

标准

中华人民共和国国家

GB/T 36627—2018

信息安全技术

等级保护测试评估技术指南

网络安全

Information security technology—

Testing and evaluation technical guide for classified cybersecurity protection

2018-04-01 实施

2018-09-17 发布

国家市场监督管理总局  
发布

国家



# 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 检查清单	2
5.2 配置检查	2
5.3 规则集检查	2
5.4 漏洞扫描	2
5.5 渗透测试	2
5.6 应急演练	2
5.7 攻防演练	2
5.8 攻防对抗	2
5.9 攻防对抗	2
5.10 攻防对抗	2
5.11 攻防对抗	2
5.12 攻防对抗	2
5.13 攻防对抗	2
5.14 攻防对抗	2
5.15 攻防对抗	2
5.16 攻防对抗	2
5.17 攻防对抗	2
5.18 攻防对抗	2
5.19 攻防对抗	2
5.20 攻防对抗	2
5.21 攻防对抗	2
5.22 攻防对抗	2
5.23 攻防对抗	2
5.24 攻防对抗	2
5.25 攻防对抗	2
5.26 攻防对抗	2
5.27 攻防对抗	2
5.28 攻防对抗	2
5.29 攻防对抗	2
5.30 攻防对抗	2
5.31 攻防对抗	2
5.32 攻防对抗	2
5.33 攻防对抗	2
5.34 攻防对抗	2
5.35 攻防对抗	2
5.36 攻防对抗	2
5.37 攻防对抗	2
5.38 攻防对抗	2
5.39 攻防对抗	2
5.40 攻防对抗	2
5.41 攻防对抗	2
5.42 攻防对抗	2
5.43 攻防对抗	2
5.44 攻防对抗	2
5.45 攻防对抗	2
5.46 攻防对抗	2
5.47 攻防对抗	2
5.48 攻防对抗	2
5.49 攻防对抗	2
5.50 攻防对抗	2
5.51 攻防对抗	2
5.52 攻防对抗	2
5.53 攻防对抗	2
5.54 攻防对抗	2
5.55 攻防对抗	2
5.56 攻防对抗	2
5.57 攻防对抗	2
5.58 攻防对抗	2
5.59 攻防对抗	2
5.60 攻防对抗	2
5.61 攻防对抗	2
5.62 攻防对抗	2
5.63 攻防对抗	2
5.64 攻防对抗	2
5.65 攻防对抗	2
5.66 攻防对抗	2
5.67 攻防对抗	2
5.68 攻防对抗	2
5.69 攻防对抗	2
5.70 攻防对抗	2
5.71 攻防对抗	2
5.72 攻防对抗	2
5.73 攻防对抗	2
5.74 攻防对抗	2
5.75 攻防对抗	2
5.76 攻防对抗	2
5.77 攻防对抗	2
5.78 攻防对抗	2
5.79 攻防对抗	2
5.80 攻防对抗	2
5.81 攻防对抗	2
5.82 攻防对抗	2
5.83 攻防对抗	2
5.84 攻防对抗	2
5.85 攻防对抗	2
5.86 攻防对抗	2
5.87 攻防对抗	2
5.88 攻防对抗	2
5.89 攻防对抗	2
5.90 攻防对抗	2
5.91 攻防对抗	2
5.92 攻防对抗	2
5.93 攻防对抗	2
5.94 攻防对抗	2
5.95 攻防对抗	2
5.96 攻防对抗	2
5.97 攻防对抗	2
5.98 攻防对抗	2
5.99 攻防对抗	2
5.100 攻防对抗	2





## 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

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,仅注日期的版本适用于本文件。凡是注日期的引用文件,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

