ICS 35.040
L 80

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

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:公安部第三研究所、中国信息安全研究院有限公司、上海市信息安全测评认证中心、中国电子技术标准化研究院、中国信息安全认证中心。

本标准主要起草人:张艳、陆臻、杨晨、顾健、徐御、沈亮、俞优、张笑笑、许玉娜、金铭彦、高志新、邹春明、陈妍、胡亚兰、赵戈、毕强、何勇亮、李晨、盛璐禕。

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、报告编制活动四个基本测评活动。本标准为方案编制活动、现场测评活动中涉及的测评技术选择与实施过程提供指导。

网络安全等级保护相关的测评标准主要有 GB/T 22239、GB/T 28448 和 GB/T 28449 等。其中 GB/T 22239 是网络安全等级保护测评的基础性标准，GB/T 28448 针对 GB/T 22239 中的要求，提出了不同网络安全等级的测评要求；GB/T 28449 主要规定了网络安全等级保护测评工作的测评过程。本标准与 GB/T 28448 和 GB/T 28449 的区别在于：GB/T 28448 主要描述了针对各级等级保护对象单元测评的具体测评要求和测评流程，GB/T 28449 则主要对网络安全等级保护测评的活动、工作任务以及每项任务的输入/输出产品等提出指导性建议，不涉及测评中具体的测试方法和技术。本标准对网络安全等级保护测评中的相关测评技术进行明确的分类和定义，系统地归纳并阐述测评的技术方法，概述技术性安全测试和评估的要素，重点关注具体技术的实现功能、原则等，并提出建议供使用，因此本标准在应用于网络安全等级保护测评时可作为对 GB/T 28448 和 GB/T 28449 的补充。

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

本标准给出了网络安全等级保护测评(以下简称“等级测评”)中的相关测评技术的分类和定义,提出了技术性测试评估的要素、原则等,并对测评结果的分析和应用提出建议。

本标准适用于测评机构对网络安全等级保护对象(以下简称“等级保护对象”)开展等级测评工作,以及等级保护对象的主管部门及运营使用单位对等级保护对象安全等级保护状况开展安全评估。

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件。凡是不注日期的引用文件,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

GB/T 25069—2010 信息安全技术 术语

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

通过建立文件校验数据库,计算、存储每一个保留文件的校验,将已存储的校验重新计算以比较当前值和存储值,从而识别文件是否被修改。

3.1.3

网络嗅探 network sniffer

一种监视网络通信、解码协议,并对关注的信息头部和有效载荷进行检查的被动技术,同时也是一种目标识别和分析技术。

3.1.4

规则集 rule set

一种用于比较网络流量或系统活动以决定响应措施(如发送或拒绝一个数据包,创建一个告警,或允许一个系统事件)的规则的集合。

3.1.5

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、设备设施及人员等。