

内网安全攻防：渗透测试实战指南



[内网安全攻防：渗透测试实战指南_下载链接1](#)

著者:徐焱

出版者:电子工业出版社

出版时间:2020-1-1

装帧:平装

isbn:9787121377938

本书由浅入深、全面、系统地介绍了内网攻击手段和防御方法，并力求语言通俗易懂、举例简单明了、便于读者阅读领会。同时结合具体案例进行讲解，可以让读者身临其境，快速了解和掌握主流的内网漏洞利用技术与内网渗透测试技巧。

阅读本书不要求读者具备渗透测试的相关背景；如有相关经验，理解起来会更容易。本书亦可作为大专院校信息安全学科的教材。

作者介绍:

徐焱，北京交通大学安全研究员，MS08067安全实验室创始人。从2002年开始接触网络安全，有丰富的渗透测试经验，主要研究方向为内网渗透测试和APT攻击。已出版图书《网络攻防实战研究：漏洞利用与提权》、《Web安全攻防：渗透测试实战指南》，在《黑客防线》、《黑客X档案》、《黑客手册》、FreeBuf、360安全客、阿里云盾先知、嘶吼等媒体发表过多篇技术文章。

贾晓璐，曾任国内某知名安全公司安全研究员，现为自由职业者。MS08067安全实验室、破晓安全团队核心成员，目前主要研究方向为内网渗透测试。从2012年开始接触网络安全，擅长渗透测试，沉迷于红蓝对抗（主要为Red Team方向）。