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。

字典式攻击 dictionary attack  
逐一些试用自定义词曲中的单词或短语的攻击方式

完整性检查 file integrity checking  
文件完整性

网络嗅探 network sniffer  
网络嗅探器

测试对象 target of testing and evaluation  
测试对象

测试策略 testing strategy  
测试策略

测试对象 target of testing and evaluation  
测试对象,主要涉及相关信息系统、设备、人员、资产、数据、流程、人员

### 3.2 缩略语

下列缩略语适用于本文件。

漏洞库(China National Vulnerability Database)	CNVD; 国家信息安全漏洞库
域名系统(Domain Name System)	DNS; 域名系统(Domain Name System)
拒绝服务(Distributed Denial of Service)	DDoS; 分布式拒绝服务
报文协议(Internet Control Message Protocol)	ICMP; Internet 控制报文协议
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
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主要分为以下三类：

- 1) 漏洞扫描技术：对目标系统进行扫描，发现系统存在的漏洞。
- 2) 渗透测试技术：模拟攻击者的行为，对系统进行攻击，验证漏洞的存在性。
- 3) 漏洞验证技术：验证漏洞的存在性，并评估漏洞的危害性。

### 4.2 技术选择

当所选择的技术方案在实际应用中可能对被测对象产生影响时，应事先与被测对象进行沟通，并征得被测对象的同意。同时，应制定详细的技术方案，明确测试的范围、方法和工具，并确保测试过程的可控性和可追溯性。

## 5 等级测评要求

### 5.1 检查要求

#### 5.1.1 文档检查

检查人员应检查被测对象的文档，包括系统架构图、网络拓扑图、安全策略、漏洞扫描报告、渗透测试报告等，以了解被测对象的安全状况。



访问规则；

相同的访

术手段和操作的黑客数据,在操作系统的击捕下,实现高性级对度的限制流量。

2) 以文件形

### 5.1.3

#### 5.1.4 配置检查

#### 5.1.5 文件完整性检查

#### 5.1.6 密码检查

### 5.2 系统入侵检测

#### 5.2.1 网络嗅探

网络嗅探的主要目的是通过扫描和监听网络流量,收集、识别网络中非法的设备、病毒程序和木马。

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;

在防止僵尸网络部署网络嗅探器,可以防止准确扫描这些主机和服务器。

### 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:

- a) 对主机及存在潜在漏洞的端口和服务进行识别;
- 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

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:

进行识别,并用于确定渗透性测试的目标;

使用含分离、复制、重叠、乱序和定时技术的工具,并利用工具

在防止僵尸网络部署网络嗅探器,可以防止准确扫描这些主机和服务器。

在防止僵尸网络部署网络嗅探器,可以防止准确扫描这些主机和服务器。

### 扫描

### 5.2.3 漏洞扫描

漏洞扫描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:

进行识别,并用于确定渗透性测试的目标;

使用含分离、复制、重叠、乱序和定时技术的工具,并利用工具

在防止僵尸网络部署网络嗅探器,可以防止准确扫描这些主机和服务器。

在防止僵尸网络部署网络嗅探器,可以防止准确扫描这些主机和服务器。

漏洞扫描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:

进行识别,并用于确定渗透性测试的目标;

使用含分离、复制、重叠、乱序和定时技术的工具,并利用工具

在防止僵尸网络部署网络嗅探器,可以防止准确扫描这些主机和服务器。

在防止僵尸网络部署网络嗅探器,可以防止准确扫描这些主机和服务器。

### 5.2.4 无线扫描

无线扫描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:

进行识别,并用于确定渗透性测试的目标;

使用含分离、复制、重叠、乱序和定时技术的工具,并利用工具

在防止僵尸网络部署网络嗅探器,可以防止准确扫描这些主机和服务器。

在防止僵尸网络部署网络嗅探器,可以防止准确扫描这些主机和服务器。

无线扫描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:

进行识别,并用于确定渗透性测试的目标;

使用含分离、复制、重叠、乱序和定时技术的工具,并利用工具

在防止僵尸网络部署网络嗅探器,可以防止准确扫描这些主机和服务器。

在防止僵尸网络部署网络嗅探器,可以防止准确扫描这些主机和服务器。

无线扫描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:

进行识别,并用于确定渗透性测试的目标;

