用含分离、复制、重叠、乱序和定时技术的工具,并利用工具改变数据包,让数据包融入正常流量中,使数据包避开 IDS/IPS 检测的同时穿越防火墙;
- 应尽量减少扫描工具对网络运行的干扰,如选择端口扫描的时间。

5.2.3 漏洞扫描

漏洞扫描的主要功能是针对主机和开放端口识别已知漏洞、提供建议降低漏洞风险;同时,有助于识别过时的软件版本、缺失的补丁和错误配置,并验证其与机构安全策略的一致性。进行漏洞扫描

- 以漏洞扫描相关信息,包含漏洞名称、类型、漏洞描述、风险等级、修复建议等数据;
- 通过工具识别并结合人工分析的方式,对发现的漏洞进行关联分析,从而准确判断漏洞的风险等级;
- 漏洞扫描前,扫描设备应更新升级至最新的漏洞库,以确保能识别最新的漏洞;
- 依据漏洞扫描工具的漏洞分析原理(如特征库匹配、攻击探测等),谨慎选择扫描策略,防止引起测评对象故障;
- 使用漏洞扫描设备时应控制扫描线程数、流量

5.2.4 无线扫描

无线扫描的主要功能是识别被测环境中没有物理连接(如网络电缆或外围电缆)情况下使一个或多个设备实现通信的方式,帮助机构

- 使用安装配置无线分析软件的移动设备,如笔记本电脑;
- 基于无线安全配置要求,对无线扫描工具进行扫描策略配置,以实现差距分析;
- 适当配置扫描工具的扫描间隔时间,既能捕获数据包;
- 可通过导入平面图或地图,以帮助定位被发现设备的物理位置;
- 对捕获的数据包进行分析,从而识别扫描范围内发现的模式;

5.3 漏洞验证技术

5.3.1 口令破解

口令破解的主要功能是在评估过程中通过采用暴力猜测(密码穷举)、字典攻击等技术手段验证数据库、操作系统、应用系统、设备的管理员口令复杂度。进行口令破解时,可考虑以下评估方法和评估原则:

- 使用字典式攻击方法或采用预先计算好的彩虹表(散列值查找表)进行口令破解尝试;
- 使用混合攻击或暴力破解的方式进行口令破解;混合攻击以字典攻击方法为基础,在字典中增加了数字和符号等字符。

○二、如前例，如果采用沛至泰菲的加密函数时，加密后的彩虹表将举行三合被解密。

522 徐 强

攻击方法:攻击等级保护对象的应用程序、系统或者网
站源码的一种操作方式,进行渗透测试时,可考虑以

渗透测试的主要功能是通过模拟恶意黑客的
等的安全功能,从而验证对系统安全要求排除

◆ 延生西素和延生固本

- 对经济刺激计划中存在的漏洞

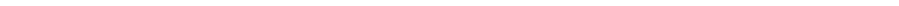
二、三、四、五、六、七、八、九、十、十一、十二、十三、十四、十五、十六、十七、十八、十九、二十、二十一、二十二、二十三、二十四、二十五、二十六、二十七、二十八、二十九、三十、三十一、三十二、三十三、三十四、三十五、三十六、三十七、三十八、三十九、四十、四十一、四十二、四十三、四十四、四十五、四十六、四十七、四十八、四十九、五十、五十一、五十二、五十三、五十四、五十五、五十六、五十七、五十八、五十九、六十、六十一、六十二、六十三、六十四、六十五、六十六、六十七、六十八、六十九、七十、七十一、七十二、七十三、七十四、七十五、七十六、七十七、七十八、七十九、八十、八十一、八十二、八十三、八十四、八十五、八十六、八十七、八十八、八十九、九十、九十一、九十二、九十三、九十四、九十五、九十六、九十七、九十八、九十九、一百。



