<<信息安全漏洞分析基础>>

图书基本信息

书名：<<信息安全漏洞分析基础>>

13位ISBN编号：9787030368324

10位ISBN编号：7030368320

出版时间：2013-4

出版时间：科学出版社

<<信息安全漏洞分析基础>>

内容概要

《信息安全漏洞分析基础》共分三部分，第1部分为理论篇，主要介绍漏洞分析理论研究基础，内容包括漏洞的定义及产生、漏洞的状态及预测、漏洞的发展等；第2部分为方法技术篇，主要介绍漏洞分析的工作内容及方法，内容包括漏洞发现、漏洞发布、漏洞修复、漏洞预防；第3部分为管理篇，主要介绍漏洞分析管理工作的机制、模式及手段，从法律法规、基础设施、市场等方面，总结国内外漏洞分析管理工作的现状及存在的问题，并对漏洞市场的管理方式进行了有益的探索，最后从漏洞标识、漏洞补丁、漏洞信息等几方面总结和分析了国内外漏洞管理标准规范并提出了漏洞分析的准则框架。

《信息安全漏洞分析基础》可作为信息安全从业人员、黑客技术发烧友的参考指南，也可作为信息安全专业的研究生或本科生的指导用书。

<<信息安全漏洞分析基础>>

书籍目录

第1部分理论篇 第1章漏洞的定义 1.1漏洞的概念 1.1.1基于访问控制 1.1.2基于状态空间 1.1.3基于安全策略 1.1.4基于信息安全风险管理 1.2本书的定义 参考文献 第2章漏洞的产生 2.1漏洞的产生 2.1.1技术角度 2.1.2经济角度 2.1.3应用环境角度 2.1.4漏洞的产生条件 2.2漏洞的类型 2.2.1典型的漏洞分类方法 2.2.2典型漏洞库及其分类 参考文献 第3章漏洞的状态 3.1生命周期理论模型 3.2生命周期经验模型 3.3漏洞生态系统模型 3.3.1漏洞生态系统模型简介 3.3.2漏洞生态系统模型主要生态链条 3.3.3漏洞客体、主体及环境间的相互关系 3.3.4漏洞生态系统模型的形式化描述及分析 参考文献 第4章漏洞的预测 4.1静态分析与预测 4.1.I预测指标 4.1.2数据分析 4.1.3漏洞继承性假设 4.1.4漏洞微观参数模型 4.2动态分析与预测 4.2.1热力学模型 4.2.2对数泊松模型 4.2.3二次模型 4.2.4指数模型 4.2.5逻辑模型 4.2.6线性模型 4.2.7多周期模型 4.2.8工作量模型 4.2.9模型拟合度的分析与验证 4.3预测模型的应用 4.3.1应用方法 4.3.2长期预测 4.3.3短期预测 4.3.4技术展望 参考文献 第5章漏洞的发展 5.1漏洞发展特点分析 5.1.1漏洞数量 5.1.2漏洞分布 5.1.3漏洞危害级别 5.1.4漏洞利用 5.1.5漏洞修复 5.1.6 2010年度重要漏洞实例分析 5.2漏洞发展趋势分析 5.2.1漏洞发现趋势 5.2.2漏洞利用趋势 5.2.3漏洞修复趋势 5.2.4应对措施 第2部分 方法技术篇 第6章漏洞的发现 6.1漏洞的挖掘 6.1.1静态挖掘方法 6.1.2动态挖掘方法 6.2漏洞的检测 6.2.1漏洞检测的主要方法 6.2.2基于OVAL的系统安全检测评估工具实例 6.3漏洞的验证 6.3.1常用技术 6.3.2主要步骤 6.3.3漏洞验证实例研究 6.4漏洞的危害 6.4.1漏洞安全危害属性分析 6.4.2漏洞危害评价方法 参考文献 第7章漏洞的发布 7.1漏洞的收集 7.1.1漏洞收集方式分析 7.1.2漏洞信息的采集 7.2漏洞的监测 7.2.1基于分布式蜜罐／蜜网的漏洞监测 7.2.2基于网页的漏洞监测 7.2.3基于受害终端的漏洞监测 7.2.4基于热点信息的漏洞监测 7.3漏洞的发布 7.3.1漏洞发布方式分析 7.3.2 国外权威机构漏洞发布情况比较 参考文献 第8章漏洞的修复 8.1补丁的主要类型 8.2补丁的技术描述 8.2.1补丁基本信息 8.2.2厂商信息 8.2.3第三方信息 8.2.4对应漏洞信息 8.3补丁的修复方式 8.3.1保护内存安全 8.3.2验证恶意输入 8.3.3监控错误与异常 8.3.4补丁修复面临的问题 8.4补丁的效用分析 8.4.1二进制代码补丁分析技术 8.4.2源代码补丁分析技术 参考文献 第9章漏洞的预防 9.1 安全教育和防范意识 9.1.1安全原则 9.1.2理解安全漏洞 9.1.3持续教育 9.2开发过程中的预防 9.2.1安全规范 9.2.2安全需求 9.2.3设计安全性 9.2.4审查 9.3使用及维护的预防 9.3.1信息系统技术防护框架 9.3.2基于可信计算的漏洞防护体系 参考文献 第3部分管理篇 第10章漏洞管理组织机构 10.1 组织机构 …… 第11章漏洞管理标准规范

