

《网络扫描技术揭秘》

图书基本信息

书名：《网络扫描技术揭秘》

出版时间：2012-1

作者：李瑞民

页数：497

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《网络扫描技术揭秘》

内容概要

《网络扫描技术揭秘:原理、实践与扫描器的实现》系统地介绍网络扫描器的概念、原理与设计方法，饱含作者十几年来在网络技术应用实践中不断总结的经验与技巧。作者从网络协议这样的基本概念开始，细致深入地分析了网络扫描器的原理，并用自己制作的大量工程代码，揭示了网络扫描器的实现方法与最佳实践。

《网络扫描技术揭秘:原理、实践与扫描器的实现》首先介绍了网络扫描技术的概念、原理、算法等，以及网络协议的意义与编程概述，随后系统分析了各种扫描器的原理与设计方法，包括TCP/UDP端口、NetBIOS、SNMP、ICMP、基于协议的服务、基于应用的服务、命名管道、服务发现、漏洞扫描器等。书中在介绍每一种扫描器的时候，都是先介绍相应协议，然后对扫描器中要使用的API函数进行详细说明，使读者知道该扫描器的各种技术细节；还介绍了Windows中相关协议程序的安装、配置、测试和验证等，使读者有了演习场地；最后展示了扫描器的编程实例。这种循序渐进、逐步深入的方式，使读者不仅全面地了解扫描器的细节，而且在遇到新情况时，能举一反三，对代码进行修改或调整。随书光盘还包含了作者精心制作与调试好的工程代码，可帮助读者快速上手，设计出自己需要的扫描器。

《网络扫描技术揭秘:原理、实践与扫描器的实现》不仅是网管员和安全技术人员必备参考书，也适合于所有想深入理解计算机网络原理、全面了解网络扫描技术的学生、教师以及安全技术爱好者。

《网络扫描技术揭秘》

作者简介

李瑞民 工学博士，资深网络安全专家兼高级系统架构师，多年来一直专注于计算机安全技术、网络设备与信号监控等领域的应用。对网络扫描技术以及串口监控、网口监控等设备类监控技术有深刻的认识，并在实践中总结出了串口通信中的嗅探技术以及通用串口协议语法。曾参与多个网络应用软件项目的研发，涉及网络安全、广播电视、通信等多个行业。曾发表论文二十余篇，拥有专利和著作权六项。此外，还积极倡导和推动开源事业，将自己精心编写的扫描器代码全部开源，旨在推动我国软件事业的发展。

