

信息安全技术

网络安全等级保护测试评估技术

g and evaluation technical guide for classified cybersecurity protection

Testing

2019.04.01 实施

2018.09.17 发布

目 次

III	前言
IV	引言
1	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
2	4 技术分类
2	4.2 技术选择
2	5 等级测评要求
2	5.1 检查技术
2	5.1.1 启动检查
3	5.1.2 日志检查
3	5.1.3 规则集检查
4	5.1.4 配置检查
4	5.2 识别和分析技术
4	5.2.1 网络嗅探
4	5.2.2 网络流量镜像识别
5	5.2.3 漏洞扫描
5	5.2.4 无线扫描
6	5.3 漏洞验证技术
6	5.3.1 口令破解
6	5.3.2 渗透测试
7	5.3.3 远程访问测试
8	附录 A (资料性附录) 测评后活动
9	附录 B (资料性附录) 渗透测试的有关概念说明
13	参考文献



2000 岭山站观测记录表

本标准按照 GB/T 1.1 的规定进行编制。

The following are the names of the people who have been named as suspects in the investigation:

[illegible]

□□。

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

信息安全研究院有限公司、上海市信息安全测评认证中

本标准起草单位:公安部第三研究所、中国

心、中国电子技术标准化研究院、中国信息安全认证中心。

宋妍、胡亚兰、赵戈、毕强、何勇亮、李晨、盛璐祿。

邹春明、陈

引 言

本标准旨在为网络安全等级保护测评活动提供测评技术选择与实施过程指导。

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本标准，GB/T 28448 针对 GB/T 22239 中的要求，给出了具体的测评过程。

本标准在 GB/T 28448 中增加了针对各等级保护项目的要求。

本标准与 GB/T 28448 的差别如下：

本标准与 GB/T 28448 的差别如下：

本标准与 GB/T 28448 的差别如下：

本标准与 GB/T 28448 的差别如下：

本标准与 GB/T 28448 的差别如下：

本标准与 GB/T 28448 的差别如下：

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 and 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。

规范性引用文件

下列文件中的内容通过文中的条款引用而成为本标准的规范性引用文件。

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 25068—2010 信息安全技术 术语

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 25068—2010 信息安全技术 术语

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 25068—2010 信息安全技术 术语

GB/T 25068—2010 信息安全技术 术语

GB/T 25068—2010 信息安全技术 术语

术语和定义、缩略语

3 术语

3.1 术语和定义

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB 17859—1999 计算机信息系统安全保护等级划分准则

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

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB 17859—1999 计算机信息系统安全保护等级划分准则

3.1.3

网络嗅探 network sniffer

一种监听网络通信,解密协议,并对监听到的数据进行分析和处理的技术。同时也是一

种监听网络通信,解密协议,并对监听到的数据进行分析和处理的技术。

3.1.4

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB 17859—1999 计算机信息系统安全保护等级划分准则

允许一个系统事件)的规则集合。

3.1.5

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB 17859—1999 计算机信息系统安全保护等级划分准则

员等。

下列綜收五種田平未立姓

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

DDoS 分布式拒绝服务(Distributed Denial)

$$|A_0| = \frac{7}{8} \sqrt{\frac{g}{\rho}} \left(\frac{H_0}{L_0} \right)^{1/2}, \quad |B_0| = \frac{7}{8} \sqrt{\frac{g}{\rho}} \left(\frac{H_0}{L_0} \right)^{1/2} + T$$

IPS: 入侵

MAC: 介川

CONJ. $\mathcal{A}^{\dagger} \mathcal{B}$

CCTV 朋友

技

松木柱半 松木柱白 5 根 桐木柱度 5 根 桐木柱度 5 根 松木柱度 5 根 松木柱度 5 根 松木柱度 5 根

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。

1b) 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。

[illegible]

当选择和确定用于等级测评活动

适用性 测评技术对测评对象可

当筛选区的技术方法在实施过程中可能对测试对象产生影响时,应优先考虑对与测试对象的产生

的技术方法进行测试,以尽量减少对测试对象业务的影响。

51

5

— — — — — 0.11.15.16

- [illegible]

- ## 策略

.....

