

ICS 35.040



1. 30

国 国 家 标 准

GB/T 36627—2018

中 华 人 民 共 和

全 技 术 制 试 评 估 技 术 指 南

technology—
classified cybersecurity protection

信 息 安 全 网 络 安 全 等 级 保 护 测

Information security
Testing and evaluation technical guide for

2019-04-01 实施

2018-09-17 发布

理 总 局
委 员 会 发 布

国 家 市 场 监 督 管 理
中 国 国 家 标 准 化 管 理

目 次

前言	III
引言	IV
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	1
3.2 缩略语	2
4 概述	2
4.1 技术分类	2
4.2 技术选择	2
4.3 等级划分要求	2
5 测试方法	2
5.1 静态检查	2
5.1.1 源代码检查	2
5.1.2 规则集检查	2
5.1.3 配置检查	2
5.1.4 文件完整性检查	2
5.1.5 漏洞检查	2
5.2 识别即分析技术	2
5.2.1 网络嗅探	2
5.2.2 网络端口和服务识别	2
5.2.3 漏洞扫描	2
5.2.4 无线扫描	2
5.3 漏洞验证技术	2
5.3.1 口令破解	2
5.3.2 渗透测试	2
5.3.3 远程访问测试	2
附录A(资料性附录) 测评活动	2
附录B(资料性附录) 渗透测试的有关概念说明	2
参考文献	2

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。

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

GB/T 36627—2018《网络安全等级保护测评过程规范》与GB 17848—2018《GB 17848—2018》的要求一致。

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

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。下列文件对于本

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 36627—2018 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负载进行过滤和记录的技术。

3.1.4

规则集 rule set

用于检测系统安全漏洞的一组规则集合。

3.1.5

测试和评估

测评对象 target of testing

测评作用的对象,主要涉及相关信息系统、配套制度文档、设备设施及人员等。

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

可田干笨级测诬的测诬技术分成以下二米：(一)测诬：笨级测诬分为笨级测诬和笨级测诬二种；

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

1. *Journal of the American Medical Association*, 1997; 277: 103-107.

Figure 1. The proposed model of the relationship between the variables.

姓名: 王 强 学号: 123456789 院系: 计算机科学与技术学院 专业: 计算机科学与技术 年级: 2020级 指导教师: 张 明 教授

Figure 1

(2) 漏洞防治技术: 漏洞漏洞存在的治理技术, 基于探查、识别漏洞分析结果, 针对性地采取

Figure 1. The structure of the proposed model.

安全培训进行验证确认, 并取得证据

4.2 技术选择

制定与实施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、当选择和确

对测评对象可能引入的安全风险,以选择合适的技术方法——应用性、测评技

三、所選擇的技術方案與實施計劃可能面臨的障礙及這些障礙對留校非全職學生與

系统相同,则系统运行正常;系统运行不正常,则系统运行不正常。

《中国书画函授大学肇庆分校建校二十周年纪念册》

[illegible]

测评要求 5 等级

5.1 检查技术

档案检查

名检查的主要功能是对其策略保护对象运营单位提供的文档、评价其策略和规则的技术基础并

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、事件响应计划等文档的完整性,通过检查执行

记录和相关表单,确认被测方安全措施的实施

的缺陷和弱点;

的文档是否满足网络安全等级保护标准、法规和符合性要求;在检查过程中,应记录发现的缺陷或已验证的

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

杂度要求时,该信息应可用于配置口令破解工具,以提高口令破解效率。

d) 验证被测对象的

策略;

e) 文档检查的结果

杂度要求时

5.1.2 日志检查

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

日志检查的主要功能

的信息,并验证被测对象的运营使用单位是否坚持记录安全管理策略,并能够发现

和修改的历史记录等活

策略变更记录

5) 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

户变更(例如账号创建和删除、账号权限分配、账号授权使用等信息)

a) IDS/IPS日志,包括恶意行为和异常使用

等,以便及时发现异常行为和异常使用

等,以便及时发现异常行为和异常使用

等,以便及时发现异常行为和异常使用

等,以便及时发现异常行为和异常使用

等,以便及时发现异常行为和异常使用

等,以便及时发现异常行为和异常使用

等,以便及时发现异常行为和异常使用

等,以便及时发现异常行为和异常使用

5.1.3 规则集检查

制措施的有效性,检查对象包括网络设备、安全数

第三级及以上等级保护对象还应包括数据库、

评估规则

主而定义的规则,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

规则集的有效性,在不需要的情况下应删除

相同的访问规则；

3) 对于非正常存储和操作的系统数据,在操作系统的支持下,应实现文件级精度的强制访问

控制;

