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—
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。

[illegible]

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

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

3 术语和定义、缩略语

3.1 术语和定义

GB 17859—1999 及 GB/T 250

3.1.1

字典式攻击 dictionary attack

在破解口令时，逐一尝试用户自

3.1.2

文件完整性检查 file integrity

通过建立文件校验数据库，计算

前值和存储值，从而识别文件是否被

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

3.1.4

规则集 rule set

3.1.5

测评对象 target of testing and ev

等级测评过程中不同测评方法作

3.2 缩略语

下列缩略语适用于本文件。

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

DNS:域名系统(Domain Name System)

DDoS:分布式拒绝服务(Distributed Denial of Service)

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

IDS:入侵检测系统(Intrusion Detection Systems)

IPS:入侵防御系统(Intrusion Prevention System)

MAC:介质访问控制(Media Access Control)

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

可用于等级测评的测评技术分成以下三类:

[illegible]

标识别和分析结果[illegible]式、远程访问测试等,对可能存在的[illegible]

c) 漏洞验证技术:验证漏洞存在性的测评技术,[illegible]手动执行或使用自动化的工具,主要包括口令破解、渗透测[illegible]安全漏洞进行验证确认,获得证据。

4.2 技术选择

[illegible]测评对象、测评技术[illegible]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[illegible]适用性、测评技术对测评对象可能引入的安全风险,以选择合适的技术方法。

[illegible]

5 等级测评要求

5.1 检查技术

5.1.1 文档检查

[illegible]文档检查的主要功能是基于等级保[illegible]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[illegible]

和完整性。进行文档检查时，可考虑以下评估要素：

a) 检查对象包括安全策略、体系结构和要求、标准作业程序、系统安全计划和授权许可、系统互连的技术规范、事件响应计划等，确保技术的准确性和完整性；

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、系统互连的技术规范、事件响应计划等文档的完整性，通过检查执行记录和对应表单，确认被测方安全措施的实施与制度文档的一致性；

c) 发现可能导致遗漏或不恰当地实施安全控制措施的缺陷和弱点；

d) 验证测评对象的文档是否与网络安全等级保护标准法规相符合，查找有缺陷或已过时的策略；

e) 文档检查的结果可用于调整其他的测试技术，例如，当口令管理策略规定了最小口令长度和复杂度要求的时候，该信息应可用于配置口令破解工具，以提高口令破解效率。

5.1.2 日志检查

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、设备设施的使用、配置和修改的历史记录等适当信息……

a) 认证服务器或系统日志……

b) 操作系统日志，包括系统和服务的启动、关闭，未授权软件的安装、文件访问、安全策略变更、账户变更（例如账户创建和删除、账户权限分配）以及权限使用等信息；

c) IDS/IPS 日志……

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制措施的漏洞，检查对象包括网络设备、安全设备、数据库、操作系统及应用系统的访问控制列表、策略集，三级及以上等级保护对象还应包括强制访问控制机制。进行规则集检查时，可考虑以下评估要素和评估原则：

a) 路由访问控制列表：

1) 每一条规则都应是有效的（例如，因临时需求而设定的规则，在不需要的时候应立刻移除）；

……

相同的访问规则；

2) [illegible]

3) [illegible]

4) 检查强制访问控制的范围，应限定在已定义的主体与客体中。

5.1.4 配置检查

配置检查的主要功能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略配置的强度，以及验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。进行配置检查时，可考虑以下评估要素：

a) 依据安全策略进行加固或配置；

1) [illegible]

2) [illegible]

3) [illegible]

5.1.5 文件完整性检查

[illegible]

可考虑以下评估要素：

a) [illegible]

b) [illegible]

c) [illegible]

5.1.6 密码检查

密码检查的主要功能是对测评对象中采用的密码技术或产品进行安全性检查。进行密码检查时，可考虑以下评估要素：

a) [illegible]

b) [illegible]

5.2 识别和分析技术

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、未授权和不恰当的行为等信息。进行网络嗅探时，可考虑以下评估要素和评估原则：

a) [illegible]

b) [illegible]

c) [illegible]

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) 在防火墙后端部署网络嗅探器，用以评估准确过滤流量处理规则集；

f) 在网络中部署网络嗅探器，用以评估网络中的流量。

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，并利用工具改变数据包，让数据包融入正常流量中，使数据包避开 IDS/IPS 检测的同时穿越防火墙；

c) 应尽量减少扫描工具对网络运行的干扰，如选择端口扫描的时间。

5.2.3 漏洞扫描

漏洞扫描的主要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，有助于识别过时的软件版本、缺失的补丁和错误配置，并验证其与机构安全策略的一致性。进行漏洞扫描时，

