<<网络信息安全监察>>

图书基本信息

书名：<<网络信息安全监察>>

13位ISBN编号：9787561226407

10位ISBN编号：7561226403

出版时间：2009-9

出版时间：王钢 刘坦 西北工业大学出版社 (2009-09出版)

作者：王钢 刘坦 编

<<网络信息安全监察>>

内容概要

《全国高等院校计算机教育『十一五』规划教材:网络信息安全监察》共分为15章，内容包括信息系统安全概述、信息系统防御、网络攻击理论及攻击技术、信息系统安全监察、信息网络安全法律法规、网络警察行政执法、虚拟社会管理、信息安全等级保护、信息安全风险评估、重要信息系统应急响应及演练、计算机犯罪侦查概述、计算机犯罪与网络犯罪现场勘查、计算机犯罪案件的管辖与侦查、网络犯罪与防控、电子证据与司法鉴定。

<<网络信息安全监察>>

书籍目录

章节摘录

版权页： 插图： 2.Botnet的危害 一般认为Botnet的危害包括5宗罪，从危害大范围和严承程度来看，威胁最大的是DDoS攻击和垃圾邮件。
有些DDoS攻击事件，曾经造成某中型城域网的全部宽带用户无法上网长达2个多小时。
垃圾邮件也大量的消耗着带宽。
此外，监听网络流量、记录键盘操作、大规模身份窃取通常只是可能给最终用户带来重大经济损失。
这些的潜在威胁虽然是针对最终用户的，但是从服务营销的角度来看，也是网络服务提供商的损失。
但是如果以积极主动的态度来应对，又可以将这些威胁转化为潜在的商机。
（1）发动DDoS攻击。
DDoS攻击已经是司空见惯的事情了，这里想强调的是DDoS攻击目标并不局限于Web服务器，实际上Internet上任何可用的服务都可以成为这种攻击的目标。
通过功能滥用的攻击，高层协议可用来更有效地提高负载，比如针对电子公告栏运行能耗尽资源的查询或者在受害网站上运行递归HTTP洪水攻击。
递归HTTP洪水指的是僵尸工具从一个给定的HTTP链接开始，然后以递归的方式顺着指定网站上所有的链接访问，这也叫蜘蛛爬行。
这种攻击可以通过一个参数来简单实现，在后面介绍DDoS命令部分时可以看到相关的参数。
僵尸网络也可用于攻击IRC网络。
流行的攻击方式是所谓的“克隆攻击”，在这种攻击中，控制者命令每个僵尸工具连接大量的IRC受害终端。
被攻击的IRC服务器被来自数千个僵尸工具或者数千个频道的请求所淹没。
通过这种方式，受到攻击的IRC网络可被类似于DDoS攻击击垮。
（2）发送垃圾邮件。
有些僵尸工具可能会在一台已感染的主机上打开SOCKS v4/v5代理（基于TCP/IP的网络应用（RFC 1928）的一般代理协议）。
在打开SOCKS代理后，这台主机可被用于执行很多恶毒任务，例如发送垃圾邮件等。
在一个僵尸网络和上千个僵尸工具的帮助下，攻击者可以发送大量的大邮件（垃圾邮件）。
有些僵尸工具也执行特殊的功能——收集电子邮件地址。
另外，这当然也可被用于发送诈骗（phishing）邮件，诈骗邮件也是一种特殊的垃圾邮件。
（3）监听用户敏感信息、记录键盘输入信息。
僵尸工具也可用数据包监听器来观察通过一台已被攻陷主机上令人感兴趣的明文数据。
监听器大部分被用于提取敏感信息，例如用户名和密码。
但监听到的数据也呵能包括其他令人感兴趣的信息。
如果一台主机不止一次被攻陷并属于多个僵尸网络，监听者收集另一个僵尸网络的关键信息。

<<网络信息安全监察>>

编辑推荐

《全国高等院校计算机教育『十一五』规划教材:网络信息安全监察》系全国高等院校计算机教育“十一五”规划教材，是由王钢，刘坦主编，西北工业大学出版社出版的。
《全国高等院校计算机教育『十一五』规划教材:网络信息安全监察》从网络安全管理的角度，提出网络安全监察工作的主要内容。
《全国高等院校计算机教育『十一五』规划教材:网络信息安全监察》可作为高等院校的教材，也可供成人夜校及其相关专业的科技人员参考。

版权说明