4) 应支持将强制访问控制策略与操作系统的安全策略管理系统的安全策略实现集成;

5) 应实现强制访问控制;

6) 检查强制访问控制策略应用,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;
- b) 对于提供网络服务和应用,应实现强制访问控制;
- c) 用户账号的唯一性标识和口令复杂度设置;
- d) 在配置策略中应实现强制访问控制策略。

应实现强制访问控制,应实现强制访问控制;

应实现强制访问控制;

应实现强制访问控制,应实现强制访问控制;

应实现强制访问控制,应实现强制访问控制;

应实现强制访问控制,应实现强制访问控制;

应实现强制访问控制,应实现强制访问控制。

文件完整性检查

5.1.5 文件完整性检查

文件完整性检查的主要功能是通过检查测评对象中重要文件的完整性,评价测评对象中重要文件的完整性。

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;

应实现强制访问控制,应实现强制访问控制;

应实现强制访问控制,应实现强制访问控制;

5.1.6 密码检查

产品进行安全性检查。进行密码检查时,

密码检查的主要功能是对测评对象中采用的密码技术或密码策略进行评价。进行密码检查时,可考虑以下评估原则:

- a) 所提供的密码算法相关功能符合国家密码主管部门的要求;
- b) 所提供的密码算法符合国家密码主管部门的要求。

5.2 识别和分析技术

5.2.1 网络嗅探

,收集、识别网络中活动的设备、操作系统和协议、

考虑以下评估要素和评估原则:

应实现强制访问控制,应实现强制访问控制;

应实现强制访问控制,应实现强制访问控制;

应实现强制访问控制,应实现强制访问控制;

应实现强制访问控制,应实现强制访问控制;

网络嗅探的主要功能是通过捕捉和重放网络流量,识别网络中活动的设备、操作系统和协议、

考虑以下评估要素和评估原则:

应实现强制访问控制,应实现强制访问控制;

应实现强制访问控制,应实现强制访问控制;

应实现强制访问控制,应实现强制访问控制;

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) 在网络边界处部署网络嗅探器,用以评估进出网络的流量;

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) 应识别最新的漏洞;
- b) 应识别最新的漏洞;
- c) 应识别最新的漏洞;
- d) 应识别最新的漏洞;
- e) 应识别最新的漏洞;
- f) 应识别最新的漏洞;
- g) 应识别最新的漏洞;
- h) 应识别最新的漏洞;
- i) 应识别最新的漏洞;
- j) 应识别最新的漏洞;
- k) 应识别最新的漏洞;
- l) 应识别最新的漏洞;
- m) 应识别最新的漏洞;
- n) 应识别最新的漏洞;
- o) 应识别最新的漏洞;
- p) 应识别最新的漏洞;
- q) 应识别最新的漏洞;
- r) 应识别最新的漏洞;
- s) 应识别最新的漏洞;
- t) 应识别最新的漏洞;
- u) 应识别最新的漏洞;
- v) 应识别最新的漏洞;
- w) 应识别最新的漏洞;
- x) 应识别最新的漏洞;
- y) 应识别最新的漏洞;
- z) 应识别最新的漏洞;

