

信息安全技术

网络安全等级保护测评技术

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
1	3.1 术语和定义
2	4 技术分类
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 检查技术
2	5.1.1 启动准备
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	5.1.5 文件完整性检查
4	6 密码检查
4	5.2 识别和分析技术
4	5.2.1 网络嗅探
4	5.2.2 网络流量异常检测
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



本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准与 GB 35271—2017 相比，除结构调整和个别条款作必要修改外，主要技术内容保持不变。

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。

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。

本标准主要起草人：宋妍、胡亚兰、赵戈、毕强、何勇亮、李晨、盛璐祯。

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。

GB/T 28448 主要规定了网络安全等级保护测评的要求。

GB/T 28449 主要规定了网络安全等级保护的测评要求。

GB/T 28449 则主要对网络安全等级保护的测评活动、工作任务等。

本标准主要规定了网络安全等级保护的测评要求。

本标准主要规定了网络安全等级保护的测评要求。

本标准主要规定了网络安全等级保护的测评要求。

本标准主要规定了网络安全等级保护的测评要求。

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规范性引用而构成本标准必不可少的部分。

注:凡是注日期的引用文件,其随后所有的修改单均不适用于本标准。

注:凡是未注日期的引用文件,其最新版本适用于本标准。

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/T 25068—2010 信息安全技术 术语

术语和定义、缩略语

3 术语和定义

3.1 术语和定义

3.1.1 字典式攻击

字典式攻击 (dictionary attack) 是一种攻击方式,攻击者使用预先准备好的字典,尝试破解密码。

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

3.1.2 网络嗅探

网络嗅探 (network sniffing) 是一种攻击方式,攻击者通过嗅探网络通信,获取敏感信息。

注:网络嗅探通常用于窃取网络通信中的敏感信息,如密码、密钥等。

注:网络嗅探通常用于窃取网络通信中的敏感信息,如密码、密钥等。

3.1.3

网络嗅探 network sniffer

一种监视网络通信,解密协议,并对攻击者感兴趣的通信数据进行分析和处理的技术。

3.1.4

注:本标准中,“系统活动”是指系统运行过程中产生的所有事件,包括登录、操作、退出等。

允许一个系统事件)的规则集合。

3.1.5

注:本标准中,“系统活动”是指系统运行过程中产生的所有事件,包括登录、操作、退出等。

注:本标准中,“系统活动”是指系统运行过程中产生的所有事件,包括登录、操作、退出等。

注:本标准中,“系统活动”是指系统运行过程中产生的所有事件,包括登录、操作、退出等。

员等。

— — — — — 0.11.15.16

- Figure 1. The effect of the number of trials on the number of correct responses. The number of correct responses was plotted against the number of trials for each participant. The number of correct responses increased with the number of trials, and the increase was more pronounced for the high-ability group than for the low-ability group.

- ## 策略

.....

1. *As a result of the above, the following is the proposed new text for the first sentence of the first paragraph of Article 10 of the Convention:*

- 应当使用： c) IDS/IPS 日志，包括

- 及由器具主、句坪影响内部迭久的虫注该移、加便只程序、本只、记进、修、

- c) 应用目录,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

- 已知漏洞的服务和应用等信息; eg) 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

● 銀河、於赤道角區區外沿每點各溫

a) 路由访问控制列表

- Figure 1. The effect of the number of trials on the number of correct responses. The number of correct responses was significantly higher for the 10 trials condition than for the 5 trials condition. Error bars represent the standard error of the mean.

- ### 1.3 培养微生物的常用培养基

- 1) “成果, 沉默, 禁止”策略:

- © 2000 Blackwell Science Ltd

- 1) 强制访问控制策略应具有

中国医药出版社

[illegible]

控制:

据左新据库管理系统的支持下, 应守理主/记录, 字段

2) 以新掘坑形式存储和掘作的用户数:

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) 検査強制:

2016 10 16 11:11 習題檢本

是通过对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

附帶檢查的主要功能

评测对象安全策略配置与评测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,以及驗

时,可考虑以下评估要素:

4.8

c) 依据安全策略进行加固或配置

27. 六万格位器与法定的联系

c) 用户账号的唯一性标识和口令复杂度设置;