权限旁路漏洞利用工具可被用于攻击功能强大的访问控制模型，如“访问控制列表”或“基于角色的访问控制”等。攻击者可非授权访问这些数据及功能模块。权限旁路漏洞漏洞通常可分三方面访问及操作权限，一是攻击者可非授权访问攻击目标应用及功能的总权限，二是攻击者可非授权访问攻击目标应用及功能的子权限，三是攻击者可非授权访问攻击目标应用及功能的子权限。

“配置不当”是指由于配置文档编写存在安全隐患,致使系统默认配置或配置不合理,所导致的网络安全风险。例如,配置文档中配置了弱口令,或者可能受系统漏洞、漏洞利用、配置不当等因素影响,造成系统被攻击。

Figure 1



5.3.3 远程访问测试

远程访问测试的主要功能是评估远程访问方法中的漏洞,发现未授权的接入方式。进行远程访问测试时,可考虑以下评估要素和评估原则:

- a) 发现除 VPN、SSH、远程桌面应用之外是否存在其他的非授权的接入方式。
- b) 发现未授权的远程访问服务。通过端口扫描定位经常用于进行远程访问的公开的端口,通过查看运行的进程和安装的应用来手工检测远程访问服务。
- c) 检测规则集来查找非法的远程访问路径。评估者应检测远程访问规则集,如 VPN 网关的规则集,查看其是否存在漏洞或错误的配置,从而导致非授权的访问。
- d) 测试远程访问认证机制。可尝试默认的账户和密码或暴力攻击(使用社会工程学的方法重设密码来进行访问)或尝试通过密码找回功能机制来重设密码从而获得访问权限。

远程访问通信。如果通信未被保护,则可利用这些数据作为远程访问凭证发送或接收的数据。

e) 一些远程访问通信。可以通过网络嗅探器监视这些通信,或者将这些数据作为远程访问的凭证信息。

附录 A

(资料性附录)

测评后活动

A.1 测评结果分析

测评结果分析的主要目标是确定和排除误报,对漏洞进行分类,并确定产生漏洞的原因,此外,找出在整个测评中需要立即处理的严重漏洞。以下列举了常见的造成漏洞的根本原因,包括:

- a) 配置管理不当,如未定期更新防病毒软件,未对操作系统、数据库、中间件、应用系统等进行定期更新,导致系统存在已知漏洞;
- b) 威胁管理不足,如未及时更新防火墙策略,未对网络流量进行有效过滤及不符合安全策略的防火墙策略等;
- c) 缺乏安全基线,同类的系统使用了不一致的安全配置策略;
- d) 在系统开发中缺乏对安全性的整合,如系统开发不满足安全要求,甚至未考虑应用程序代码中是否存在漏洞;
- e) 安全体系结构存在缺陷,如安全技术未能有效集成至系统中(例如,安全防病毒软件未与操作系统、数据库、中间件、应用系统等集成);
- f) 安全事件响应措施不足,如对渗透测试评估报告未及时响应;
- g) 对最终用户(例如,对运维人员)的安全培训不足,使用了非授权无线设备,或有网络,系统管理员(例如,缺乏安全意识)的人员培训不足;
- h) 缺乏安全策略或未执行安全策略,如开放的端口、主动的服务,不安全的协议、非授权主机以及弱口令等。

A.2 提出改进建议

针对每个测评结果中出现的安全问题,都提出相应的改进建议;改进建议中宜包括问题根源分析结果。改进建议通常包括技术性建议(例如,应用特定的补丁程序)和非技术性建议(例如,更新补丁管理制度)。改进措施的包括:制度修改、流程修改、策略修改、安全体系架构变更、应用新的安全技术以及部署操作系统和应用的补丁程序等。

A.3 报告

在测评结果分析完成之后,宜生成包括系统安全问题、漏洞及其改进建议的报告。测评结果可用于以下几个方面:

- a) 作为实施改正措施的参考;
- b) 制定改进措施以修补确认的漏洞;
- c) 作为测评对象运营单位为使等级保护对象满足安全要求而采取改进措施的基准;
- d) 用以反映等级保护对象安全要求的实现状况;
- e) 为改进等级保护对象的安全而进行的成本效益分析;
- f) 用来加强其他生命周期活动,如风险评估等;
- g) 用来满足网络安全等级保护测评的报告要求。

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) 系统对现实世界攻击模式的容忍度如何;
- b) 攻击者需要攻破系统所面对的总体复杂程度;
- 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能修复这些漏洞,但不能完全避免漏洞,因而渗透测试应经清楚理解,并应定期测试。

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策略限制。

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策略限制。

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策略限制。

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策略限制。

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策略限制。

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策略限制。

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策略限制。

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策略限制。

B.2 渗透测试

B.2.1 概述

渗透测试

测试阶段

试

试通常包括规划、发现、攻击、报告四个阶段,如图 B.1 所示。

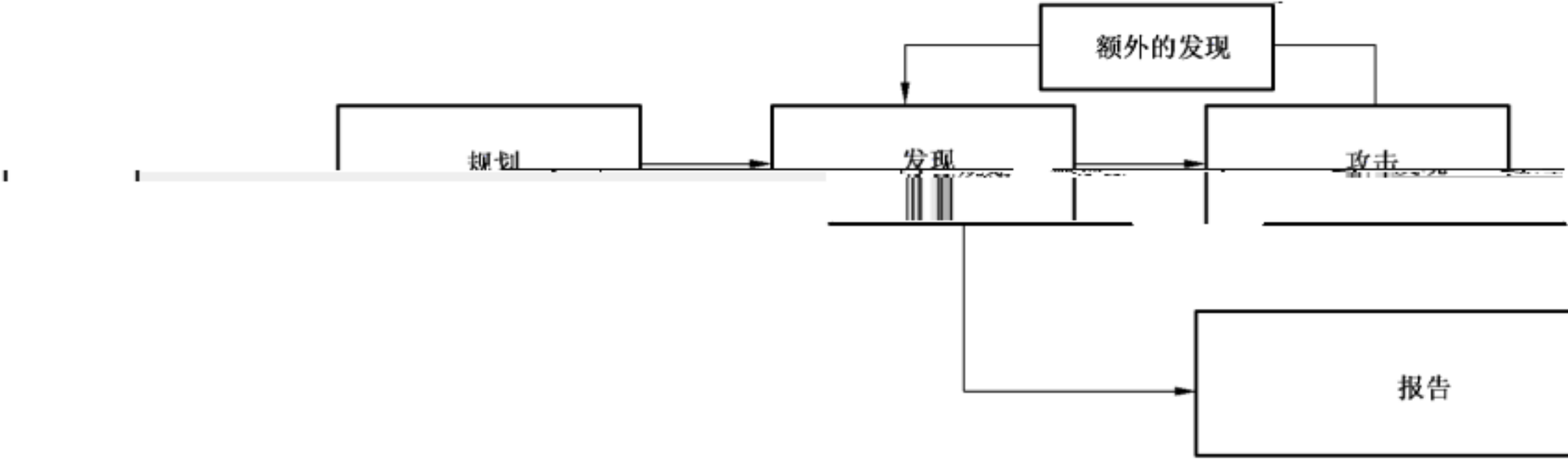


图 B.1 渗透测试的四个阶段

B.2.2 规划阶段

阶段为一个成功的渗透

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：

网络端口和服务器标识符进行潜在目标的梳理。

收集信息是渗透测试的第一步。

识别网络空间中的多种资源并获取主机名和 IP 地址等信息。

对服务器或网络系统内部配置进行交互性联系与设置。

a) 通过 DNS 和 WHOIS 数据库获取目标系统名称和 IP 地址信息。

b) 通过搜索引擎和公开信息获取目标系统名称和 IP 地址信息。

c) 通过搜索引擎和公开信息获取目标系统名称和 IP 地址信息。

d) 通过搜索引擎和公开信息获取目标系统名称和 IP 地址信息。

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,证明漏洞得到验证,确定相应的保护措施能够降低相关安全风险。在