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

环境带来的安全风险。进行无线扫描时,

- a) 应识别最新的漏洞;
- b) 应识别最新的漏洞;
- c) 应识别最新的漏洞;
- d) 应识别最新的漏洞;
- e) 应识别最新的漏洞;
- f) 应识别最新的漏洞;
- g) 应识别最新的漏洞;
- h) 应识别最新的漏洞;
- i) 应识别最新的漏洞;
- j) 应识别最新的漏洞;
- k) 应识别最新的漏洞;
- l) 应识别最新的漏洞;
- m) 应识别最新的漏洞;
- n) 应识别最新的漏洞;
- o) 应识别最新的漏洞;
- p) 应识别最新的漏洞;
- q) 应识别最新的漏洞;
- r) 应识别最新的漏洞;
- s) 应识别最新的漏洞;
- t) 应识别最新的漏洞;
- u) 应识别最新的漏洞;
- v) 应识别最新的漏洞;
- w) 应识别最新的漏洞;
- x) 应识别最新的漏洞;
- y) 应识别最新的漏洞;
- z) 应识别最新的漏洞;

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

加了数字和特殊字符;

如采用双字攻击方法时,应同时考虑双字攻击的字典;

不宜使用彩虹表方式进行口令破解尝试;

c) 如测评对象采用带有盐值的哈希散列函数时,应

采用暴力破解的方式进行口令破解尝试;

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,攻击等级保护对象的应用程序、系统或者网络的安全功能,从而验证测评对象弱点、技术缺陷或漏洞的一种评估方法。进行渗透测试时,可考虑以下评估要素和评估原则:

- a) 通过渗透测试评估确认以下漏洞的存在:

1) 系统/服务类漏洞。由于操作系统、数据库、中间件等为用户系统提供服务或支撑的环境,

系统/服务类漏洞通常是指操作系统、数据库、中间件等存在的安全漏洞,如操作系统漏洞、数据库漏洞、中间件漏洞等。系统/服务类漏洞通常是指操作系统、数据库、中间件等存在的安全漏洞,如操作系统漏洞、数据库漏洞、中间件漏洞等。

2) 应用代码类漏洞。由于开发人员编写代码不规范或缺少必要的校验措施,导致应用系统存在安全漏洞,包括SQL注入、跨站脚本、任意文件上传等漏洞。攻击者利用这些漏洞,

可以

3) 权限类漏洞。由于对数据访问、功能操作访问控制规则不严或存在缺陷,攻击者可非授权访问这些数据及功能模块。权限类漏洞通常可分为越权访问或平行越权访问。越权访问是指低权限用户非授权访问高权限用户的功能模块或数据信息;平行越权访问是指攻击者利用自身权限的功能模块,非授权访问或操作他人的数据信息。

4) 配置不当类漏洞。由于未对配置文件进行安全加固,或使用默认配置或配置不合理,导致存在安全漏洞。如中间件配置支持HTTP方法,可能暴露攻击者利用HTTP方法上传文件。

5) 信息泄露类漏洞。由于系统未对重要数据及信息进行必要的保护,导致攻击者可

6) 业务逻辑缺陷类漏洞。由于程序逻辑存在缺陷或逻辑太复杂,导致

7) 业务逻辑缺陷类漏洞。由于程序逻辑存在缺陷或逻辑太复杂,导致

6) 相关内容参见附录B。

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。

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:

- [illegible]

A.2 提出改进建议

[illegible]

A3 報告

报告。测试结果可用于在测试结果全部完成之后,产生或包含系统安全问题的漏洞及其改进建议的,且可应用于:

- 作为实施改进措施的参考；
- b) 确定改进措施是否纠正确认的漏洞；
- c) 作为对评价对象运营单位实施改进措施对新满足安全要求而采取改进措施的依据；
- d) 用以对同等级别评价对象安全要求的实施状况；
- e) 对改进措施体系对安全而进行的有效性进行验证；
- f) 用来证明其他生命周期要求，如风险管理等；
- g) 用来证明评价对象安全改进措施的有效性。

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) 系统对现实世界攻击措施的脆弱度如何;
- 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;
- d) 防御者能够检测攻击并且做出正确反应的能力。