a) 以漏洞相关信息（含漏洞名称、类型、漏洞描述、修复建议等）作为漏洞扫描参考；

b) 通过工具识别结合人工分析的方式来发现漏洞并确认漏洞的风险；

c) 漏洞扫描前，扫描设备应更新升级至最新的漏洞库，以确保能识别最新的漏洞；

d) 依据漏洞扫描工具的漏洞分析原理（如特征库匹配、攻击探测等），谨慎选择扫描策略，防止引起测评对象故障；

e) 使用漏洞扫描设备应对扫描线程数、流量进行限制，以降低测评对测评对象产生的风险。

5.2.4 无线扫描

无线扫描的主要功能是识别被测环境中没有物理连接（如网络电缆或外围电缆）情况下使一个或多个设备实现通信的方式，帮助机构评估、分析无线技术对扫描对象所带来的安全风险，进行无线扫描时，可考虑以下评估要素和评估原则：

a) 使用安装配置无线分析软件的移动设备（如笔记本电脑、手持设备或专业设备）；

b) 基于无线安全配置要求对无线扫描工具进行扫描策略配置，以实现差距分析；

c) 适当配置扫描工具的扫描间隔时间，既能捕获数据包，又能有效地扫描每个频段；

d) 可通过导入平面图或地图，以帮助定位被发现设备的物理位置；

e) 对捕获的数据包进行分析，从而识别扫描范围内发现的潜在的恶意设备和未授权的网络连接模式；

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:

a) 使用字典式攻击方法或采用预先计算好的彩虹表(散列值查找表)进行口令破解尝试;

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等;

c) 如评估对象采用击存盗窃的加密散列函数时,宜使用彩虹表方式进行口令破解尝试;

d) 被测试对象采用了口令破解防护措施时,宜采用绕过口令破解防护措施的方式进行口令破解尝试;

e) 应记录并测试不同复杂度口令的破解所需时间和资源,评估口令复杂度是否符合相关要求;

f) 应检测被测试对象是否对默认口令进行了修改,检测口令更换周期是否合理,评估是否存在弱口令。

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,对评估过程中发现的可利用漏洞进行验证,或通过渗透测试发现被测试对象可能存在的安全漏洞,从而验证被测试对象对于各种攻击方法和攻击等级保护对象的应用程序、系统或者网络的安全功能,以及验证被测试对象对于自身所宣称的安全保护能力的程度是否符合其设计说明书中描述的指标要求。渗透测试是一种评估方法,进行渗透测试时可参考以下评估要求和评估原则:

a) 应在通过漏洞扫描、人工验证等方式对系统的已知漏洞有较为全面的了解并确认系统当前处于可控状态后进行渗透测试;

b) 应对渗透测试过程进行详细记录,包括渗透测试使用的工具、方法、过程、结果和风险等;

c) 应在渗透测试前与被测试对象的相关负责人签订相关协议,规定渗透测试可能带来的风险,以及双方的权利义务等内容;

d) 应在渗透测试过程中对被测试对象采取技术手段保护,避免对业务连续性造成影响,渗透测试结束后应清除测试过程中留下的数据,避免残留数据带来安全问题;

e) 渗透测试人员应具备丰富的经验和较高的技术水平,并了解最新的漏洞和渗透测试技术方法;

f) 渗透测试人员应在授权的范围内开展渗透测试活动,未经授权不得扩大渗透测试范围或者访问未授权的系统或数据;

g) 渗透测试人员不得泄露在测试过程中获取的被测试对象的敏感信息,包括但不限于系统数据、业务数据、个人隐私和商业秘密等。

5.3.3 web应用安全检测

web应用安全检测的主要功能是采用人工检查结合工具测试的方式对web应用程序及其组件(如中间件、开发框架等)进行安全检测,检查web应用程序及其组件是否存在SQL注入、跨站脚本攻击、弱口令、web应用程序及其组件配置不当、web应用程序及其组件存在已知漏洞等问题。

5.3.4 操作系统安全检测

操作系统安全检测的主要功能是采用人工检查结合工具测试的方式对操作系统进行安全检测,检查操作系统是否存在弱口令、权限设置不当、多余无效账户、未及时修补安全漏洞、不必要的服务、默认配置、默认共享、错误的系统审计设置等问题。

5.3.5 数据库安全检测

数据库安全检测的主要功能是采用人工检查结合工具测试的方式对数据库进行安全检测,检查数据库是否存在弱口令、权限设置不当、多余无效账户、未及时修补安全漏洞、不必要的服务、默认配置、默认共享、错误的系统审计设置等问题。

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。进行远程访问测试时，可考虑以下评估要素和评估原则：

a) 发现除 VPN、SSH、远程桌面应用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。通过端口扫描定位经常用于进行远程访问的公开的端口，通过查看运行的进程和安装的应用来手工检测远程访问服务。

c) 检测规则集来查找非法的远程访问路径。评估者应检测远程访问规则集，如 VPN 网关的规则集，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。

d) 测试远程访问认证机制。可尝试默认的账户和密码或暴力攻击（使用社会工程学的方法重设密码来进行访问）或尝试通过密码找回功能机制来重设密码从而获得访问权限。

e) 监视远程访问通信。如未正确实施保护，可泄露用户名和密码等敏感信息。评估者应检测远程访问通信，可以通过网络监视工具来监视这些数据作为远程访问的认证信息或者将这些数据作为远程访问期间发送或接收的数据。