章节摘录

版权页： 插图： （7）隐通道分析。
分析并验证被测目标当中是否存在非预期的信道（例如非法信息流），并分析其危害程度，有可能的情况下，计算其潜在的通道容量。
（8）其他分析方法。
分析被测对象在其他情况下的安全隐患，例如，升级过程中的安全机制、物理可接触情况下的安全性等。
分析的过程，仍然是从攻击者的角度发起攻击行为，观察被测对象的反应并与预期结果进行比对，以确定其安全隐患。
渗透测试是从一个攻击者的角度出发的，测试的环境也是普通攻击者所处的环境。
然而，不同的攻击者有不同的环境。
例如，内部人员可以直接访问到软件系统，而外部人员则需要先获得访问权限，因此研究者提出了渗透测试的层次模型，该模型主要将测试分为三层：（1）对软件及所在运行环境没有任何了解的外部攻击者。
在这个层次上，测试人员只知道目标环境的存在以及当他们到达该环境时，他们有足够的信息来识别它。
他们必须自己来决定如何才能得到访问权限。
这一层主要是社会人员，他们需要从各处收集信息才能艰难地达到目标。
（2）能够访问软件所在的环境或系统外部攻击者。
在这一层，测试人员可以访问被测软件。
例如，对一个Web应用程序来说，他们可以登录并使用对网上所有主机开通的服务，然后他们可以发起攻击，其攻击方式主要是口令猜测、寻找没有保护的账号、攻击网络服务器等。
服务器上的缺陷常常能提供所需的访问权限。
（3）具有软件系统访问权限的内部攻击者。
测试人员拥有软件的系统账号，并可以作为授权用户来使用软件系统。
这类测试通常包含得到没有授权的权限或信息，并通它们来实现攻击者的目的。
在这个层次上，测试者对目标软件系统的设计和操作有很好的了解，攻击是以对软件系统具有足够的认知和访问权限为基础发起的。
4）渗透测试过程 图6·10介绍的渗透测试过程，主要是参考了漏洞假设计。
（1）制定测试目标。
制定测试的范围、基本规则，定义测试目的等。
（2）信息收集。
利用所有可以利用的资源对测试对象的功能、设计、实现和操作步骤进行检查，可以利用的资源可能包括系统设计文档、源代码、用户手册等。
根据所获测试对象相关信息的多少，渗透测试可以分为白盒测试、灰盒测试和黑盒测试。
（3）漏洞假设。
比较步骤（2）获得的信息和已知安全漏洞（如开放的安全漏洞）信息资源，这些资源包括供应商的安全警告、CERT发布的漏洞信息等，得出测试对象可能存在的漏洞。

编辑推荐

《信息安全漏洞分析基础》可作为信息安全从业人员、黑客技术发烧友的参考指南，也可作为信息安全专业的研究生或本科生的指导用书。

<<信息安全漏洞分析基础>>

版权说明