<<网络扫描技术揭秘>>

图书基本信息

书名：<<网络扫描技术揭秘>>

13位ISBN编号：9787111365327

10位ISBN编号：7111365321

出版时间：2012-1

出版时间：机械工业出版社华章公司

作者：李瑞民

<<网络扫描技术揭秘>>

内容概要

《网络扫描技术揭秘：原理、实践与扫描器的实现》系统地介绍网络扫描器的概念、原理与设计方法，饱含作者十几年来在网络技术应用实践中不断总结的经验与技巧。
作者从网络协议这样的基本概念开始，细致深入地分析了网络扫描器的原理，并用自己制作的大量工程代码，揭示了网络扫描器的实现方法与最佳实践。

《网络扫描技术揭秘：原理、实践与扫描器的实现》首先介绍了网络扫描技术的概念、原理、算法等，以及网络协议的意义与编程概述，随后系统分析了各种扫描器的原理与设计方法，包括tcp/udp端口、netbios、snmp、icmp、基于协议的服务、基于应用的服务、命名管道、服务发现、漏洞扫描器等。
书中在介绍每一种扫描器的时候，都是先介绍相应协议，然后对扫描器中要使用的api函数进行详细说明，使读者知道该扫描器的各种技术细节；还介绍了windows中相关协议程序的安装、配置、测试和验证等，使读者有了演习场地；最后展示了扫描器的编程实例。
这种循序渐进、逐步深入的方式，使读者不仅全面地了解扫描器的细节，而且在遇到新情况时，能举一反三，对代码进行修改或调整。
随书光盘还包含了作者精心制作与调试好的工程代码，可帮助读者快速上手，设计出自己需要的扫描器。

《网络扫描技术揭秘：原理、实践与扫描器的实现》不仅是网管员和安全技术人员必备参考书，也适合于所有想深入理解计算机网络原理、全面了解网络扫描技术的学生、教师以及安全技术爱好者。

作者简介

李瑞民，工学博士，资深网络安全专家兼高级系统架构师。
多年来一直专注于计算机安全技术、网络设备与信号监控等领域的研究与应用，对网络扫描技术以及串口监控、网口监控等设备类监控技术有深刻的认识。
并在实践中总结出了串口通信中的嗅探技术以及通用串口协议语法。
曾参与多个网络应用软件项目的研发，涉及网络安全、广播电视、通信等多个行业。
曾发表论文二十余篇.拥有专利和著作权六项。
此外。
还积极倡导和推动开源事业，将自己精心编写的扫描器代码全部开源，旨在推动我国软件事业的发展。

<<网络扫描技术揭秘>>

书籍目录

章节摘录

版权页：插图：1.2.2 网络扫描扫描源于物理术语，是通过对一定范围内的光或电信号进行检测处理，然后以数值或图形方式进行展示的一个操作。
网络扫描也一样，是通过对一定范围内的主机的某种属性进行试探性地连接和读取操作，最终将结果展示出来的一种操作。
端口具有独占性，一旦一个服务使用了某个端口，则另外的服务不能再使用这个端口。
端口的占用原则是：先申请的先使用，后申请的在申请时报错。
同时，上述的这种对应关系，只是一种约定，但任何操作系统都没有强制软件遵照执行，因此在使用时，存在如下几个情况：某个主机不向外界提供WWW服务，所以该主机的80端口是空闲的。
但该主机上的另一个不提供WWW服务的程序使用了80端口。
因此，该主机80端口是对外打开的，但不提供WWW服务。
某主机虽然提供WWW服务，但该主机并不想让别的人都知道该主机提供该服务，于是该主机的管理员将该主机上的WWW服务的端口由默认的80端口，改为了其他的端8000，并将该端口告诉了他允许访问的用户。
在这种情况下，需要通过其他联系方式通知所有允许访问的主机。
某主机对外界想同时提供基于ASP的WWW服务和基于JSP的WWW服务，二者虽然同为WWW服务，但运行机制、配置等各不相同，并且没有一个通用的软件能同时提供，且二者占用了同一个端口80，于是该主机的管理员将ASP设定为80端口，而将JSP的端口设定为8080端口，并在双方主页上互相告知对方端口的存在。