將 耶和華頭的面具除收 將聖父的面具除

同权限；

e) 合理设置文件访

1) 主系统安全是创建主体(如用户)、客体(如数据)的安全标记

[illegible]

5.1.5 文件完整性檢查

可考慮以下評估要素：

④ 采用哈希或数字签名等手段,保证重要文件的完整性。

b) 采用其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

[illegible]

密网检测的主要功能是对检测对象由聚网检测网技术或产品进行安全检测。进行密网检测时

可考慮以下評估原則：

[illegible]

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

[illegible][illegible]

群在《红楼梦》中却如死信。其死信的死法与平常的死法迥然不同。

1. $\int_0^1 \frac{1}{x^2} dx = -\frac{1}{x} \Big|_0^1 = -1 - (-\infty) = \infty$

[illegible]

論文 基于溫路亞紋和熵紋取名的新規則的已知紋組規則

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;
g) 在冗余网络段上部署网络嗅探器,用以验证加密协议的有效性

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正在运行的服务。网络端口和服务识别是网络安全评估的重要组成部分,可以帮助安全人员了解网络主机的配置和状态,发现潜在的安全漏洞。

网络端口和服务识别可以通过多种方式进行,包括手动扫描和自动扫描。手动扫描通常使用网络扫描工具,如 Nmap,来识别网络主机的开放端口和正在运行的服务。自动扫描通常使用网络扫描工具,如 Nessus,来识别网络主机的开放端口和正在运行的服务。网络端口和服务识别的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。

5.2.3 漏洞扫描

漏洞扫描是指通过自动化工具,对网络主机进行扫描,发现潜在的安全漏洞。漏洞扫描的主要目的是发现网络主机上的安全漏洞,评估漏洞的严重性,并采取相应的安全措施。漏洞扫描可以分为主动扫描和被动扫描。主动扫描是指通过向网络主机发送请求,来发现潜在的安全漏洞。被动扫描是指通过监听网络流量,来发现潜在的安全漏洞。

漏洞扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。

漏洞扫描可以通过多种方式进行,包括手动扫描和自动扫描。手动扫描通常使用漏洞扫描工具,如 Nessus,来识别网络主机上的安全漏洞。自动扫描通常使用漏洞扫描工具,如 Nessus,来识别网络主机上的安全漏洞。漏洞扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。

等级;

漏洞扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。漏洞扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。漏洞扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。

漏洞扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。

5.2.4 无线扫描

无线扫描是指通过无线方式,对网络主机进行扫描,发现潜在的安全漏洞。无线扫描的主要目的是发现网络主机上的安全漏洞,评估漏洞的严重性,并采取相应的安全措施。无线扫描可以分为主动扫描和被动扫描。主动扫描是指通过向网络主机发送无线请求,来发现潜在的安全漏洞。被动扫描是指通过监听无线流量,来发现潜在的安全漏洞。

无线扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。

无线扫描可以通过多种方式进行,包括手动扫描和自动扫描。手动扫描通常使用无线扫描工具,如 Aircrack-ng,来识别网络主机上的安全漏洞。自动扫描通常使用无线扫描工具,如 Aircrack-ng,来识别网络主机上的安全漏洞。无线扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。

发送包的数目;

无线扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。无线扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。无线扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。

无线扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。

无线扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。无线扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。无线扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。

无线扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。

模式;

无线扫描的结果可以用于评估网络主机的安全性,发现潜在的安全漏洞,并采取相应的安全措施。

5.3 漏洞验证技术

5.3.1 口令破解

正数。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,在字典中增加系统默认口令和简单口令;
- b) 使用混合攻击或暴力破解的方式对口令进行破解;字典攻击以系统默认口令为基础,在字典中增加系统默认口令和简单口令;
- c) 使用暴力破解的方式对口令进行破解;暴力攻击以系统默认口令为基础,在字典中增加系统默认口令和简单口令;
- d) 使用暴力破解的方式对口令进行破解;暴力攻击以系统默认口令为基础,在字典中增加系统默认口令和简单口令;