书籍目录

《网络扫描技术揭秘：原理、实践与扫描器的实现》

前言

第1章 绪论 / 1

1.1 网络安全的概念 / 1

1.2 网络扫描的概念 / 2

1.2.1 服务和端口 / 2

1.2.2 网络扫描 / 4

1.3 网络扫描原理概述 / 5

1.4 扫描编程与客户端编程的区别 / 5

1.5 网络扫描的目的 / 5

1.6 网络扫描算法 / 6

1.6.1 非顺序扫描 / 6

1.6.2 高速扫描 / 8

1.6.3 分布式扫描 / 8

1.6.4 服务扫描 / 8

1.6.5 指纹识别算法 / 8

1.6.6 漏洞扫描 / 9

1.6.7 间接扫描 / 9

1.6.8 秘密扫描 / 9

1.6.9 认证扫描 / 10

1.6.10 代理扫描 / 10

1.6.11 手工扫描 / 10

1.6.12 被动扫描 / 10

1.7 网络扫描器的分类 / 11

1.8 网络扫描技术的发展史 / 12

1.8.1 手工扫描阶段 / 12

1.8.2 使用通用扫描器阶段 / 13

1.8.3 设计专用扫描器阶段 / 14

1.9 扫描器的限制 / 14

1.10 当前网络常见的漏洞 / 14

1.10.1 dos和ddos / 15

1.10.2 缓冲区溢出 / 15

1.10.3 注入式攻击 / 17

1.10.4 明文传输 / 17

1.10.5 简单密码 / 18

第2章 网络协议和网络编程例程 / 19

2.1 常用的网络编程 / 19

2.1.1 tcp/ip协议编程 / 20

2.1.2 netbios/netbeui协议编程 / 41

2.1.3 win inet高层编程 / 47

2.1.4 命名管道和邮槽高层编程 / 48

2.2 扫描器中公用编程示例 / 49

2.2.1 ctrectrl控件的应用 / 49

2.2.2 clistctrl控件的应用 / 51

2.2.3 ini文件的操作 / 53

2.2.4 数据库ado的简单应用 / 56

2.2.5 ip格式的互换 / 59

- 2.2.6 windows操作系统类型的判断 / 62
- 2.2.7 多线程的局限性和使用方式 / 63
- 2.2.8 vc++ 下windows socket的使用 / 66
- 2.2.9 网卡的混杂模式 / 69
- 2.3 嵌入外部程序 / 71
 - 2.3.1 可执行外部程序的几个函数 / 71
 - 2.3.2 编程实例：使用重定向接收外部程序运行结果 / 76
 - 2.3.3 编程实例：使用管道接收外部程序运行结果 / 80
- 第3章 tcp/udp端口扫描器的设计 / 85
 - 3.1 端口扫描的概念 / 85
 - 3.1.1 端口的概念 / 85
 - 3.1.2 端口扫描原理 / 87
 - 3.2 端口扫描技术 / 87
 - 3.2.1 网络通信实例分析 / 87
 - 3.2.2 tcp扫描 / 90
 - 3.2.3 udp扫描 / 92
 - 3.3 手工扫描 / 93
 - 3.3.1 检测单主机单端口开与否 / 93
 - 3.3.2 检测单主机单端口是否有相应服务 / 94
 - 3.3.3 检测多主机或多端口 / 95
 - 3.4 编程实例：tcp端口扫描器 / 98
 - 3.4.1 程序主界面 / 99
 - 3.4.2 程序代码 / 100
 - 3.5 编程实例：udp端口扫描器 / 112
 - 3.5.1 程序主界面 / 112
 - 3.5.2 程序代码 / 113
- 第4章 netbios扫描器的设计 / 120
 - 4.1 netbios协议的使用 / 120
 - 4.1.1 查看和修改netbios配置 / 120
 - 4.1.2 查看netbios配置的命令 / 122
 - 4.2 ip和主机名的互换 / 127
 - 4.2.1 主机名转ip地址 / 127
 - 4.2.2 ip地址转主机名 / 127
 - 4.3 mac地址的读取 / 128
 - 4.4 本地域名、子网掩码、网卡类型的读取 / 129
 - 4.5 用户名、共享目录、组列表的读取 / 134
 - 4.5.1 unicode编程与ansi之间的互换 / 134
 - 4.5.2 用户名列表的读取 / 137
 - 4.5.3 共享目录的读取 / 150
 - 4.5.4 组列表的读取 / 156
 - 4.5.5 远端主机时间的读取 / 159
 - 4.5.6 远端服务支持类型的读取 / 161
 - 4.5.7 主机信息的读取 / 163
 - 4.6 netbios的安全性 / 166
 - 4.7 编程实例：反“ip欺骗”——mac地址扫描器的设计 / 169
 - 4.7.1 反“ip欺骗”的原理 / 169
 - 4.7.2 mac地址扫描器的主界面 / 170
 - 4.7.3 程序代码 / 170
 - 4.8 编程实例：netbios的通用扫描器 / 176

