

《矛与盾：黑客攻防命令大曝光》紧紧围绕黑客命令与实际应用展开，在剖析黑客入侵中用户迫切需要用到或迫切想要用到的命令时，力求对其进行“傻瓜式”的讲解，使读者对网络入侵防御技术形成系统的了解，能够更好地防范黑客的攻击。全书共分为11章，包括：windows系统命令行基础、常用windows网络命令行、windows系统命令行配置、基于windows认证的入侵、远程管理windows系统、来自局域网的攻击与防御、做好网络安全防御、dos命令的实际应用、制作dos和windows pe启动盘、批处理bat文件编程，以及病毒木马的主动防御和清除等内容。

《矛与盾：黑客攻防命令大曝光》内容丰富、图文并茂、深入浅出，不仅适用于广大网络爱好者，而且适用于网络安全从业人员及网络管理员。

作者介绍:

目录: 前言

第1章 windows系统命令行基础 1

1.1 windows系统中的命令行 2

1.1.1 windows系统中的命令行概述 2

1.1.2 windows系统中的命令行操作 5

1.1.3 启动windows系统中的命令行 5

1.2 在windows系统中执行dos命令 6

1.2.1 以菜单的形式进入dos窗口 6

1.2.2 通过ie浏览器访问dos窗口 6

1.2.3 编辑命令行 7

1.2.4 设置窗口风格 8

1.2.5 windows 7系统命令行 10

1.3 全面认识dos系统 11

1.3.1 dos系统的功能 11

1.3.2 文件与目录 12

1.3.3 文件类型与属性 13

1.3.4 目录与磁盘 14

1.3.5 命令分类与命令格式 16

1.4 ip地址和端口 17

1.4.1 ip地址概述 17

1.4.2 ip地址的划分 18

1.4.3 端口的分类与查看 19

1.4.4 关闭和开启端口 21

1.4.5 端口的限制 24

1.5 可能出现的问题与解决方法 26

1.6 总结与经验积累 26

第2章 常用windows网络命令行 27

2.1 必备的几个内部命令 28

2.1.1 命令行调用的command命令 28

2.1.2 复制命令copy 29

2.1.3 更改文件扩展名关联的assoc命令 31

2.1.4 打开/关闭请求回显功能的echo命令 32

2.1.5 查看网络配置的ipconfig命令 33

2.1.6 命令行任务管理器的at命令 35

2.1.7 查看系统进程信息的tasklist命令 38

2.2 基本的windows网络命令行 39

2.2.1 测试物理网络的ping命令 39

2.2.2 查看网络连接的netstat命令 41

2.2.3 工作组和域的net命令 44

- 2.2.4 23端口登录的telnet命令 50
- 2.2.5 传输协议ftp/tftp命令 50
- 2.2.6 替换重要文件的replace命令 52
- 2.2.7 远程修改注册表的reg命令 53
- 2.2.8 关闭远程计算机的shutdown命令 56
- 2.3 其他网络命令 57
 - 2.3.1 tracert命令 58
 - 2.3.2 route命令 59
 - 2.3.3 netsh命令 60
 - 2.3.4 arp命令 63
- 2.4 可能出现的问题与解决方法 64
- 2.5 总结与经验积累 64
- 第3章 windows系统命令行配置 65
 - 3.1 config.sys文件配置 66
 - 3.1.1 config.sys文件中的命令 66
 - 3.1.2 config.sys配置实例 68
 - 3.1.3 config.sys文件中常用的配置项目 69
 - 3.2 批处理与管道 70
 - 3.2.1 批处理命令实例 70
 - 3.2.2 批处理中的常用命令 71
 - 3.2.3 常用的管道命令 74
 - 3.2.4 批处理的实例应用 76
 - 3.3 对硬盘进行分区 79
 - 3.3.1 硬盘分区的相关知识 79
 - 3.3.2 利用diskpart进行分区 80
 - 3.4 可能出现的问题与解决方法 87
 - 3.5 总结与经验积累 87
- 第4章 基于windows认证的入侵 88
 - 4.1 ipc\$的空连接漏洞 89
 - 4.1.1 ipc\$概述 89
 - 4.1.2 ipc\$空连接漏洞详解 90
 - 4.1.3 ipc\$的安全解决方案 91
 - 4.2 telnet高级入侵 94
 - 4.2.1 突破telnet中的ntlm权限认证 94
 - 4.2.2 telnet典型入侵 96
 - 4.2.3 telnet杀手锏 100
 - 4.2.4 telnet高级入侵常用的工具 101
 - 4.3 实现通过注册表入侵 102
 - 4.3.1 注册表的相关知识 102
 - 4.3.2 远程开启注册表服务功能 104
 - 4.3.3 连接远程主机的“远程注册表服务” 106
 - 4.3.4 编辑注册表 (reg) 文件 107
 - 4.3.5 通过注册表开启终端服务 113
 - 4.4 实现ms sql入侵 116
 - 4.4.1 用ms sql实现弱口令入侵 116
 - 4.4.2 入侵ms sql数据库 120
 - 4.4.3 入侵ms sql主机 121
 - 4.4.4 ms sql注入攻击与防护 124
 - 4.4.5 用nbsi软件实现ms sql注入攻击 125
 - 4.4.6 ms sql入侵安全解决方案 128
 - 4.5 获取账号密码 129
 - 4.5.1 利用sniffer获取账号密码 130
 - 4.5.2 字典工具 135
 - 4.5.3 远程暴力破解 140

