《计算机系统安全与维护》

图书基本信息

书名：《计算机系统安全与维护》

13位ISBN编号：9787301217542

10位ISBN编号：7301217544

出版社：吕新荣、 陆世伟 北京大学出版社 (2013-01出版)

《计算机系统安全与维护》

书籍目录

《计算机系统安全与维护》

章节摘录

版权页： 插图： 2.2相关知识 1.木马攻击的基本原理 黑客用木马进行网络入侵，从过程上看大致可分为6步，下面用这6步来详细阐述木马的攻击原理。 1）配置木马 一般来说，一个设计成熟的木马配置程序，从具体的配置内容看，主要是为了实现以下两个方面的功能。 （1）木马伪装。木马配置程序为了在服务器端尽可能好地隐藏木马，会采用多种伪装手段，如修改图标、捆绑文件、定制端、自我销毁等。 （2）信息反馈。木马配置程序将信息反馈的方式或地址进行设置，如设置信息反馈的E—mail、IRC号、QQ号等。 2）传播木马 （1）传播方式。木马的传播方式主要有两种：一种是通过电子邮件，即控制端将木马程序以附件的形式夹在邮件中发送出去，收件人只要一打开附件，系统就会感染木马；另一种是软件下载，即一运行这些程序，木马就会自动安装。 （2）伪装与隐藏方式。木马设计者为了使自己所设计的木马程序不轻易被人发现，往往在开发时采用多种方式来伪装木马，以达到降低用户警觉、欺骗用户的目的。比如和某个视频文件绑定、和某张图片绑定等。 3）运行木马 服务器端用户运行木马或捆绑木马的程序后，木马就会自动进行安装。首先自身复制到Windows的系统文件夹中，然后在注册表、启动组、非启动组中设置好木马的触发条件，这样木马的安装就完成了。安装后达到了一定的触发条件，就开始运行木马。 4）盗取信息 一般来说，设计成熟的木马都有一个信息反馈机制。所谓信息反馈机制，是指木马成功安装后会收集一些服务器端的软、硬件信息，并通过E—mail、IRC、QQ或ICQ的方式告知控制端用户。 控制端从反馈信息中可以知道服务器端的一些软、硬件信息，包括使用的操作系统、系统目录、硬盘分区状况、系统口令等，在这些信息中，最重要的是服务器端IP地址，因为只有得到这个参数，控制端才能与服务器端建立连接。 5）建立连接 一个木马连接的建立首先必须满足两个条件：一是服务器端已安装了木马程序；二是控制端、服务器端都要在线。在此基础上控制端可以通过木马端口与服务器端建立连接。 假设A机为控制端，B机为服务器端，对于A机来说要与B机建立连接，必须知道8机的木马端口和IP地址。由于木马端口是A机事先设定的，为已知项，所以最重要的是如何获得B机的IP地址。获得B机的IP地址的方法主要有两种：信息反馈和IP扫描。由于扫描整个IP地址既费时又费力，一般来说控制端都是通过信息反馈获得服务器端的IP地址。

《计算机系统安全与维护》

编辑推荐

《全国高职高专计算机立体化系列规划教材:计算机系统安全与维护》适合作为高职高专计算机类和信息安全类专业及相近专业的教材，也可作为中小企业信息系统管理员、网络管理员、信息安全员的培训教材或工作参考书。

《计算机系统安全与维护》

版权说明