目录: 第1章 内网渗透测试基础

1.1 内网基础知识 1

1.1.1 工作组 1

1.1.2 域 2

1.1.3 活动目录 5

1.1.4 域控制器和活动目录的区别 6

1.1.5 安全域的划分 6

1.1.6 域中计算机的分类 7

1.1.7 域内权限解读 8

1.2 主机平台及常用工具 12

1.2.1 虚拟机的安装 12

1.2.2 Kali Linux渗透测试平台及常用工具 13

1.2.3 Windows渗透测试平台及常用工具 15

1.2.4 Windows PowerShell基础 16

1.2.5 PowerShell的基本概念 17

1.2.6 PowerShell的常用命令 18

1.3 构建内网环境 23

1.3.1 搭建域环境 23

1.3.2 搭建其他服务器环境 31

第2章 内网信息收集

2.1 内网信息收集概述 33

2.2 收集本机信息 33

2.2.1 手动收集信息 33

2.2.2 自动收集信息 44

2.2.3 Empire下的主机信息收集 45

2.3 查询当前权限 46

2.4 判断是否存在域 47

2.5 探测域内存活主机 50

2.5.1 利用NetBIOS快速探测内网 50

2.5.2 利用ICMP协议快速探测内网 51

2.5.3 通过ARP扫描探测内网 52

2.5.4 通过常规TCP/UDP端口扫描探测内网 53

2.6 扫描域内端口 54

2.6.1 利用telnet命令进行扫描 54

2.6.2 S扫描器 55

2.6.3 Metasploit端口扫描 55

2.6.4 PowerSploit的Invoke-portscan.ps1脚本 56

2.6.5 Nishang的Invoke-PortScan模块 56

2.6.6 端口Banner信息 57

2.7 收集域内基础信息 59

2.8 查找域控制器 61

2.9 获取域内的用户和管理员信息 63

2.9.1 查询所有域用户列表 63

- 2.9.2 查询域管理员用户组 65
- 2.10 定位域管理员 65
 - 2.10.1 域管理员定位概述 65
 - 2.10.2 常用域管理员定位工具 66
- 2.11 查找域管理进程 70
 - 2.11.1 本机检查 70
 - 2.11.2 查询域控制器的域用户会话 71
 - 2.11.3 查询远程系统中运行的任务 73
 - 2.11.4 扫描远程系统的NetBIOS信息 73
- 2.12 域管理员模拟方法简介 74
- 2.13 利用PowerShell收集域信息 74
- 2.14 域分析工具BloodHound 76
 - 2.14.1 配置环境 76
 - 2.14.2 采集数据 80
 - 2.14.3 导入数据 81
 - 2.14.4 查询信息 82
- 2.15 敏感数据的防护 87
 - 2.15.1 资料、数据、文件的定位流程 87
 - 2.15.2 重点核心业务机器及敏感信息防护 87
 - 2.15.3 应用与文件形式信息的防护 88
- 2.16 分析域内网段划分情况及拓扑结构 88
 - 2.16.1 基本架构 89
 - 2.16.2 域内网段划分 89
 - 2.16.3 多层域结构 90
 - 2.16.4 绘制内网拓扑图 90
- 第3章 隐藏通信隧道技术
 - 3.1 隐藏通信隧道基础知识 91
 - 3.1.1 隐藏通信隧道概述 91
 - 3.1.2 判断内网的连通性 91
 - 3.2 网络层隧道技术 94
 - 3.2.1 IPv6隧道 94
 - 3.2.2 ICMP隧道 96
 - 3.3 传输层隧道技术 103
 - 3.3.1 lcx端口转发 104
 - 3.3.2 netcat 104
 - 3.3.3 PowerCat 115
 - 3.4 应用层隧道技术 123
 - 3.4.1 SSH协议 123
 - 3.4.2 HTTP/HTTPS协议 129
 - 3.4.3 DNS协议 131
 - 3.5 SOCKS代理 146
 - 3.5.1 常用SOCKS代理工具 146
 - 3.5.2 SOCKS代理技术在网络环境中的应用 148
 - 3.6 压缩数据 159
 - 3.6.1 RAR 160
 - 3.6.2 7-Zip 162
 - 3.7 上传和下载 164
 - 3.7.1 利用FTP协议上传 164
 - 3.7.2 利用VBS上传 164
 - 3.7.3 利用Debug上传 165
 - 3.7.4 利用Nishang上传 167
 - 3.7.5 利用bitsadmin下载 167
 - 3.7.6 利用PowerShell下载 168
- 第4章 权限提升分析及防御

- 4.1 系统内核溢出漏洞提权分析及防范 169
 - 4.1.1 通过手动执行命令发现缺失补丁 170
 - 4.1.2 利用Metasploit发现缺失补丁 174
 - 4.1.3 Windows Exploit Suggester 174
 - 4.1.4 PowerShell中的Sherlock脚本 176
- 4.2 Windows操作系统配置错误利用分析及防范 178
 - 4.2.1 系统服务权限配置错误 178
 - 4.2.2 注册表键AlwaysInstallElevated 181
 - 4.2.3 可信任服务路径漏洞 184
 - 4.2.4 自动安装配置文件 186
 - 4.2.5 计划任务 188
 - 4.2.6 Empire内置模块 189
- 4.3 组策略首选项提权分析及防范 190
 - 4.3.1 组策略首选项提权简介 190
 - 4.3.2 组策略首选项提权分析 191
 - 4.3.3 针对组策略首选项提权的防御措施 195
- 4.4 绕过UAC提权分析及防范 195
 - 4.4.1 UAC简介 195
 - 4.4.2 bypassuac模块 196
 - 4.4.3 RunAs模块 197
 - 4.4.4 Nishang中的Invoke-PsUACme模块 199
 - 4.4.5 Empire中的bypassuac模块 200
 - 4.4.6 针对绕过UAC提权的防御措施 201
- 4.5 令牌窃取分析及防范 201
 - 4.5.1 令牌窃取 202
 - 4.5.2 Rotten Potato本地提权分析 203
 - 4.5.3 添加域管理员 204
 - 4.5.4 Empire下的令牌窃取分析 205
 - 4.5.5 针对令牌窃取提权的防御措施 207
- 4.6 无凭证条件下的权限获取分析及防范 207
 - 4.6.1 LLMNR和NetBIOS欺骗攻击的基本概念 207
 - 4.6.2 LLMNR和NetBIOS欺骗攻击分析 208
- 第5章 域内横向移动分析及防御
 - 5.1 常用Windows远程连接和相关命令 211
 - 5.1.1 IPC 211
 - 5.1.2 使用Windows自带的工具获取远程主机信息 213
 - 5.1.3 计划任务 213
 - 5.2 Windows系统散列值获取分析与防范 216
 - 5.2.1 LM Hash和NTLM Hash 216
 - 5.2.2 单机密码抓取与防范 217
 - 5.2.3 使用Hashcat获取密码 224
 - 5.2.4 如何防范攻击者抓取明文密码和散列值 228
 - 5.3 哈希传递攻击分析与防范 231
 - 5.3.1 哈希传递攻击的概念 231
 - 5.3.2 哈希传递攻击分析 232
 - 5.3.3 更新KB2871997补丁产生的影响 234
 - 5.4 票据传递攻击分析与防范 235
 - 5.4.1 使用mimikatz进行票据传递 235
 - 5.4.2 使用kekeo进行票据传递 236
 - 5.4.3 如何防范票据传递攻击 238
 - 5.5 PsExec的使用 238
 - 5.5.1 PsTools工具包中的PsExec 238
 - 5.5.2 Metasploit中的psexec模块 240
 - 5.6 WMI的使用 242

