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—Technical guide for testing and evaluation of 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

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，仅注日期的版本适用于本文

和定义适用于本文件。

3 术语和定义、缩略语

3.1 术语和定义

GB 17859—1999 及 GB/T 25069—2010 界定的以及下列术语

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

测评对象 target of 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
DNS：域名系统(Dom
DDoS：分布式拒绝服
ICMP：Internet 控制
IDS：入侵检测系统(I
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：

[redacted]

5.1.2 日志检查

[redacted]

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[redacted]

[redacted]

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[redacted]

[redacted]

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) 在防止渗后端部署网络嗅探器，用以评估突破防护措施的攻击流量。

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被测设备/系统开放的端口及运行在端口之上的服务与应用程序，进行网络端口和服务识别时，可参照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，并用于确定远程测试目标；

b) 在扫描过程中和在扫描时，应使用全面、有效、合适的端口扫描技术和扫描参数，以获得准确和完整的端口、协议和服务清单；

c) 应使用最新的端口扫描器版本，以确保能识别最新的端口；

d) 应采用多种端口扫描技术（如特征匹配、攻击探测等），并根据扫描策略、防护对象数量、扫描时间要求等因素选择合适的端口扫描技术；

e) 应使用多种端口扫描工具，以降低测试遗漏和测试结果不准确的风险。

5.2.3 漏洞扫描

漏洞扫描的评估要素和评估原则如下：

a) 应采用最新的漏洞库，以确保能识别最新的漏洞；

b) 漏洞扫描前，扫描设备应是最新版本；

c) 应根据扫描对象的操作系统类型、开放端口、提供服务等因素选择合适的扫描策略，如特征匹配、攻击探测等，并根据扫描策略、防护对象数量、扫描时间要求等因素选择合适的扫描等级；

d) 依据漏洞扫描工具的漏洞分析原理，判断漏洞扫描结果的准确性，排除漏报和误报，提高测评对象风险；

e) 使用漏洞扫描设备应从发现扫描结果、

5.2.4 无线扫描

无线扫描的评估要素和评估原则如下：

5.3 漏洞验证技术

5.3.1 口令破解

5.3.2 渗透测试

渗透测试的主要功能是通过模拟恶意黑客的攻击方法，攻击等级保护对象的应用程序、系统或者网

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) 缺乏安全基准或同类的系统使用了不一致的安全配置策略；

b) 系统开发时设定的安全性检查、设置未考虑安全要求或系统开发不满足安全要求、设置未考虑安全要求或系统

c) 系统存在缺陷，如安全技术未能有效集成至系统中或打补丁不合理或漏洞不及时；

d) 安全机制

e) 安全

f) 安全

A.2 提出改进建议

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措施的基准；

d) 为决策部门提供等级保护对象安全符合或不符合要求的结论；

e) 为等级保护对象安全面向用户提供安全保证；

f) 为等级保护对象的安全监督、检查提供参考。

附 录 B
（资料性附录）
渗透测试的有关概念说明

B.1 综述

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。

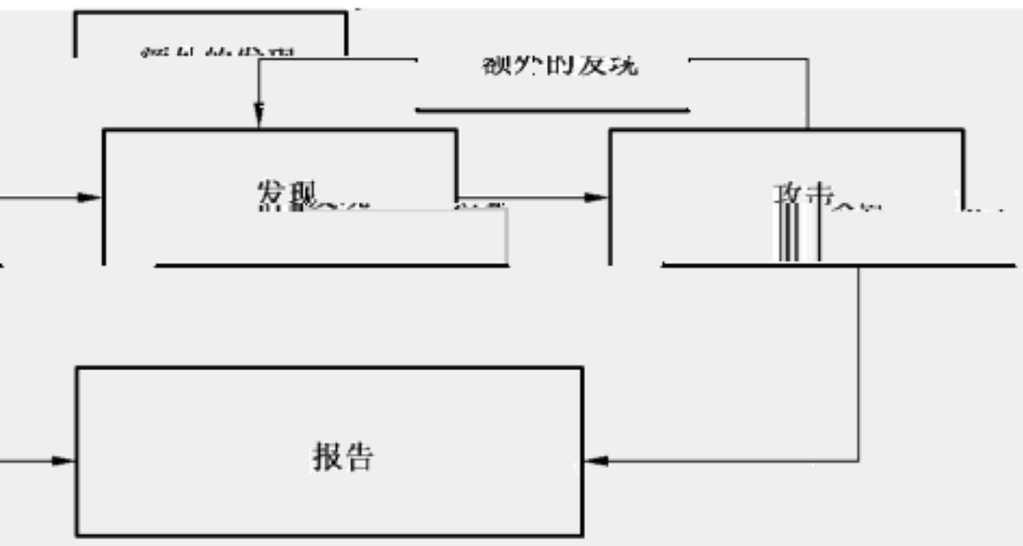

图 B.1 渗透测试的四个阶段

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

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

B.4 渗透测试风险

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，测试人员通

B.5 渗透测试风险规避

参 考 文 献

GB/T 20269—2006 信息安全技术 信息系统安全管理要求

GB/T 20270—2006 信息安全技术 网络基础安全技术要求

[1] GB

[2] GB

[3] GB/T 20984—2007 信息安全技术 信息系统安全管理要求

[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