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 …… 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　检查技术 …… 2

5.1.1　[illegible] …… 2

5.1.2　[illegible] …… 3

5.1.3　规则集检查 …… 3

5.1.4　[illegible] …… 3

[illegible] …… [illegible]

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

3.1 术语和定义

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 及 G

3.1.1

字典式攻击 dictiona

ary attack

3.1.2

文件完整性检查 File i

ntegrity checking

3.1.3

3.1.4

规则集 rule set

3.1.5

测评对象 target of testing and evaluation

3.2 缩略语

下列缩略语适用于本文件。

[illegible]

GSVD:国家信息安全

DNS:域名系统(Doma

DDoS:分布式拒绝服

ICMP:Internet 控制报

IDS:入侵检测系统(I

[illegible]

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]

[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

[illegible]

和完整性。进行文档检查时，可考虑以下评估要素：

[redacted]

[redacted]

5.1.2 日志检查

[redacted]

[redacted]

[redacted]

[redacted]

5.1.3 规则集检查

[redacted]

问规则；

相同的访

[illegible]

[illegible]

5.1.4 配置检查

[illegible]

5.1.5 文件完整性检查

[illegible]

5.1.6 密码检查

[illegible]

5.2 [illegible]

5.2.1 网络嗅探

[illegible]

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：

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，并利用工具[illegible]

c) 应[illegible]

5.2.3 漏洞扫描

[illegible]

a) 识别漏洞相[illegible]

b) 通过工具识[illegible]等级；

c) 漏洞扫描前[illegible]

d) 依据漏洞扫[illegible]

[illegible]

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（如网络电缆或外置电缆）情况下使一个或多[illegible]

[illegible]

c) 使用安装配置无线分析软件的移动设备，如笔记本电脑、手持设备或专业设备；

d) 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；

e) 适当配置扫描工具的扫描间隔时间，既能捕获数据包，又能有效地扫描每个频段；

f) 可通过导入平面图或地图，以协助定位被发现设备的物理位置；

g) 对捕获的数据包进行分析，从而识别扫描范围内发现的潜在的恶意设备和未授权的网络连接[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。进行远程访问测试[illegible]

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[illegible]

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）[illegible]

b）[illegible]

c）[illegible]

d）[illegible]

e）[illegible]

f）[illegible]

g）[illegible]

A.2 提出改进建议

[illegible]

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） [illegible]

e） [illegible]

[illegible]

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、终端系统或网络的安全功能发动直实的攻击。

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。

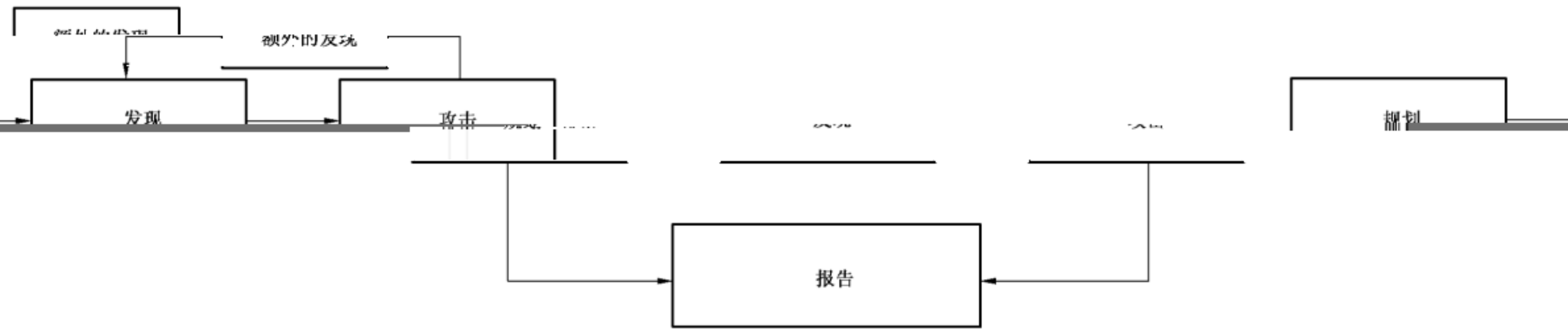

图 B.1 渗透测试阶段

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.2.5 报告阶段

B.3 渗透测试方案

渗透测试方案它侧重于在应用程序、系统或网络中的设计和实现中，定位和挖掘出可利用的漏

内部攻击是模拟组织内部违规操作者的行为，除了测试人员位于内部网络(即防火墙后面)并已

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 20282—2006 信息安全技术 信息系统安全工程管理要求

[4] GB/T 28449—2018 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