- 4.8.1 程序主界面 / 176
- 4.8.2 程序代码 / 177
- 第 5 章 snmp扫描器的设计 / 186
 - 5.1 snmp协议 / 186
 - 5.1.1 管理信息结构 / 187
 - 5.1.2 管理信息库 / 187
 - 5.1.3 通信协议 / 191
 - 5.2 snmp的api / 193
 - 5.2.1 数据类型和常用结构 / 194
 - 5.2.2 管理程序api / 197
 - 5.3 snmp安装和验证 / 204
 - 5.4 编程实例：snmp通用读设工具 / 207
 - 5.4.1 程序主界面 / 208
 - 5.4.2 程序代码 / 209
 - 5.5 编程实例：基于snmp的主机扫描器 / 213
 - 5.5.1 程序主界面 / 214
 - 5.5.2 程序代码 / 214
- 第 6 章 icmp扫描器的设计 / 221
 - 6.1 icmp协议简介 / 222
 - 6.2 ping与tracert命令简介 / 222
 - 6.2.1 ping程序使用 / 222
 - 6.2.2 tracert程序使用 / 224
 - 6.3 icmp通信实例分析 / 226
 - 6.4 icmp协议内容 / 227
 - 6.4.1 目的不可达消息 / 227
 - 6.4.2 超时消息 / 228
 - 6.4.3 参数问题消息 / 229
 - 6.4.4 源拥塞消息 / 229
 - 6.4.5 重定向消息 / 230
 - 6.4.6 回送请求或回送响应消息 / 231
 - 6.4.7 时间戳请求和时间戳响应消息 / 231
 - 6.4.8 信息请求或信息响应消息 / 232
 - 6.5 icmp扫描的安全性 / 233
 - 6.6 编程实例：快速多ip的icmp扫描器 / 234
 - 6.6.1 程序主界面 / 234
 - 6.6.2 程序原理 / 237
 - 6.6.3 程序代码 / 238
- 第 7 章 基于协议的服务扫描器的设计 / 250
 - 7.1 www服务扫描 / 251
 - 7.1.1 www服务器架构 / 251
 - 7.1.2 协议消息格式 / 254
 - 7.1.3 www服务器的安装与配置 / 260
 - 7.2 编程实例：www服务扫描器 / 264
 - 7.2.1 扫描原理 / 265
 - 7.2.2 程序主界面 / 266
 - 7.2.3 程序代码 / 266
 - 7.3 ftp服务扫描 / 272
 - 7.3.1 ftp简介 / 272
 - 7.3.2 ftp服务器的安装与配置 / 274

- 7.4 编程实例：ftp服务扫描器 / 278
 - 7.4.1 程序主界面 / 278
 - 7.4.2 程序代码 / 278
- 7.5 telnet服务扫描 / 281
 - 7.5.1 telnet协议简介 / 281
 - 7.5.2 telnet的安装与配置 / 284
- 7.6 编程实例：telnet服务扫描器 / 286
 - 7.6.1 程序主界面 / 287
 - 7.6.2 程序代码 / 287
- 7.7 email服务扫描 / 291
 - 7.7.1 电子邮件协议简介 / 291
 - 7.7.2 电子邮件服务器的安装与配置 / 299
- 7.8 编程实例：email服务扫描器 / 306
 - 7.8.1 程序主界面 / 306
 - 7.8.2 程序代码 / 307
- 第8章 基于应用的服务扫描器的设计 / 314
 - 8.1 win inet编程接口 / 314
 - 8.1.1 cinternetsession类 / 315
 - 8.1.2 cinternetconnection类 / 322
 - 8.1.3 chttpconnection类 / 323
 - 8.1.4 cftpconnection类 / 324
 - 8.1.5 cinternetfile类 / 237
 - 8.1.6 cinternetexception类 / 329
 - 8.2 编程实例：基于应用的www服务扫描器 / 329
 - 8.3 编程实例：基于应用的ftp服务扫描器 / 330
 - 8.4 网络资源协议 / 332
 - 8.4.1 netresource结构 / 332
 - 8.4.2 wnetopenenum函数 / 333
 - 8.4.3 wnetenumresource函数 / 334
 - 8.4.4 wnetcloseenum函数 / 335
 - 8.5 编程实例：网络资源扫描器 / 336
 - 8.5.1 程序主界面 / 336
 - 8.5.2 程序代码 / 337
- 第9章 命名管道扫描器的设计 / 341
 - 9.1 命名管道 / 341
 - 9.2 命名管道api / 342
 - 9.2.1 命名管道的unc格式 / 342
 - 9.2.2 命名管道编程的api / 342
 - 9.3 命名管道编程示例 / 349
 - 9.3.1 命名管道服务器端 / 349
 - 9.3.2 命名管道客户端 / 350
 - 9.4 邮槽 / 352
 - 9.4.1 邮槽的unc格式 / 352
 - 9.4.2 邮槽编程的api / 352
 - 9.5 邮槽编程示例 / 354
 - 9.5.1 邮槽服务器端编程 / 354
 - 9.5.2 邮槽客户端编程 / 355
 - 9.6 编程实例：sql server命名管道扫描器的设计 / 356
 - 9.6.1 microsoft sql server

