<<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：9787111332886

10位ISBN编号：7111332881

出版时间：2011-5

出版时间：肖军模、周海刚、 刘军 机械工业出版社 (2011-05出版)

作者：肖军模 等 著

页数：342

<<网络信息对抗>>

内容概要

《普通高等教育“十一五”国家级规划教材·高等院校信息安全专业规划教材：网络信息对抗（第2版）》网络信息系统已成为21世纪人类社会的重要基础设施之一。
在充满着利益对立和竞争的社会中，网络信息对抗成为一种无法避免的社会现象。
研究网络信息对抗技术的原理与方法，对于提高网络信息系统的安全与防范能力有着重要作用。
《普通高等教育“十一五”国家级规划教材·高等院校信息安全专业规划教材：网络信息对抗（第2版）》在介绍信息对抗概念、原理与作用，TCP/IP网络安全知识以及网络风险分析方法的基础上，根据网络攻击的一般顺序，详细地介绍了网络攻击的方法和步骤，并在合理分类的基础上，介绍各种攻击手段，包括网络探测、扫描、口令破解、漏洞攻击、网络欺骗、窃听、木马攻击、路由器攻击和逻辑炸弹等手段的原理与实现技术；根据边界防护和主机防护的分类，详细介绍了各种防护手段，包括路由器、防护墙、虚拟专网（VPN）、蜜罐、入侵检测系统（IDS）以及Windows和UNIX、因特网信息服务器（IIS）和阿帕奇服务器（ApacheServer）、病毒防护和应急响应等手段的原理与实现技术；基于无线计算机网络的对抗技术。
《普通高等教育“十一五”国家级规划教材·高等院校信息安全专业规划教材：网络信息对抗（第2版）》可以作为信息安全专业、信息对抗专业、计算机应用专业或其他相关专业的大专、本科的教科书，也可以作为从事网络信息安全工作的研究生、科技人员和信息安全管理人员的参考书。

<<网络信息对抗>>

书籍目录

章节摘录

版权页：插图：1.验证数据的明文传送方式在这种验证方式中，用户的密码与ID以明文的形式从客户端传送给服务器端的验证程序，验证程序检查传送来的用户密码与ID是否存储在服务端上的该用户的密码与ID是否一致。
如果一致，验证程序就向终端用户回送认可的信息，并允许该用户进行下一步的操作。
这种认证方式的优点就是实现简单，最大的缺点是不安全可靠。
攻击者可以很容易地在客户端与服务端之间通过侦听手段获取用户的密码与ID，然后假冒该用户去欺骗验证服务器，获准对系统进行合法的访问。
因此，这种验证方式是不可取的。
如果服务端也用明文方式存储全部用户的验证数据（用户的密码与ID），就会对系统的安全造成全局性的影响。
如果系统管理员的ID与密码也被泄露了，整个系统就不存在安全性。
2.利用单向散列函数传送随机或时间数据为了防止攻击者半路窃听用户的密码（口令）与ID，x·509建议了这种利用单向散列函数的传送方式。
这种传送方式又分为两种：一种是采用直接单向散列函数传送密码，另一种是基于随机或时间数据的单向散列函数传送密码。
第一种方法是利用单向散列技术，在客户端把需要散列的数据（如用户登录的ID与密码）通过单向函数以近似的、随机的方式映射到一个固定长度的序列的散列值，然后把该散列值直接传输到验证服务器进行验证。
在该服务器上不直接存储用户的ID与密码，只存储用户ID与密码的散列，对管理员也做到了保密。
在理论与实践上都已表明，反向破解散列函数，即把散列值恢复为散列函数的输入值是非常困难的。
由于在网络内传输的是散列值，即使被攻击者窃听了，也无法还原出用户真实的登录ID和密码。
第一种传送密码的方法虽然解决了防破解的问题，但仍不能防止攻击者从半路截获用户登录的散列值。
攻击者可以利用重放攻击方式，把截获的用户登录散列值发送到验证服务器，服务器无法辨别这个验证信息是用户自己发送过来的，还是攻击者发来的，因此，服务器仍然可能被欺骗。
解决这个问题的办法是使传送的散列值是基于随机数的或是基于时间标记的。

<<网络信息对抗>>

编辑推荐

《网络信息对抗(第2版)》信息对抗基本概念，TCP／IP中与网络安全相关的知识及网络风险分析方法。
网络攻击的方法和各种网络信息对抗技术。
网络基础设施的安全机制。

<<网络信息对抗>>

版权说明