

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—

protection—Testing and evaluation technical guide for classified cyberscurity r



# 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 基本要求	2
5.1.1 人员要求	2
5.1.2 工具要求	2
5.1.3 规则集检查	2
5.1.4 漏洞扫描	2
5.1.5 文件完整性检查	2
5.1.6 配置检查	2



# 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

## 规范性引用文件

## 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件。凡是未注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999 计算机信息系统安全保护等级划分准则

## 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。

GB 17859—1999 及 GB/T 25069—2010

#### 3.1.1

字典式攻击 dictionary attack  
在破解口令时,逐一尝试用

字典式攻击 dictionary attack  
在破解口令时,逐一尝试用

#### 3.1.2

文件完整性检查 file integrity

文件完整性检查 file integrity

#### 3.1.3

规则 rule set

规则

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

### 3.2 缩略语

下列缩略语适用于本文件。

漏洞库(China National Vulnerability Database)	CNVD; 国家信息安全
域名系统(Domain Name System)	DNS; 域名系统(Doma
拒绝服务(Distributed Denial of Service)	DDoS; 分布式拒绝服
报文协议(Internet Control Message Protocol)	ICMP; Internet 控制报
入侵检测系统(Intrusion Detection System)	IDS; 入侵检测系统
入侵防御系统(Intrusion Prevention System)	IPS; 入侵防御系统
应用层网关(Application Gateway)	AG; 应用层网关
安全外壳协议(Secure Shell)	SSH; 安全外壳协议(Secure Shell)
服务集标识(Service Set Identifier)	SSID; 服务集标识(Service Set Identifier)
结构化查询语言(Structured Query Language)	SQL; 结构化查询语言(Structured Query Language)
虚拟专用网络(Virtual Private Network)	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为以下三类。

### 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

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。文档检查的主要功能是其于



问规则；

相同的访

...操作的用户数据,在操作系统的日志中,应记录高级别数据的强制访问...

3) 以文件形

控制;

3) 以新指令或程序代码作的用户数据,在新指令或程序代码中,应记录高级别数据的强制访问...

### 5.1.4 配置检查

...配置检查... 应检查... 配置文件的完整性... 配置文件的版本... 配置文件的权限...

### 5.1.5 文件完整性检查

...文件完整性检查... 应检查... 文件的完整性... 文件的完整性... 文件的完整性...

### 5.1.6 密码检查

...密码检查... 应检查... 密码的强度... 密码的复杂度... 密码的有效期...

## 3.2 攻击和防御技术

5.0 识别和入侵技术

### 5.2.1 网络嗅探

网络嗅探的主要功能是通过捕捉和重放网络流量,收集、识别网络中活动的设备、操作系统和协议...

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;

在网络边界处部署网络嗅探器,可以验证网络边界设备的配置。

### 5.2.2 网络端口和服务识别

进行网络

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:

并利用工具

- 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;

扫描时间

应设置最少扫描工具扫描网络运行在单一网络扫描面

### 5.2.3 漏洞扫描

漏洞扫描是指对网络中的主机或设备进行扫描,以识别已知漏洞。漏洞扫描工具通常提供漏洞扫描引擎,用于扫描主机或设备,并生成漏洞扫描报告。

漏洞扫描工具通常提供漏洞扫描引擎,用于扫描主机或设备,并生成漏洞扫描报告。

可考虑以下评估要素和评估原则:

扫描等级、修复建议等内容;

a) 识别漏洞相关信息,包含漏洞名称、类型、漏洞描述、从

扫描策略分析,从而准确判断漏洞的风险;

b) 通过工具识别结合人工分析的方式,对发现的漏洞进行等级;

并确保识别最新的漏洞;

c) 漏洞扫描前,扫描设备应更新至最新的漏洞库;

扫描策略等,谨慎选择扫描策略,防止引

d) 依据漏洞扫描工具的漏洞分析原理,如将漏洞匹配、改

起测评对象故障;