简介 / 356
9.6.2 程序主界面 / 359
9.6.3 程序代码 / 360
第10章 服务发现扫描器的设计 / 364
10.1 服务发现简介 / 364
10.2 upnp协议 / 365
10.2.1 寻址 / 367
10.2.2 发现 / 367
10.2.3 描述 / 368
10.2.4 控制 / 369
10.2.5 事件 / 369
10.2.6 展示 / 370
10.3 xml协议 / 371
10.4 ssdp协议分析实例 / 373
10.4.1 设备类型 / 374
10.4.2 协议消息格式 / 377
10.5 编程实例：服务发现扫描器 / 381
10.5.1 程序主界面 / 382
10.5.2 程序代码 / 383
第11章 漏洞扫描器的设计 / 395
11.1 注入式漏洞扫描器 / 395
11.1.1 sql注入式攻击原理 / 396
11.1.2 注入式攻击的局限性 / 398
11.1.3 单机模式或c/s模式的攻击 / 398
11.1.4 b/s模式下扫描程序设计 / 401
11.2 主机弱密码扫描 / 412
11.2.1 网络连接的api / 412
11.2.2 密码穷举分析 / 416
11.2.3 程序主界面 / 418
11.2.4 程序代码 / 419
11.3 dos/ddos攻击 / 425
11.3.1 程序主界面 / 427
11.3.2 程序代码 / 427
11.4 明文密码嗅探 / 432
11.4.1 程序主界面 / 433
11.4.2 程序代码 / 434
11.5 端口对照 / 443
11.5.1 程序主界面 / 443
11.5.2 程序代码 / 445
第12章 扫描防范技术的研究 / 451
12.1 更换端口 / 452
12.2 预留陷阱技术 / 453
12.3 基于哨兵的端口扫描监测 / 454
12.3.1 程序主界面 / 455
12.3.2 程序代码 / 456
12.4 基于嗅探的端口扫描监测及ddos拒绝服务监测 / 460
12.4.1 程序主界面 / 461
12.4.2 程序代码 / 462
12.5 实时监测本地所有tcp/udp连接及端口 / 467

- 12.5.1 程序主界面 / 467
- 12.5.2 结构与函数api / 468
- 12.5.3 程序代码 / 471
- 12.6 如何关闭端口 / 478
 - 12.6.1 ftp端口 / 478
 - 12.6.2 www端口 / 480
 - 12.6.3 telnet端口 / 480
 - 12.6.4 netbios端口 / 481
- 附录a 本书容易混淆概念解析 / 482
- 附录b windows socket错误返回码 / 486
- 附录c win inet错误返回码 / 491
- 附录d http错误返回码 / 493
- 参考文献 / 498
- 后记 / 499

精彩短评

- 1、书的质量很好，不错，推荐
- 2、网络扫描
- 3、还没看，不好评论，不过该书的质量很好，到手都是用封塑封着的，而且纸张的质量也很好，等看了再来评论。
- 4、这本书能够通过扫描深入理解网络的拓扑结构，还可以帮助编写自己的扫描程序。特别是光盘中有许多示例，拿来就能用。很棒！
- 5、暂时还没看，看目录还好
- 6、还可以啦，排版啥的都挺好的
- 7、这是为了上个学期的一门课程而购买的书，书写的不错，不足之处就是用的平台比较老了。
- 8、很好很强大，送人的，偏编程的扫描书。
- 9、还没有看,不过应该不错,32个赞
- 10、很专业的计算机图书
- 11、这一次总共买了四本安全方面的书，其中有三本有问题，本来打算在当当买但还是贵了几块钱而且我没当当的网银，所以只好在卓越买，我以前也在卓越买过很多书和其他的东西，但这一次是让我最失望的一次。刚开始没发现问题，夏天一热，手上容易出汗，然后拿着在看，竟然书上的字体可以退色，稍微用力一插，字体就模模糊糊了。而且我买了《Oday软件漏洞分析》竟然中间有十多页重印看不清，我... [阅读更多](#)
- 12、内容很多，详细，再有整体源代码就更好了
- 13、纯粹垃圾。没有什么深度，很多地方居然在介绍WINDOWS的API。。。作者这是在骗稿费吗？只要看看TCP/IP详解，弄清楚这些协议之间的数据包格式、规范，自然就懂了。
- 14、有网络编程的详细基础知识，以及各种扫描器的完整实例
- 15、scan
- 16、网络扫描技术揭秘
- 17、其实书收到后，还没有怎么看呢，不过看纸张都还好
- 18、实践经验丰富的一本书

《网络扫描技术揭秘》

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:www.tushu000.com