<<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：9787508390796

10位ISBN编号：7508390792

出版时间：2009-1

出版时间：中国电力出版社

作者：中国标准出版社

页数：476

前言

在对逾20，000起针对信息基础设施和应用程序的渗透测试进行过绩效管理之后，我越来越认识到技术测试和提供信息安全保障的重要性。
本书精确地定义了一种纯粹的技术评估方法学，阅读本书会让读者对现今的公共网络所面临的威胁、所存在的漏洞及漏洞披露方式有一个更为深刻的理解。
我在信息系统安全领域20余年的工作经历中，所进行的数以万计的渗透测试的目的是“识别被测系统的技术漏洞，以便纠正这些漏洞或者降低由这些漏洞所带来的风险”。
在我看来，对于为什么要进行渗透测试而言，这是一个清晰简明但也是错误的理由。
阅读本书时，你会逐渐认识到，在大多数情况下，漏洞及其披露源于系统管理不善、没有及时打补丁、弱口令策略、不完善的存取控制机制等。
因此，进行渗透测试的主要原因和目的应该是识别和纠正系统管理过程的失效，正是这种失效导致了系统漏洞的出现，并在渗透测试的过程中被披露出来。
最常见的系统管理过程失效包括：系统软件配置的失效；应用程序软件配置的失效；软件维护的失效用户管理和系统管理的失效。
遗憾的是，很多IT安全顾问仅仅提供特定测试所发现问题的详细列表，但从来不尝试进行更高层次的分析，以便回答“为什么会存在这些问题”。
缺乏对那些系统管理失效（系统管理失效是引发测试中所发现的问题的本质原因）的识别和纠正所带来的后果是，在六个月之后，当IT安全顾问再一次对信息系统进行测试之后，新的问题又会出现。

<<网络安全评估>>

内容概要

你的网络有多安全？
要回答这一问题，最好的方法是对其进行攻击。
网络安全评估(第二版)为你提供了专业安全顾问用于识别与评估Internet网络的技巧与工具，及其用于对政府、军事与商业网络进行安全加固的渗透测试模型，通过本书的学习，你可以采纳、提炼并重用这一渗透测试模型来部署网络，并对其进行安全加固，使其可以免受攻击。
本书展示了意志坚定的攻击者如何在基于Internet的网络中搜索存在漏洞的系统组件，从网络层到应用层都在其攻击范围内。
第二版包含了最新的黑客技术，但并不是集中于单独的安全问题，而是通过在较高层面对安全威胁进行分组与分析，来获取对网络安全的整体了解。
通过本书，你将学会如何针对整体攻击行为制定防护策略，为网络提供现实的与将来的安全防护。
评估是任何组织在正确管理信息风险时所应采用的第一个步骤。
通过使用符合CESG CHECK与NSA IAM政府标准的技术来识别与评估风险，本书提供了实现评估的精确方法。

作者简介

Chris McNab是设在伦敦的安全公司Matta的技术总监，该公司提供技术培训与渗透测试服务。
作为一位全职的网络安全分析师，Chris从业已有9年，为世界各地的很多大型客户与政府组织提供过安全培训与渗透测试，并有效地提高了其网络安全性。