1. *As a result of the above, the following is the proposed solution:*

- 创建和删除、账户权限分配)以及权限使用等信息; 户变更(例如账户信息变更、账户权限变更)以及权限使用等信息;

- 恶意行为和不恰当使用； c) IDS/IPS 日志, 包括

- 收由器且主,句坪影响内部设备的连接,如偏置程序,大只,河泄格件

- e) 应用日志,包括未授权的连接尝试、账号变更、权限使用,以及应用等;

- 其他事件：_____ 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

- 已知漏洞的服务和应用等信息;

- h) 网络运行状态、网络安全事件相关日志

● 根据《合伙企业法》第 4 条第 2 款的规定，自然人、法人和其他组织可以成为普通合伙人，但是法律另有规定的除外。

a) 路由访问控制列表

- ### a) 路由访问控制列表

- Figure 1. The effect of the concentration of the *Agrobacterium* suspension on the transformation efficiency of *Agrobacterium* strains.

- as in (1.1)–(1.3). Also, take into account that $\|u\|_{L^2(\mathbb{R}^n)}^2 = \int_{\mathbb{R}^n} |u|^2 dx = \int_{\mathbb{R}^n} |\nabla u|^2 dx = 1$ and $\|u\|_{L^2(\mathbb{R}^n)}^2 = \int_{\mathbb{R}^n} |u|^2 dx = \int_{\mathbb{R}^n} |\nabla u|^2 dx = 1$.

- 1.3 冷却板生肌及解酸佳

- Figure 1. The effect of the initial concentration of the monomer on the polymerization of *l*-lysine. The polymerization was carried out at 40°C for 24 h in the presence of 0.05 mol/L of *l*-lysine and 0.05 mol/L of *l*-phenylalanine. The initial concentration of the monomer was 0.05 mol/L (□), 0.1 mol/L (○), 0.2 mol/L (△), 0.3 mol/L (◇), 0.4 mol/L (▽), 0.5 mol/L (◇), 0.6 mol/L (▽), 0.7 mol/L (◇), 0.8 mol/L (▽), 0.9 mol/L (◇), 1.0 mol/L (▽).

- ⑤ 2000年人口出生率

- 1) 强制访问控制策略应具有

和所有第三方访问；

2) 以数据库形式存储和提供用户数据,在操作系統故障状态下,应实现身份鉴别数据的限制访问;

控制;

2) 以数据库形式存储和操作的用户数据;

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

5.1.1.1 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

配置检查的主要功能

和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

策略配置的强度,以及验

时,可考虑以下评估要素:

a) 依据安全策略进行加固或配置

上;

2) 访问策略是否有效实施和可用;

e) 用户账号的唯一性标识和口令复杂度设置;

3) 用户必须设置并修改 密码及策略

访问权限;

e) 合理设置文件访

1) 安全策略安全是创建文件(如程序)、客体(如数据)的安全标识

安全策略、访问策略和策略实施;

安全策略安全是创建文件(如程序)、客体(如数据)的安全标识

安全策略

5.1.5 文件完整性检查

是指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

可考虑以下评估要素:

a) 采用哈希或数字签名等手段,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

5.1.6 配置检查

配置检查的主要功能是评价测评对象采用配置管理技术或产品进行安全配置

可考虑以下评估原则:

a) 配置检查应采用配置管理技术或产品进行安全配置

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

网络嗅探是指通过在网络接口处捕获数据包,分析数据包内容,获取网络数据

中敏感和不敏感的行为等数据

网络嗅探技术主要用于网络接口处,对网络数据进行捕获、分析和处理

网络嗅探技术主要用于网络接口处,对网络数据进行捕获、分析和处理

1)