攻击阶段,测试人员应记录攻击过程,包括攻击工具、攻击方法、攻击结果等信息。

攻击阶段的目标是验证漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

攻击阶段的结果是确定漏洞的存在,并评估漏洞的严重性。

渗透测试方案

B.3

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

渗透测试方案是可复现的,因此,测试方案应包含详细的测试步骤和测试工具。此外,测试方案还应

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。

外部攻击是模拟攻击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或了解有限

的一个外部攻击者。测试人员不知道任何关于目标环境以外的信息,特别是 IP 地址或域名等信息。真正

的攻击者通常会对目标环境进行深入的调查,以获取必要的信息。因此,外部测试通常用于验证系统

的安全性,并评估系统对外部攻击的防御能力。外部测试的结果通常用于指导内部测试,以提高系统

的安全性。外部测试的结果通常用于指导内部测试,以提高系统的安全性。外部测试的结果通常用于

指导内部测试,以提高系统的安全性。外部测试的结果通常用于指导内部测试,以提高系统的安全性。

外部测试的结果通常用于指导内部测试,以提高系统的安全性。外部测试的结果通常用于指导内部

测试,以提高系统的安全性。外部测试的结果通常用于指导内部测试,以提高系统的安全性。外部测试

的结果通常用于指导内部测试,以提高系统的安全性。外部测试的结果通常用于指导内部测试,以

提高系统的安全性。外部测试的结果通常用于指导内部测试,以提高系统的安全性。外部测试的结果

通常用于指导内部测试,以提高系统的安全性。外部测试的结果通常用于指导内部测试,以提高系

统的安全性。外部测试的结果通常用于指导内部测试,以提高系统的安全性。外部测试的结果通常

其访问权限(通常是作为一个用户,但有时层次更高)之外,内部渗透测试员通过权限提升器获得无限制的网终及系统的控制权限。

授予在网络或特定系统上定程序
以其他资源来利用。网络资源可

通过测试发现的一个在运行程序时从内存中读取数据时发生段错误的问题，在开发中，需要安全访问内存，以便在发生故障时，对内存系统和数据进行修复，可能对网络和系统引入额外的风险。因此，在开发中，需要安全访问内存，以便在发生故障时，对内存系统和数据进行修复，可能对网络和系统引入额外的风险。

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

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。

Copyright © 2005, Pearson Education, Inc. All rights reserved. Printed in the United States of America. This book is published under the name of Pearson Education, Inc., a company that has no affiliation with the Communist Party of China. The publisher disclaims any responsibility for the content of this book.

可能会根据该漏洞的复杂性、主机或设备、受影响设备数量、补丁服务价

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, e) 在对 Web 应用程序/操作系统/数据库的账号被锁定,暂时无法使用; 导致 Web 应用程序/操

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

B.5 渗透测试风险规避

试验过程中,应持续的风险进行提示。当出现如下内容时,应停止做好渗透测试的风

Figure 1

可得到如下结论:

——测试策略为人工测试时,测试人员数量有进行招徕或不被招徕之分;

——风险分析(如主机故障概率估计)与验证测试(DVCS)等工具用于系统管理大受好评;

在应用系统管理表要输入数据时,可以进行测试,输入数据时,生产系统即可运行。



图 2-3-1 决策树分析流程图

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负责,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

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	信息安全等级保护基本要求	
[4]	GB/T 22239—	信息安全技术	信息安全等级保护测评要求	
[5]	GB/T 28448—	信息安全技术	信息安全等级保护测评过程指南	
[6]	GB/T 28449—	信息安全技术	信息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

版权专有 侵权必究



GB/T 36627-2018