ICS 35.040

L 80

国家标准 中华人民共和国

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

# 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

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[illegible]下列[illegible]的引用文[illegible]最新版本（包括所有的修改单）适用于本文件。

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

25069—2010 界定的以及下列术语和定义适用于本文件。

GB 17859—1999 及 GB/T

3.1.1

**字典式攻击 dictionary att**

**tack**

[illegible]户自定义词典中的单词或短语的攻击方式[illegible]

在破解口令时，逐一尝试用

3.1.2

**ty-checking**

文件完整性检查 file integri

[illegible]

3.1.3

[illegible]

**集 rule set**

规则

[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[illegible]

[illegible]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 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类见下表。

### 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

文档检查的主要功能是基于

和完整性。进行文档检查时，可考虑以下评估要素：

[redacted]

5.1.2 日志检查

[redacted]

5.1.3 规则集检查

[redacted]

### 5.2.1 网络嗅探

网络嗅探的主要功能是简单捕捉和重放网络流量，监测网络active动的设备，操作系统和协议

### 5.1.6 密码检查

### 5.1.5 文件完整性检查

### 5.1.4 防病毒

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，用以评估被防火墙阻断的流量。

。进行网络

并利用工具

### 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，

### 5.2.3 漏洞扫描

等级；

### 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

### 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) 缺乏安全基准或安全基准未得到正确的应用；

b) 系统设计、实现或配置存在导致未经授权访问的已知问题；

c) 由于系统管理员缺乏安全意识造成配置错误，如系统被设置为在不安全模式下运行，或者启用了不必要的服务；

d) 软件或硬件缺陷，如操作系统或固件中的缺陷；

e) 安全策略缺陷或不充分，如对渗透测试活动缺乏适当的授权。

## 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) 作为测评组织实施单位为使其组织满足安全要求而采取改正措施的基准；

d) 用于支持实施满足组织安全要求的实施过程；

e) 为实施组织使用对组织安全面临的威胁进行更为全面的分析；

f) 用于[illegible]

# 附 录 B
（资料性附录）
# 渗透测试的有关概念说明

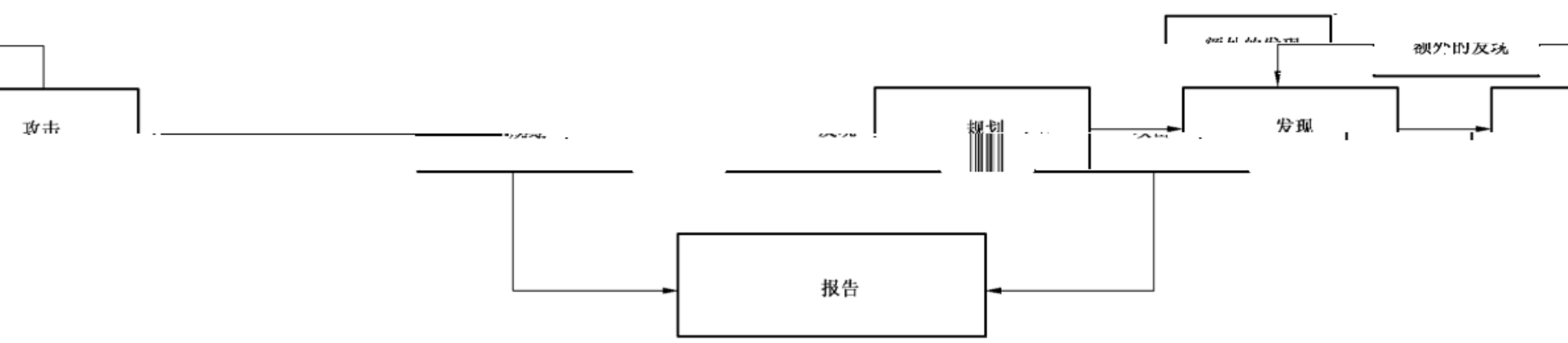
## B.1 综述

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

渗透测试的发现阶段包括两个部分：

第三部分是漏洞验证分析与信息获取阶

有比对。测试人员可决定是否自己的数据库

### B.2.4 攻击阶段

执行攻击是渗透测试的核心。攻击阶段是

### B.2.5 报告阶段

## B.3 渗透测试方案

B.3

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洞缺

R 4 渗透测试风险

者常用的工具和技术来对被测系统和数据发动真实 在渗透测试过程中，测试人员通常会利用攻击

B.3 渗透测试风险机理

# 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 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