网络嗅探技术主要用于网络接口处,对网络数据进行捕获、分析和处理

网络嗅探技术主要用于网络接口处,对网络数据进行捕获、分析和处理

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;

在网络边界内部署网络嗅探器,用以评估进出网络的流量;
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

网络嗅探器,用以验证加密协议的有效性;
h) 在冗余网段上部署网络嗅探器,用以验证冗余网段的有效性;

5.2.2 网络端口和服务识别

网络端口和服务识别是指通过扫描网络主机,识别其开放的端口和运行的服务,并记录其版本和配置信息。网络端口和服务识别是网络安全评估的重要环节,可以帮助安全人员了解网络资产的安全状况,及时发现潜在的安全风险。

网络端口和服务识别的方法有多种,常用的有主动扫描和被动扫描。主动扫描是指通过向目标主机发送探测请求,根据返回的结果来判断端口是否开放和服务是否存在。被动扫描是指通过分析网络流量,识别出正在运行的端口和服务。网络端口和服务识别的工具也有很多,常用的有 Nmap、Wireshark 等。

网络端口和服务识别的结果可以用于安全评估和漏洞扫描。通过识别出的端口和服务,安全人员可以进一步分析其安全状况,发现潜在的安全漏洞。同时,识别出的服务版本和配置信息也可以用于漏洞扫描,帮助安全人员及时发现已知漏洞。

5.2.3 漏洞扫描

漏洞扫描是指通过自动化工具,对网络资产进行安全评估,发现潜在的安全漏洞。漏洞扫描的主要目的是发现网络资产中的安全漏洞,并及时进行修复,以降低安全风险。

漏洞扫描的方法有多种,常用的有基于特征的扫描和基于行为的扫描。基于特征的扫描是指通过匹配已知漏洞的特征码来发现漏洞。基于行为的扫描是指通过分析网络资产的行为模式,发现异常行为,从而发现漏洞。

漏洞扫描的结果可以用于安全评估和漏洞修复。通过扫描出的漏洞,安全人员可以了解网络资产的安全状况,并及时进行修复。同时,扫描出的漏洞也可以用于安全评估,帮助安全人员了解网络资产的安全风险。

漏洞扫描的工具也有很多,常用的有 Nessus、Metasploit 等。漏洞扫描的过程通常包括扫描计划制定、扫描执行、结果分析和报告生成等步骤。

漏洞扫描的结果可以用于安全评估和漏洞修复。通过扫描出的漏洞,安全人员可以了解网络资产的安全状况,并及时进行修复。同时,扫描出的漏洞也可以用于安全评估,帮助安全人员了解网络资产的安全风险。

漏洞扫描的结果可以用于安全评估和漏洞修复。通过扫描出的漏洞,安全人员可以了解网络资产的安全状况,并及时进行修复。同时,扫描出的漏洞也可以用于安全评估,帮助安全人员了解网络资产的安全风险。

漏洞扫描的结果可以用于安全评估和漏洞修复。通过扫描出的漏洞,安全人员可以了解网络资产的安全状况,并及时进行修复。同时,扫描出的漏洞也可以用于安全评估,帮助安全人员了解网络资产的安全风险。

漏洞扫描的结果可以用于安全评估和漏洞修复。通过扫描出的漏洞,安全人员可以了解网络资产的安全状况,并及时进行修复。同时,扫描出的漏洞也可以用于安全评估,帮助安全人员了解网络资产的安全风险。

漏洞扫描的结果可以用于安全评估和漏洞修复。通过扫描出的漏洞,安全人员可以了解网络资产的安全状况,并及时进行修复。同时,扫描出的漏洞也可以用于安全评估,帮助安全人员了解网络资产的安全风险。

漏洞扫描的结果可以用于安全评估和漏洞修复。通过扫描出的漏洞,安全人员可以了解网络资产的安全状况,并及时进行修复。同时,扫描出的漏洞也可以用于安全评估,帮助安全人员了解网络资产的安全风险。