丰富的专业知识和技能。尽管有经验的测试

渗透测试是一种非常重要的安全测试,测试人员需要

就这些边界条件和约束进行探索。

只要求降低这种风险,但不能完全避免风险,某些渗透测试

渗透测试人员可以绕过安全防护机制的。

渗透测试通常包括非技术攻击方法。例如,一个渗透

测试人员可能通过社会工程学手段获取信息,或者通过物理手段进入系统。

在测试过程中,测试人员可能会发现新的漏洞,或者发现系统已经存在的安全漏洞。

渗透测试通常包括非技术攻击方法。例如,一个渗透测试人员可能会通过社会工程学手段获取信息,或者通过物理手段进入系统。

在测试过程中,测试人员可能会发现新的漏洞,或者发现系统已经存在的安全漏洞。

渗透测试通常包括非技术攻击方法。例如,一个渗透测试人员可能会通过社会工程学手段获取信息,或者通过物理手段进入系统。

在测试过程中,测试人员可能会发现新的漏洞,或者发现系统已经存在的安全漏洞。

B.2 渗透测试阶段

B.2.1 概述

规划、发现、攻击、报告四个阶段,如图 B.1 所示。

渗透测试通常包括

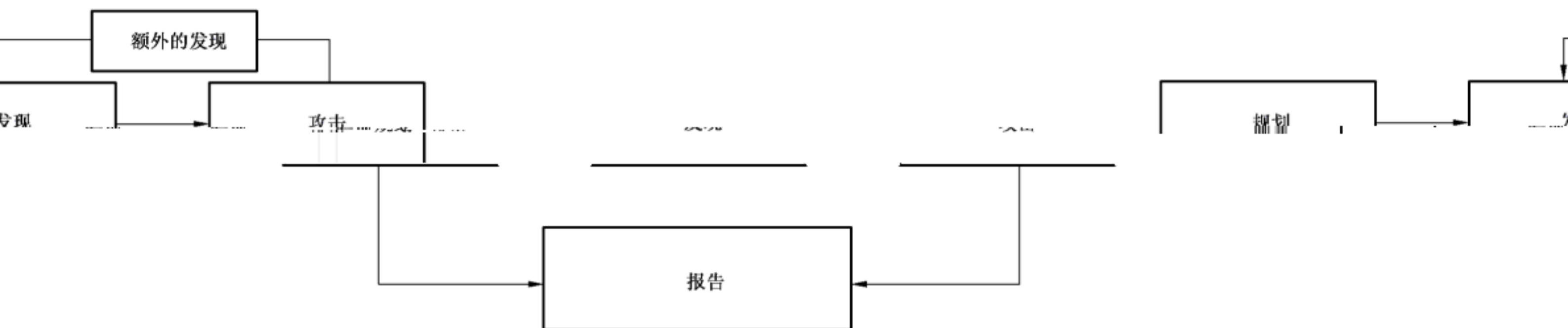


图 B.1 渗透测试的四个阶段

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：

第三部分是实验测试设计。首先,包括信息收集和整理、网络端口和服务标识、进行潜在目标识别。然后,对目标地址进行探测和验证。最后,对目标地址进行攻击。

5) 通过 DNS、Whois、NetWhois 等工具和网络监听等

数据库系统、操作系统、编译系统、解释系统、语言处理系统、数据库系统、操作系统、编译系统、解释系统、语言处理系统

4. 通过搭建“N2O108”校企合作平台,围绕企业需求,校企共同培养人才,共同开展技术研发,共同进行成果转化。

4. 在“数据”菜单下，选择“数据有效性”，在弹出的“数据有效性”对话框中，选择“数据源”选项卡，在“数据源”列表框中，单击“数据源”按钮，在弹出的“数据源”对话框中，选择“数据源”列表框中的“数据源”，单击“确定”按钮，完成数据源的设置。

第三部分是應用社會分析, 其中包括終端掃描器、下載的服務、應用程

行对比。测试人员可以使用他们自己的数据集,或者 CNYC 等公共数据集。

B.2.4 攻击阶段

根据《岩土工程勘察规范》(GB 50021-2001)第 10.2.2 条规定,土体渗透系数 k 的确定应符合下列规定:

能够减轻相关的贸易摩擦。

飛天牌香煙 上海煙草公司出品 每包 10 支 售價 0.50 元

资料来源：根据《中国统计年鉴》、《中国农村统计年鉴》和《中国人口统计年鉴》有关数据整理。

[关于《中国好声音》第二季选手被搜身事件的声明](#)

的表示,我虽以各不通,测试人员却连续测试另一个也发现的漏洞。如果测试人员能够发现漏洞漏洞!

