ICS 35.040

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—Technical guide for classified cybersecurity protection testing and evaluation

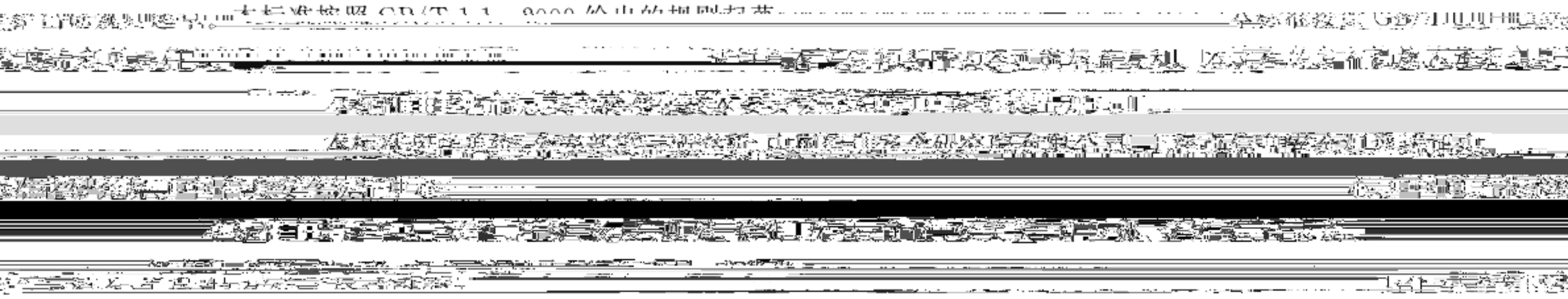
2018-09-17 发布　　2019-04-01 实施

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　技术共性 …… 2
5.2　物联网扩展 …… 3
5.3　云计算扩展 …… 3
5.4　移动互联扩展 …… 3
5.5　工业控制系统扩展 …… 3
5.6　安全管理 …… 3
6　等级测评过程 …… 3
6.1　测评单元 …… 3
6.2　测评对象 …… 3
6.3　测评指标 …… 3
6.4　测评内容 …… 3
6.5　测评结果 …… 3
7　单元测评 …… 3
7.1　概述 …… 3
7.2　安全物理环境 …… 3
7.3　安全通信网络 …… 3
7.4　安全区域边界 …… 3
7.5　安全计算环境 …… 3
7.6　安全管理中心 …… 3
7.7　安全管理制度 …… 3
7.8　安全管理机构 …… 3
7.9　安全管理人员 …… 3
7.10　安全建设管理 …… 3
7.11　安全运维管理 …… 3
8　整体测评 …… 3
8.1　概述 …… 3
8.2　安全控制间 …… 3
8.3　层面间 …… 3
8.4　区域间 …… 3
9　测评结论 …… 3
9.1　概述 …… 3
9.2　结果记录 …… 3
9.3　结果汇总 …… 3
9.4　等级测评结论 …… 3
附录A（规范性附录）　测评力度 …… 3
A.1　概述 …… 3
A.2　访谈 …… 3
A.3　检查 …… 3
A.4　测试 …… 3
附录B（规范性附录）　单项测评结果判定 …… 3
B.1　概述 …… 3
B.2　符合 …… 3
B.3　部分符合 …… 3
B.4　不符合 …… 3
B.5　不适用 …… 3
附录C（规范性附录）　单元测评结果判定 …… 3
C.1　概述 …… 3
C.2　结果判定 …… 3
附录D（规范性附录）　风险分析方法 …… 3
D.1　概述 …… 3
D.2　风险分析要素 …… 3
D.3　风险分析过程 …… 3
D.4　风险分析结果 …… 3
附录E（规范性附录）　等级测评结论 …… 3
E.1　概述 …… 3
E.2　等级测评结论 …… 3
参考文献 …… 3

前　言



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
3 术语和定义、缩略语
4 概述
5 测试对象
6 测试指标
7 测试内容
8 测试实施
9 测试结果判定
10 测试结果记录
11 测试结果文档输出
附录A（资料性附录） 测试工具接口
附录B（资料性附录） 测试结果记录表单
附录C（资料性附录） 测试结果文档输出格式
附录D（资料性附录） 测试指标扩展
附录E（资料性附录） 测试内容扩展
附录F（资料性附录） 测试实施扩展
附录G（资料性附录） 测试结果判定扩展
附录H（资料性附录） 测试结果记录扩展
附录I（资料性附录） 测试结果文档输出扩展
参考文献

1 范围

2 规范性引用文件

3 术语和定义、缩略语

3.1 术语和定义

及 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

GB 17859—1999

3.1.1

字典式攻击 dict

tionary attack

一类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 f

ile integrity checking

3.1.3

3.1.4

规则集 rule set

3.1.5

测试对象 target of testing and evaluation

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 System)

IP：互联网协议(Internet Protocol)

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、目标识别和分析结果，针对性地采取

b)

c) 渗

安全渗透进行验证和发现。

4.2 技术选择

4

等级测评要求 5

1 检查技术 5.

