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　技术类 …… 2
5.1.1　物理安全 …… 2
5.1.2　网络安全 …… 3
5.1.3　规见集检查 …… 3
5.1.4　主机检查 …… 4
5.1.5　应用检查 …… 4
5.1.6　数据检查 …… 4

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准起草单位：

本标准主要起草人：

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

注日期的版本适用于本文 下列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

3 术语和定义、缩略语

3.1 术语和定义

GB 17859—1999 及 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1.1

字典式攻击 dictionary attack

在破解口令时，逐一尝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 file integrity checking

3.1.3

规则集 rule set

1.5 3.

tion 测评对象 target of testing and evalua

对象，主要涉及相关信息系统、网络制度与管理等。 等级测评过程中不同测评方法作用的

1

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

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

和完整性。进行文档检查时，可考虑以下评估要素：

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，这

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

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) 查验已部署网络嗅探器，用以评估准确过滤流量的规则集；

f) 查验网络设备的配置，评估其是否能够阻断非法流量；

g) 查验网络设备的配置，评估其是否能够对网络流量进行控制；

h) 查验网络设备的配置，评估其是否能够对网络流量进行记录；

i) 查验网络设备的配置，评估其是否能够对网络流量进行分析；

j) 查验网络设备的配置，评估其是否能够对网络流量进行报警。

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) 应尽量减少扫描工具对网络造成的干扰，如选择端口扫描的时间；

[illegible]

5.2.3 漏洞扫描

[illegible]

a) 识别漏洞相关信息，包含漏洞名称、类型、漏洞描述、威胁等级、修复建议等内容；

b) 通过工具扫描结合人工分析的方式，发现可被利用进行攻击或导致系统不能正常运行的漏洞，并确定漏洞风险等级；

c) 漏洞扫描前对扫描设备的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），合理选择扫描策略，防止引起测试对象故障；

e) 在网络设备上安装扫描代理程序，在本机进行漏洞检测，减少网络流量。

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（如网络电缆或终端电缆）情况下连接一个或多个设备实现通信的无线网络，并对其进行安全检查或进行指定攻击测试。

[illegible]

a) 使用无线网卡连接无线设备，如笔记本电脑、手持设备或专业设备；

b) 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，以实现差异分析；

c) 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；

d) 可通过导入平面图或地图以期到定位被发现设备的物理位置；

e) 对扫描结果进行分析，并可预测扫描范围内发生的某种业务异常或非授权的网络连接。

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
在整个测评中需要立即处理的严重
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：
a)
b)
c) 缺乏安全基
d)
应用程序代
e) 安全体系结

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使等级保护对象满足安全要求而采取改进

d)

e)

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真实的攻击。

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。

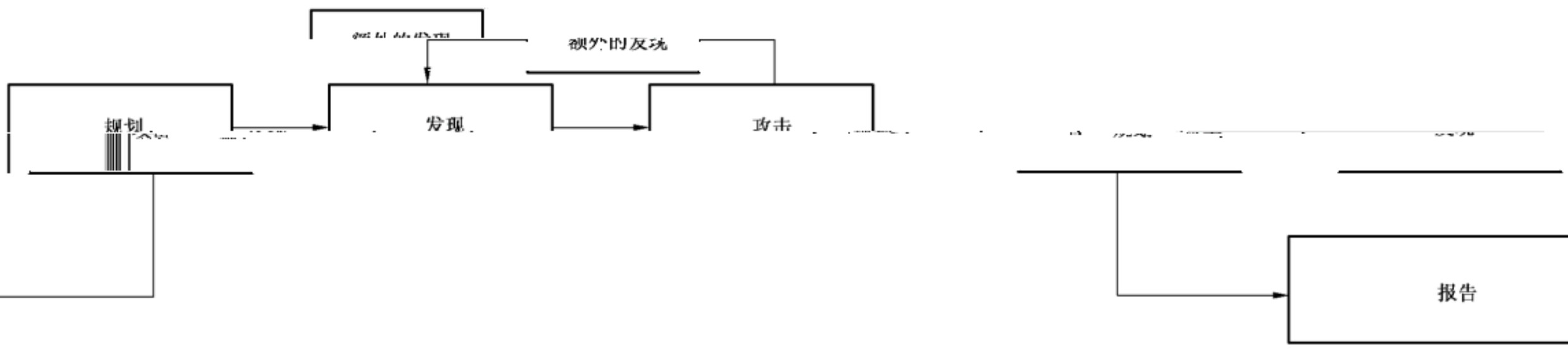


图 B.1 渗透测试的四个阶段

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测试奠定了基础。

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

渗透测试方案 B.3

渗透测试方案宜侧重于在应用程序、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

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，测试人员

在使用

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

版权专有 侵权必究