<<网络信息对抗>>

图书基本信息

书名：<<网络信息对抗>>

13位ISBN编号：9787563525027

10位ISBN编号：7563525025

出版时间：2011-1

出版时间：北京邮电大学出版社

作者：杜晔，梁颖 编

页数：230

<<网络信息对抗>>

内容概要

本书详细地介绍了信息对抗基本概念、原理与方法，详尽、具体地披露了攻击技术的真相，以及防范策略和技术实现措施。
全书共分3个部分，内容由浅入深，分技术专题进行讨论。
第1部分介绍了网络信息对抗的基础知识、计算机及网络系统面临的威胁与黑客攻击方法、网络信息对抗的基础知识及典型的安全评估标准和模型。
第2部分是本书的核心内容，介绍了有代表性的网络攻击技术，包括网络扫描、嗅探、欺骗、缓冲区溢出、拒绝服务攻击、恶意代码等手段的原理与实现技术。
第3部分根据网络边界防护的要求着重讨论了防御手段，详细介绍了身份认证技术、访问控制技术和两种得到广泛应用的安全设备，即防火墙和入侵检测系统。
　　本书既可作为信息安全、信息对抗、计算机、通信等专业本科生、硕士研究生的教科书，也适合于网络管理人员、安全维护人员和相关技术人员参考和阅读。

<<网络信息对抗>>

书籍目录

章节摘录

版权页：插图：传播模块又可以分为3个基本模块：扫描模块、攻击模块和复制模块。
蠕虫程序的一般传播过程包括如下步骤。
①扫描。
由蠕虫的扫描功能模块负责探测存在漏洞的主机。
当程序向某个主机发送探测漏洞的信息并收到成功的反馈信息后，就得到一个可传播的对象。
②攻击。
攻击模块按漏洞攻击步骤自动攻击步骤①中找到的对象，取得该主机的权限（一般为管理员权限），获得一个shell。
③复制。
复制模块通过原主机和新主机的交互，将蠕虫程序复制到新主机并启动。
这里可以看到，传播模块实现的实际上是自动人侵的功能。
所以蠕虫的传播技术是蠕虫技术的首要技术，没有蠕虫的传播技术，也就谈不上什么蠕虫技术了。
2.入侵过程的分析①用各种方法收集目标主机的信息，找到可利用的漏洞或弱点。
搜集信息，有很多种方法，包括技术的和非技术的。
采用技术的方法包括用扫描器扫描主机，探测主机的操作系统类型和版本、主机名、用户名、开放的端口、开放的服务、开放的服务器软件版本等。
非技术的方法包括和主机的管理员拉关系套口风，骗取信任，威逼利诱等各种少儿不宜的手段。
当然是信息搜集的越全越好。
搜集完信息后进入下一步。
②针对目标主机的漏洞或缺陷，采取相应的技术攻击主机，直到获得主机的管理员权限。
对搜集来的信息进行分析，找到可以有效利用的信息。
如果有现成的漏洞可以利用，上网找到该漏洞的攻击方法，如果有攻击代码就直接复制下来，然后用该代码取得权限就好了；如果没有现成的漏洞可以利用，就用根据搜集的信息试探猜测用户密码，另一方面试探研究分析其使用的系统，争取分析出一个可利用的漏洞。

编辑推荐

《网络信息对抗》：北京市重点学科共建项目：计算机应用技术

<<网络信息对抗>>

版权说明