[illegible]

《中国书画函授大学肇庆分校建校二十周年纪念册》

1573031 致会刊用这些漏洞来骗钱

B.2.5 报告阶段

与北航一个实验室团队合作(见图 15)，在规划阶段，将新实验计划，在发现

[illegible]

Figure 1

B.3 渗透测试方案

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

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。由于陷,渗透测试重现最可

2019年12月10日

要緊的——就是常常去讀《武備要略》和《孫子兵法》。

大部分工作是靠回忆完成的。我想起的歌词有六句，能记得上次组织唱的歌有三首，所知的歌子有八首。

第三个外部攻击测试人员不知道任何关于书籍和发送外的信息,特别是 IP 地址或地址,使用 IP 地址或地址

在站前广场的南端设置公共绿地，而公共绿地南端设置公共绿地，

Figure 1 The effect of the number of nodes on the performance of the proposed algorithm.

Figure 1. The relationship between the number of species and the number of genera in the studied communities.

Downloaded from <http://ajphaphysocpharm.sagepub.com/> at 11:01 11 November 2014

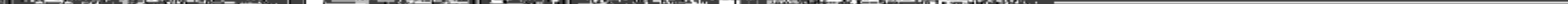
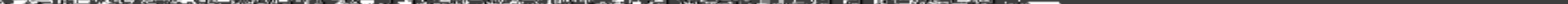
[illegible]

在病毒肆虐肆虐之际，网络系统的安全问题也日益突出。网络系统的安全问题，不仅关系到企业的正常运营，也关系到国家的安全。因此，企业必须采取有效的措施，加强网络系统的安全防护。首先，企业应建立完善的安全管理制度，明确安全责任，规范操作流程。其次，企业应加强员工的安全意识教育，提高员工的安全防范能力。最后，企业应定期对网络系统进行安全检查和漏洞扫描，及时发现和修复安全隐患。只有这样，才能有效保障网络系统的安全，确保企业的正常运营。

1. 2019年12月31日，本公司在途待运商品金额为1,000,000.00元，其中：

B.4 渗透测试风险

用安眠药作自杀工具的时间多选择在睡前和起床时。因此，在睡前和起床时，应特别注意病人的情况，如发现有异常表现，应立即报告医生，以便及时处理。

[illegible][illegible]