编辑推荐

《网络扫描技术揭秘:原理、实践与扫描器的实现》是一类重要的网络安全技术。
通过对网络的扫描，网络管理员可以了解网络的安全配置和运行的应用服务缺陷，赶在黑客攻击之前发现安全漏洞，客观评估网络风险等级，随后根据扫描的结果弥补网络安全漏洞，更正系统中的错误配置。
如果说防火墙和网络监控系统是被动的防御手段，那么网络扫描就是一种主动的排查措施，可以有效减少黑客攻击成功的概率，做到防患于未然。
《网络扫描技术揭秘:原理、实践与扫描器的实现》全面系统地介绍网络扫描技术的概念、原理和分类，用实例讲解了各种扫描器的设计方法，涉及ICMP、SNMP、SSDP、HTTP、FTP、Telnet等与网络安全息息相关的协议内容，最后给出了防扫描技术的研究成果。
《网络扫描技术揭秘:原理、实践与扫描器的实现》所有实例都直接来自实战操作，并且所有扫描器均提供源代码工程文件，可帮助读者快速上手，设计出自己需要的扫描器。
《网络扫描技术揭秘:原理、实践与扫描器的实现》最大的特点就是几乎囊括了当前所有的扫描方式，而每一种方式又是八仙过海，各显神通这些扫描方式包括：ICMP扫描：快速ICMP扫描可以扫描出哪些主机是运行的，进而初步预测一下对方的操作系统类型。
这便于在某一不熟悉的网段中快速定位哪些主机可以作为下一步的扫描对象。
端口扫描：以快速、非顺序的扫描算法高效率地扫出对方TCP/UDP端口的状态。
相对于后续的扫描，端口扫描通常是网络攻击的第一步。
NetBIOS扫描：扫描出对方的组名、用户名、目录，甚至是密码。
如果有幸扫出对方管理员的密码，那随后的操作和使用自己的计算机差别就不大了。
SNMP扫描：只要对方提供SNMP协议的支持，那么你在本地任务管理器中能看到什么，就能在对方任务管理器中看到什么。
基于协议和基于应用的扫描：该扫描的最大优势就是发现对方提供的服务类型，对于常规的WWW、FTP、Telnet服务，一切尽收眼底，为后面的漏洞扫描搜集素材。
漏洞扫描：漏洞扫描的主要目的就是发现漏洞、实现攻击，其作用不言而喻。
命名管道扫描：作为一种冷僻的扫描方式，自然有其独特的使用领域，对于一些专有的场景，正是该扫描方式大显身手的场所，也许别人花费九牛二虎之力完成的任务，在这里只是探囊取物。
服务发现扫描：服务发现扫描是“温柔一刀”，因为这种扫描方式不用背负黑客工具的神秘名声，完全可以作为一个受欢迎的网络管理工具。
总之，系统主机五花八门，而扫描的方式也是多种多样，无论怎样的系统，总能找到合适的扫描方式。
资深网络安全专家十余年研究与实践经验的结晶，重点突出，针对性地讲解了核心网络扫描技术的原理与最佳实践，实战性强，各种主流扫描器的设计方法和原理尽含其中，附有完整源代码可供参考。
网络安全是一个永恒的话题。
中国是一个早在五千年前就发现面对困难时“堵”不如“疏”的伟大国家。
面对网络安全也是一样，与其“讳疾忌医”。
不如“坦然面对”。
网络扫描是一切网络攻击的基础，也是检测自身安全防护系统的有效方法。
因此，网络管理员和安全技术人员完全有必要掌握端口、服务等概念和技术。
并利用扫描技术扫描自身系统。
通过对扫描结果的判断，关闭无实质性作用的端口或服务。
而对于必须开放的端口和服务，则尽可能地安装其漏洞补丁程序。

版权说明