<<黑客攻防入门与实战详解>>

图书基本信息

书名：<<黑客攻防入门与实战详解>>

13位ISBN编号：9787113132439

10位ISBN编号：711313243X

出版时间：2011-9

出版时间：中国铁道

作者：至诚文化

页数：268

<<黑客攻防入门与实战详解>>

内容概要

由至诚文化编著的《黑客攻防入门与实战详解》秉承“知己知彼”的理念。
《黑客攻防入门与实战详解》详细阐述了在网络安全的具体实践中所用到的各类原理、技巧和工具，例如：了解黑客、命令行、端口扫描、漏洞扫描、网络嗅探、局域网干扰防御、木马攻防、痕迹清除与加密破解等，旨在帮助读者清晰地了解入侵者的攻击方式，进而能制作出完善的防御方案，同时从另一个完全不同的角度全面解读系统安全，从而洞察防御的死角，组织更为严密防御体系以应对层出不穷的入侵挑战。

<<黑客攻防入门与实战详解>>

书籍目录

章节摘录

版权页：插图：虽然反弹连接可穿透内网，并利用防火墙开放的端口连接外网的客户端，但它也有不足的地方，那就是要求客户端必须拥有固定的IP地址（或域名）和通信端口。
如果管理员察觉到隐藏于主机的。
服务器端，很容易顺藤摸瓜，通过服务器端的连接请求找到黑客。
3.中继连接中继连接是反弹连接的加强，它在服务器端和客户端连接的过程中添加了一个代理服务器作为跳板，服务器端不再需要指定客户端的IP地址和端口，从而增强了客户端的隐蔽性。
中继连接有半反弹端口技术和全反弹端口技术两种。
半反弹技术是指客户端将自己的IP地址、监听端口，以及连接命令上传到充当跳板的代理服务器，而服务器端则每隔一段时间会自动查看代理服务器上有没有来自客户端的连接指令。
如果发现有，则会向客户端上传到代理服务器的IP地址和监听端口发送连接请求，当客户端回复请求后，客户端和服务器端就可以开始建立连接了，如图9-3所示。
全反弹技术是指客户端将对服务器端的控制指令（如破坏指令）上传到代理服务器，服务器端则每隔一段时间查看代理服务器上有没有控制指令。
如果发现有，则按照指令执行，并将执行结果上传到代理服务器，而客户端也会每隔一段时间查看代理服务器上有无来自服务器端的执行结果。
与半反弹技术相比较，全反弹技术显然更具隐蔽性，如图9-4所示。

编辑推荐

《黑客攻防入门与实战详解》所谓“知己知彼，百战不殆”，要应对这类黑客入侵，最切实可行的方法就是了解广泛流传的各类黑客“兵器”，从它们的攻击特性着手，有的放矢进行针对性的拦截及防御。

版权说明