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:
- b) 通过渗透测试评估确认以下漏洞的存在:
- c) 通过渗透测试评估确认以下漏洞的存在:
- d) 通过渗透测试评估确认以下漏洞的存在:
- e) 通过渗透测试评估确认以下漏洞的存在:
- f) 通过渗透测试评估确认以下漏洞的存在:
- g) 通过渗透测试评估确认以下漏洞的存在:
- h) 通过渗透测试评估确认以下漏洞的存在:
- i) 通过渗透测试评估确认以下漏洞的存在:
- j) 通过渗透测试评估确认以下漏洞的存在:
- k) 通过渗透测试评估确认以下漏洞的存在:
- l) 通过渗透测试评估确认以下漏洞的存在:
- m) 通过渗透测试评估确认以下漏洞的存在:
- n) 通过渗透测试评估确认以下漏洞的存在:
- o) 通过渗透测试评估确认以下漏洞的存在:
- p) 通过渗透测试评估确认以下漏洞的存在:
- q) 通过渗透测试评估确认以下漏洞的存在:
- r) 通过渗透测试评估确认以下漏洞的存在:
- s) 通过渗透测试评估确认以下漏洞的存在:
- t) 通过渗透测试评估确认以下漏洞的存在:
- u) 通过渗透测试评估确认以下漏洞的存在:
- v) 通过渗透测试评估确认以下漏洞的存在:
- w) 通过渗透测试评估确认以下漏洞的存在:
- x) 通过渗透测试评估确认以下漏洞的存在:
- y) 通过渗透测试评估确认以下漏洞的存在:
- z) 通过渗透测试评估确认以下漏洞的存在:

5.3.3 远程访问测试

测试时，可参考图 5-3-1 远程登录和远程桌面。

- 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) 监视远程连接通信。可以通过网络抓包器监视远程连接通信，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,应进行验证,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) 威胁管理策略的有效性分析。威胁管理策略的有效性分析,主要是对威胁管理策略的覆盖范围、及时性、有效性等方面进行评估。例如,威胁管理策略是否覆盖了所有可能的威胁源,是否及时发现了新的威胁,是否有效地阻止了威胁的扩散等。通过分析,可以了解威胁管理策略的优缺点,为改进策略提供依据。

2) 应急响应策略的有效性分析。应急响应策略的有效性分析,主要是对应急响应策略的响应时间、处理流程、人员配备等方面进行评估。例如,应急响应策略是否规定了明确的响应时间,是否建立了完善的处理流程,是否配备了足够的人员等。通过分析,可以了解应急响应策略的优缺点,为改进策略提供依据。

3) 安全事件应急响应策略的有效性分析。安全事件应急响应策略的有效性分析,主要是对安全事件应急响应策略的响应时间、处理流程、人员配备等方面进行评估。例如,安全事件应急响应策略是否规定了明确的响应时间,是否建立了完善的处理流程,是否配备了足够的人员等。通过分析,可以了解安全事件应急响应策略的优缺点,为改进策略提供依据。

4) 安全事件应急响应策略的有效性分析。安全事件应急响应策略的有效性分析,主要是对安全事件应急响应策略的响应时间、处理流程、人员配备等方面进行评估。例如,安全事件应急响应策略是否规定了明确的响应时间,是否建立了完善的处理流程,是否配备了足够的人员等。通过分析,可以了解安全事件应急响应策略的优缺点,为改进策略提供依据。

A.2 提出改进建议

针对每个测评结果中出现的的安全问题,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,更新补丁管理策略、改进策略的包、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软件补丁和库等)。

以下几个方面:

a) 作为实施改进措施的参考;

b) 作为改进措施实施过程中的安全风险评估的参考;

附录 B

(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) 可减小系统威胁的其他对策。

安全威胁和风险。因此,渗透测试应经过深思熟虑和认真规划。

它可降低这种风险,但不

模型,攻击者可能使用多种攻击手段。

攻击者可能使用多种攻击手段,包括:

攻击者可能使用多种攻击手段,包括:

攻击者可能使用多种攻击手段,包括:

攻击者可能使用多种攻击手段,包括:

攻击者可能使用多种攻击手段,包括:

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。

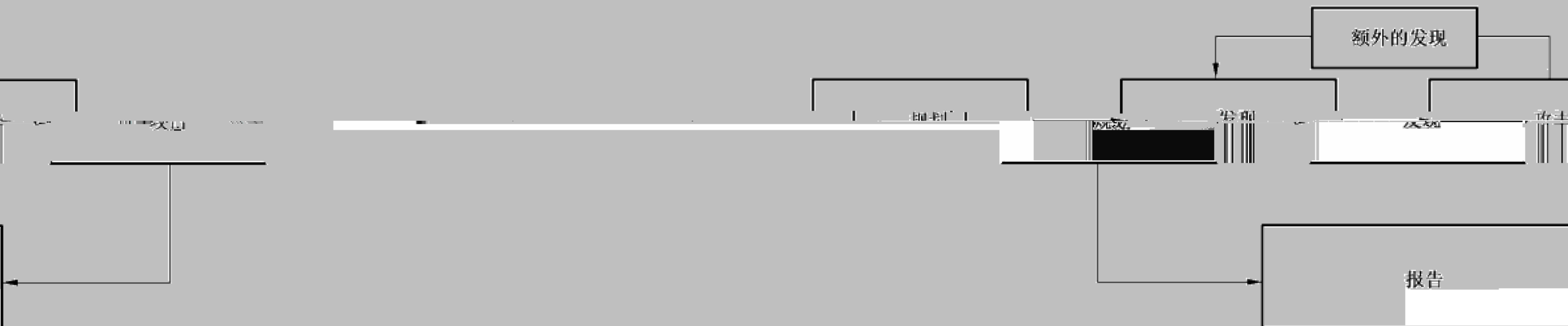


图 B.1 渗透测试的四个阶段

B.2.2 规划阶段

确定规则,确定攻击范围,记录攻击,并记录测试目标。规划阶段为:攻击者的渗透

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]

二、利用网络监听等各种方法获取主机名和地址信息

通过服务器获得系统内部用户姓名,联系王武策。

[illegible][illegible]

B.2.4 攻击阶段

Figure 1. The proposed system architecture.

DOI: 10.1002/for

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，定漏洞的攻击被证明行不通

Figure 1. The location of the study area in the north-east of Iran. The map shows the location of the study area in the north-east of Iran, with a scale bar indicating distances up to 100 km. The map also shows the location of the study area in the north-east of Iran, with a scale bar indicating distances up to 100 km.

R 25 招生聯席

B.3 渗透测试方案

意行为。由于 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

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。

Figure 1. The effect of the number of trials on the mean number of correct responses for the 100 trials condition. The number of correct responses was significantly higher than the number of incorrect responses for all conditions. Error bars represent the standard error of the mean.

[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,使用端口扫描工具对目标主机进行端口扫描,发现开放的端口,从而获得主机的系统信息。测试人员可通过

[illegible]

Figure 1. The proposed model for the development of the self-regulation of learning.

士的访问

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,帮助系统管理员和(或管理

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,测试工具通常会对受攻击者常用工具是

1. 由于信息系统存在某些特定安全漏洞时可能会产生

的风险,从而会对被测试系统带来安全风险,有些测试工

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 漏洞扫描时有可能会对数

记录/文件、修改数据/文件等;

该漏洞的特性对主机或 Web 应用程序造成宕机、服务停

c) 在进行特定漏洞验证时,可能会根据

止等风险;