- 4.6 可能出现的问题与解决方法 142
- 4.7 总结与经验积累 142
- 第5章 远程管理windows系统 143
- 5.1 实现远程计算机管理入侵 144
 - 5.1.1 计算机管理概述 144
 - 5.1.2 连接到远程计算机并开启服务 145
 - 5.1.3 查看远程计算机信息 147
 - 5.1.4 用远程控制软件实现远程管理 150
- 5.2 远程命令执行与进程查杀 151
 - 5.2.1 远程执行命令 151
 - 5.2.2 查杀系统进程 152
 - 5.2.3 远程执行命令方法汇总 154
- 5.3 ftp远程入侵 155
 - 5.3.1 ftp相关内容 155
 - 5.3.2 扫描ftp弱口令 158
 - 5.3.3 设置ftp服务器 159
- 5.4 可能出现的问题与解决方法 161
- 5.5 总结与经验积累 161
- 第6章 来自局域网的攻击与防御 162
- 6.1 arp欺骗与防御 163
 - 6.1.1 arp欺骗概述 163
 - 6.1.2 用winarpattacker实现arp欺骗 164
 - 6.1.3 网络监听与arp欺骗 166
 - 6.1.4 金山arp防火墙的使用 168
 - 6.1.5 antiarp-dns防火墙 170
- 6.2 mac地址的克隆与利用 172
 - 6.2.1 mac地址利用 172
 - 6.2.2 mac地址克隆 175
- 6.3 arp广播信息 177
 - 6.3.1 netsend攻击与防御 177
 - 6.3.2 局域网助手 (lanhelper) 攻击与防御 178
- 6.4 断网攻击防范 182
 - 6.4.1 dns服务器介绍 182
 - 6.4.2 用opendns解决断网问题 183
 - 6.4.3 用网络守护神反击攻击者 185
- 6.5 可能出现的问题与解决方法 189
- 6.6 总结与经验积累 189
- 第7章 做好网络安全防御 190
- 7.1 建立系统漏洞体系 191
 - 7.1.1 检测系统是否存在漏洞 191
 - 7.1.2 如何修复系统漏洞 192
 - 7.1.3 监视系统的操作过程 195
- 7.2 轻松防御间谍软件 197
 - 7.2.1 轻松实现拒绝潜藏的间谍 198
 - 7.2.2 用spybot找出隐藏的间谍 199
 - 7.2.3 出色的反间谍工具 203
 - 7.2.4 间谍广告杀手 206
- 7.3 拒绝网络广告干扰 208
 - 7.3.1 过滤弹出式广告的工具——傲游maxthon 208
 - 7.3.2 过滤网络广告的广告杀手——ad killer 210
 - 7.3.3 广告智能拦截的利器——zero popup 211
- 7.4 拒绝流氓软件侵袭 212
- 7.5 可能出现的问题与解决方法 215
- 7.6 总结与经验积累 215