扫描策略等,谨慎选择扫描策略,防止引

e) 使用漏洞扫描设备时,应谨慎设置扫描策略,防止引

### 5.2.4 无线扫描

(如网络有线或外置有线)情况下使用一个或多个

无线扫描的主要功能是识别被扫描环境中没有物理连接

扫描策略等,谨慎选择扫描策略,防止引

无线扫描的主要功能是识别被扫描环境中没有物理连接

扫描策略等;

a) 使用无线扫描设备时,应谨慎设置扫描策略,防止引

b) 基于无线安全标准要求,对无线扫描工具进行漏洞策略分析;

c) 适当设置扫描工具扫描扫描时间,既能捕获数据包,又能有效地扫描每个频段;

d) 可通过捕获数据包生成网络图,以辅助识别被扫描设备的物理位置;

e) 对被扫描设备有非正常行为,应识别出扫描策略,防止引

f) 对被扫描设备有非正常行为,应识别出扫描策略,防止引

### 5.3 漏洞验证技术

#### 5.3.1 口令破解

口令破解的主要功能是在系统运行过程中通过采用暴力猜测、字典攻击、

#### 漏洞

#### 漏洞验证技术

漏洞验证技术用于验证漏洞是否存在，如漏洞扫描器、渗透测试工具等。

#### 渗透测试

5.3.2

渗透测试的主要功能是通过模拟攻击者攻击系统，攻击系统保护对象的漏洞，攻击系统或者利

用系统漏洞，攻击系统保护对象的漏洞，攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

#### 漏洞验证技术

漏洞验证技术用于验证漏洞是否存在。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

#### 漏洞

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

#### 漏洞验证技术

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

攻击系统或者利用系统漏洞，攻击系统保护对象的漏洞。

### 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

测试应遵循以下评估要素和评估流程:

a) 发现除 VBN、SSH 远程桌面规则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:通过端口扫描定期经常用于进行远程访问的公开的端口

通过

附录 A  
(资料性附录)  
测评后活动

A.1 测评结果分析

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:

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

安全配置策略;

c) 缺乏安全基线,同类的系统使用了不一致的

开发不满足安全要求,甚至未考虑安全要求或系统

d) 在系统开发阶段,缺乏安全管控制整合,如系统

架构存在缺陷,如安全设计未能有效集成于系统和组件,安全防护设施、设备数量

e) 安全体系

安全事件响应策略不足,如对渗透测试策略响应不及时;

f) 安全

A.2 提出改进建议

A.3 报告

可用于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) 作为测评引各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) 用于验证等级保护对象安全要求符合性;
- e) 为改进等级保护对象安全而进行的大致成本效益分析;



渗透测试的发现阶段包括两个部分：

1) 扫描器如 Nessus 枚举方法和网络侦察系统枚举系统名称、IP 地址、操作系统、端口、主机名、数据库服务、应用程序、操作系统和漏洞数据库；

第三部分是漏洞分析引擎包含新发现的漏洞进行比对。测试人员可以使用自己的数据库。

### B.2.4 攻击阶段

攻击阶段是渗透测试的核心。攻击阶段是通过对原先确定的漏洞进一步探索，进而挖空漏洞。

攻击阶段是渗透测试的核心。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。

渗透测试方案宜包括以下要素：测试范围、测试目标、测试方法、测试工具、测试环境、测试时间、测试人员、测试报告。

测试范围是指测试的范围，包括测试的系统、网络、应用程序、数据库、操作系统、中间件、第三方组件等。

测试目标是指测试的目的，包括发现漏洞、评估漏洞的严重性、验证漏洞的利用、验证漏洞的修复等。

测试方法是指测试的方法，包括手动测试、自动测试、混合测试等。

测试工具是指测试的工具，包括漏洞扫描器、渗透测试框架、漏洞利用工具、漏洞验证工具等。

测试环境是指测试的环境，包括测试的系统、网络、应用程序、数据库、操作系统、中间件、第三方组件等。

测试时间是指测试的时间，包括测试的开始时间、结束时间、测试的持续时间等。

测试人员是指测试的人员，包括测试的负责人、测试的执行人员、测试的审核人员等。

测试报告是指测试的报告，包括测试的范围、测试的目标、测试的方法、测试的工具、测试的环境、测试的时间、测试的人员、测试的结果等。

#### B.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

的操作系统漏洞等漏洞,通过暴力破解可能引发该漏洞的安全漏洞。

a) 在对 Web 应用进行

攻击 Web 应用时

#### 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—2015 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](http://www.spc.org.cn)

服务热线: 400-168-0010

2018年9月第一版

\*

书号: 155066 · 1-61231

