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—
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

[redacted]

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

3.1 术语和定义

GB 17859—1999 及 GB/T 25069—2010

3.1.1

字典式攻击 dictionary attack

3.1.2

文件完整性检查 file integrity checking

3.1.3

3.1.4

规则集 rule set

3.1.5

测试评估 test 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：网际协议(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类如下：

a) 指令

b) 目标识别的分析结果引发的生成或获取

c) 漏洞验证技术：验证漏洞存在性的测评技术，基于检

4.2 技术选择

5 等级测评要求

5.1 检查技术

5.1.1 文档检查

文档检查的主要测评内容是检查

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 [illegible]

a) 路由访问控制列表:

[illegible]

b) 防火墙设备策略集:

1) 应采用默认禁止策略;

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匹配;

4) 仅开放必要的端口,以增强网络安全;

5) 防止流量绕过测评对象的安全防御措施;

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；

[illegible]

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[illegible]络上开放的端口、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：

a) 对主机及存在潜在漏洞的端口进行识别，[illegible]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，应使用多个[illegible]

[illegible]

5.2.3 漏洞扫描

[illegible]

a) [illegible]

b) [illegible]等级；

c) 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；

d) 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；

e) [illegible]

5.2.4 无线扫描

[illegible]

5.3 漏洞验证技术

5.3.1 口令破解

5.3.2 渗透测试

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
[redacted]

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

在整个测评中需要立即处理的严重

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

重漏洞。以下列举了常见的造成漏洞的根本原因，包括：

A.2 提出改进建议

A.3 报告

附 录 B
（资料性附录）
渗透测试的有关概念说明

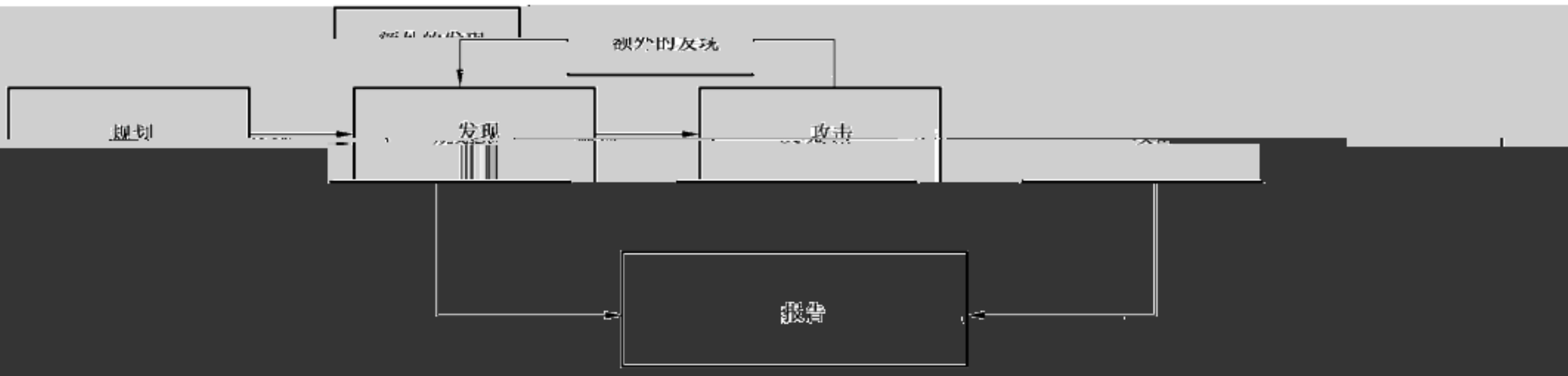
B.1 综述

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

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。



B.2.2 规划阶段

渗透测试的发现阶段包括两个部分：

B.2.4 攻击阶段

B.2.3 渗透测试方案

渗透测试方案宜细化到具体实施项目，包括但不限于各应用程序、系统或网络中的设备和

R 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

B.5　渗透测试风险规避

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 信息系统安全等级保护基本要求

[4] GB/T 22240—2008 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

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