漏洞扫描的结果可以用于安全评估和漏洞修复。通过扫描出的漏洞,安全人员可以了解网络资产的安全状况,并及时进行修复。同时,扫描出的漏洞也可以用于安全评估,帮助安全人员了解网络资产的安全风险。

漏洞扫描的结果可以用于安全评估和漏洞修复。通过扫描出的漏洞,安全人员可以了解网络资产的安全状况,并及时进行修复。同时,扫描出的漏洞也可以用于安全评估,帮助安全人员了解网络资产的安全风险。

漏洞扫描的结果可以用于安全评估和漏洞修复。通过扫描出的漏洞,安全人员可以了解网络资产的安全状况,并及时进行修复。同时,扫描出的漏洞也可以用于安全评估,帮助安全人员了解网络资产的安全风险。

漏洞扫描的结果可以用于安全评估和漏洞修复。通过扫描出的漏洞,安全人员可以了解网络资产的安全状况,并及时进行修复。同时,扫描出的漏洞也可以用于安全评估,帮助安全人员了解网络资产的安全风险。

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使用暴力猜测(密码穷举)、字典攻击等技术手段验证口令复杂度。进行口令破解时,可考虑以下评估方法和评估原则:

- a) 使用暴力破解的方式对口令进行破解;混合攻击以字典攻击方法为基础,在字典中增加自定义的口令字典;
- b) 使用混合攻击或暴力破解的方式对口令进行破解;字典攻击以暴力破解为基础,在暴力破解中增加自定义的口令字典;
- c) 使用暴力破解的方式对口令进行破解;暴力破解以字典攻击为基础,在字典中增加自定义的口令字典;
- d) 使用混合攻击的方式对口令进行破解;混合攻击以暴力破解为基础,在暴力破解中增加自定义的口令字典;

5.3.2 渗透测试

- a) 通过渗透测试评估确认以下漏洞的存在:
- 1) 系统/设备漏洞:由于操作系统、数据库、中间件软件、应用系统组件服务或专接的设备
- b) 通过渗透测试评估确认以下漏洞的存在:
- 1) 系统/设备漏洞:由于操作系统、数据库、中间件软件、应用系统组件服务或专接的设备

5.3.3 远程访问测试

测试时，可参考图 5-3-1 远程登录和远程执行。

- 1) 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开放的端口，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。

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。

则

他如想查看设备配置和策略访问策略。

设备未进行任何配置，则设备配置策略是空。

地保障，则可利用。

3) 监视远程访问通信。可以通过网络抓包器监视远程访问通信，如用嗅探卡。

料性附录)	附
评后活动	(资 测

A.1 测评结果分析

测评结果分析的主要目的是确定测评发现的问题,并对其进行分类、分析和处理。分析发现的问题时,应结合被测对象的实际情况,考虑问题的严重性、影响范围、发生频率等因素,对问题进行定性或定量分析。对于发现的问题,应根据问题的性质和严重程度,采取相应的整改措施。对于严重的问题,应立即采取措施进行整改;对于一般的问题,可以根据实际情况,制定整改计划,并在规定的时间内完成整改。整改完成后,应进行复查,确保问题得到有效解决。此外,还应定期对测评结果进行分析,总结经验教训,提高测评工作的质量和效率。

1) 威胁模型:威胁模型是安全策略的重要组成部分,用于识别和分析系统面临的威胁。在测评过程中,应检查威胁模型是否完整、准确,是否能够覆盖系统面临的所有威胁。如果威胁模型存在缺陷,应对其进行补充和修正。

2) 安全策略:安全策略是指导系统安全工作的纲领性文件,用于规定系统的安全目标、原则和措施。在测评过程中,应检查安全策略是否明确、具体,是否能够指导系统的安全工作。如果安全策略存在缺陷,应对其进行修订和完善。

