ICS 35.040

国国家标准 中华人民共和

GB/T 36627—2018

全技术 信息安全

测试评估技术指南 网络安全等级保护测

technology— Information security

classified cybersecurity protection Testing and evaluation technical guide for

2019-04-01 实施 2018-09-17 发布

理总局
理委员会 发布

国家市场监督管理
中国国家标准化管理

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。

[illegible]

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

GB/T 28448—2012 与 GB/T 28448—2019 相比，主要技术变化如下：

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

[illegible]

2 规范性引用文件

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 下列文件对于本

[illegible]

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

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，同时也是一

[illegible]

3.1.4

规则集 rule set

[illegible]

3.1.5

测评对象 target of testing and evaluation

等级测评过程中不同测评方法作用的对象，主要涉及相关信息系统、配套制度文档、设备设施及人员等。

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

[illegible]

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其于等级保护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、

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、系统互连的技术规范、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，确认被测方安全措施的实施与制度文档的一致性；

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、系统互连的技术规范、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，确认被测方安全措施的实施与制度文档的一致性；

c) 发现可能导致遗漏或不恰当地实施安全控制措施的缺陷和弱点；

d) 验证测评对象的文档是否与网络安全等级保护标准法规符合，有没有缺陷或已过时的策略；

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小口令长度和复杂度要求的时候，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

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、设备设施的使用、配置和修改的日志记录等信息，[illegible]

a) 检查操作系统日志，包括系统和服务的启动、关闭，未授权软件的安装、访问、安全策略变更（例如，创建和删除非主权限、配置主要权限使用等）等信息；

b) 检查IDS日志，包括恶意行为和不合理使用；

[illegible]

5.1.3 规则集检查

规则集检查的主要功能是验证当前规则集的安全控制措施的设置，检查不合理和冗余的规则，检查不合理和缺失的规则，并针对发现的问题给出规则集的优化建议。规则集检查的方法如下：

a) 将当前规则集与前一次规则集进行比较，发现变更的规则，并分析变更的合理性；

b) 检查规则集中是否有冗余规则，并分析冗余规则的合理性；

c) 检查规则集中是否有缺失规则，并分析缺失规则的合理性；

d) 检查规则集中是否有不合理规则，并分析不合理规则的合理性；

e) 检查规则集中是否有过期规则，并分析过期规则的合理性；

f) 检查规则集中是否有不合理的规则顺序，并分析不合理的规则顺序的合理性；

g) 检查规则集中是否有不合理的规则组织方式，并分析不合理的规则组织方式的合理性；

h) 检查规则集中是否有不合理的注释内容，并分析不合理的注释内容的合理性；

i) 检查规则集中是否有违反最小化原则的规则，并分析违反最小化原则的规则的合理性；

j) 检查规则集中是否有违反完整性原则的规则，并分析违反完整性原则的规则的合理性；

k) 检查规则集中是否有违反保密性原则的规则，并分析违反保密性原则的规则的合理性；

l) 检查规则集中是否有违反可用性原则的规则，并分析违反可用性原则的规则的合理性；

m) 检查规则集中是否有违反一致性原则的规则，并分析违反一致性原则的规则的合理性；

n) 检查规则集中是否有违反标识鉴别原则的规则，并分析违反标识鉴别原则的规则的合理性；

o) 检查规则集中是否有违反授权原则的规则，并分析违反授权原则的规则的合理性；

p) 检查规则集中是否有违反数据保护原则的规则，并分析违反数据保护原则的规则的合理性；

q) 检查规则集中是否有违反审计原则的规则，并分析违反审计原则的规则的合理性；

r) 检查规则集中是否有违反入侵防范原则的规则，并分析违反入侵防范原则的规则的合理性；

s) 检查规则集中是否有违反恶意代码防范原则的规则，并分析违反恶意代码防范原则的规则的合理性；

t) 检查规则集中是否有违反网络设备运维管理原则的规则，并分析违反网络设备运维管理原则的规则的合理性；

u) 检查规则集中是否有违反其他原则的规则，并分析违反其他原则的规则的合理性。

相同的访问规则；

2) [illegible]

[illegible]

5.1.4 配置检查

策
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) [illegible]

e) 用户账户等唯一性标识和口令复杂度设置；

[illegible]

[illegible]

理设置文件访问权限；

级及以上等级保护对象中敏感信息资源主、客体的安全标记；

由系统安全员创建主体(如用户)、客体(如数据)的安全标记；

实施标记强制访问控制安全策略的主、客体应标以标记的安全标记；

检查标记的范围应扩展到测评对象中的所有主体与客体。

件完整性检查

5.1.5 文件

[illegible]

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；

[illegible]

[illegible]

5.1.6 密码检查

产品进行安全性检查。进行密码检查时，

密码检查的主要功能是对测评对象中采用的密码技术或

可考虑以下评估原则：

a) 所提供的密码算法相关功能符合国家密码主管部门的

[illegible]