- 5.6.1 基本命令 243
- 5.6.2 impacket工具包中的wmiexec 244
- 5.6.3 wmiexec.vbs 244
- 5.6.4 Invoke-WmiCommand 245
- 5.6.5 Invoke-WMIMethod 246
- 5.7 永恒之蓝漏洞分析与防范 247
- 5.8 smbexec的使用 250
 - 5.8.1 C++ 版smbexec 250
 - 5.8.2 impacket工具包中的smbexec.py 251
 - 5.8.3 Linux跨Windows远程执行命令 252
- 5.9 DCOM在远程系统中的使用 258
 - 5.9.1 通过本地DCOM执行命令 259
 - 5.9.2 使用DCOM在远程机器上执行命令 260
- 5.10 SPN在域环境中的应用 262
 - 5.10.1 SPN扫描 262
 - 5.10.2 Kerberoast攻击分析与防范 266
- 5.11 Exchange邮件服务器安全防范 270
 - 5.11.1 Exchange邮件服务器介绍 270
 - 5.11.2 Exchange服务发现 272
 - 5.11.3 Exchange的基本操作 274
 - 5.11.4 导出指定的电子邮件 276
- 第6章 域控制器安全
 - 6.1 使用卷影拷贝服务提取ntds.dit 282
 - 6.1.1 通过ntdsutil.exe提取ntds.dit 282
 - 6.1.2 利用vssadmin提取ntds.dit 284
 - 6.1.3 利用vssown.vbs脚本提取ntds.dit 285
 - 6.1.4 使用ntdsutil的IFM创建卷影拷贝 287
 - 6.1.5 使用diskshadow导出ntds.dit 288
 - 6.1.6 监控卷影拷贝服务的使用情况 291
 - 6.2 导出NTDS.DIT中的散列值 292
 - 6.2.1 使用esedbexport恢复ntds.dit 292
 - 6.2.2 使用impacket工具包导出散列值 295
 - 6.2.3 在Windows下解析ntds.dit并导出域账号和域散列值 296
 - 6.3 利用dcsync获取域散列值 296
 - 6.3.1 使用mimikatz转储域散列值 296
 - 6.3.2 使用dcsync获取域账号和域散列值 298
 - 6.4 使用Metasploit获取域散列值 298
 - 6.5 使用vshadow.exe和quarkspwdump.exe导出域账号和域散列值 301
 - 6.6 Kerberos域用户提权漏洞分析与防范 302
 - 6.6.1 测试环境 303
 - 6.6.2 PyKEK工具包 303
 - 6.6.3 goldenPac.py 307
 - 6.6.4 在Metasploit中进行测试 308
 - 6.6.5 防范建议 310
- 第7章 跨域攻击分析及防御
 - 7.1 跨域攻击方法分析 311
 - 7.2 利用域信任关系的跨域攻击分析 311
 - 7.2.1 域信任关系简介 311
 - 7.2.2 获取域信息 312
 - 7.2.3 利用域信任密钥获取目标域的权限 315
 - 7.2.4 利用krbtgt散列值获取目标域的权限 318
 - 7.2.5 外部信任和林信任 321
 - 7.2.6 利用无约束委派和MS-RPRN获取信任林权限 323
 - 7.3 防范跨域攻击 327

