<<计算机使用安全与防护>>

图书基本信息

书名：<<计算机使用安全与防护>>

13位ISBN编号：9787121146633

10位ISBN编号：7121146630

出版时间：2011-9

出版时间：电子工业出版社

作者：徐津，胡晓菲，潘威　主编

页数：268

<<计算机使用安全与防护>>

内容概要

本书采用通俗易懂的方式介绍了计算机使用安全与防护所涉及的知识，精心选取典型的案例，系统地介绍如何降低网络威胁，提高计算机的使用安全系数。
本书以大量的实例对计算机使用安全防范设置进行详细的分析，并对一些需要注意的安全事项进行重点提示，在讲解过程中还加入一些安全防范技巧，旨在帮助读者了解计算机使用安全与防护领域的相关知识，建立计算机使用的安全意识，对保证计算机系统的安全具有实际的指导意义。

<<计算机使用安全与防护>>

书籍目录

章节摘录

版权页：插图：按漏洞的成因分类，是对漏洞进行分类最令人头疼的一个话题。
因为对漏洞研究的不同抽象层次，会对同一个漏洞做出不同的分类。
对下面提到的ps竞争条件漏洞，从最低层次上来说是参数验证错误，因为系统调用并没有检查它们所处理的是否为同一个对象。
从高一些的层次看，这是一个同步或竞争条件错误。
从更高的层次看，这则是一个逻辑错误，因为对象可能在使用过程中被删除。
至今也没看到一个比较完美的分类方案，包括一些专业的技术论坛网站上的分类也不能让人满意，现大致分成以下几类。
（1）输入验证错误。
大多数的缓冲区溢出漏洞和cgi类漏洞都是由于未对用户提供的输入数据的合法性作适当的检查。
（2）访问验证错误。
漏洞的产生是由于程序的访问验证部分存在某些可利用的逻辑错误，使绕过这种访问控制成为可能。
上面提到的那个早期AIX（UNIX操作系统）的rlogin（选程登录）漏洞就是这种典型。
（3）竞争条件。
漏洞的产生在于程序处理文件等实体时在时序和同步方面存在问题，这处理的过程中可能存在一个机会窗口使攻击者能够施以外来的影响。
早期的Solaris系统的ps命令存在这种类型的漏洞，ps命令在执行的时候会在/tmp产生一个基于它系统进程的pid值的临时文件，然后把它chown（改变档案的拥有者）为root（超级用户），改名为ps_data。
如果在ps命令运行时能够创建这个临时文件指向攻击者有兴趣的文件，这样ps命令执行以后，攻击者就可以对这个root拥有文件做任意的修改，这可以帮助攻击者获得root权限。
（4）意外情况处置错误。
漏洞的产生在于程序在它的实现逻辑中没有考虑到一些意外情况，而这些意外情况是应该被考虑到的。
大多数的/tmp目录中的盲目跟随符号链接覆盖文件的漏洞属于这种类型。
临时文件一般都存储在/tmp目录中，该目录通常设置为任何人都可以读和写操作。
例如，Sco UNIX openserver的/etc/sysadm.d/bin/userOsa存在盲目覆盖调试日志文件的问题，而文件名是固定的，通过把文件名指向某些特权文件，可以完全破坏系统。
（5）设计错误。
这个类别是非常笼统的，严格来说，大多数的漏洞存在都是设计错误，因此所有暂时无法放入到其他类别的漏洞。
（6）配置错误。
漏洞的产生在于系统和应用的配置有误，或是软件安装在错误的地方，或是错误的配置参数，或是错误的访问权限，策略错误。

编辑推荐

《计算机使用安全与防护》是职业教育课程改革系列教材之一。

<<计算机使用安全与防护>>

版权说明