数据库等进行口令暴力破解时,可能触发其设置的安全机制,

d) 在对 Web 应用程序/操作系统/数据

导致 Web 应用程序、操作系统、数据库的某些被破坏,暂时无法使用。

在测试过程中,测试工具可能会对系统/数据造成一定程度的破坏,测试结束后可能会导致系统/数据

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,通常分为手工工具和自动化工具。

手工工具

手工工具是指由测试人员手动操作的工具,通常用于发现漏洞、验证漏洞、利用漏洞。

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,测试结束后应及时清理测试数据,防止数据泄露。

1) 测试结束后,应及时清理测试数据,防止数据泄露。

在测试过程中,测试人员应严格遵守测试规范,不得擅自扩大测试范围,不得擅自使用高危工具。

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。

测试过程中,测试人员应严格遵守测试规范,不得擅自扩大测试范围,不得擅自使用高危工具。

在测试过程中,测试人员应严格遵守测试规范,不得擅自扩大测试范围,不得擅自使用高危工具。

渗透测试工具与设备

在测试过程中,测试人员应严格遵守测试规范,不得擅自扩大测试范围,不得擅自使用高危工具。

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

安全工程管理要求

信息系统安全等级保护基本要求

GB/T 20269—2006 信息安全技术 信息系统安全管理要求

[3] GB/T 20282—2006 信息安全技术 信息系统

[4] GB/T 22239 信息安全技术 信

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

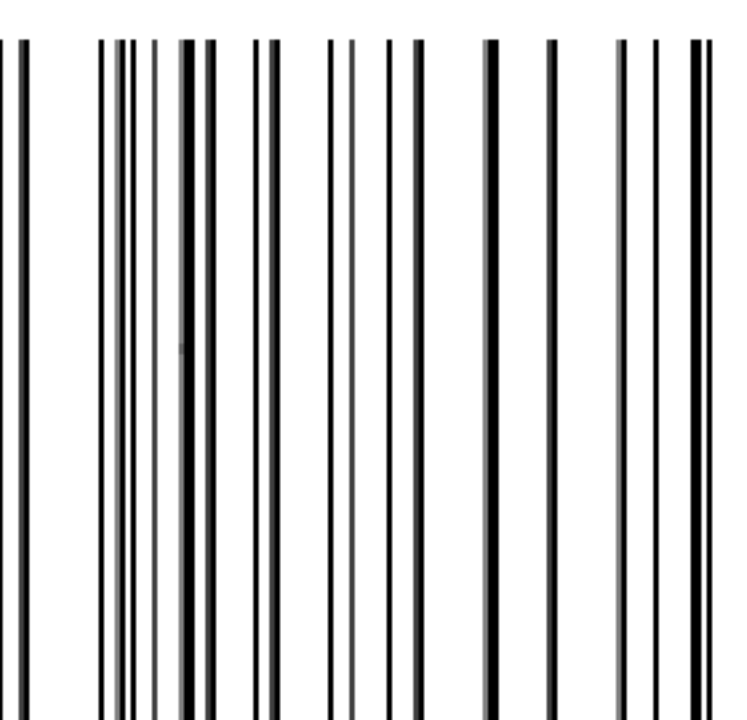
发行热线: (010) 66116007

2018年9月第一版

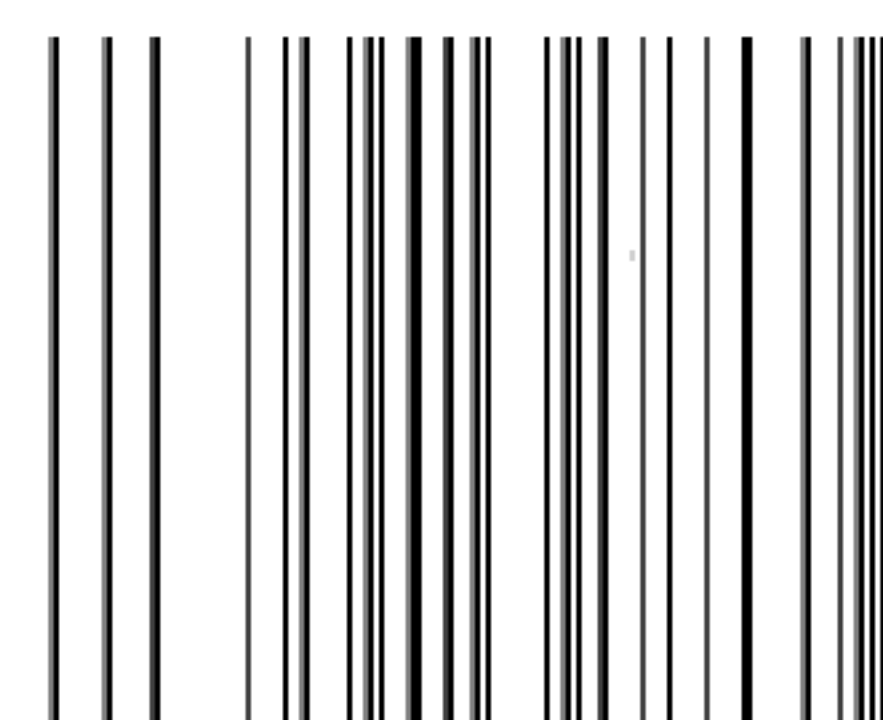
*

书号: 155066 · 1-61231

版权专有 侵权必究



27-2018



GB/T 366