第一图书网, tushu007.com

<<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

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

第一图书网, tushu007.com

<<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”。

第一图书网, tushu007.com

作者简介

第一图书网, tushu007.com

<<Metasploit渗透测试指南>>

书籍目录

目 录
第1章 渗透测试技术基础
1.1 PTES标准中的渗透测试阶段
1.1.1 前期交互阶段
1.1.2 情报搜集阶段
1.1.3 威胁建模阶段
1.1.4 漏洞分析阶段
1.1.5 渗透攻击阶段
1.1.6 后渗透攻击阶段
1.1.7 报告阶段
1.2 渗透测试类型
1.2.1 白盒测试
1.2.2 黑盒测试
1.3 漏洞扫描器
1.4 小结
第2章 Metasploit基础
2.1 专业术语
2.1.1 渗透攻击（Exploit）
2.1.2 攻击载荷（Payload）
2.1.3 Shellcode
2.1.4 模块（Module）
2.1.5 监听器（Listener）
2.2 Metasploit用户接口
2.2.1 MSF终端
2.2.2 MSF命令行
2.2.3 Armitage
2.3 Metasploit功能程序
2.3.1 MSF攻击载荷生成器
2.3.2 MSF编码器
2.3.3 Nasm Shell
2.4 Metasploit Express和Metasploit Pro
2.5 小结
第3章 情报搜集
3.1 被动信息搜集
3.1.1 whois查询
3.1.2 Netcraft
3.1.3 NSLookup
3.2 主动信息搜集
3.2.1 使用Nmap进行端口扫描
3.2.2 在Metasploit中使用数据库
3.2.3 使用Metasploit进行端口扫描
3.3 针对性扫描
3.3.1 服务器消息块协议扫描
3.3.2 搜寻配置不当的Microsoft SQL Server
3.3.3 SSH服务器扫描

第一图书网, tushu007.com

3.3.4 FTP扫描
3.3.5 简单网管协议扫描
3.4 编写自己的扫描器
3.5 小结
第4章 漏洞扫描
4.1 基本的漏洞扫描
4.2 使用NeXpose进行扫描
4.2.1 配置
4.2.2 将扫描报告导入到Metasploit中
4.2.3 在MSF控制台中运行NeXpose
4.3 使用Nessus进行扫描
4.3.1 配置Nessus
4.3.2 创建Nessus扫描策略
4.3.3 执行Nessus扫描
4.3.4 Nessus报告
4.3.5 将扫描结果导入Metasploit框架中
4.3.6 在Metasploit内部使用Nessus进行扫描
4.4 专用漏洞扫描器
4.4.1 验证SMB登录
4.4.2 扫描开放的VNC空口令
4.4.3 扫描开放的X11服务器
4.5 利用扫描结果进行自动化攻击
第5章 渗透攻击之旅
5.1 渗透攻击基础
5.1.1 msf＞ show exploits
5.1.2 msf＞ show auxiliary
5.1.3 msf＞ show options
5.1.4 msf＞ show payloads
5.1.5 msf＞ show targets
5.1.6 info
5.1.7 set和unset
5.1.8 setg和unsetg
5.1.9 save
5.2 你的第一次渗透攻击
5.3 攻击一台Ubuntu主机
5.4 全端口攻击载荷：暴力猜解目标开放的端口
5.5 资源文件
5.6 小结
第6章 Meterpreter
6.1 攻陷Windows XP 虚拟机
6.1.1 使用Nmap扫描端口
6.1.2 攻击MS SQL
6.1.3 暴力破解MS SQL服务器
6.1.4 xp_cmdshell
6.1.5 Meterpreter基本命令
6.1.6 获取键盘记录
6.2 挖掘用户名和密码