第8章 权限维持分析及防御	
8.1 操作系统后门分析与防范	328
8.1.1 粘滞键后门	328
8.1.2 注册表注入后门	330
8.1.3 计划任务后门	331
8.1.4 meterpreter后门	335
8.1.5 Cymothoa后门	335
8.1.6 WMI型后门	336
8.2 Web后门分析与防范	339
8.2.1 Nishang下的WebShell	339
8.2.2 weeveily后门	340
8.2.3 webacoo后门	344
8.2.4 ASPX meterpreter后门	347
8.2.5 PHP meterpreter后门	347
8.3 域控制器权限持久化分析与防范	347
8.3.1 DSRM域后门	347
8.3.2 SSP维持域控权限	352
8.3.3 SID History域后门	354
8.3.4 Golden Ticket	356
8.3.5 Silver Ticket	362
8.3.6 Skeleton Key	367
8.3.7 Hook PasswordChangeNotify	370
8.4 Nishang下的脚本后门分析与防范	371
第9章 Cobalt Strike	
9.1 安装Cobalt Strike	374
9.1.1 安装Java运行环境	374
9.1.2 部署TeamServer	376
9.2 启动Cobalt Strike	378
9.2.1 启动cobaltstrike.jar	378
9.2.2 利用Cobalt Strike获取第一个Beacon	379
9.3 Cobalt Strike模块详解	384
9.3.1 Cobalt Strike模块	384
9.3.2 View模块	384
9.3.3 Attacks模块	385
9.3.4 Reporting模块	386
9.4 Cobalt Strike功能详解	387
9.4.1 监听模块	387
9.4.2 监听器的创建与使用	389
9.4.3 Delivery模块	391
9.4.4 Manage模块	392
9.4.5 Payload模块	393
9.4.6 后渗透测试模块	395
9.5 Cobalt Strike的常用命令	403
9.5.1 Cobalt Strike的基本命令	403
9.5.2 Beacon的常用操作命令	404
9.6 Aggressor脚本的编写	415
9.6.1 Aggressor脚本简介	415
9.6.2 Aggressor-Script语言基础	415
9.6.3 加载Aggressor脚本	418
跋	419
• • • • •	(收起)

标签

网络安全

安全

网络

业余爱好

评论

内容有点水，网上教程集合，不过内网渗透步骤还算清晰

相比网络安全理论，这种战术级的实操书过瘾多了。

等了两个月的新书，非常失望。和web安全攻防那本一样，整本书就是各种工具的简单使用介绍，一个WMIC的概念前面刚介绍过，后面又介绍一遍，凑字又内容毫无营养。

[内网安全攻防：渗透测试实战指南 下载链接1](#)

书评

毫无营养。从头到尾就是告诉你有什么工具，这个工具怎么用。最基本的原理讲解都没有。第一次见到这么垃圾的书。。。。。。。。。。而且定价居然是99块。。。。。。。。截图也不上心，居然有绘图工具随手画的圈。这么不用心还有必要写书吗？浪费自己的...

[内网安全攻防：渗透测试实战指南_下载链接1](#)