第一图书网, tushu007.com

<<网络安全评估>>

图书基本信息

书名：<<网络安全评估>>

13位ISBN编号：9787030232410

10位ISBN编号：7030232410

出版时间：2009-1

出版时间：科学出版社

作者：(美)曼佐克

页数：217

译者：张建标

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

前言

我已经以多种方式公开从事有关计算机和软件漏洞方面的工作十多年了。
在非公开场合，我似乎一生都在参与计算机及其他相关方面的工作。
我通过Lopht组织发表了一些早期的建议。
有些报告被送往了政府部门，有些攻击和防御工具发布出来，从LOPhtCrack到Anti-Snff，再到SLINT，还有一些个人和工作专用工具。
保护备受关注的各种网络，无论是大型的还是小型的网络，都是平常事，受命侵入防御坚固的网络更是平常。
但是只关注这些事情的本身并不能得到什么信息。
通过不断对更全面情况的理解（也就是说，所有变化的部分如何从技术层面一直到项目经理和公司态度都能够相互联系）可以制定出实际的目标。
不管攻击者还是防御者，都会遇到这个问题。
发现漏洞是很有趣的事情，多半是因为所要寻找的是鲜为人知的东西。
过去，人们并不总是想把如何发现安全漏洞的信息隐藏起来，而是因为漏洞搜查还是一个新兴领域。
现在，有大量的网络和出版文档可以用来处理一般的和特殊的安全漏洞。
但是从更加广阔的角度来看，这种资料真正地能告诉读者什么，并且如何与读者在现实世界的情况联系起来？
这种资料如何能让负责一个公司小组或者是整个公司的人来做好他们的工作？
让一个攻击者搜寻漏洞有什么风险呢？
很多情况下，攻击者可以获得要进攻的软件或者操作系统的一份拷贝，然后在自己的测试环境中进行测试，这样搜寻漏洞的风险很小。
这种情形也经常发生。
然而，现实的世界毕竟与实验室环境不同。
对于攻击者而言，复制一个特定的环境可能是不可行的，因为这太过于复杂且需要精心策划。
可能目标环境是完全未知的。
在这些情况下，人们乐于探索和实验不属于他们的实用系统时有何种风险呢？
除了搜寻实用外部系统中未知漏洞存在的风险，试图利用这些漏洞还有什么风险吗？
是一个系统崩溃还是引起攻击者注意？
网络是否变得过于拥挤，不仅阻止合法用户使用，而且也阻止攻击者使用网上的服务和资源？
在一个真实的环境中，有多少种破解的机会留给攻击者？
组织提供的服务和系统是否在任何时候，任何地方都是可用的？
在进行维护和回滚的时期，有可变的机会窗口吗？
这个机会窗口会受到软件升级和版本更新的限制吗？
成本同样会影响机会成分。
有些举措可能在财政上是不允许的，如果其他一些举措以开发、交付和使用的时间段作为成本标尺，则可能太昂贵了。
何种动机驱使攻击者对你的环境感兴趣呢？
对有些人而言，可能是机会主义的想法；然而对其他人而言，他们都有明确的目标。
可能有人受命于一个国家、竞争对手或者基于某种特定的信念。
或者有些人就是无聊，这对你来说就不走运了。
这种特殊的对手模型技术也称之为ROM（风险、机会及动机）模型，是非常强大的。
它开始考虑对手目标更多的组成部分，并对应到现有真实世界的环境中决定用来防范或取证的重要地点和各种措施。
这个模型有一个好处是在没有考虑环境、对手目标，以及没有对模型存在的问题和环境进行鉴定的情况下，就不必考虑一个漏洞，并且也不用考虑可能受命攻击或者防御的网络和系统里存在的问题进行处理。

内容概要

随着计算机和网络技术的迅速发展，人们对网络的依赖性达到了前所未有的程度，网络安全也面临着越来越严峻的考验。
如何保障网络安全就显得非常重要，而网络安全评估是保证网络安全的重要环节。
本书从漏洞评估、漏洞评估工具、漏洞评估步骤和漏洞管理等方面介绍了网络安全评估。
通过本书的学习，一方面可以使读者了解网络安全评估的一些基本概念、基本原理，另一方面，更重要的是可以指导读者一步步地完成整个评估过程。
此外，详细介绍了网络安全评估中各种常用的开源工具和商业工具及其特点．有助于读者能够快速地找到合适的评估工具。