<<网络安全评估>>

书籍目录

序言前言第一章 网络安全评估 商业利益 IP：Internet的基础 对Internet攻击者的分类 评估服务定义 网络安全评估方法学 循环的评估方法第二章 网络安全评估平台 虚拟化软件 操作系统 探测工具 网络扫描工具 渗透工具框架 Web应用程序测试工具第三章 Internet主机与网络枚举 查询Web与新闻组搜索引擎 查询域的WHOIS登记处 查询IP WHOIS登记处 BGP查询 DNS查询 Web服务器Crawling 自动化的枚举 SMTP探测 枚举技术回顾 枚举攻击应对措施第四章 IP网络扫描 ICMP探测 TCP端口扫描 UDP端口扫描 进行UDP端口扫描的工具 底层IP评估 网络扫描回顾 网络扫描的应对措施第五章 远程信息服务评估 远程信息服务 DNS Finger Auth NTP SNMP LDAP rwho RPC rusers 远程信息服务攻击应对措施第六章 Web服务器评估 Web服务器 对可访问的Web服务器进行“指纹”识别 识别与评估反向代理机制 枚举虚拟主机与Web站点 识别子系统与激活的组件 研究已知的漏洞 基本的Web服务器Crawling Web服务器攻击应对措施第七章 Web应用程序评估 Web应用程序技术概览 构造Web应用程序的profile Web应用程序攻击策略 Web应用程序漏洞 Web安全检查列表第八章 远程维护服务评估 远程维护服务 FTP SSH Telnet R-Services X Windows Citrix Microsoft远程桌面协议 VNC 远程维护服务攻击的应对措施第九章 数据库服务评估 Microsoft SQL Server Oracle MySQL 数据库服务攻击应对措施第十章 Windows网络服务评估 微软Windows网络服务 微软RPC服务 NetBIOS名服务 NetBIOS数据报服务 NetBIOS会话服务 CIFS／1E务 Unix Samba漏洞 Windows网络服务攻击应对措施第十一章 电子邮件服务评估 电子邮件服务协议 SMTP POP－2与POP－3 IMAP 电子邮件服务攻击应对措施第十二章 IP VPN服务评估 IPsec VPNS 攻击IPsec VPN 微软PPTP SSL VPN VPN服务应对措施第十三章 Unix RPC服务评估 枚举Unix RPC服 RPC服漏洞 Unix RPC服攻击应对措施第十四章 应用程序层风险 Hacking的基本概念 软件存在漏洞的原因分析 网络服务漏洞与攻击 经典的缓冲区溢出漏洞 堆溢出 整数溢出 格式化字符串Bug 内存操纵攻击回顾 降低进程操纵的风险 关于安全开发的推荐读物第十五章 运行Nessus Nessus体系结构 部署选项与系统需求 Nessus安装 配置Nessus 运行Nessus Nessus报告 运行Nessus的回顾第十六章 渗透工具框架 Metasploit Framework CORE IMPACT Immunity CANVAS 渗透工具框架回顾附录A TCP、UDP端口与ICMP消息类型附录B 漏洞信息源附录C 渗透工具框架模块

章节摘录

插图：Internet主机与网络枚举攻击者可以通过很多探测技术查询公开的信息源，以便识别出那些感兴趣的主机与网络。
这些开放的信息源包括web与新闻组搜索引擎、wHOIS数据库、DNs名服务器等。
通过这些公开的信息源，攻击者通常可以从Internet获取目标网络结构等有用的信息，而不需要真正地对目标网络进行直接的扫描和探测。
这些初始的探测是非常重要的，能帮助黑客识别那些没有做好足够安全加固的网络和主机。
坚定的攻击者愿意在外围的网络和主机上花费一些精力，而公司和组织往往只是把注意力放到那些显而易见的公开系统（如公开的web服务器和邮件服务器），但却忽略了那些通常不被注意的主机和网络，这就增加了攻击者通过这些外围设备入侵系统的成功几率。
坚定的攻击者还可以对目标网络的第三方供应商或商业伙伴的网络进行枚举，由于供应商和商业伙伴通常会具有对目标网络的相应的访问权限，通过这种迂回的策略，攻击者也可以获取一些相关的信息。
现今，第三方通常通过VPN隧道或其他形式的专门通道连接到目标网络中来，这在客观上增加了攻击者的难度。
通过这种初始探测可以获取的信息包括基于Internet的网络段的一些详细资料、通过DNS服务器获得的内部IP地址、目标组织内部DNs服务器结构的信息（包括域名、子域、主机名等），以及物理位置不同的IP网络之间的关系。
攻击者可以利用这些信息对目标网络进行结构化的大规模网络扫描和探测，以探究目标网络空间可能存在的漏洞。
通过进一步的探测可能会提取用户的一些详细资料，包括电子邮件地址、电话号码、办公室地址等。

<<网络安全评估>>

版权说明