<<C++黑客编程揭秘与防范>>

图书基本信息

书名：<<C++黑客编程揭秘与防范>>

13位ISBN编号：9787115280640

10位ISBN编号：7115280649

出版时间：2012-6

出版时间：人民邮电出版社

作者：冀云

页数：265

字数：406000

<<C++黑客编程揭秘与防范>>

内容概要

《C++黑客编程揭秘与防范》旨在通过简单的语法知识及常用的系统函数编程，完成一些有特定功能的安全工具，让读者对系统知识等各方面有一个全面的了解，并且在笔者的带领下一步步完成书中的实例。
本书主要内容为：第1章了解黑客编程，主要讲解了VC(Visual C++的缩写)和Windwos下安全编程方面的基础知识。
第2章 从剖析简单的木马说起，讲解有关的网络编程和协议知识。
第3章
Windows应用编程基础，讲解API编程的技术。
第4章 加密与解密，讲解PE等加密有关的知识。
第5章
HOOK编程，讲解了与钩子有关的知识。
第6章
黑客编程剖析，剖析了病毒的原理和攻防技术，以及安全工具的开发。
第7章最后的旅程——简单驱动开发及逆向。

《C++黑客编程揭秘与防范》适合网络安全人员、黑客爱好者，以及相关的程序员阅读。

<<C++黑客编程揭秘与防范>>

书籍目录

章节摘录

版权页： 插图： 从图6—6中看到了反弹木马的工作原理。
通常情况下攻击者的IP地址是变动的，那么“小白”是如何连接到“黑客”的主机的呢？
一般情况下黑客要把自己的IP地址动态地保存到某个固定的IP地址下（比如保存到网上FTP空间中），然后木马通过读取该IP地址下保存的黑客的IP地址进行连接，同样用图来说明，如图6—7所示。
从图6—7中可以看出，黑客开启木马客户端后，首先会更新服务器上保存着的自己的IP地址。
“小白”会去读取服务器中保存着的黑客的IP地址，然后“小白”去连接“黑客”的主机，主动地让黑客去控制它，这就是木马中的“自动上线”。
关于反弹端口的介绍就到这里。
有了思路，通过前面学习的Wmsock的知识自己可以试着实现一下，这里就不做更多的介绍了。
二、木马的配置生成与配置信息的保护 木马写好以后，通常会发布一个程序，在木马程序中通过配置一些相关的内容和参数后，会生成一个木马的服务器端程序。
为什么木马的客户端会生成木马的服务端程序呢？
其实木马的客户端和服务端本来就是两个程序，只是通过某种方式使其成为了一个文件而已。
让木马的服务端和客户端成为一个文件可以有多种方法，常见的有资源法和文件附加数据法两种。
在PE文件结构中有一个数据目录称作资源，资源可以是图片、图标、音频、视频等内容。
资源法也就是把服务端以资源的形式连接到客户端的程序中，然后客户端通过一些操作资源的函数将资源读取出来并生成文件。
文件附加数据法是将服务端保存到客户端的末尾，然后通过文件操作函数，直接将服务端读取出来并生成新的文件。
反弹端口连接是要访问某个固定的IP地址去读取保存着黑客的动态IP地址的信息，而这个固定的IP地址是保存在木马程序中的。
也就是说，我们的客户端在把服务端生成以后，会把一些配置信息写入服务端程序的指定位置中，服务端程序会读取指定位置的信息来进行使用。
配置信息的写入与读出必须要一致，否则就没有意义了。
对于配置信息中往往会存在一些比较敏感的信息，比如邮箱账号、密码等内容。
比如，我们在分析盗QQ的木马时会发现接收QQ密码的邮箱，由于现在很多邮箱都需要SMTP的验证，因此在配置信息中也会看到邮箱的账号及密码信息。
这样配置信息中的这些敏感信息很容易被人获取到，甚至接收QQ密码邮箱的账号和密码也会被别人获取到，真是“偷鸡不成蚀把米”。
对于此类情况，正确的做法是对配置信息进行加密。
也就是说客户端往服务端中写配置信息前需要加密后再写入，而服务端在使用这些信息前需要先解密再使用。
关于配置生成客户端与配置信息的保护上面已经介绍得差不多了，接下来应该把重点放在代码的实现上了。
我们的代码是模拟实现上面的内容，而不是真的去生成木马。

编辑推荐

1、讲解windows安全和网络编程知识；2、讲解内核编程以及软件逆向知识；

<<C++黑客编程揭秘与防范>>

版权说明