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) [illegible]

b) [illegible]

c) 缺乏安全基准，同类的系统使用了不一致的安全配置策略；

d) 在系统开发中缺乏对安全性的整合，如系统开发不满足安全要求，甚至未考虑[illegible]应用程序代码中存在漏洞；

e) 安全体系结构存在缺陷，如安全技术未能有效地集成至系统中（例如，安全防[illegible]

[illegible]

g) 对最终用户（例如，对网络设备、在线政务等缺乏防范意识，使用非授权无线接入点或对网络系统管理员（例如，缺乏安全维护的人员培训不足；

h) 缺乏安全策略或未执行安全策略，如高级别端口长期开启服务、不安全的协议、非授权主机远程登录等。

A.2 提出改进建议

针对每个测评结果中出现的安全问题，都提出相应的改进建议；改进建议中宜包括问题根源分析结果。改进建议通常包括技术性建议（例如，应用特定的补丁程序）和非技术性建议（例如，更新补丁管理制度）。改进措施的包括：制度修改、流程修改、策略修改、安全体系架构变更、应用新的安全技术以及部署操作系统和应用的补丁程序等。

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) 作为测评对象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) 用以反映等级保护对象安全要求的实现状况；

e) 为改进等级保护对象的安全而进行的成本效益分析；

f) 用来加强其他生命周期活动，如风险评估等；

g) 用来满足网络安全等级保护测评的报告要求。

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、信息系统或者网络的安全功能发动真实的攻击。相对于单一的漏洞，大多数渗透测试试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）一类人员需要成功破坏系统安全所必须的专业复杂程度；

c）可减少系统威胁的其他对策；

d）防御者能够检测攻击并且做出正确反应的能力。

渗透测试是一种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。尽管有经验的测试人员可能知道如何[illegible]，但不能[illegible]。

渗透测试通常[illegible]技术攻击方法[illegible]，一个渗透测试人员可以通过破坏物理安全[illegible]，[illegible]电话给客服[illegible]，大多要求重置密码[illegible]，更多关于物理安全测试、社会工程学技术发展[illegible]，[illegible]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。

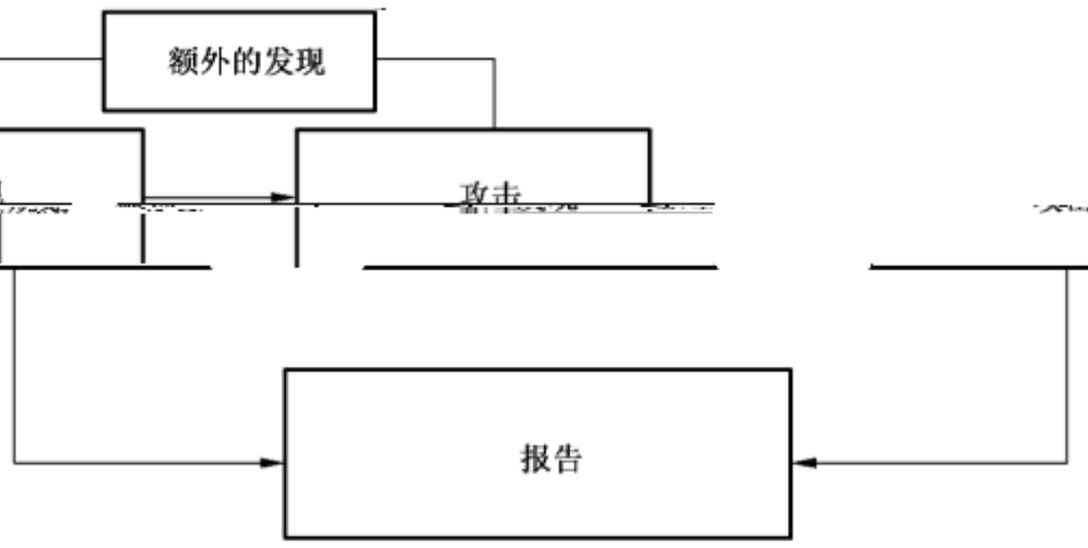

图 B.1　渗透测试的四个阶段

B.2.2　规划阶段

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测试奠定基础，在该阶段不发生实际的测试。

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

B.2.5 报告阶段

渗透测试的报告阶段与其他三个阶段同时进行(见图 B.1)。在规划阶段,将编写测试计划;在发现和攻击阶段,通常是保存测试记录并定期向系统管理员和/或管理部门报告。在测试结束后,报告通常

B.3 渗透测试方案

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缺陷。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,诸如管理员的恶意行为。由于

B.4 渗透测试风险

B.5 渗透测试风险规避

中止渗透测试，并配合用户进行修复处理；在确认问题并恢复系统后，经用户同意方可继续进行其余的测试；

e) 沟通机制：在测试前，宜确定测试人员和用户配合人员的联系方式，用户方宜在测试期间安排专人职守，与测试人员保持沟通，如发生异常情况，可及时响应，测试人员宜在测试结束后要求

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

[5] GB/T 28448—2012 信息安全技术 信息系统安全等级保护测评要求

[6] GB/T 28449—2012 信息安全技术 信息系统安全等级保护测评过程指南

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

GB/T 36627-2018