1.1 文档检查 5.

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：

[illegible]

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[illegible]

[illegible]

5.1.3 规则集检查

规则集检查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、安全设备、数据库、操作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控制规则。进行规则集检查时，可考虑[illegible]：

a) 路由访问控制列表：

1) 每一条规则[illegible]；

2) [illegible]；

b) 安全设备安全策略：

1) 应采用默认拒绝策略；

2) 应实施最小权限访问，例如限定可信的IP地址或端口；

3) 特定规则应在一般规则之前被触发；

4) 仅开放必要的端口，以增强边界安全；

5) 防止流量绕过测评对象的安全防御措施[illegible]；

c) 强制访问控制机制：

[illegible]

相同的访问规则；

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) 在防火墙后部署网络嗅探器，用以评估防火墙过滤流量的规则集。

5.2.2 网络端口和服务识别

5.2.3 漏洞扫描

5.2.4 无线扫描

5.3 漏洞验证技术

5.3.1 口令破解

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

渗透测试活动能确认现下漏洞没有在

渗透测试活动应制定详细的渗透测试方案，包含每次渗透测试对象、渗透测试人员及规避措施等内容（相关内容参见附录B）。

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

a) 发现除VPN、SSL等远程接入外是否存在其他的未授权的接入方式。

b) 发现未授权的远程访问服务，通过端口扫描检查经常用于进行远程访问的公开的端口

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) 缺乏安全基准，同类的系统使用了不一致的安全配置策略；

b) 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、甚至未考虑安全要求或系统应用程序代码中存在漏洞；

c) 缺乏安全基准，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、甚至未考虑安全要求或系统应用程序代码中存在漏洞；

e) 安全体系结构存在缺陷，如安全技术未能有效地集成至系统中（例如，安全防护设施、设备放置

A.2 提出改进建议

A.3 报告

在测评结果分析完成之后，应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) 作为测评组织运营单位为如等级保护对象满足安全要求而采取改进措施的基准；

d) 为决策者和运营单位领导机构提供关于信息安全状况的详细信息；

e) 为改正等级保护对象中安全问题而进行的成本效益分析；

f) 为运营单位的等级保护对象安全管理提供指导；

g) 为测评组织和测评人员的能力评价提供证据。

附 录 B
（资料性附录）
渗透测试的有关概念说明

B.1 综述

拟攻击者，利用攻击者常用的工具和技

渗透测试是一种安全性测试，在该类测试中，测试人员将模

术对应用程序、终端系统或网络的安全功能发动真实的攻击

B.2 渗透测试方法

B.2.1 概述

发现、攻击、报告四个阶段，如图 B.1 所示。

渗透测试通常包括规划

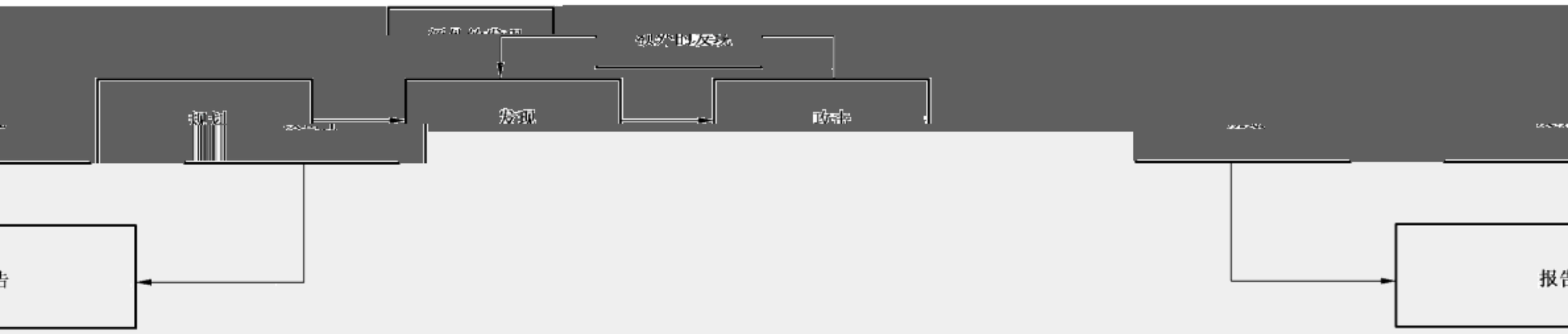


图 B.1 渗透测试的四个阶段

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

渗透测试的发现阶段包括两个部分：

B.2.4 攻击阶段

B.3 渗透测试方案

[illegible]

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[illegible]

a) 在使用[illegible]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[illegible]

b) [illegible]

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[illegible]

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[illegible]服务器操作系统/数据库[illegible]

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[illegible]

[illegible]

a) 备份策略：为防范渗透测试过程中的异常问题，建议在测试前[illegible]备份[illegible]

[illegible]

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 20271—2006 信息安全技术 信息系统通用安全技术要求

[4] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

[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

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