第一图书网, tushu007.com

作者简介

Steve Manzuik，目前在Juniper网络公司任高级安全研究主管。
他在信息技术和安全行业有超过14年的经验，尤其侧重于操作系统和网络设备。
在加入Juniper网络公司之前，Steve在eEye Digital Security公司任研究经理。
2001年，他成立了EntrenchTechnologies公司，并任技术领导。
在Entrench之前，Steve在Ernst & Young公司的Security & Technology Solutions Practice部门任经理，他是Canadian Penetration Testing Practice部门的solution line leader。
在加入Ernst & Young之前，他是世界性组织“白帽黑客”的安全分析师，并在BindView RAZOR Team任安全研究员。

Steve是“Hack Proofing Your Network”（Syngress出版社出版，1928994709）第二版的合著者。
此外，他在Defcon，Black Hat，Pacsec和CERT等世界性会议上多次演讲，并且他的文章在许多行业出版物上（包括CNET，CNN，InfoSecuritv Maga—zinc，Linux Security Magazine，Windows IT Pro，以及Windows Magazine）被引用。

书籍目录

主要作者合著者编者译者序序言第1章 漏洞窗口 引言 什么是漏洞？
理解漏洞造成的风险 小结 快速解决方案 常见问题第2章 漏洞评估101 引言 什么是漏洞评估？
第一步：信息收集/发现 第二步：列举 第三步：检测 查找漏洞 利用安全技术检测漏洞 解释通过安全技术收集的漏洞评估数据 通过修复技术存取漏洞 从修复知识库中提取漏洞评估数据 利用配置工具评估漏洞 查找漏洞的重要性 看一些具体的数字 小结 快速解决方案 常见问题第3章 漏洞评估工具 引言 一个好的漏洞评估工具的特征 使用漏洞评估工具 第一步：识别网络上的主机 第二步：把主机分组 第三步：创建一个审计策略 第四步：执行扫描 第五步：分析报告 第六步：在必要的地方做出修复 小结 快速解决方案 常见问题第4章 漏洞评估：第一步 引言 认识你的网络 对资产分类 我认为这是一个漏洞评估章节 小结 快速解决方案 常见问题第5章 漏洞评估：第二步 引言 一个有效的扫描计划 扫描你的网络 何时扫描 小结 快速解决方案 常见问题第6章 更进一步 引言 渗透测试类型 场景：一次内部网络攻击 客户端网络 第一步：信息收集 第二步：测定漏洞 渗透测试 第三步：攻击和渗透 漏洞评估vs渗透测试 决定实施漏洞评估还是渗透测试的提示 内部vs外部 小结 快速解决方案 常见问题第7章 漏洞管理第8章 漏洞管理工具第9章 漏洞和配置管理第10章 遵守管理法规第11章 融会贯通附录A 信息安全评价的法律案例附录B 信息安全基线活动工具

章节摘录

插图：第1章 漏洞窗口引言本书不是典型的介绍信息技术（Information Technology，IT）安全的书。
虽然本书作者具有专业技术背景，而且也写过一些很畅销的书，如Syngress出版的“ Hack Proofing Your Network ”，但是本书还是主要将漏洞管理的技术融人到业务管理中。
尽管熟悉最新的黑客技术是很重要的，但是只有当能够把黑客所实施的威胁与对组织所造成的风险联系在一起时，这些知识才是有价值的，本书将介绍做这件事情的工具。
本章主要介绍漏洞及其重要性，我们还将讨论一个被称作“ 漏洞窗口 ”（Windows of Vulnerabilities）的概念，以及如何确定一个已知的漏洞对环境造成的风险。
什么是漏洞？
那么，什么是漏洞呢？
在过去，很多人把漏洞看作是有恶意的人能够利用的软件或硬件的缺陷。
然而，在近几年中，漏洞的定义发展成为有恶意的人能够利用的软硬件的缺陷及配置错误（misconfiguration）。
补丁管理、配置管理和安全管理等常常相互竞争的学科，都已从单一的学科发展成为同一个信息技术（IT）方面的问题，那就是今天的漏洞管理。

编辑推荐

《网络安全评估:从漏洞到补丁》为21世纪信息安全大系丛书之一，由科学出版社出版。

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com