《高度安全环境下的高级渗透测试》

图书基本信息

书名：《高度安全环境下的高级渗透测试》

13位ISBN编号：9787115342563

出版时间：2014-4-1

作者：Lee Allen

页数：322

译者：孙松柏,李聪,陈力波

《高度安全环境下的高级渗透测试》

内容概要

《高度安全环境下的高级渗透测试》

作者简介

Lee Allen目前是一家世界500强公司漏洞管理项目的领导，主要负责安全评估和渗透测试等工作。Lee对渗透测试和安全研究相当具有激情。在20世纪80年代，Lee借助他挚爱的Commodore 64电脑，在满地都是5.25英寸磁盘的房间里登录到BBS，由此步入激动人心的安全世界。经过在安全行业和社区内多年的浸淫，他一直是这个圈子里最伟大的专家。
他持有多个行业认证，其中包括OSWP，而且已经在IT领域工作了15年之久。他爱好并执着于对概念攻击代码的验证和评审、编程、安全研究、出席安全会议、技术探讨、写作、3D游戏开发和滑雪。

《高度安全环境下的高级渗透测试》

书籍目录

第1章　计划和界定一次成功的渗透测试　1
1. 1　什么是高级渗透测试　1
1. 1. 1　漏洞评估　1
1. 1. 2　渗透测试　2
1. 1. 3　高级渗透测试　2
1. 2　渗透测试开始之前　3
1. 2. 1　界定范围　4
1. 2. 2　设定你的范围——凡事总有结束时　5
1. 3　制订执行计划　6
1. 3. 1　安装VirtualBox　7
1. 3. 2　安装你的BackTrack虚拟机　8
1. 4　探索BackTrack　14
1. 4. 1　登录　14
1. 4. 2　修改默认密码　15
1. 4. 3　更新应用程序和操作系统　15
1. 5　安装OpenOffice　16
1. 6　有效地管理你的测试结果　16
1. 7　Dradis框架介绍　21
1. 7. 1　导出一个项目模板　23
1. 7. 2　导入一个项目模板　24
1. 7. 3　准备导入样本数据　24
1. 7. 4　将导出数据转成HTML格式　27
1. 7. 5　Dradis类别区域　27
1. 8　总结　29
第2章　高级侦查技术　30
2. 1　侦查介绍　30
2. 2　DNS侦查　33
2. 2. 1　nslookup——你需要的时候它就在那　33
2. 2. 2　域名信息搜索器(Dig)　39
2. 2. 3　使用fierce对DNS进行暴力破解　44
2. 3　搜集并验证域名和IP信息　48
2. 4　使用搜索引擎为你工作　50
2. 4. 1　Shodan　51
2. 4. 2　在Web中查找人物(和他们的文档)　54
2. 4. 3　在Internet上寻找线索　58
2. 4. 4　搜集元数据　59
2. 5　总结　63
第3章　扫描：明智地选择目标　64
3. 1　添加虚拟机到实验环境　64
3. 2　开始了解Nmap　69
3. 2. 1　常用的Nmap扫描类型和选项　69
3. 2. 2　基本扫描——预热　71
3. 2. 3　其他Nmap技术　72
3. 2. 4　在你的工具库中添加常用的Nmap脚本　80
3. 2. 5　在数据库中添加新脚本　83
3. 3　SNMP：一个等待开发的信息金矿　83
3. 3. 1　SNMP扫描　83

3．3．2　SNMPCheck　86
3．3．3　当团体字符串不是“public”时　88
3．4　使用scanPBNJ创建网络基准　89
3．4．1　为PBNJ设置MySQL数据库　89
3．4．2　启动MySQL　90
3．4．3　准备PBNJ数据库　90
3．4．4　第一次扫描　91
3．4．5　查看数据　92
3．5　规避扫描技术　95
3．5．1　命名规则　95
3．5．2　Port Knocking技术　95
3．5．3　入侵检测和规避系统　96
3．5．4　触发点　96
3．5．5　关闭SNMP　96
3．6　总结　96
第4章　远程漏洞利用　98
4．1　为什么要进行漏洞测试　98
4．2　实践——添加Kioptrix虚拟机　99
4．3　手动漏洞利用　101
4．3．1　列举服务　101
4．3．2　利用Nmap进行完全扫描　104
4．3．3　使用Netcat和Ncat来获取旗标　105
4．3．4　搜索Exploit-DB　107
4．3．5　离线的Exploit-DB　108
4．3．6　运行漏洞利用程序　113
4．4　在受害机器上上传和下载文件　117
4．4．1　在BackTrack 5虚拟机中安装和启动TFTP服务　117
4．4．2　安装和配置pure-ftpd　118
4．4．3　启动pure-ftpd　119
4．5　密码：你懂的……　120
4．5．1　破解哈希　120
4．5．2　暴力破解密码　122
4．5．3　THC Hydra　123
4．6　Metasploit——学习并喜欢它　127
4．6．1　更新Metasploit框架　128
4．6．2　Metasploit和数据库　129
4．6．3　使用Metasploit对Kioptrix进行漏洞利用　133
4．7　总结　138
第5章　Web应用攻击　139
5．1　实践出真知　140
5．1．1　安装Kioptrix Level 3虚拟机　141
5．1．2　创建Kioptrix VM Level 3克隆　142
5．1．3　在Ubuntu上安装和配置Mutillidae 2．1．7　143
5．1．4　安装和配置pfSense　145
5．1．5　为pfSense准备虚拟机　145
5．1．6　使pfSense虚拟机器持续运作　147
5．1．7　配置pfSense的DHCP服务器　149
5．1．8　启动虚拟试验环境　150
5．1．9　pfSense DHCP——保存设置　150

