<<Metasploit渗透测试指南>>

图书基本信息

书名：<<Metasploit渗透测试指南>>

13位ISBN编号：9787121154874

10位ISBN编号：7121154870

出版时间：2012-1

出版时间：电子工业出版社

作者：(美)David Kennedy Jim O'Gorman Devon Kearns Mati Aharoni

页数：312

译者：诸葛建伟,王珩,孙松柏

<<Metasploit渗透测试指南>>

内容概要

本书介绍Metasploit——近年来最强大、最流行和最有发展前途的开源渗透测试平台软件，以及基于Metasploit进行网络渗透测试与安全漏洞研究分析的技术、流程和方法。

本书共有17章，覆盖了渗透测试的情报搜集、威胁建模、漏洞分析、渗透攻击和后渗透攻击各个环节，并包含了免杀技术、客户端渗透攻击、社会工程学、自动化渗透测试、无线网络攻击等高级技术专题，以及如何扩展Metasploit情报搜集、渗透攻击与后渗透攻击功能的实践方法，本书一步一个台阶地帮助初学者从零开始建立起作为渗透测试者的基本技能，也为职业的渗透测试工程师提供一本参考用书。
本书获得了Metasploit开发团队的一致好评，Metasploit项目创始人HD Moore评价本书为：“现今最好的Metasploit框架软件参考指南”。

作者简介

<<Metasploit渗透测试指南>>

书籍目录

章节摘录

版权页：插图：渗透攻击可能是在渗透测试过程中最具魅力的环节，然而在实际情况下往往没有你所预想的那么“一帆风顺”，而往往是“曲径通幽”。
最好是在你基本上能够确信特定渗透攻击会成功的时候，才真正对目标系统实施这次渗透攻击，当然在目标系统中很可能存在着一些你没有预期到的安全防护措施，使得这次渗透攻击无法成功。
但是要记住的是，在你尝试要触发一个漏洞时，你应该清晰地了解在目标系统上存在这个漏洞。
进行大量漫无目的的渗透尝试之后期待奇迹般地出现一个shell根本是痴心妄想，这种方式将会造成大量喧闹的报警，也不会为身为渗透测试者的你以及你的客户组织提供任何帮助。
请先做好功课，然后再针对目标系统实施已经经过了深入研究和测试的渗透攻击，这样才有可能取得成功。
1.1.6 后渗透攻击阶段后渗透攻击阶段从你已经攻陷了客户组织的一些系统或取得域管理权限之后开始，但离你搞定收工还有很多事情要做。
后渗透攻击阶段在任何一次渗透测试过程中都是一个关键环节，而这也是最能够体现你和那些平庸的骇客小子们的区别，真正从你的渗透测试中为客户提供有价值信息的地方。
后渗透攻击阶段将以特定的业务系统作为目标，识别出关键的基础设施，并寻找客户组织最具价值和尝试进行安全保护的信息和资产，当你从一个系统攻入另一个系统时，你需要演示出能够对客户组织造成最重要业务影响的攻击途

编辑推荐

《Metasploit渗透测试指南》将教你如何进行发现和攻击缺乏维护、错误配置和未打补丁的系统：进行网络侦察，搜索关于目标系统有价值的情报信息：绕过反病毒技术，挫败安全控制措施：在Metasploit中集成Nmap、NeXpose和Nessus进行自动漏洞发现：使用MeterpreterShell从网络内部发起进一步攻击：利用Metasploit独立功能程序、第三方工具和插件：编写你自己的Meterpreter后渗透攻击模块和脚本。
你还会进一步了解到如何对Oday安全漏洞进行渗透代码开发，编写模糊测试器，将已有渗透代码移植到Metasploit中，以及如何来掩踪灭迹。
无论你的目标是加固你自己网络的安全性，还是对别人的网络进行渗透测试，《Metasploit渗透测试指南》都将能够带领你达到并超越你的目标。
Metasploit框架软件使得安全漏洞的挖掘、利用和共享变得非常快速和便捷。
尽管Metasploit目前已经被安全技术人员们广泛普遍使用，但该工具对初学者而言还难以很快上手掌握。
《Metasploit渗透测试指南》填补了这一鸿沟，能够教你如何使用Metasploit实施渗透测试的各个环节，并让你能够和庞大的Metasploit贡献者社区进行更好地交互。
当你建立起渗透测试的基础之后，你可以学到在Metasploit框架中对应的组件、接口与模块，并进行模拟的渗透攻击。
你将进一步了解到高级的渗透测试技术，包括网络侦察与探测、客户端攻击、无线攻击、和针对性的社会工程学攻击。

<<Metasploit渗透测试指南>>

版权说明