1. 2017年12月31日，甲公司“应付账款”科目所属各明细科目期末贷方余额如下表所示：

应付账款明细科目	期末贷方余额（元）
应付账款—A公司	100,000
应付账款—B公司	200,000
应付账款—C公司	300,000
应付账款—D公司	400,000
应付账款—E公司	500,000
应付账款—F公司	600,000
应付账款—G公司	700,000
应付账款—H公司	800,000
应付账款—I公司	900,000
应付账款—J公司	1,000,000
应付账款—K公司	1,100,000
应付账款—L公司	1,200,000
应付账款—M公司	1,300,000
应付账款—N公司	1,400,000
应付账款—O公司	1,500,000
应付账款—P公司	1,600,000
应付账款—Q公司	1,700,000
应付账款—R公司	1,800,000
应付账款—S公司	1,900,000
应付账款—T公司	2,000,000
应付账款—U公司	2,100,000
应付账款—V公司	2,200,000
应付账款—W公司	2,300,000
应付账款—X公司	2,400,000
应付账款—Y公司	2,500,000
应付账款—Z公司	2,600,000
应付账款—A公司	2,700,000
应付账款—B公司	2,800,000
应付账款—C公司	2,900,000
应付账款—D公司	3,000,000
应付账款—E公司	3,100,000
应付账款—F公司	3,200,000
应付账款—G公司	3,300,000
应付账款—H公司	3,400,000
应付账款—I公司	3,500,000
应付账款—J公司	3,600,000
应付账款—K公司	3,700,000
应付账款—L公司	3,800,000
应付账款—M公司	3,900,000
应付账款—N公司	4,000,000
应付账款—O公司	4,100,000
应付账款—P公司	4,200,000
应付账款—Q公司	4,300,000
应付账款—R公司	4,400,000
应付账款—S公司	4,500,000
应付账款—T公司	4,600,000
应付账款—U公司	4,700,000
应付账款—V公司	4,800,000
应付账款—W公司	4,900,000
应付账款—X公司	5,000,000
应付账款—Y公司	5,100,000
应付账款—Z公司	5,200,000
应付账款—A公司	5,300,000
应付账款—B公司	5,400,000
应付账款—C公司	5,500,000
应付账款—D公司	5,600,000
应付账款—E公司	5,700,000
应付账款—F公司	5,800,000
应付账款—G公司	5,900,000
应付账款—H公司	6,000,000
应付账款—I公司	6,100,000
应付账款—J公司	6,200,000
应付账款—K公司	6,300,000
应付账款—L公司	6,400,000
应付账款—M公司	6,500,000
应付账款—N公司	6,600,000
应付账款—O公司	6,700,000
应付账款—P公司	6,800,000
应付账款—Q公司	6,900,000
应付账款—R公司	7,000,000
应付账款—S公司	7,100,000
应付账款—T公司	7,200,000
应付账款—U公司	7,300,000
应付账款—V公司	7,400,000
应付账款—W公司	7,500,000
应付账款—X公司	7,600,000
应付账款—Y公司	7,700,000
应付账款—Z公司	7,800,000
应付账款—A公司	7,900,000
应付账款—B公司	8,000,000
应付账款—C公司	8,100,000
应付账款—D公司	8,200,000
应付账款—E公司	8,300,000
应付账款—F公司	8,400,000
应付账款—G公司	8,500,000
应付账款—H公司	8,600,000
应付账款—I公司	8,700,000
应付账款—J公司	8,800,000
应付账款—K公司	8,900,000
应付账款—L公司	9,000,000
应付账款—M公司	9,100,000
应付账款—N公司	9,200,000
应付账款—O公司	9,300,000
应付账款—P公司	9,400,000
应付账款—Q公司	9,500,000
应付账款—R公司	9,600,000
应付账款—S公司	9,700,000
应付账款—T公司	9,800,000
应付账款—U公司	9,900,000
应付账款—V公司	10,000,000
应付账款—W公司	10,100,000
应付账款—X公司	10,200,000
应付账款—Y公司	10,300,000
应付账款—Z公司	10,400,000
应付账款—A公司	10,500,000
应付账款—B公司	10,600,000
应付账款—C公司	10,700,000
应付账款—D公司	10,800,000
应付账款—E公司	10,900,000
应付账款—F公司	11,000,000
应付账款—G公司	11,100,000
应付账款—H公司	11,200,000
应付账款—I公司	11,300,000
应付账款—J公司	11,400,000
应付账款—K公司	11,500,000
应付账款—L公司	11,600,000
应付账款—M公司	11,700,000
应付账款—N公司	11,800,000
应付账款—O公司	11,900,000
应付账款—P公司	12,000,000
应付账款—Q公司	12,100,000
应付账款—R	

[illegible]

● 中国古语有言：君子不重，则威仪折矣。意思是说，一个人如果不够庄重，那么他的威严和仪态就会折损。这句话强调了庄重的重要性，认为它是个人修养和威仪的基础。只有做到庄重，才能展现出真正的威严和仪态。

B.5 渗透测试风险规避

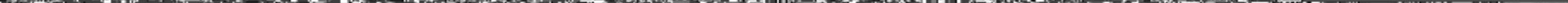
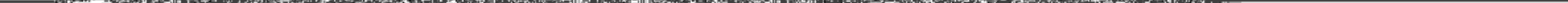
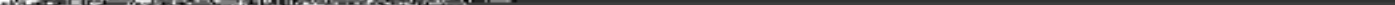


Figure 1



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负责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

用户检查系统是否异常,以确保系统的正常运行。

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

~~GB/T 20282—2006 信息安全技术 信息系统安全工程实施要求~~ [3] GB

~~GB/T 28289—信息安全技术—信息系统安全等级保护基本要求~~ [4] GB

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

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

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

版权专有 侵权必究



GB/T 36627-2018