S 35.040 L 80 IC

信息安全技术

网络安全等级保护测试评估技术指

26627—2018 GB/T

Information security technology

g and evaluation technical guide for classified cybersecurity protection

Testing

2018-04-11 发布 2018-11-1 实施

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:邹春明、陈妍、胡亚兰、赵戈、毕强、何勇亮、李晨、盛璐韡。

引　言

[illegible]网络安全等级保护测评活动[illegible]

基本测评活动，本标准为[illegible]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[illegible]的测评过程[illegible]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[illegible]规定了[illegible]各等级保护测评活动[illegible]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[illegible]测评的具体测评要求和测评[illegible]

[illegible]

适用于网络安全等级保护测评时可作为对 GB/T 28448 和 GB/T 28448 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

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。

2 规范性引用文件

[illegible]

[illegible]

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

[illegible] GB 17859—1999 和 GB/T 25069—2010 界定的术语和定义

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

[illegible]

3.1.3

网络嗅探 network sniffer

[illegible]

3.1.4

[illegible]

允许一个系统事件）的规则的集合。

3.1.5

[illegible]

员等。

3.2 缩略语

下列缩略语适用于本文件。

tabase)

CNVD:国家信息安全漏洞共享平台(China National Vulnerability Da

DNS:域名系统(Domain Name System)

el of Service)

DDoS:分布式拒绝服务(Distributed Deni

(ICMP:Internet控制报文协议(Internet Control Message Protocol)

防御系统(Intrusion Prevention System)

IPS:入侵

质访问控制(Media Access Control)

MAC:介

ccm:服务

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成以下二类:

技术。通常采用手动方式,主要包括文档检查、日志检查、规则集检查、系统配置检查、文件完整性检查、密码检查等。

b) 识别和分析技术:识别系统、端口、服务以及潜在安全性漏洞的测评技术。这些技术可以手动描等。

c) 漏洞验证技术:验证漏洞存在性的测评技术。基于检查、目标识别和分析结果,针对性地采取安全漏洞进行验证确认,获得证据。

4.2 技术选择

当选择和确定用于等级测评活动的技术方法时,考虑的因素主要包括但不限于测评对象、测评技术能引入的安全风险,以选择合适的技术方法。

活用性:测评技术对测评对象可

当所选择的技术方法在实施过程中可能对测评对象产生影响时,宜优先考虑对与测评对象的生产的技术方法进行测试,以尽量减少对测评对象业务的影响。

等级测评要求 5

检查技术 5.

和完整性。进行文档检查时，可考虑以下评估要素：

b) 检查安全策略、体系结构和要求、标准作业程序、系统安全计划和授权许可、系统互连的技术规

施与制度文档的一致性；

策略；

5.1.2 日志检查

和修改的历史记录等适当信息，等级保护对象的运营使用单位是否坚持了日志管理策略，并且能

潜在的问题和违反安全策略的情况。进行日志检查时，可考虑以下评估要素：

创建和删除、账户权限分配）以及权限使用等信息；

恶意行为和不恰当使用；

用程序或数据库的使用信

其他事件；

已知漏洞的服务和应用等信息；

，留存时间不少于6个月。

户变更（例如账户

c) IDS/IPS日志，包

d) 防火墙、交换机和

等），以及未授权连接的尝试和不恰当使用；

e) 应用日志，包括未授权的连接尝试、账号变更、权限使用，以及应

息等；

f) 防病毒日志，包括病毒查杀、感染日志，以及升级失败、软件过期等

g) 其他安全日志，如补丁管理等，应记录已

h) 网络运行状态、网络安全事件相关日志

5.1.3 规则集检查

列表、策略集，三级及以上等级保护对象还应包括强制访问

评估要素和评估原则。

备、数据库、操作系统及应用系统的访问控制

控制规则，进行规则集检查时，可考虑以下评

a) 路由访问控制列表。

1) 应采用默认禁止策略；

一致性，系统由多个安全子集应具有一致的主、客体安全标记和

1) 强制访问控制策略应具有

相同访问权限的主体

2) 以文件形式存储和操作的用户数据，在操作系统的支持下，应实现主体属性与数据的强制访问控制；

据，在数据库管理系统的支持下，应实现表/记录/字段

级粒度的强制访问控制；

访问控制的范围，应限定在已定义的主体与客体中。

4) 检查强制

5.1.4 配置检查

是通过检查测评对象的安全策略设置和安全配置文件，评价测评对象安全策

证测评对象安全策略配置与测评对象安全加固策略的符合程度，进行配置检查

路配置的强度，以及检

对，可考虑以下评估要素：

a) 依据安全策略进行加固或配置

c；

b)

c) 用户账号的唯一性标识和口令复杂度设置；

d)

