ICS 35.040
[illegible]

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

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

[redacted]

2 规范性引用文件

[redacted]

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于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 25069—2010 信息安全技术 术语

3 术语和定义、缩略语

3.1 术语和定义

GB 17859—1999 及 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1.1

字典式攻击 dictionary attack

在破解口令时，逐一尝试用户自定义词典中的单词或短语的攻击方式。

3.1.2

文件完整性检查 file integrity checking

通过建立文件校验数据库，计算、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前值和存储值，从而识别文件是否被修改。

3.1.3

网络嗅探 network sniffer

[redacted]

[redacted]

规则集 rule set

[redacted]

[redacted]

[redacted]

[redacted]

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:

[illegible]

c) 漏洞验证技术:验证漏洞存在性的测评技术,基于检查、目标识别和[illegible]分析结果,针对性地采取[illegible]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、远程访问测试等,对可能存在的安全漏洞进行验证确认,获得证据。

4.2 技术选择

[illegible]

5 等级测评要求

5.1 检查技术

5.1.1 文档检查

文档检查的主要功能是基于等级保护对象运营单位提供的文档,评价其策略和规程[illegible]的技术准确性[illegible]

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、系统互连的技术把关、事件响应计划等，确保技术的准确性和完整性；

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、系统互连技术把关、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，确认被测方安全措施实施与制度文档间一致性；

c) 发现可能导致潜在漏洞无检当的实施安全控制措施的相关问题点。

策略；

e) 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

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

设施的使用、配置

略，并且能够发现

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

和修改的历史记录等适当信息，等级保护对象的运营使用单位是否坚持了日志管理策

全策略要求一致

a) 识别需要备份系统日志的系统组件或其他相关组件；

b) 操作系统日志包括系统和服务的启动和关闭、与安全相关措施的安全文件的访问

变更（例如，创建和删除）、系统权限配置以及被使用等信息；

c) DNS日志包括查询和响应消息的适当使用；

5.1.3 规则集检查

安全设

规则集检查的主要功能是发现某一规则集的安全控制措施的漏洞，检查对象包括网络设备、

备、数据库、操作系统及应用系统的访问控制列表、策略集、二级及以上等级保护对象应包括

控制规则，进行规则集检查时，至少应关注以下评估要素和评估原则：

a) 防火墙规则控制列表：

b) 每一条规则都应是有效的控制规则，因此对未明确定义的规则，在不需要的情况下应

c) 规则集中的规则应与安全策略一致；

d) 规则集中的规则应无冗余；

e) 规则集中的规则应无矛盾；

f) 规则集中的规则应完整；

g) 规则集中的规则应无隐蔽；

h) 规则集中的规则应无错误。

相同的访问规则；

2) 以文件形式存储和操作的用户数据，在操作系统的支撑下，应实现文件级粒度的强制访问控制；

3) 以数据库形式存储和操作的用户数据，在数据库管理系统的支撑下，应实现记录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；

1) 仅开放必要的服务和应用；

2) 设置保护进程的守护进程；

c) 用户账号的唯一性标识和口令复杂度设置；

1) 开启必要的审计策略，设置各项策略

2) 设置合理设置文件访问权限

3) 三级及以上等级保护对

1) 由系统安全员创建

2) 实施者可强制访问

3) 检查标记的范围，

5.1.5 文件完整性检查

可考虑以下评估要素：

a) 采用备份软件

5.1.6 密码检查

密码检查的主要功能是

可考虑以下评估原则：

a) 所提供的密码算法

1) 所生成的密钥长度

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

未授权和不恰当的行为

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；

e) 在防火墙后端部署网络嗅探器，用以评估准确过滤流量的规则集。

进行网络

并利用工具

火墙；

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。端口和服务识别时，可考虑以下评估要素和评估原则：

a) 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；

b) 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

c) 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

时，有助于

洞扫描时，

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；同识别计时的软件版本、缺失的补工和错误配置，并验证其与机构安全策略的一致性。进行漏

[redacted]

5.2.4 无线扫描

[redacted]

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:

a) 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;

b) 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字符

c) 如测评对象采用带有盐值的加密散列函数时,不宜使用彩虹表方式进行口令破解尝试;

d) 对存在口令破解次数限制的情况,应验证是否能够绕过口令破解次数限制,

5.3.2 渗透测试

客的攻击方法,攻击等级保护对象的应用程序、系统或者网缺陷或漏洞的一种评估方法。进行渗透测试时,可考虑以

存在:

系统、数据库、中间件等为应用系统提供服务或支撑的环境

缓冲区溢出漏洞、堆溢出、内存泄露等,可能造成程序

等后果,更为严重的,可以导致程序执行非授权指令甚至

非法操作。

员编写代码不规范或缺少必要的校验措施,导致应用系统

、跨站脚本、任意上传文件等漏洞;攻击者可利用这些漏洞,

数据库中的敏感信息,甚至可以是篡改数据库

访问功能模块权限控制规则不完善或存在缺失,导致攻击者

能模块。权限旁路类漏洞通常可分为越权访问及平行权限。

授权访问高权限用户的功能模块或数据信息。平行权限是指

模块,非授权访问或修改其他人的数据信息。

配置文件进行安全加固,仅使用默认配置或配置不合理,例如

置支持 put 方法,可能导致攻击者利用 put 方法上传木马文

渗透测试的主要功能是通过模拟恶意黑络的安全功能,从而验证测评对象弱点、技术下评估要素和评估原则:

a) 通过渗透测试评估确认以下漏洞的

1) 系统/服务类漏洞。由于操作系存在缺陷,所导致的安全漏洞运行失败、系统宕机、重新启动

致得系统特权,进而进行各种

2) 应用代码类漏洞。由于开发人存在安全漏洞,包括 SQL 注入

3) 权限旁路类漏洞。由于对数可非授权访问这些数据及功越权访问是指低权限用户

攻击者利用自身权限的功能

4) 配置不当类漏洞。由于未对致的安全风险,如未配置

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。

e) 监测远程访问通信。可以通过网络嗅探器监视远程访问通信，如果通信未被加密，则可查看这些数据作为远程访问的认证信息，或者将这些数据作为远程访问用户发送或接收的数据。

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：

[redacted]

A.2　提出改进建议

[redacted]

A.3　报告

[redacted]

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

[illegible]

渗透测试通常包括非技术攻击方法。例如，一个渗透

[illegible]

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。

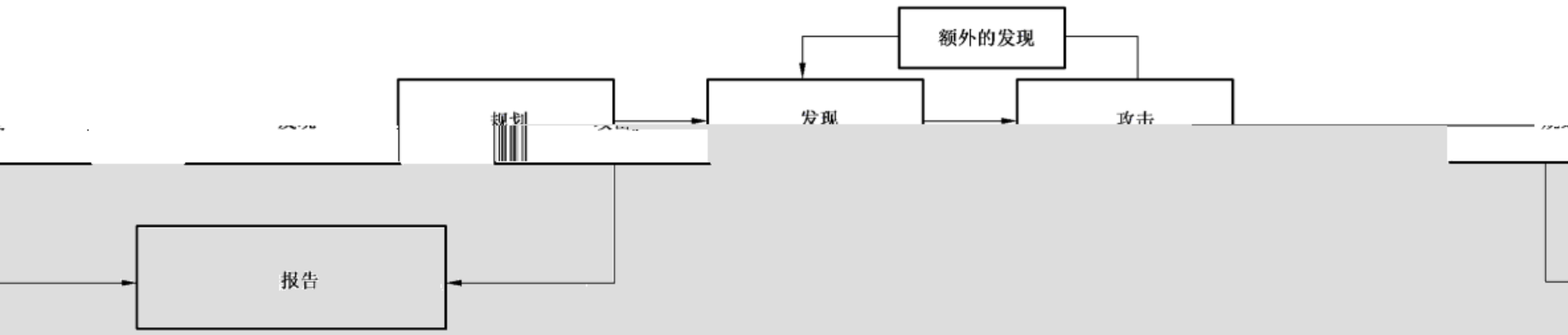

图 B.1　渗透测试的四个阶段

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[illegible]除了[illegible]在目标范围[illegible]：

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) 通过检查系统 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) [illegible]

d) [illegible]

第二部分是漏洞分析，其中包括将被扫描主机提供的服务、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[illegible]

[illegible]

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[illegible]

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[illegible]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[illegible]

[illegible]

B.4 渗透测试风险

B.5 渗透测试风险规避

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 22239—2008 信息安全技术 信息系统安全等级保护基本要求

[4] GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

[5] GB/T 28448—2012 信息安全技术 信息系统安全等级保护测评要求

[6] GB/T 28449—2012 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