5. 1. 10 为负载平衡安装HAProxy 152
5. 1. 11 将Kioptrix3. com添加至host文件 153
5. 2 检测负载平衡 154
5. 3 检测Web应用防火墙(WAF) 156
5. 4 渗透Kioptrix Level 3 158
5. 5 Web应用攻击和审计框架(w3af) 159
5. 5. 1 使用w3af GUI(图形界面)以节省时间 161
5. 5. 2 使用w3af命令行(console)进行扫描 161
5. 6 Mantra介绍 173
5. 7 总结 175
第6章 客户端渗透攻击与利用 176
6. 1 缓存区溢出回顾 176
6. 1. 1 C代码编写的漏洞程序 177
6. 1. 2 在BackTrack中打开和关闭地址空间布局随机化(ASLR) 179
6. 1. 3 理解缓存区溢出的原理 180
6. 2 fuzzing(模糊测试)介绍 185
6. 3 vulnserver介绍 188
6. 4 BackTrack中包含的fuzzing工具 190
6. 4. 1 渗透利用点的暴力探测器(Bruteforce Exploit Detector——BED) 190
6. 4. 2 简单的fuzzer——SFUZZ 199
6. 5 Fast-Track 202
6. 5. 1 更新Fast-Track 206
6. 5. 2 利用Fast-Track进行客户端攻击 207
6. 6 社会工程学工具包 208
6. 7 总结 212
第7章 后渗透攻击 214
7. 1 规则约定 214
7. 1. 1 什么是允许的 215
7. 1. 2 你是否有修改的权限 215
7. 1. 3 是否允许对目标进行控制 216
7. 1. 4 你和你的团队手动搜集和存储的数据怎样处理 216
7. 1. 5 员工数据和个人信息 216
7. 2 数据搜集、网络分析 216
7. 2. 1 Linux 217
7. 2. 2 使用搜集到的信息 218
7. 2. 3 Microsoft Windows环境下的后渗透攻击 242
7. 3 跳板攻击 253
7. 4 总结 254
第8章 绕过防火墙和规避入侵检测系统 256
8. 1 实验环境准备 256
8. 1. 1 BackTrack客户机 257
8. 1. 2 Ubuntu客户机 258
8. 1. 3 pfSense客户机配置 258
8. 1. 4 防火墙配置 261
8. 2 绕过防火墙的隐蔽扫描 263
8. 3 规避IDS 267
8. 3. 1 标准化 267
8. 3. 2 时间安排就是一切 269
8. 4 流量整合 269

8.5 查找流量模式 271
8.6 清理目标机 272
8.6.1 使用清单 272
8.6.2 清理的时间点 272
8.6.3 本地日志文件 272
8.7 其他规避技术 273
8.7.1 任务分割与实现 273
8.7.2 隐藏(在被控制的主机上) 273
8.7.3 文件完整性监测 273
8.7.4 使用常用的网络管理工具来进行测试 274
8.8 总结 274
第9章 数据收集工具与结果汇报 275
9.1 先记录，后分类 275
9.2 文本编辑方法回顾 276
9.2.1 Nano 276
9.2.2 VIM——强大的文本编辑器 277
9.2.3 NoteCase 279
9.3 利用Dradis架构来协作 279
9.4 报告 281
9.5 留给读者的挑战 287
9.6 总结 287
第10章 建立虚拟的测试实验环境 288
10.1 为什么要建立实验环境 288
10.2 保持简单 289
10.2.1 实际测试案例 289
10.2.2 网络划分以及防火墙 290
10.2.3 配置需求 290
10.2.4 安装 290
10.3 加入复杂性或模拟目标环境 295
10.3.1 配置Firewall1 298
10.3.2 安装和配置Firewall2 301
10.3.3 Web1 301
10.3.4 DB1 302
10.3.5 App1 303
10.3.6 Admin1 303
10.4 总结 304
第11章 综合挑战 305
11.1 场景 305
11.2 环境设置 306
11.2.1 NewAlts研究实验室的虚拟网络 306
11.2.2 其他的系统更改 309
11.3 挑战 310
11.4 完整攻略 312
11.4.1 确定测试的范围 312
11.4.2 确定测试的原因 313
11.4.3 制定规则文档 313
11.4.4 攻击的最初计划 314
11.4.5 服务枚举和漏洞利用 315
11.5 撰写报告 321

11.6 总结 322

《高度安全环境下的高级渗透测试》

精彩短评

1、感觉除了第7章“后渗透攻击”、其他的都给力。。。BackTrack.... 不推荐购买
2、生产环境部署大量安全防护措施的前提下，通过渗透测试实现系统入侵难度增高，道高一尺，魔高一丈，高度安全环境下绕过安全防护测试实现渗透是渗透测试工程师该赏的技术活。本书还是基于backtrack环境，有些工具已被淘汰，但是理念思路，构建攻防演练环境的价值依然值得肯定。
3、主要内容就是BT下工具的使用。讲清楚了渗透测试的主要流程，这是优点。但内容含金量达不到“高级”这个书名关键词。三百页的内容如果压缩掉环境配置、不必要的截图和代码输出，全书压缩到200页是有可能的。

《高度安全环境下的高级渗透测试》

版权说明