3) 安全措施:安全措施是用于防止、检测和响应安全事件的具体措施。在测评过程中,应检查安全措施是否有效、可靠,是否能够防止安全事件的发生。如果安全措施存在缺陷,应对其进行改进和优化。

4) 应急响应:应急响应是用于处理安全事件的流程和方法。在测评过程中,应检查应急响应流程是否清晰、可行,是否能够及时、有效地处理安全事件。如果应急响应流程存在缺陷,应对其进行修订和完善。

5) 安全培训:安全培训是提高员工安全意识、技能和知识的重要途径。在测评过程中,应检查安全培训是否定期开展,是否能够提高员工的安全意识和技能。如果安全培训存在缺陷,应对其进行改进和优化。

6) 安全审计:安全审计是用于检查系统安全状况的重要手段。在测评过程中,应检查安全审计是否定期进行,是否能够及时发现系统的安全问题。如果安全审计存在缺陷,应对其进行改进和优化。

7) 安全评估:安全评估是用于评估系统安全状况的重要手段。在测评过程中,应检查安全评估是否定期进行,是否能够及时发现系统的安全问题。如果安全评估存在缺陷,应对其进行改进和优化。

8) 安全维护:安全维护是用于保持系统安全状况的重要手段。在测评过程中,应检查安全维护是否定期进行,是否能够及时发现系统的安全问题。如果安全维护存在缺陷,应对其进行改进和优化。

9) 安全改进:安全改进是用于提高系统安全水平的重要手段。在测评过程中,应检查安全改进是否定期进行,是否能够及时发现系统的安全问题。如果安全改进存在缺陷,应对其进行改进和优化。

10) 安全记录:安全记录是用于记录系统安全状况的重要手段。在测评过程中,应检查安全记录是否定期进行,是否能够及时发现系统的安全问题。如果安全记录存在缺陷,应对其进行改进和优化。

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、改进措施、改进责任人、改进时限等。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,更新补丁管理政策、改进措施的包干、制度修订、流程修订、政策修订、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软件补丁和库等)。

改进建议应具体、可行,能够指导被测对象进行整改。改进建议应明确改进措施、改进责任人、改进时限等,以便于被测对象进行整改。改进建议应定期进行跟踪和评估,确保问题得到有效解决。此外,还应定期对改进建议进行总结和分析,总结经验教训,提高改进工作的质量和效率。

1) 作为实施改进措施的参考;

2) 作为评估改进措施效果的依据;

3) 作为改进措施实施情况的记录;

4) 作为改进措施实施情况的报告;

5) 作为改进措施实施情况的总结;

6) 作为改进措施实施情况的评估;

7) 作为改进措施实施情况的反馈;

8) 作为改进措施实施情况的改进;

9) 作为改进措施实施情况的优化;

10) 作为改进措施实施情况的完善。

B.2.3 发现阶段

渗透测试的发现阶段包括两个部分：

- 信息收集。信息收集是渗透测试的第一步，信息收集包括收集目标系统的基本信息，如域名、IP地址、端口、操作系统、服务等。信息收集可以通过多种方式进行，如搜索引擎、网络扫描、社会工程学等。
- 漏洞扫描。漏洞扫描是发现阶段的一个重要部分，它通过自动化工具扫描目标系统，寻找已知漏洞。漏洞扫描可以分为主动扫描和被动扫描。主动扫描是通过发送特定的数据包来探测漏洞，而被动扫描则是通过分析网络流量来发现漏洞。

B.2.4 攻击阶段

攻击阶段是渗透测试的核心，它是指利用发现的漏洞对目标系统发起攻击。攻击阶段可以分为两个部分：一是漏洞利用，二是数据窃取。漏洞利用是指通过利用漏洞来执行恶意代码，从而获得对目标系统的控制权。数据窃取是指通过利用漏洞来窃取目标系统中的敏感信息，如用户名、密码、信用卡号等。攻击阶段的目标是证明目标系统存在安全漏洞，并评估这些漏洞对系统安全的影响。