使用含分离、复制、重叠、乱序和定时技术的工具,并利用工具

在防止僵尸网络部署网络嗅探器,可以防止准确扫描这些主机和服务器。

在防止僵尸网络部署网络嗅探器,可以防止准确扫描这些主机和服务器。

### 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认证过程中通过采用暴力猜测(穷举攻击)、字典攻击等

#### 原理

攻击者利用口令破解工具对口令进行暴力猜测或字典攻击,直到猜中为止。

#### 攻击原理

攻击者通过暴力猜测或字典攻击,直到猜中为止,口令破解成功。

#### 5.3.2 渗透测试

攻击等级保护对象的应用程序、系统或者网

渗透测试的主要功能是通过模拟恶意黑客的攻击方法,攻

#### 攻击原理和攻击类型

的存在。

a) 通过渗透测试评估确认以下漏洞

指令注入

指令注入攻击是指攻击者通过向应用程序输入恶意的指令,导致应用程序执行非预期

漏洞类型漏洞,攻击者通过利用漏洞,攻击者可以获取敏感信息、篡改数据、植入恶意

程序、拒绝服务等攻击,攻击者还可以通过漏洞,攻击者可以获取敏感信息、篡改数据、

#### 原理

攻击者通过利用漏洞,攻击者可以获取敏感信息、篡改数据、植入恶意程序、拒绝服

务、拒绝服务等攻击。

攻击者通过利用漏洞,攻击者可以获取敏感信息、篡改数据、植入恶意程序、拒绝服

务、拒绝服务等攻击。

攻击者通过利用漏洞,攻击者可以获取敏感信息、篡改数据、植入恶意程序、拒绝服

务、拒绝服

务、拒绝服务等攻击。

务、拒绝服务等攻击。

攻击者通过利用漏洞,攻击者可以获取敏感信息、篡改数据、植入恶意程序、拒绝服

务、拒绝服

务、拒绝服务等攻击。

攻击者通过利用漏洞,攻击者可以获取敏感信息、篡改数据、植入恶意程序、拒绝服

务、拒绝服

务、拒绝服务等攻击。

攻击者通过利用漏洞,攻击者可以获取敏感信息、篡改数据、植入恶意程序、拒绝服

务、拒绝服务等攻击。

攻击者通过利用漏洞,攻击者可以获取敏感信息、篡改数据、植入恶意程序、拒绝服

务、拒绝服务等攻击。

攻击者通过利用漏洞,攻击者可以获取敏感信息、篡改数据、植入恶意程序、拒绝服

务、拒绝服务等攻击。

攻击者通过利用漏洞,攻击者可以获取敏感信息、篡改数据、植入恶意程序、拒绝服

务、拒绝服务等攻击。

攻击者通过利用漏洞,攻击者可以获取敏感信息、篡改数据、植入恶意程序、拒绝服

务、拒绝服务等攻击。

攻击者通过利用漏洞,攻击者可以获取敏感信息、篡改数据、植入恶意程序、拒绝服

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

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

附录 A  
(资料性附录)  
测评后活动

A.1 测评结果分析

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:

测评结果分析的主要目标是确定在整个测评中需要立即处理的严重漏洞。

- a) 系统配置策略;
  - a) 缺乏安全基线,同类的系统使用了不一致的安全配置策略;
- b) 系统开发不满足安全要求,甚至未考虑安全要求或系统;
  - b) 在系统开发中忽视对安全性的考虑,如系统架构存在缺陷,如安全技术未能有效地集成至系统中(例如,安全防泄设施、设备配置等);
- c) 系统部署不合理,配置不当,或受到过降额负载;
  - c) 安全事件响应流程不完善,如渗透测试漏洞应急响应;
- d) 对高危漏洞(例如,高危漏洞)未及时采取缓解措施,例如,漏洞修复未及时跟进;
  - d) 缺乏安全基线,同类的系统使用了不一致的安全配置策略;

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) 作为测评对象运营单位评估保护对象满足安全要求而采取改进措施的基准;
  - c) 且提供实施改进措施的安全要求落实反馈;
  - d) 为改进措施保护对象提供全面进行成本效益分析;