间权限；

e) 合理设置文件访

1) 主要安全总创建主体(如用户)、客体(如数据)的安全标记；

5.1.5 文件完整性检查

可考虑以下评估要素：

a) 采用临行收数字签名等手段保证重要文件的完整性；

b) 采用基准样本与重要文件进行比对的方式，实现重要文件的完整性校验；

c) 采用部署基于主机的 IDS 设备，实现对重要文件完整性破坏的告警。

检查的主要内容已计算评对象由采用密码技术或产品进行安全性检查，进行密码检查时

可考虑以下评估原则：

a)

关规定。

b) 所使用的密钥长度符合等级保护对象行业主管部门的有

5.2 识别和分析技术

5.2.1 网络嗅探

主机对不检查的行为等方面 网络的探针、设备的主要处理对象

口及端口的状态。

d) 在网络边界外部署网络嗅探器，用以评估进出网络的流量；

[redacted]

是否被触发并得到适当的响应；

f) 在 IDS/IPS 后端部署网络嗅探器，用以确定特征码

[redacted]

网络嗅探器，用以验证加密协议的有效性。

h) 在具体网段上部署

5.2.2 网络端口和服务识别

[redacted]

5.2.3 漏洞扫描

功能是针对主机和开放端口识别已知漏洞、提供建议降低漏洞风险；同时，有助于

漏洞扫描的主要

[redacted]

可考虑以下评估要素和评估原则：

[redacted]

等级；

[redacted]

进则评对象故障；

[redacted]

[redacted]

时，可考虑以下评估要求和评估原则：

[redacted]

送包的数目；

[redacted]

[redacted]

技术

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评估过程中通过采用暴力猜测(密码穷举)、字典攻击等技术手段验证数据库、操作系统、应用系统、设备的管理员口令复杂度。进行口令破解时,可考虑以下评估方法和评估原则:

b) 使用混合攻击或暴力破解的方式进行口令破解:混合攻击以字典攻击方法为基础,在字典中增加了数字和符号字符;

d) 使用暴力破解时,可采用分布式执行的方式提高破解的效率。

5.3.2 渗透测试

漏洞的存在:

a) 通过渗透测试评估确认以下漏洞:

