《Metasploit渗透测试手册》

图书基本信息

书名：《Metasploit渗透测试手册》

13位ISBN编号：9787115323836

出版时间：2013-9-1

作者：Abhinav Singh

页数：226

译者：王一

《Metasploit渗透测试手册》

内容概要

Metasploit渗透测试手册特色：
描述方式直截了当、简单易懂；
书中示例经过仔细甄选，涵盖了大多数常见问题；
剖析问题直击本质，解决问题简单高效；
步骤式解读问题的解决方案；
书中的解决方案可以应用到其他场景。
Metasploit渗透测试手册书在内容编排上实现了理论与实战的完美结合，
涵盖了Metasploit常见使用问题的解决方案，
通过书中提供的70条“秘笈”，
读者可以掌握这一广泛使用的渗透测试工具。

《Metasploit渗透测试手册》

作者简介

Abhinav Singh是来自印度的一位信息安全专家，年轻有为。他在破解和网络安全领域有浓厚的兴趣。他以自由职业者的身份积极服务于多家安全公司，为他们提供咨询服务。当前，他是印度Tata Consultancy Services公司的一名系统工程师。他因其博客（http://hackingalert.blogspot.com）而被人所知，他在其博客中与他人分享了遇到的破解和网络安全问题。Abhinav的文章已经被多家技术杂志和门户网站所引用。

《Metasploit渗透测试手册》

书籍目录

第1章给安全专业人员的Metasploit快速提示1
1.1介绍1
1.2在Windows操作系统中配置Metasploit3
1.3在Ubuntu操作系统中配置Metasploit4
1.4BackTrack5与Metasploit——终极组合6
1.5在单机上建立渗透测试环境8
1.6在带有SSH连接的虚拟机上构建Metasploit环境10
1.7从界面开始——Metasploit的“HelloWorld”12
1.8在Metasploit框架中建立数据库13
1.9使用数据库存储渗透测试结果15
1.10分析数据库中存储的渗透测试结果17
第2章信息收集与扫描19
2.1介绍19
2.2被动式信息收集1.0——传统方式20
2.3被动式信息收集2.0——升级方式23
2.4端口扫描——Nmap方式26
2.5探索用于扫描的辅助模块31
2.6使用辅助模块进行目标服务扫描33
2.7使用Nessus进行漏洞扫描36
2.8使用NeXpose进行扫描39
2.9使用Dradis框架共享扫描信息41
第3章操作系统漏洞评估与利用45
3.1介绍45
3.2Exploit用法快速提示46
3.3在WindowsXPSP2上进行渗透测试48
3.4绑定远程访问目标机器的shell53
3.5在Windows2003Server上进行渗透测试56
3.6Windows7/Server2008R2SMB客户端无限循环漏洞58
3.7对Linux（Ubuntu）机器进行攻击渗透60
3.8理解WindowsDLL注入漏洞64
第4章客户端漏洞利用与防病毒软件规避69
4.1介绍69
4.2IE浏览器不安全脚本错误配置漏洞71
4.3IE浏览器CSS递归调用内存损坏漏洞76
4.4MicrosoftWordRTF栈溢出漏洞79
4.5AdobeReaderutil.printf（）缓冲区溢出漏洞82
4.6使用msfpayload生成二进制程序和shellcode86
4.7使用msfencoe规避客户端防病毒软件防护90
4.8使用killav.rb脚本禁用防病毒软件95
4.9深度解读killav.rb脚本99
4.10从命令行中禁用防病毒软件服务102
第5章使用meterpreter探索已攻陷目标105
5.1引言105
5.2分析meterpreter系统命令107
5.3权限提升和进程迁移109
5.4与目标建立多重通信信道111
5.5meterpreter文件系统命令114

5.6使用timestomp更改文件属性115
5.7使用meterpreter网络命令117
5.8getdesktop与keystroke监听120
5.9使用scrapermeterpreter脚本124
第6章高级Meterpreter脚本设计127
6.1介绍127
6.2Passingthehash128
6.3使用后门建立持久连接130
6.4使用meterpreter进行拓展133
6.5使用meterpreter进行端口转发136
6.6MeterpreterAPI与mixins138
6.7Railgun——将Ruby转换为武器142
6.8向Railgun中添加DLL和函数定义144
6.9构建“Windows防火墙反激活”meterpreter脚本146
6.10分析现有的meterpreter脚本150
第7章使用模块进行渗透测试157
7.1引言157
7.2使用扫描器辅助模块158
7.3使用辅助管理模块161
7.4SQL注入与DOS攻击模块162
7.5后渗透阶段模块166
7.6理解模块构建的基础167
7.7分析现有的模块170
7.8构建自己的后渗透阶段模块174
第8章使用漏洞利用代码179
8.1介绍179
8.2探索模块结构180
8.3常用的漏洞利用代码mixins182
8.4使用msfvenom183
8.5将漏洞利用代码转换为Metasploit模块185
8.6移植并测试新的漏洞利用代码模块190
8.7使用Metasploit进行模糊测试191
8.8编写FileZillaFTP模糊测试器194
第9章使用Armitage199
9.1介绍199
9.2使用Armitage200
9.3扫描与信息收集202
9.4发现漏洞与攻击目标204
9.5使用Tab切换处理多个目标206
9.6使用Armitage进行后渗透阶段操作208
9.7使用Armitage进行客户端攻击渗透210
第10章社会工程学工具包213
10.1引言213
10.2使用社会工程学工具包（SET）214
10.3使用SET配置文件215
10.4钓鱼式攻击矢量218
10.5网站攻击矢量220
10.6多攻击Web矢量223
10.7介质感染攻击224

《Metasploit渗透测试手册》

《Metasploit渗透测试手册》

精彩短评

1、相关书籍里面写得不错的
2、讲了某些模块gongneng 以及原理
3、适合快速入门用，主要讲的是软件使用，很简洁。非常薄的一本书。

《Metasploit渗透测试手册》

版权说明