的有关规定；

[illegible]

5.2 识别和分析技术

,收集、识别网络中活动的设备、操作系统和协议、

考虑以下评估要素和评估原则：

[illegible]

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

未授权和不恰当的行为等信息。进行网络嗅探时，可考

a) 监视网络流量，记录和报告协议类型、

b) 识别主机之间的联系，包括哪些主机相互通

c) 通过自动化工具向常用的端口发送多种类

响应，并与操作系统和网络服务的数据包的

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

关服务与应用程序。进行网络

试的目标；

和定时技术的工具，并利用工具

S 检测的同时穿越防火墙；

间。

议降低漏洞风险；同时，有助于

络的一致性，进行漏洞扫描时，

网络电缆或外围电缆）情况下使一个或多

对象所带来的安全风险，进行无线扫描，

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

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

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
改变数据包，让数据包融入正常流量中，使数据包避开 IDS/IPS

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

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

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

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

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;

5.3.2 渗透测试

渗透测试的主要功能是通过模拟恶意黑客的攻击方法,攻击等级保护对象的应用程序、系统或者网络的安全功能,从而验证测评对象弱点、技术缺陷或漏洞的一种评估方法。进行渗透测试时,可考虑以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存在:

1) 系统/服务类漏洞:由于操作系统、数据库、中间件等为应用系统提供服务或支撑的环境

2) 通用化类漏洞:由于开发人员编写代码不规范或缺少必要的校验措施,导致通用系统存在安全漏洞,包括SQL注入、跨站脚本、文件上传等漏洞,攻击者可利用这些漏洞

3) 信息泄露类漏洞:由于系统不重要数据没有经过必要的保护或者可

4) 配置不当类漏洞:由于对配置文件进行安全加固没有使用默认配置或配置不合理

5) 弱口令类漏洞:由于对口令复杂度设置不满足安全要求,攻击者可

6) 逻辑错误类漏洞:由于程序逻辑设计不严或逻辑太复杂导致

b) 通过渗透测试评估确认测评对象在经历渗透测试攻击后,仍然保持原有部分等级保护对象的安全

c) 渗透测试内容

d) 相关内容参见附录D。

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

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

渗透测试通常包括

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。

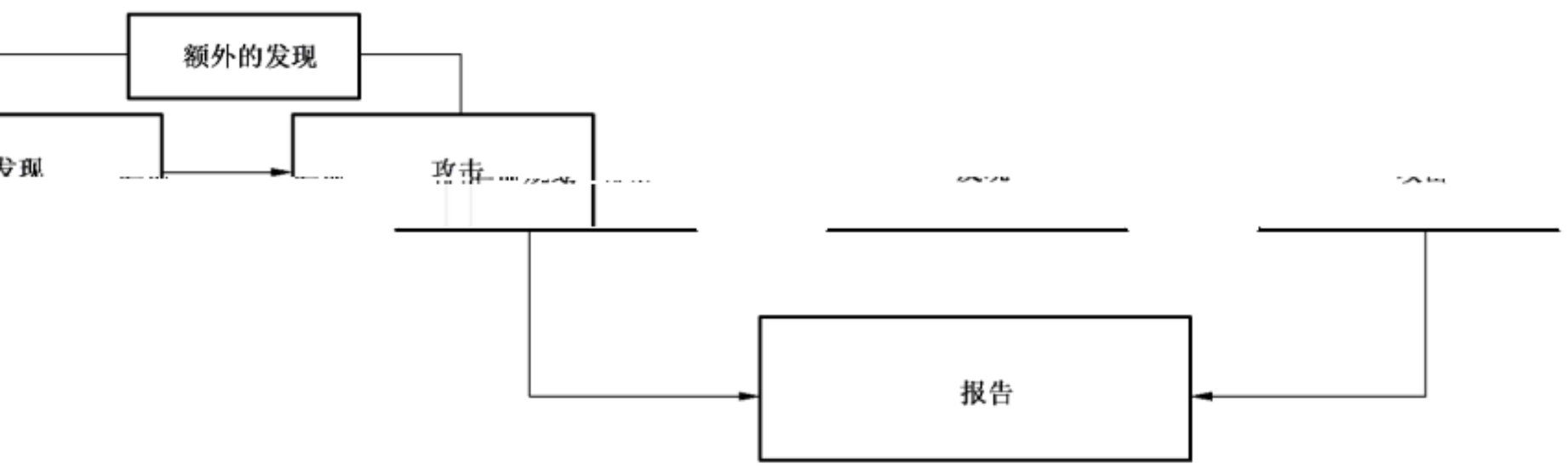

图 B.1　渗透测试的四个阶段

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：

B.2.4 攻击阶段

B.2.5 报告阶段

B.3 渗透测试方案

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

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

GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 28448—2012 信息安全技术 信息系统安全等级保护测评要求

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