6.2.1 提取密码哈希值
6.2.2 使用Meterpreter命令获取密码哈希值
6.3 传递哈希值
6.4 权限提升
6.5 令牌假冒
6.6 使用ps
6.7 通过跳板攻击其他机器
6.8 使用Meterpreter脚本
6.8.1 迁移进程
6.8.2 关闭杀毒软件
6.8.3 获取系统密码哈希值
6.8.4 查看目标机上的所有流量
6.8.5 攫取系统信息
6.8.6 控制持久化
6.9 向后渗透攻击模块转变
6.10 将命令行Shell升级为Meterpreter
6.11 通过附加的Railgun组件操作Windows API
6.12 小结
第7章 免杀技术
7.1 使用MSF攻击载荷生成器创建可独立运行的二进制文件
7.2 躲避杀毒软件的检测
7.2.1 使用MSF编码器
7.2.2 多重编码
7.3 自定义可执行文件模板
7.4 隐秘地启动一个攻击载荷
7.5 加壳软件
7.6 小结：关于免杀处理的最后忠告
第8章 客户端渗透攻击
8.1 基于浏览器的渗透攻击
8.1.1 基于浏览器的渗透攻击原理
8.1.2 空指令
8.2 使用Immunity调试器来揭秘空指令机器码
8.3 对IE浏览器的极光漏洞进行渗透利用
8.4 文件格式漏洞渗透攻击
8.5 发送攻击负载
8.6 小结
第9章 Metasploit辅助模块
9.1 使用辅助模块
9.2 辅助模块剖析
9.3 小结
第10章 社会工程学工具包
10.1 配置SET工具包
10.2 针对性钓鱼攻击向量
10.3 Web攻击向量
10.3.1 Java Applet
10.3.2 客户端Web攻击
10.3.3 用户名和密码获取

10.3.4 标签页劫持攻击
10.3.5 中间人攻击
10.3.6 网页劫持
10.3.7 综合多重攻击方法
10.4 传染性媒体生成器
10.5 Teensy USB HID攻击向量
10.6 SET的其他特性
10.7 小结
第11章 Fast-Track
11.1 Microsoft SQL注入
11.1.1 SQL注入——查询语句攻击
11.1.2 SQL注入——POST参数攻击
11.1.3 手工注入
11.1.4 MSSQL破解
11.1.5 通过SQL自动获得控制（SQLPwnage）
11.2 二进制到十六进制转换器
11.3 大规模客户端攻击
11.4 小结：对自动化渗透的一点看法
第12章 Karmetasploit无线攻击套件
12.1 配置
12.2 开始攻击
12.3 获取凭证
12.4 得到Shell
12.5 小结
第13章 编写你自己的模块
13.1 在MS SQL上进行命令执行
13.2 探索一个已存在的Metasploit模块
13.3 编写一个新的模块
13.3.1 PowerShell
13.3.2 运行Shell渗透攻击
13.3.3 编写powershell_upload_exec函数
13.3.4 从十六进制转换回二进制程序
13.3.5 计数器
13.3.6 运行渗透攻击模块
13.4 小结：代码重用的能量
第14章 创建你自己的渗透攻击模块
14.1 Fuzz测试的艺术
14.2 控制结构化异常处理链
14.3 绕过SEH限制
14.4 获取返回地址
14.5 坏字符和远程代码执行
14.6 小结
第15章 将渗透代码移植到Metasploit
15.1 汇编语言基础
15.1.1 EIP和ESP寄存器
15.1.2 JMP指令集
15.1.3 空指令和空指令滑行区

第一图书网, tushu007.com

15.2 移植一个缓冲区溢出攻击代码
15.2.1 裁剪一个已有的渗透攻击代码
15.2.2 构造渗透攻击过程
15.2.3 测试我们的基础渗透代码
15.2.4 实现框架中的特性
15.2.5 增加随机化
15.2.6 消除空指令滑行区
15.2.7 去除伪造的Shellcode
15.2.8 我们完整的模块代码
15.3 SEH覆盖渗透代码
15.4 小结
第16章 Meterpreter脚本编程
16.1 Meterpreter脚本编程基础
16.2 Meterpreter API
16.2.1 打印输出
16.2.2 基本API调用
16.2.3 Meterpreter Mixins
16.3 编写Meterpreter脚本的规则
16.4 创建自己的Meterpreter脚本
16.5 小结
第17章 一次模拟的渗透测试过程
17.1 前期交互
17.2 情报搜集
17.3 威胁建模
17.4 渗透攻击
17.5 MSF终端中的渗透攻击过程
17.6 后渗透攻击
17.6.1 扫描Metasploitable靶机
17.6.2 识别存有漏洞的服务
17.7 攻击Apache Tomcat
17.8 攻击一个偏门的服务
17.9 隐藏你的踪迹
17.10 小结
附录A 配置目标机器
附录B 命令参考列表

第一图书网, tushu007.com

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

第一图书网, tushu007.com

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。

第一图书网, tushu007.com

<<Metasploit渗透测试指南>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com