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
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
5.1.1　身份鉴别 …… 2
5.1.2　访问控制 …… 3
5.1.3　安全审计 …… 3
5.1.4　边界防护 …… 4
5.1.5　恶意代码防范 …… 4
5.1.6　可信计算 …… 4
5.1.7　入侵防范 …… 4
5.1.8　数据完整性检查 …… 5
5.1.9　数据备份恢复 …… 5
5.1.10　剩余信息保护 …… 5
5.1.11　个人信息保护 …… 5

前　言

[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

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 2506

3.1.1

字典式攻击 dictionary attack

3.1.2

文件完整性检查 file integrity ch

3.1.3

网络嗅探器 network sniffer

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。

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)

[illegible]

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

可用于等级测评的测评技术分成以下三类：

[illegible]

c) 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[illegible]安全漏洞进行验证确认，获得证据。

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[illegible]

和完整性。进行文档检查时，可考虑以下评估要素：

a) [illegible]

b) [illegible]

c) [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机制。进行规则集检查时，可考虑以下评估要素和检查规则：

a) 路由访问控制列表：

[illegible]

b) 防火墙规则集要素：

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触发；

4) 仅开放必要的端口，以增强周边安全；

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：

[redacted]

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

[redacted]

c) [redacted]

5.2.3 漏洞扫描

[redacted]

能识别最新的漏洞；

[redacted]

探测等，[redacted]选择扫描策略，防止[redacted]

[redacted]

[redacted]

5.2.4 无线扫描

[redacted]

5.3 漏洞验证技术

5.3.1 口令破解

[illegible]

5.3.2 渗透测试

[illegible]

c) 评估者应制定详细的渗透测试方案，内容包括渗透测试对象、渗透测试风险及规避措施(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

漏洞。以下列举了常见的造成漏洞的根本原因，包括：

c) 缺乏安全基准，同类的系统使用了不一致的安

d) 在系统开发中缺乏对安全管理整合，如系统应

e) 安全体系结构存在缺陷，如安全技术未能有效

f) 安全事件响应措施不足，如对渗透测试和

g) 对缺乏用户

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其等级保护对象进行安全建设整改提供改进措施的基准；

d) 为主管部门监督检查网络安全等级保护的实施情况；

e) 为运营单位保护对象的安全组织开展安全检查提供参考；

f) 为运营单位开展网络安全教育培训提供参考。

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 渗透测试阶段

B.2.1 概述

划、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

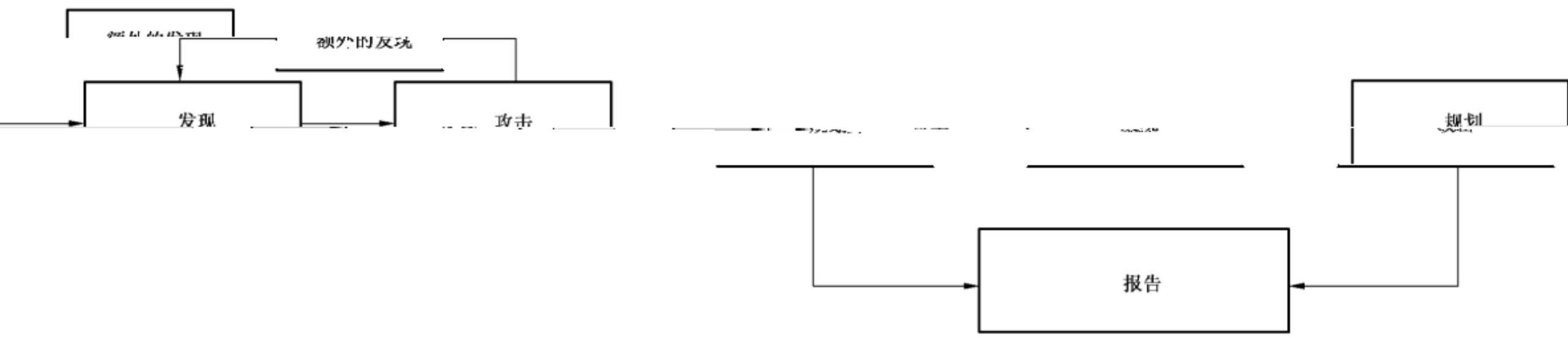


图 B.1 渗透测试的四个阶段

B.2.2 规划阶段

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

在规划阶段，确定规则，管理层

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

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

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 在渗透测试过程中

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

GB/T 22239—2019 信息安全技术 信息系统安全等级保护基本要求

GB/T 28448—2019 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