B.2.5 报告阶段

报告阶段是渗透测试的最后一步，它是指将测试的结果整理成报告，并提交给目标系统的所有者。报告应该包括测试的范围、测试的方法、发现的漏洞、漏洞的严重性、以及修复建议。报告的目的是让目标系统的所有者了解系统的安全状况，并采取相应的措施来修复漏洞。

B.3 渗透测试方案

渗透测试方案是指为进行渗透测试而制定的详细计划。方案应该包括测试的目标、测试的范围、测试的方法、测试的时间表、以及测试的人员。方案的目的是确保测试能够按照计划进行，并达到预期的目标。方案还应该包括风险评估，以评估测试过程中可能遇到的风险，并制定相应的应对措施。此外，方案还应该包括测试结果的报告，以便目标系统的所有者能够及时了解测试的结果，并采取相应的措施来修复漏洞。

中部分工具模拟组织内部违规操作者的行为,除了测试工具位于内部网络(即内网环境),并且

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

内部已开发了解测试进度。

是它重视渗透测试过程及结果的交流,帮助系统管理者和(或)系统所有者了解系统脆弱性,以及攻击者可能利用的攻击方法和攻击途径。

4.2 渗透测试目标

实施非破坏性测试系统和数据危害性。

在渗透测试过程中,测试工具通常会对系统资源使用非破坏性

非破坏性测试工具,测试工具通常会对系统资源使用非破坏性

测试工具,测试工具通常会对系统资源使用非破坏性

全风险:

如下安

在使系统漏洞扫描工具进行漏洞扫描时,可能会对 Web 服务器及 Web 应用程序带来一定

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、

制、访问控制等措施,则在

Update 等命令),且未对该功能模块实施数据有效性校验,验证逻辑

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,可能会根据

止等风险;

d) 在对 Web 应用程序/操作系统/数据

据库等进行口令暴力破解时,可能触发其设置的安全机制,

导致 Web 应用程序/操作系统/数据库的某些功能暂时无法使用。

在渗透测试过程中,测试工具通常会对系统资源使用非破坏性

务器操作系统/数据库出现死机或重启现象。

4.3 渗透测试工具与设备

4.3.1 渗透测试工具

渗透测试工具是指用于发现系统漏洞、验证漏洞、利用漏洞的工具。

渗透测试工

渗透测试工具是指用于发现系统漏洞、验证漏洞、利用漏洞的工具。

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太

使用,避免造成系统性能下降,影响业务运行。

渗透测试工具是指用于发现系统漏洞、验证漏洞、利用漏洞的工具。

在渗透测试过程中,测试工具通常会对系统资源使用非破坏性

量减少对生产

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

避免对系统造成不可逆的损失;