### B.1 综述

拟攻击者,利用攻击者常用的工具和技  
相对于单一的漏洞,大多数渗透测试

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,自身系统或者网络的安全功能发动真实的攻击

攻击破坏系统所面对的大体复杂程度

攻击者需要

威胁的其他对策;

可减少系统

渗透攻击的防御也叫做渗透防御

攻击者能够

非常重要的安全测试,测试人员需要丰富的专业知识和技能,尽管有经验的测试

渗透测试是

攻击者能够安全地测试系统,测试人员需要具备高级技能和知识,测试人员

攻击者能够

攻击者能够安全地测试系统,测试人员需要具备高级技能和知识,测试人员

攻击者能够

攻击者能够安全地测试系统,测试人员需要具备高级技能和知识,测试人员

攻击者能够

攻击者能够安全地测试系统,测试人员需要具备高级技能和知识,测试人员

攻击者能够

攻击者能够安全地测试系统,测试人员需要具备高级技能和知识,测试人员

攻击者能够

攻击者能够安全地测试系统,测试人员需要具备高级技能和知识,测试人员

攻击者能够

攻击者能够安全地测试系统,测试人员需要具备高级技能和知识,测试人员

攻击者能够

#### B.2.1 概述

攻击、报告四个阶段,如图 B.1 所示。

渗透测试通常包括规划、发现

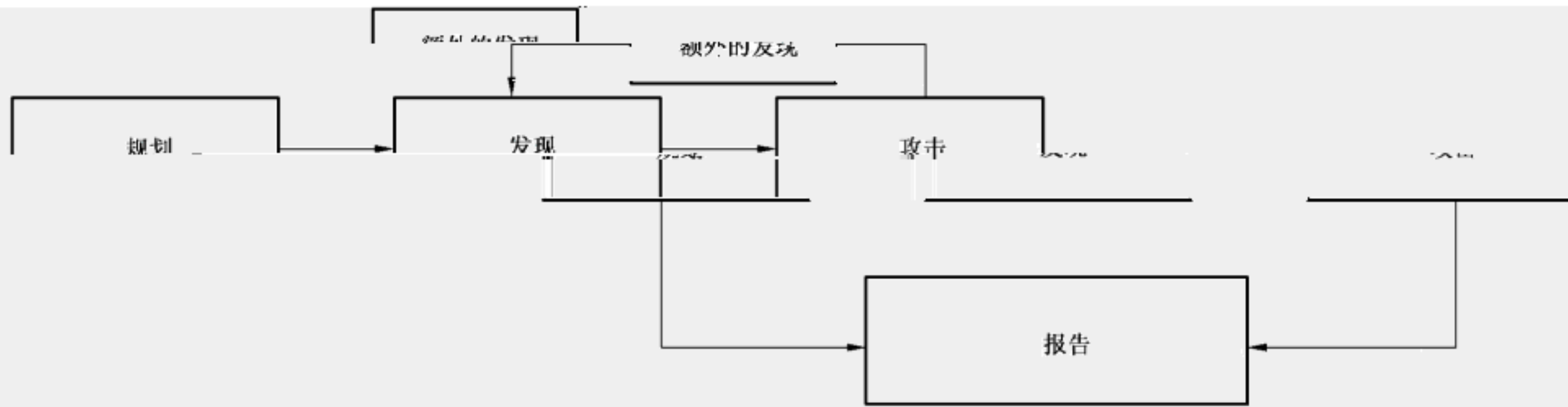


图 B.1 渗透测试

图 B.1 渗透测试

#### B.2.2 规划阶段

案,并设定测试目标。规划阶段为一个成功的渗透  
测试。

在规划阶段,确定规则,管理层审批定稿,记录在案  
测试。

B.2.3 发现阶段

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

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

渗透测试方案宜





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 20271—2006 信息安全技术 网络基础安全技术要求 应用接口
- [4] GB/T 20272—2006 信息安全技术 信息系统安全等级保护基本要求
- [5] GB/T 20273—2006 信息安全技术 信息系统安全等级保护测评要求
- [6] GB/T 20274—2006 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