- 第8章 dos命令的实际应用 216
 - 8.1 dos命令的基础应用 217
 - 8.1.1 在dos下正确显示中文信息 217
 - 8.1.2 恢复误删除文件 218
 - 8.1.3 让dos窗口无处不在 219
 - 8.1.4 dos系统的维护 221
 - 8.2 dos中的环境变量 222
 - 8.2.1 set命令的使用 223
 - 8.2.2 使用debug命令 223
 - 8.2.3 认识不同的环境变量 224
 - 8.2.4 环境变量和批处理 227
 - 8.3 在dos中实现文件操作 228
 - 8.3.1 抓取dos窗口中的文本 228
 - 8.3.2 在dos中使用注册表 229
 - 8.3.3 在dos中实现注册表编程 229
 - 8.3.4 在dos中使用注册表扫描程序 231
 - 8.4 网络中的dos命令运用 231
 - 8.4.1 检测dos程序执行的目录 231
 - 8.4.2 内存虚拟盘软件xms-dsk的使用 232
 - 8.4.3 在dos中恢复回收站中的文件 233
 - 8.4.4 在dos中删除不必要的文件 233
 - 8.5 可能出现的问题与解决方法 234
 - 8.6 总结与经验积累 234
- 第9章 制作dos和windows pe启动盘 236
 - 9.1 制作启动盘 237
 - 9.1.1 认识启动盘 237
 - 9.1.2 制作windows pe启动盘 239
 - 9.1.3 制作dos启动盘 240
 - 9.2 u盘启动盘的使用 243
 - 9.2.1 进入u盘系统 243
 - 9.2.2 使用启动u盘安装系统 244
 - 9.3 使用启动盘排除故障 246
 - 9.3.1 使用启动盘备份数据 246
 - 9.3.2 使用启动盘替换损坏的系统文件 247
 - 9.3.3 使用启动盘维修注册表故障 247
 - 9.3.4 使用windows诊断工具排除故障 248
 - 9.4 可能出现的问题与解决方法 251
 - 9.5 总结与经验积累 251
- 第10章 批处理bat文件编程 252
 - 10.1 在windows中编辑批处理文件 253
 - 10.2 在批处理文件中使用参数与组合命令 254
 - 10.2.1 在批处理文件中使用参数 254
 - 10.2.2 组合命令的实际应用 255
 - 10.3 配置文件中常用的命令 256
 - 10.3.1 分配缓冲区数目的buffers命令 257
 - 10.3.2 加载程序的device命令 257
 - 10.3.3 扩展键检查的break命令 258
 - 10.3.4 程序加载的devicehigh命令 259
 - 10.3.5 设置可存取文件数files命令 259
 - 10.3.6 安装内存驻留程序的install命令 260
 - 10.3.7 中断处理的stacks命令 260
 - 10.3.8 扩充内存管理程序himem.sys 261
 - 10.4 用bat编程实现综合应用 262
 - 10.4.1 系统加固 262

10.4.2 删除日志	263
10.4.3 删除系统中的垃圾文件	264
10.5 windows xp开/关机脚本	264
10.5.1 指派开/关机脚本	264
10.5.2 开/关机脚本高级设置	267
10.5.3 开/关机应用示例	269
10.6 可能出现的问题与解决方法	272
10.7 总结与经验积累	273
第11章 病毒木马的主动防御和清除	274
11.1 关闭危险端口	275
11.1.1 通过安全策略关闭危险端口	275
11.1.2 自动优化ip安全策略	278
11.1.3 系统安全设置	283
11.2 用防火墙隔离系统与病毒	284
11.2.1 使用windows xp防火墙	284
11.2.2 使用windows 7防火墙	288
11.2.3 设置windows 7防火墙的入站规则	290
11.3 对未知病毒木马进行全面监控	292
11.3.1 监控注册表与文件	292
11.3.2 监控程序文件	294
11.3.3 未知病毒木马的防御	297
11.4 使用windows defender清除恶意软件	300
11.4.1 windows defender对恶意软件的报警及处理方式	300
11.4.2 设置自动扫描的时间	301
11.4.3 手动扫描	302
11.4.4 设置不扫描的位置和文件类型	304
11.4.5 禁用windows defender	305
11.5 可能出现的问题与解决方法	306
11.6 总结与经验积累	307
附录	308
附录a dos命令中英文对照表	309
附录b 系统端口一览表	315
附录c windows系统文件详解	318
附录d windows xp命令集	319
附录e 正常的系统进程	323
• • • • •	(收起)

[矛与盾：黑客攻防命令大曝光_下载链接1](#)

标签

黑客

计算机

安全

信息安全

评论

[矛与盾：黑客攻防命令大曝光 下载链接1](#)

书评

[矛与盾：黑客攻防命令大曝光 下载链接1](#)