1) 系统/服务类漏洞:由于操作系统、数据库、中间件等为应用系统提供服务或支撑的环境……

5.3.3 远程访问测试

集，查看其是否存在漏洞或错误的配置，从而导致非授权的访问。

录 A

料性附录）

评后活动

A.1 测评结果分析

A.2 提出改进建议

（资料性附录）

渗透测试的有关概念说明

B.1 综述

图寻找一组安全漏洞，从而获得更多能够进入系统的机会。渗透测试也可用于确定：

a) 系统对现实世界的攻击模式的容忍度如何；

b) 攻击者需要成功破坏系统所面对的大体复杂程度；

c) 可减少系统威胁的其他对策；

……来安全或系统风险，因此渗透测试应经过深思熟虑和认真规划。……也可降低这种风险。

……打电话询问用户的密码，或者伪……一种非技术攻击手段是通过社会工程学，如伪装成客服坐席人员……技术手段的渗透攻击测试，不在本标准的讨论范围。

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。

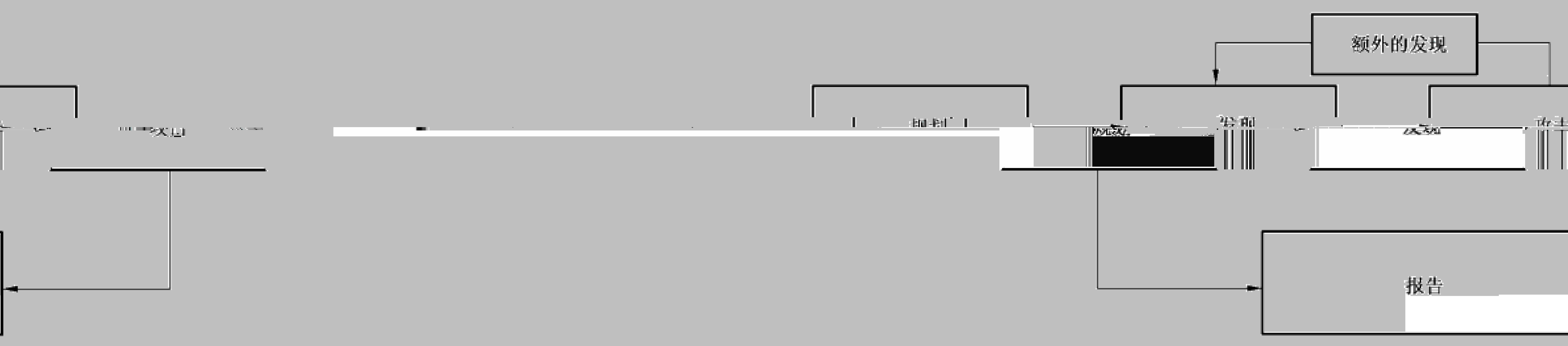

图 B.1 渗透测试的四个阶段

B.2.2 规划阶段

确定规则……在规划阶段……

B.2.3 发现阶段

渗透测试的发现阶段包括两个部分：

[illegible]

[illegible] 通过搜索系统、Web 服务器或目 [illegible]

[illegible]

B.2.4 攻击阶段

[illegible] 执行攻击是渗透测试的核心。攻击阶段是一个通过对原先确定的漏洞进一步探查，进 [illegible]

[illegible]

测试人员可尝试利用另一个已发现的漏洞。如果测试人员能够利用漏洞，[illegible] 定漏洞的攻击被证明行不通 [illegible]

[illegible]

段会利用这些漏洞来确认其存在性。

B.2.5 报告阶段

[illegible]

B.3 渗透测试方案

[illegible]

意行为。由于 [illegible] 陷，渗透测试重现最可能的和最具破坏性的攻击模式，包括最坏的情况，诸如管理员的恶 [illegible]

[illegible] 要考虑到。如果内部和外部测试都要执行，则通常优先执行外部测试。

[illegible]

[illegible] 一个外部攻击，测试人员不知道任何关于目标环境以外 [illegible]

[illegible] 公共网页、新闻页面以及类似的网站收集目标信息，进行综合分析，使用端口 [illegible] 实信息。测试人员可通过 [illegible]

[illegible]

[illegible] 的渗透测试是一个迭代的过程，利用最小的访问权限取得更 [illegible]

内部攻击是模拟组织内部违规操作者的行为。除了测试人员位于内部网络(即防火墙后面)并已

渗透测试对确定一个信息系统的脆弱性以及如果网络受到破坏所可能发生的损害程度非常重要

攻击,可能对网络和系统引入额外的风险,因此

由于渗透测试使用真正的资源并对生产系统和数据进行

测试人员定义渗透测试过程及结果的交流,帮助系统管理员和(或)管

以及攻击者可能利用的攻击方法和攻击途径。

在渗透测试过程中,测试人员通常会利用攻击者常用的攻击

如下安

的负载,占用一定的资源,在极端情况下可能会造成Web服务器宕机或服务停止;

b) 如Web应用程序某功能模块提供对数据库、文件写操作的功能(包括执行Insert、Delete、

Update等命令),且未对该功能模块实施数据有效性校验,验证码机

数据库、文件产生误操作,如在数据库中插入垃圾数据、删除

进行Web漏洞扫描时有可能会对数

记录/文件、修改数据/文件等;

c) 在进行特定漏洞验证时,可能会根

止等风险;

d) 在对Web应用程序/操作系统/数

务器操作系统/数据库出现死机或重启现象。

业务

a) 测试时间,为减轻渗透测试造成的压力和预备风险排除时间,宜尽可能选择访问量不大

进行测试,在非业务运营时间进行测试或在业务运营时间使用非限制技术,以尽

行其余的测试；

用户技术系统且不正常工况系统为正常运行

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 20282—2006 信息安全技术 信息系统安全工程管理要求

[4] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB

3/T 36627—201

3

国 家 标 准

信息安全技术

GB/T 36627—2018

*

网址:www.spc.org.cn

2018 年 9 月第 一版

*

书号：155066 · 1-61231

27-2018

GB/T 366