在渗透测试过程中,测试工具通常会对系统资源使用非破坏性

在渗透测试过程中,测试工具通常会对系统资源使用非破坏性

渗透测试工具是指用于发现系统漏洞、验证漏洞、利用漏洞的工具。

在渗透测试过程中,测试工具通常会对系统资源使用非破坏性

25

行其余的测试；

一旦检测到系统不正常，以确保系统的正常运行，应进行故障排除。

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

安全工程管理体系要求

[3] GB/T 20282—2006 信息安全技术 信息系统

信息安全等级保护基本要求

[4] GB/T 22239 信息安全技术 信

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

GB

GB/T 36627—2018

中华人民共和国
国家标准

信息安全技术

GB/T 36627—2018

*

中国标准出版社出版发行

北京市西城区百万庄大街24号 邮政编码 100037

网址: www.spc.org.cn

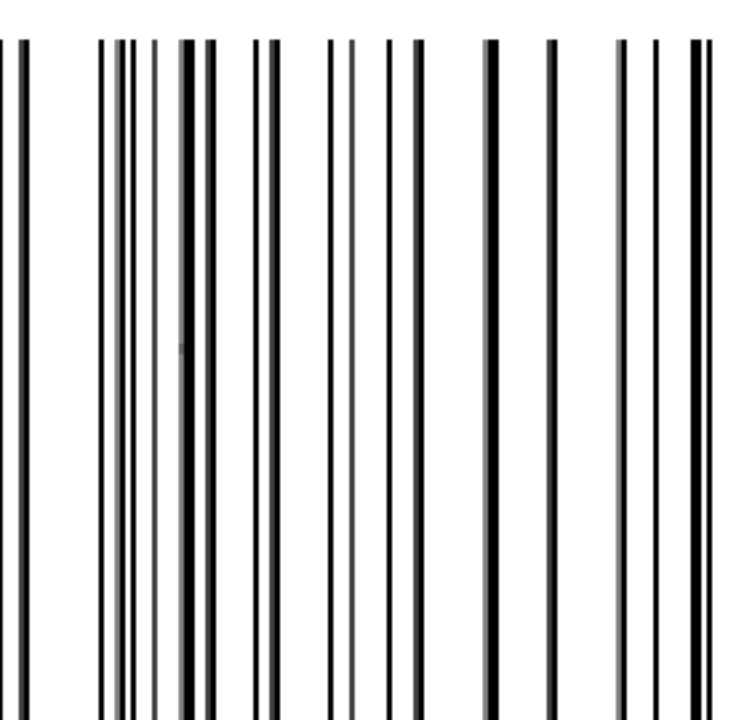
发行热线: (010) 66116007

2018年9月第一版

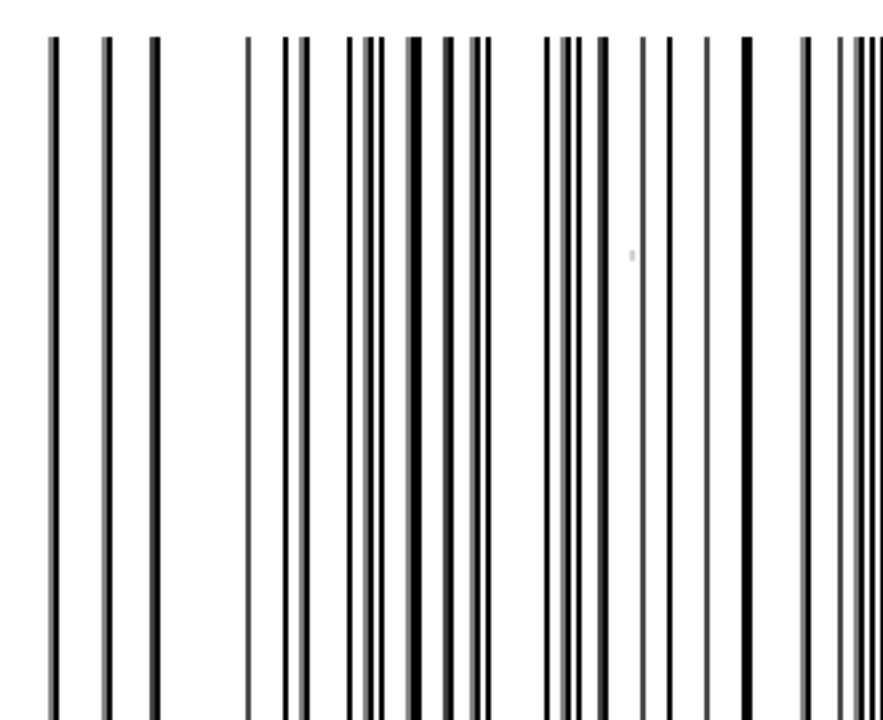
*

书号: 155066 · 1-61231

版权专有 侵权必究



27-2018



GB/T 366